האוניברסיטה הפתוחה

המחלקה לסוציולוגיה, מדע המדינה ותקשורת

The Construction of the Cryptocurrency Ecosystem: The Problematization of Trust in a Socio-Technical Assemblage

הבניית המערכת האקולוגית של המטבעות הדיגיטליים : תפיסת בעיית האמון באסמבלאז' סוציו-טכנולוגי

מוגש על ידי : בנימין רייך

עבודה זו נכתבה בהנחיית : פרופסור זאב רוזנהק

תזה זו מוגשת כחלק מהדרישות לשם קבלת תואר מוסמך

בתוכנית ללימודי דמוקרטיה בין תחומיים

באוניברסיטה הפתוחה

המחלקה לסוציולוגיה, מדע המדינה ותקשורת

מרץ 2025 רעננה

Abstract

This study examines the constitution, trust dynamics, and long-term stability of the U.S. cryptocurrency ecosystem through an interdisciplinary framework combining Elinor Ostrom's Institutional Analysis and Development (IAD) framework and Actor-Network Theory (ANT), a conceptual approach rooted in society and technology studies. Using poststructural discourse analysis, the research analyzes government-initiated policy documents and public responses to trace how institutional arrangements and key actors emerge, interact, and evolve within a technologically rich social ecosystem. The study describes how trust is problematized by stakeholders, arguing that both interpersonal and institutional trust and distrust contribute to the ecosystem's resilience by selectively constituting and accepting the institutional arrangements that incorporate technological innovation. It also examines the reciprocal effect of these institutional arrangements on trust. Cryptocurrencies do not fundamentally alter what money is, but they shift the perception of society from a socio-political construct to a socio-technical assemblage. To capture this shift, the study integrates ANT's descriptive attention to fluid relativism with IAD's focus on institutional resilience. By tracing how trust is continuously reassembled through sociotechnical interactions, the study offers a conceptual framework for understanding how trust and institutional arrangements are co-produced in decentralized systems as substitutes for state-backed monetary trust.

תקציר

מחקר זה בוחן את התגבשות מערכת המטבעות הדיגיטליים בארצות הברית, את הדינמיקה של האמון בה, וסיכויי ההישרדות שלה לטווח ארוך באמצעות השילוב בין תיאורית האנליזה והעיצוב המוסדי של אלינור אוסטרום (IAD) ותיאורית רשת השחקנים השייכת לתחום לימודי חברה וטכנולוגיה (ANT). המחקר מנתח מסמכי מדיניות של הממשל ותגובות ציבוריות למדיניות המוצעת באמצעות ניתוח שיח פוסט-סטרוקטורליסטי כדי להתחקות אחר האופן בו הסדרים מוסדיים ושחקנים מתהווים, מקיימים אינטראקציה ביניהם, ומתפתחים עם הזמן. המחקר מתאר כיצד שאלת האמון מובנית על ידי בעלי העניין במערכת, וטוען כי גם אמון וגם חוסר אמון—בין אישי ומוסדי—תורמים לעמידותה של המערכת, בכך שהם מעצבים ומקבלים באופן סלקטיבי הסדרים מוסדיים המשולבים בטכנולוגיה. בנוסף, בוחן המחקר באיזה אופן משפיעים ההסדרים המוסדיים המתגבשים על האמון במערכת. מטבעות דיגיטליים אינם משנים את מהות הכסף. אולם הם מעבירים את תפישת החברה מהבניה סוציו-פוליטית להבניה סוציו-טכנולוגית. כדי לבחון את המעבר הזה, אני משלב את היכולת של ANT לתאר יחסים סוציו-טכנולוגיים דינמיים עם ההתמקדות של IAD על שרידות ועמידות מוסדית. בהתחקות אחר האופן בו אמון נבנה מחדש בכל פעם דרך אינטראקציות סוציו-טכנולוגיות, המחקר מציע מסגרת מושגית להבנת היצירה המקבילית של אמון והסדרים מוסדיים במערכת מבוזרת כתחליף לאמון בכסף מדינתי.

Table of Contents

List of Tables

List of Abbreviations and Acronyms

Abbreviation	Meaning
AML	Anti-Money Laundering
ANT	Actor-Network Theory
BIS	Bank of International Settlements
BNB	Binance Coin
CBDC	Central Bank Digital Currency
CCI	Crypto Council for Innovation
CFTC	Commodity Futures Trading Commission
CPR	Common Pool Resource
DAI	MakerDao Stablecoin
DLT	Distributed Ledger Technologies
DOJ	Department of Justice
DOT	Department of the Treasury
EIP	Ethereum Improvement Proposal
ETH	Ethereum
FATF	Financial Action Task Force
FCC	Federal Communications Commission
FED	Federal Reserve
ICO	Initial Coin Offering
KYC	Know Your Customer
MKR	Maker Governance Token
NER	Named Entity Recognition
NLP	Natural Language Processing
NYIC	New York Information Center
OECD	Organization for Economic Co-operation and Development
OPP	Obligatory Passage Point
OSTP	Office of Science and Technology Policy
PDA	Poststructural Discourse Analysis
QDA	Qualitative Data Analysis
RFC	Request for Comment
SEC	Securities and Exchange Commission
TON	Toncoin Cryptocurrency
US	United States
USDC	USD Coin, a stablecoin issued by Circle
USDD	USD Decentralized, a stablecoin
USDT	Tether, a stablecoin
WPR	What is the Problem Represented to Be?
WTO	World Trade Organization
XRP	Coin used in Ripple payment protocol

Chapter One.

Introduction

Background

In 2008 a mysterious programmer using the pseudonym Satoshi Nakamoto released a white paper introducing Bitcoin, a peer-to-peer version of electronic cash that eliminates the need for intermediaries to record the exchange of funds, while ensuring the complete integrity and security of financial transactions. The solution is based on Blockchain, a decentralized and distributed ledger system that assures the integrity and transparency of Bitcoin transactions, marking a paradigm shift in the traditional financial landscape that depended on intermediation by financial institutions in the maintenance of financial ledgers (Nakamoto, 2008, pp. 1–9). This development is seen by many as a pivotal turning point in monetary history (Auer et al., 2021; Bordo, 2021).

Money serves three main functions in an economy: as a medium of exchange, it facilitates transactions by providing a common standard of value that eliminates the inefficiencies of barter; as a unit of account, it provides a standard measure for pricing goods and services, allowing for consistent valuation and comparison across different transactions; and as a store of value, it allows for saving and transferring purchasing power over time by maintaining its value and enabling individuals and institutions to defer consumption (Dodd, 2014, pp. 51–53). While the functions of money remained relatively stable for millennia, the history of money is a story of shifts in social trust and the reciprocal effect it has on the stability and security of money in the face of uncertainty (Strange, 2016, pp. 86–87).

At the beginning of the nineteenth century, most of the trust in money started to gravitate from trust in the material of which coins are made towards trust in various authorities to support fiduciary money. This process culminated in an outcome that Ingham terms “the dematerialization of money” (Ingham, 2013, pp. 41–49). As a result, the nominal role of money as a store of value became largely dependent on the nation-state as an authority that controls its supply and has the power to coerce market players, thereby enabling trust in market stability and integrity (Ingham, 2013, pp. 64–66).

Bitcoin and other cryptocurrencies have emerged as a response to the erosion of trust in government, fueled by increasing financialization and mass digitization of the economy. The introduction of Bitcoin coincides with governments' rescue of banks in the aftermath of the 2008 global financial crisis (GFC) which is believed to have played a significant role in driving its momentum (Baldwin, 2018, p. 3). The GFC and its outcome are conceived as a manifestation of the ineffectiveness of government and financial institutions to manage the monetary system with equity and fairness. The bailout of financial institutions by governments, and by the United States government in particular, was seen as a solution to the GFC that involved indirect taxation of the ordinary people in the interest of those who instigated the crisis, thereby increasing social inequality (Vaz & Brown, 2019, p. 5).

The linkage between inequality and societal trust has been scientifically validated by sociologists and economists (Jordahl, 2007, pp. 17–18; Uslaner, 2010, pp. 119–121; Roth, 2009, p. 204). These studies indicate that levels of generalized trust, encompassing interpersonal trust along with trust in government and business, receded significantly in the aftermath of the GFC from 34% in 2007 to 29% in 2010. A decrease in generalized trust is a sign of waning confidence in the current financial ecosystem and a leading indicator that society will look for alternatives to the current system (Uslaner, 2010, pp. 113–114). Nakamoto himself wrote that "the root problem with conventional currency is all the trust that is required to make it work", pointing the finger at governments and banks as the violators of that trust (Nelms et al., 2018, p. 21).

The introduction of Bitcoin sparked the creation of a diverse cryptocurrency ecosystem, encompassing both privately and publicly issued digital currencies, all of which rely on blockchain technology for transaction verification and trust, instead of using intermediaries such as banks. While some researchers have heralded the appearance of an "algorithmic democracy", eliminating the need for trust (Parkin, 2019, p. 482), the construction of algorithmic governance and its effects on trust are the subject of heavy debate (Zook & Blankenship, 2018, p. 254). Hence, sociologists have raised questions about the assertion that blockchain establishes a truly trustless environment. Several types of cryptocurrencies have emerged, classified by their money supply mechanisms. Bitcoin and other decentralized cryptocurrencies have fixed or predictable supplies, creating scarcity like gold and limiting inflationary risk. Stablecoins, such as Tether, have an elastic supply, expanding or contracting based on demand, as issuers create or

redeem tokens to maintain a 1:1 peg with existing fiat currencies. Central Bank Digital Currencies (CBDCs) operate under state-controlled monetary policy, where supply is determined by government authorities. Finally, platform and utility tokens, such as Ethereum (ETH) and Solana (SOL), have variable or inflationary supplies, based on supply and demand algorithms. Because stablecoins and CBDCs are designed to maintain a stable value and have supply mechanisms that align with existing monetary frameworks, they are the best candidates for use as money (Auer et al., 2023).

As of mid-2023, consumer adoption of cryptocurrencies has been maintaining a steady growth rate of between 10%-20% per year since 2019. The number of active bitcoin accounts is approaching 45 million, and over 13% of Americans are active cryptocurrency holders (Rule, 2023). Despite the considerable growth of the cryptocurrency market, the question remains about its use as real money. As of 2023, cryptocurrencies barely qualify as a medium of exchange with only a minute fraction of firms accepting them as payment for services and goods. Yet, cryptocurrencies are starting to grow as a store of value and a unit of account. This growth can be detected by monitoring the increase in market cap of stablecoins from $2.5bn at the beginning of 2019 to $120bn as of September 2023 (Milkroad, 2023). Stablecoins are a type of cryptocurrency that is pegged to an established financial commodity, such as the US dollar or gold (Fantacci & Gobbi, 2021, pp. 5–7). The growth of stablecoins demonstrates the adoption of cryptocurrency as money since it neutralizes the speculative element in consumers' intentions when they hold digital coins as a vehicle for profit.

This ecosystem is abundant with institutional innovation, where institutions are a coherent set of formal and informal rules that promote long-term credible commitment by stakeholders (North & Weingast, 1989). Apart from formal institutions that are being created, such as cryptocurrency exchanges, the cryptocurrency ecosystem is producing unprecedented semi-formal institutions such as secure peer-to-peer lending (Yan & Zhou, 2023, pp. 711–714) and smart contracts (Bekemeier, 2021, p. 6). Trust is a critical foundation upon which such cooperation and collective action are constructed in the political economy (Korczynski, 2000, p. 3), and it is a crucial building block that lies at the heart of the functioning of fiscal and monetary systems (Prasad, 2023, p. 17). The emergence of cryptocurrencies is now challenging the monopoly that nation-states have had since the nineteenth century as the sole source of social trust that drives the

monetary system. Some posit that cryptocurrency shifts trust from the credibility of market players led by the state, to trust in the determinism of software code (Maurer et al., 2013, p. 263). Others emphasize the shift of trust to decentralized consensus mechanisms (Prasad, 2023, pp. 119–121). However, most scholars agree that the determinism and distribution of technology cannot fully describe and explain the changes in trust dynamics in the context of cryptocurrencies.

The Problematization of Trust

Building on the argument that trust is foundational to the functioning of financial systems, this study examines the problematization of trust that arises in the transformed institutional landscape of the United States cryptocurrency ecosystem. While the precise definition of trust is a matter of contention, there is broad agreement that it is the confidence, reliance, and belief that individuals and institutions have in each other's integrity, intentions, and abilities. In a social context, trust is often linked to the confidence that other actors in a society will not exploit one's vulnerabilities, leading to a willingness to expose those vulnerabilities to seize opportunities or mitigate risk (Levi & Stoker, 2000, p. 476). My research focuses on the formation of trust in the cryptocurrency ecosystem, under the assumption that cryptocurrencies are intended to play the role of real money.

The enigmatic nature of stakeholders' behavior in the cryptocurrency ecosystem, marked by ambivalence and a heightened propensity for risk, illustrates the problem of trust. Government efforts to regulate the market alongside consideration of a central bank digital currency (CBDC)—send mixed signals: regulation implies support, while a state-issued coin suggests distrust in a self-governing crypto system and introduces direct competition (Cunha et al., 2021, p. 14). Additionally, the growing exposure of financial institutions to crypto has trust implications, as shown by the 2022 collapse of banks that took risks beyond government-insured deposits (Gorton & Zhang, 2023, pp. 21–26). Finally, the issue of consumer trust within the cryptocurrency ecosystem revolves around the reasons individuals might have to trust in a coin that lacks federal government backing and does not provide viable means for enforcing the law in cases of fraud or mismanagement (Sousa et al., 2022, p. 3).

My primary objective is to unveil the inner workings of mechanisms imagined by these stakeholders, which consist of innovative institutional frameworks and processes through which trust emerges in the context of cryptocurrencies, and the reciprocal effect that trust has on these mechanisms (Bodó, 2021, p. 2674). I argue that trust in money is going through a transformative shift as part of the establishment of these mechanisms. This shift is driven by the development of a distributed form of trust between actors in the cryptocurrency ecosystem to replace trust in governments' ability to maintain stable and predictable markets and protect consumers. The distributed trust in cryptocurrency is shaped by shared norms and understandings that emerge in an environment that is self-organized and decentralized due to the diminishing role of the state.

The present thesis will address the problem of trust in cryptocurrencies by exploring how actors' trust interacts with the socio-technical infrastructure of institutions in the cryptocurrency assemblage in a bid to form a stable ecosystem. The emergence and sustainability of trust within this decentralized and technologically mediated environment are linked to the formation of intersubjective understandings based on commonly accepted norms and heuristics (Poteete, 2010, pp. 225–226). Norms are social standards that emerge as individuals assign positive or negative values to specific behaviors in particular contexts, serving to regulate behavior by establishing shared expectations within a community. Heuristics are essentially rules of thumb that individuals develop over time based on experience, aiding them in responding to various situations and anticipating potential outcomes. These rules facilitate decision-making processes by drawing on accumulated knowledge (Poteete, 2010, pp. 223–225).

I argue that the stability of the cryptocurrency ecosystem is contingent upon the development and adherence to shared norms and heuristics within the socio-technical infrastructure of institutions, resulting in the formation of trust. This reliance on emergent norms and heuristics becomes particularly evident in the U.S. cryptocurrency ecosystem, where regulatory uncertainty, governance shifts, and evolving technological frameworks create an environment in which control and legitimacy remain in flux. As competing authorities redefine legal boundaries and institutional innovations challenge traditional oversight, trust is continuously reshaped through interactions between algorithmic processes, institutional oversight, and market forces.

Given these dynamics, the concept of a socio-technical assemblage provides a strong fit for the analysis of the cryptocurrency ecosystem. Conceptualized by Actor-Network Theory (ANT), an assemblage is a network of hybrid actors, referred to as actants, which has real, material effects, but its stability depends on ongoing interactions and alignments within the network. Epistemologically, its significance and legitimacy are also shaped by subjective interpretations, rendering it materially grounded, but also contingent and contested, as its stability depends on ongoing enactment and negotiation (Latour, 2005, pp. 217–218).

This study seeks to examine the problematization of trust within the U.S. cryptocurrency ecosystem by pursuing the following research goals, where problematization refers to how actors define a problem in a way that aligns with their interests, shaping the web of relations in the assemblage:

1. Analyze the Constitution and Structure of the Assemblage – Identify the key actants and institutional arrangements that define the assemblage, examining how they contribute to its formation and evolution.
2. Investigate the Dynamics of Trust – Assess how trust is problematized within the assemblage, identify emergent trust patterns, and analyze the reciprocal relationship between trust and institutional developments, demonstrating how trust both shapes and is shaped by evolving institutional mechanisms.
3. Evaluate the Implications for Long-Term Stability – Determine whether the discursive construction of the cryptocurrency ecosystem fosters resilience or fragility, considering the sustainability of its governance mechanisms and institutional structures.

Thesis Outline

The remainder of this thesis is structured as follows. Chapter Two provides a literature review, positioning this study within research on the social aspects of money and the rapidly expanding scholarship on the role of trust in the monetary system in the wake of the shifts of power and trust resulting from decentralization and automation.

Chapter Three outlines the theoretical framework, integrating Actor-Network Theory (ANT), Elinor Ostrom's institutional framework as complementary theories to examine

trust in the U.S. cryptocurrency ecosystem. Additionally, it introduces the literature on Poststructural Discourse analysis as a critical lens to examine how trust is problematized in policy documents and related responses.

Chapter Four details the methodology, explaining the research design and analytical approach. This study employs Poststructural Discourse Analysis (PDA) to examine how trust is problematized within policy documents and public discourse. It also introduces computational methods that aided in the analysis of large textual material.

Chapters Five through Eleven present the empirical analysis organized in seven sections, each addressing one of Elinor Ostrom's design principles. Each chapter begins with a short theoretical analysis of the design principle in the context of cryptocurrency. Next, the main findings from PDA are presented, highlighting how different stakeholders problematize trust in the context of the design principle. I end each section with a conclusion, discussing key takeaways from the analysis. This analysis is based on Bacchi's WPR framework.

Chapter Twelve concludes the thesis by synthesizing the findings to answer the three research questions outlined in the introduction. It integrates insights from the empirical analysis, highlighting how trust is constructed, problematized, and institutionalized within the U.S. cryptocurrency ecosystem.

Chapter Two.

Literature Review: The Evolution of Money and Trust

Theories of Money and Trust

Theories of money have evolved over time, reflecting shifts in economic thought and societal structures. Classical monetary theories are considered to have originated with Adam Smith in the late eighteenth century, but it was only a hundred years later that William Stanley Jevons first articulated the functions of money as a medium of exchange, a unit of account, and a store of value (Jevons, 1875). At that time the dominant theory was that the value of money originates in the commodity that it represents. Thus, even banknotes, which carried no intrinsic physical value were considered a promise to redeem a specific amount of precious metal (Jevons, 1875, pp. 239–240).

This view of money was first challenged by Georg Friedrich Knapp who analyzed the prevalent monetary systems of the nineteenth century and concluded that the value of money, and specifically its paper form, is dependent on the state's authority. This authority stems from the function of money as a unit of account for taxation and public debt transactions. Knapp referred to this theory as chartalism, deriving the term from the Latin word *charta*, meaning "token", to emphasize that money's value is not tied to its material composition (Knapp, 1924, pp. 142–145). The credit theory of money is a complement to chartalism, analyzing money from a more social perspective. Rather than focusing solely on state authority, the credit theory posits that money originates from social credit-debt relationships, where its value is derived from the legal obligations between debtors and creditors. When goods are exchanged for money, they are traded for an obligation to reciprocate value (Mitchell-Innes, 1914, pp. 152–153). In this view, the state's role is significant not because it defines the value of money through taxes and public debt, but because it operates as a central creditor.

The Credit Theory of Money marks a turning point where the theoretical discussion transitions from an economic frame of reference to the social domain. If money derives its value from the interactions between debtors and creditors, then that value emerges from a social relationship of trust. Georg Simmel's conceptualization of money as a claim on society advances this line of thinking. Simmel contends that money is a claim

on society rather than a claim on an individual creditor. He regards money as a social construct that reflects the dynamics of a network of relationships where value is rooted in a collective commitment to honor obligations. This collective commitment is sustained through continuous social interactions and the trust that emerges from them. The social impact of money lies in its ability to structure human interactions by abstracting and simplifying commercial exchanges, controlling social distance and creating individual autonomy (Simmel, 2004, pp. 176–177).

Viviana Zelizer (2010, pp. 95–97) challenges Simmel's objectification of money as a neutral entity, equipped with "uncompromising objectivity" and agnostic to history or social relations. She contends that, while Simmel was right about the impact of money on society, he ignores the reciprocal impact of society on money. Money is not indifferent to culture and morality. It may be corrupted or otherwise labeled by social practices and moral values. Thus, Zelizer removes any remaining essentialism that Simmel left behind in the conceptualization of money, arguing that while money forms social relationships, it is these relationships themselves that construct money. Nigel Dodd expands on this idea, asserting that money is not merely a "thing" interacting with social processes but is woven into their fabric. He frames money as a process of constant negotiation, shaped by conflict, utopian aspirations, and institutional change. Money, for Dodd, is never fixed; it is always in the process of becoming something else (Dodd, 2014, pp. 393–394).

Geoffrey Ingham reintroduces a form of chartalism by framing money as an institutionalized social relation of credit and debt, based on enduring state-sponsored structures rather than fluid cultural meanings alone. While acknowledging the relational dynamics emphasized by Dodd and Zelizer, Ingham asserts that money's existence is anchored in specific institutional arrangements that generate stability and continuity. These institutional arrangements are created and supported by the state as the largest economic agency. He further argues that economic theories are performative, meaning they do not merely describe monetary systems but actively shape them through their influence on institutions, policies, and practices. Thus, Ingham brings back the essentialism that earlier sociological perspectives sought to deconstruct, by attributing the nature of money to the ideologies that underlie economic theories (Ingham, 2013, Location 2042).

Trust in money manifests as the confidence that coins or other tokens, held by a party, will be honored and exchanged for a value equivalent to their perceived worth within the economic system (Keynes, 1930, pp. 47–48). When money was perceived to be backed by a commodity, this trust was rooted in the value of the commodity itself. With the emergence of Chartalism, trust became set in the authority and stability of the state, which guarantees the acceptance of money for taxes and legal obligations. The legal system reinforces this trust by institutionalizing the value of money, ensuring that debts and financial obligations are honored within the framework of the state's legal system. The acceptance of this value does not just originate in state coercion. It is also driven by institutional trust where individuals and entities rely on the consistency, legitimacy, and enforcement capabilities of state-led legal and financial institutions (Knapp, 1924, p. 39).

The Credit Theory of Money eliminates the emphasis on coercion and enforcement, contending that the trust in government-issued money derives from the status of government as the largest creditor and debtor in the economy. Thus, monetary trust is a social relationship linking debtor and creditor, with the relationship between government and other actors differing just due to its economic scale, making government credit the most widely accepted form of money (Mitchell-Innes, 1914, pp. 157–158).

This relational perspective on trust developed alongside shifts in the conceptualization of money. Simmel conceptualizes relational trust as a social binding that underpins credit transactions. However, this social binding is not negotiated ad-hoc; it is contingent on the social status of the trustee. Thereby reflecting an essentialist perspective, where trust is presumed to be inherent in the identity of stakeholders rather than actively constructed through interactions (Simmel, 2004, pp. 484–486). In contrast, Ingham (2013, pp. 74–75) rejects an essentialist view of trust and instead conceptualizes it as a social relation, “rooted in a social and political legitimacy”. He defines money as "assignable trust", a social relation that is transferable to others through economic interactions. This shifts the focus from trust as a presumed quality of individuals to trust as a dynamic socially constructed product of an institutional framework.

Ingham describes a stratified framework in which money exists as a *"hierarchy of promises to pay"*, organized by varying degrees of acceptability and risk. At the top of this hierarchy is sovereign money, issued by the state and accepted for tax payments, followed by bank credit, which is widely used but depends on trust in financial institutions (Ingham, 2013, p. 225). This stratification reflects the institutional organization of monetary trust, where central banks and financial institutions mediate and reinforce the credibility of different forms of money within the system. However, as Dodd points out, trust in money is not an interpersonal agreement between transactors, nor is it trust in one of the stratified layers. Rather, it is an institutionalized and systemic trust, extending beyond interpersonal interactions to the broader social, political, and cultural environment in which money circulates.

Theories of Cryptocurrency and Trust

Kevin Werbach explores the consequences of systemic trust failure, focusing on the 2008 global financial crisis as a defining moment. He points out that what distinguishes this crisis was not only the collapse of the financial system but also the failure of the safeguards intended to stabilize it. The institutions responsible for maintaining stability, including central banks and regulators, either mismanaged their response or were compromised by corruption. This prompted Werbach to consider the possibility that the financial system is flawed beyond repair, as it is structured in a way that incentivizes risk-taking. Thus, if systemic trust cannot be restored, the system may be destined to collapse, leaving an open door to alternative solutions (Werbach, 2018a, Locations 1277–1307).

This is the sentiment behind the conceptualization held by early cryptocurrency enthusiasts. Their conceptualization of trust in cryptocurrencies aligns with what Maurer et al. (2013, pp. 268–269) describe as 'digital metallism', representing the view that Bitcoin and other similar cryptocurrencies are digital equivalents of gold. This perspective, rooted in libertarian and Austrian economic theories, posits that cryptographic scarcity and decentralized mining eliminate the reliance on institutional trust. Ludwig von Mises, a central figure in the Austrian school, argued that the gold standard ensures purchasing power remains independent of government policies and political manipulation, thereby securing monetary stability by anchoring trust in gold, rather than in financial institutions or state authorities (Von Mises, 2009, pp. 416–417).

The conceptual independence from centralized government control and traditional intermediation opens the way for a decentralized organization where trust emerges from the collective actions of a network of participants. The result is a community based on what the Maurer et al. (Maurer et al., 2013, pp. 272–274) terms 'the wisdom of the crowds', putting people together to adopt preferred solutions. This crowd characteristic, the strength of the material characteristics of algorithms, as well as the emergence of a society with weak relational links, are strong indicators of an essentialist point of view, where ideology is said to be inscribed into the very structure of the technology itself.

These essentialist tendencies are also evident in the research of other scholars, particularly among critics of cryptocurrencies. David Golumbia characterizes cryptocurrencies as products of conspiracy theories about governments and central banks that are perpetrated by far-right political ideas (Golumbia, 2015, p. 123). He associates cryptocurrency with what he terms cyberlibertarianism, an ideological framework that merges libertarian economic thought with technological determinism, reinforcing post-truth narratives that challenge traditional institutions of knowledge and (Golumbia & Justice, 2024, Location 780). Another essentialist perspective on cryptocurrencies, proposed by Brekke (2021, pp. 653–656), contends that the cryptocurrency ecosystem is shaped by the intersection of hacker culture and cyberpunk ideals. Hacker culture prioritizes decentralization, technical expertise, and open-source collaboration as mechanisms to challenge centralized authority, while cyberpunk is a cultural genre that emphasizes privacy and personal autonomy as safeguards against corporate and governmental control. The fusion of these overlapping ideas manifests in the cypherpunk movement, which actively seeks to implement cryptographic solutions for privacy and decentralization. By prioritizing privacy and decentralization as foundational principles, trust is envisioned as an emergent property of cryptographic systems rather than a socially constructed process.

However, most sociologists do not agree that monetary trust can be reduced solely to scarcity or ideological embedding (Dodd, 2018; Maurer et al., 2013; Swartz, 2018). Their arguments are based on relational thinking, which emphasizes that trust in money emerges through ongoing social interactions, institutional arrangements, and governance mechanisms rather than being solely determined by its material properties or ideological foundations. Maurer et al. (2013, p. 261) suggest that the trust model of

cryptocurrencies emerges from the same social relations that underpin money in general. However, what sets it apart is that some of these relations are formalized through their embedding in the software that governs the monetary system.

Nigel Dodd rejects this deterministic view of cryptocurrencies, arguing that it endorses essentialist views of ideological hegemony rather than relationism. He argues that technology cannot enact social organization without human intervention in the form of "structure, leadership, friendship, and community". Arguing that "There is not one Bitcoin, but several", he makes the point that Bitcoin is as multifaceted and politically contested as money. He completely rejects the essentialist perspective, stating that the assertion that Bitcoin replaces social relations with trust in machine code is false (Dodd, 2018, p. 37).

While Dodd views Bitcoin as a social reconfiguration, Hayes (2019, pp. 65–67) sees it as an institutional transformation, where blockchains function as self-enforcing institutional technologies that replace traditional intermediaries of trust. Hayes argues that blockchains create credible commitments by embedding governance mechanisms directly into code, thereby replacing traditional institutional structures. This technology acts as a testing ground for institutional experimentation, where competing rule sets can be created, modified, and contested, based on open-source software. Thus, the decentralized nature of blockchain should be analyzed as institutional rather than a technological innovation.

Primavera De Filippi (2020, p. 7) adopts a socio-technical perspective on the objects of trust in the cryptocurrency ecosystem. Rather than focusing on institutional rules, she contends that governance in blockchain ecosystems is shaped by an assemblage of social and technical elements bound together to perform a specific function. Trust in a socio-technical entity relies on confidence in the entire assemblage of actors within the network. While blockchain technology reduces dependence on any single actor, it does not eliminate the need to trust the assemblage in its entirety.

The institutional and socio-technical perspectives on cryptocurrency trust reveal complementary aspects of trust in blockchain governance. The institutional approach frames blockchain as an alternative governance structure that embeds formalized commitments within its code, while the socio-technical perspective emphasizes the interplay between technological design and human actors in maintaining trust.

Together, these frameworks illustrate that while blockchain reduces reliance on traditional intermediaries, it does not eliminate trust but rather reconfigures its focal points. While essentialist perspectives emphasize cryptocurrency's ideological roots and its capacity to replace institutional trust with technological mechanisms, relational and institutional approaches argue that trust remains a dynamic, socially embedded phenomenon. Most institutional and social theories analyze how trust is maintained, reconfigured, or reinforced, but they do not fully explain how trust first emerges in a monetary system with no prior legitimacy. Existing research focuses on institutional continuity or technological reinforcement, rather than describing how an untrusted system becomes trusted. The theoretical goal of the current research is to gain some understanding into this nascent process.

Chapter three.

Theoretical Framework: Institutions, Assemblages and the Construction of Trust

Institutional Analysis and Common Pool Resource Theory

Institutional theorists define institutions as the rules, norms, and structures that shape social settings by regulating the interactions of their constituents. These structures encompass formal instruments such as laws, regulations, and governance frameworks of authority, as well as informal mechanisms, including cultural norms, social conventions, and traditions (Hodgson, 2006, p. 2; North, 1990, p. 6). Scott (2008, pp. 50–59) defines institutions through three interconnected pillars: regulative, normative, and cultural-cognitive. The regulative pillar consists of formal rules, laws, and enforcement mechanisms that regulate interactions in the social setting. The normative pillar reflects social values and expectations that shape legitimacy of stakeholders and processes, providing guidelines for conduct. The cultural-cognitive pillar encompasses shared beliefs and mental frameworks that influence how individuals perceive and interact with institutions. Together, these pillars create stability and continuity, reinforcing institutional structures over time.

Institutional theory examines the reciprocal relationship between institutions and social norms, emphasizing how institutions shape behavior through rules, structures, and conventions of conduct, while also being influenced and transformed by changing norms and agency in the social setting. While traditional old institutionalism is focused on institutional persistence and stability as criteria for success, new institutionalism emphasizes that institutions are not static; they evolve over time, undergoing processes of resistance, constitution and destruction. This dynamic approach allows institutional theory to explain the stability of social systems and the mechanisms of institutional change (Dacin et al., 2002, pp. 45–46).

New institutional theories are broadly categorized into three approaches. Rational Choice Institutionalism conceptualizes institutions as structures that reduce transaction costs and solve collective choice issues through logical reasoning. Institutions become resilient as they incentivize stakeholders sufficiently to adhere to the rules, because any

other alternative would impose higher costs. Historical Institutionalism emphasizes path dependence, where past institutional choices constrain future developments, leading to stability. Institutional change is attributed to critical junctures or crises. Over time, stability is achieved as organizational topologies and power structures are solidified. Sociological Institutionalism emphasizes norms, symbols, and heuristics that shape behaviors of actors beyond the utilitarianism of rational choices. Institutions remain resilient because they legitimize the social setting rather than being justified through functional benefits (Hall & Taylor, 1996, pp. 950–955). While these subgroups are theoretically explicative of the types of institutional factors that regulate human behavior, many theories do not fall neatly into one of these categories (Hall & Taylor, 1996, pp. 956–958).

The Institutional Analysis and Development (IAD) framework, developed by Elinor Ostrom and colleagues, combines elements from rational choice, historical, and sociological institutionalism. While rooted in rational choice, Ostrom acknowledges that individuals often rely on norms and heuristics shaped by past experiences, requiring a broader institutional lens (Ostrom, 1998, p. 9). The IAD framework analyzes how institutions structure decision-making by creating constraints and opportunities for actors in complex social settings. It breaks down institutions into components to understand how they interact and evolve over time. “Design” refers to how institutions are constituted, while “diagnosis” focuses on identifying institutional failures (McGinnis, 2011, p. 170).

Within this framework, two major theoretical tools allow it to be applied to social settings with various complex governance challenges, Common-Pool Resource (CPR) theory and polycentric governance theory. CPR governance is an application of IAD, focusing on the institutional arrangements that enable sustainable resource management. Ostrom identified eight design principles that correlate with the resilience of CPR institutions (Ostrom, 2015, p. 90). These principles serve as diagnostic tools to assess how well governance structures enable adaptation, trust-building, and long-term resilience.

The second theoretical tool proposed as part of the IAD is polycentric governance theory, which describes systems where multiple centers of decision-making operate autonomously but interact to coordinate governance. Rather than assuming a

hierarchical or monocentric approach to governance, polycentricity emphasizes decentralized, overlapping institutions that together form the governance structure of an ecosystem (Ostrom et al., 1961, p. 831). While no single governance system is flawless, polycentric systems provide notable advantages by enabling mutual oversight, shared learning, and the continuous refinement of strategies over time (Ostrom, 2010b, p. 552).

Several scholars have researched Blockchain-based solutions in the context of Ostrom's theories (Davidson et al., 2018; Jain et al., 2022; Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2021; Werbach, 2018a). Davidson et al. (2018) view blockchain as an institutional development aimed at improving the governance of a decentralized self-governing organization. They argue that blockchain increases the variety of institutional mechanisms available to the ecosystem, thereby augmenting its resilience. This is based on Ostrom's contention that institutional diversity and decentralization enhance the capacity of ecosystems to effectively manage resources (Ostrom, 2009, pp. 283–286). The connection between diversity and resilience is reinforced by the similarities between the democratic vision of governance in cryptocurrency ecosystems, where governance is based on the wisdom of the crowd, and Ostrom's view that trust is created through the stabilization of institutional structures (Werbach, 2018a, Location 4221).

Rozas et al. (2021, p. 5) map the capabilities of blockchain to Ostrom's design principles for resilient common-pool resources, using these principles to evaluate governance instead of resource depletion. They argue that capabilities such as decentralization of power and codification of trust support the soundness of Ostrom's principles in blockchain-based ecosystems, enabling decentralized governance of a Commons-Based Peer Production (CBPP) environment (Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2021, pp. 10–11). CBPP is a term for social settings enabled by the internet where communities engage in socio-economic production to create shared resources without relying on centralized hierarchical governance (Benkler, 2006, p. 60).

While these scholars associate blockchain-based systems with IAD, they fail to identify a shared resource that behaves as a common pool resource. Moreover, some scholars point to the problems in applying Ostrom's theories to blockchains, highlighting a mismatch between the predominantly local focus of Ostrom's theories and the global

operation of cryptocurrencies (Rozas, Tenorio-Fornés, & Hassan, 2021, p. 3). Others critique the characterization of blockchain-based ecosystems as polycentric, arguing that influence often remains centralized, concentrated in the hands of a few powerful actors (De Filippi et al., 2020, pp. 10–11). Finally, the IAD framework assumes relatively stable governance structures, whereas blockchain ecosystems are highly dynamic. Therefore, the analysis of a temporary, self-governing pool of shared knowledge and information that emerges at the early stages of a new technology requires the complementing of the IAD framework with approaches that account for the adaptability of self-organizing systems in early-stage technological development (Allen & Potts, 2016, p. 1038). I propose that these theoretical requirements can be met by extending institutional analysis with innovation-focused theories that are better equipped to describe the dynamic evolution of social systems. While institutional analysis provides a structured framework for understanding governance and rulemaking, the innovative focus of Science and Technology Studies (STS) adds insights into how social constructs are formed and evolve around cryptocurrencies.

STS Perspectives and Actor-Network Theory

Science and Technology Studies (STS) is an interdisciplinary field that examines the co-production of science, technology, and society, where scientific ideas and technological artifacts evolve together with societal structures and cultural practices (Jasanoff, 2004b, pp. 15–19). This framework challenges the traditional assumption that technology functions as an autonomous force in shaping society, devoid of reciprocal influence.

A concise definition of technology by Frederick Ferré (1995, p. 26), as the "practical implementation of intelligence", implies that it is both a material and conceptual phenomenon. This definition captures the application of knowledge and problem-solving capabilities to create tools, systems, and processes that enhance human activities. Ferré distinguishes between mental and embodied phenomena, emphasizing that technology is embedded and excludes purely mental tools, such as language, from the definition (Ferré, 1995, pp. 24–26). In internet studies, however, technology is often understood more broadly. It includes not only data, software, networks, machines, protocols, and standards, but also the economic, political, social, and cultural contexts

that shape and are shaped by these technologies, along with the institutions that support them (Bodó, 2021, p. 2674).

Early STS theories, including the Strong Program (Bloor, 1976, pp. 141–144) and the Social Construction of Technology (SCOT) (Pinch & Bijker, 1984, pp. 429–432), argue that science and technology are socially constructed, with SCOT showing how technological closure emerges through the resolution of competing interpretations. Lee Humphreys (2005, pp. 248–249) critiques closure and stabilization modeled in SCOT by arguing that closure is not final, technologies continue evolving, and their relationships remain dynamic. This critique aligns closely with Actor-Network Theory (ANT), which rejects closure altogether, viewing stabilization as a temporary effect of ongoing negotiations among actors (Law, 1992, p. 5).

In ANT, the four moments of translation: problematization, interessement, enrolment, and mobilization, describe how networks are continually formed, negotiated, and reconfigured. Problematization occurs when a focal actor defines a central problem and positions itself as indispensable by establishing an obligatory passage point that others must go through. Interessement involves strategies to convince and stabilize other actors into the roles envisioned by the focal actor, aligning their interests through negotiation or persuasion. Enrolment follows when actors accept these roles and agree to the relationships proposed, allowing the network to take shape. Mobilization then ensures that these actors speak and act on behalf of their constituencies, maintaining coherence and preventing betrayal or fragmentation. This process is ongoing and dynamic, as actors may resist, redefine, or exit their roles, requiring continuous translation to adapt and preserve the network's stability

ANT regards the synthesis of humans and technology into assemblages, where agency is distributed across both human and non-human entities, as critical for understanding how networks form, stabilize, and evolve over time. This results in a theory that is highly relativistic (Latour, 1990, p. 129).

This type of relativism is the distinction of ANT. By allowing the construction of assemblages of human and non-human components, ANT provides a lens through which socio-technical environments are correctly configured to provide meaningful insights and explanations of complex systems (Callon, 1999, pp. 192–194). ANT considers these hybrid assemblages as continuously changing, rendering stabilization a

process rather than a steady state. In this process order is a temporary achievement that must be constantly maintained through interactions between human and non-human entities of agency (Law, 1992, p. 5).

While ANT remains foundational, modern STS has moved toward selectively integrating power and politics as pre-existing factors in the formation and stabilization of socio-technical settings rather than as solely emerging from these settings (Brown, 2015, p. 24). Scholars supporting SCOT and the Sociology of Scientific Knowledge (SSK) branch of STS have critiqued ANT on several grounds. Jasanoff (2004a, p. 23) points to the inability of ANT to explain stability and institutionalization, claiming that ANT primarily describes the emergence and contingent alignment of actants, ignoring the mechanisms through which social order solidifies over time. This claim is related to the contention that ANT is overly descriptive while failing to explain why some configurations succeed and others fail (Collins & Yearley, 2010, p. 322).

A final critique I have chosen to emphasize here is the claim that ANT relies on counterfactual hypotheses, substituting speculation for empirical research. This reflects the lack of structured research methodologies to investigate the actual influence of objects (Collins & Yearley, 2010, p. 318). John Law responds to this critique in his book titled “After Method” by arguing that traditional research methods impose rigid structures on reality. He supports methodological flexibility that adapts to the real-world problem being investigated. Law emphasizes that reality itself is "messy" and that methods should not impose artificial order but instead be open to capturing the fluid, contingent, and emergent nature of social settings (Law, 2004, pp. 2–5).

Poststructural Discourse Analysis and WPR

Notwithstanding the ongoing debate between critics and proponents of ANT, its methodological flexibility has been addressed by a range of both explicit and implicit approaches in empirical research. While some scholars advocate for maintaining ANT’s radical relational ontology as a unique methodological stance, others integrate it with complementary approaches to address specific research questions more effectively. Scholars have employed a variety of complementary methods in their endeavors to explain socio-technical settings. These methods include ethnographic

research (Latour & Woolgar, 1986), semiotic analysis (Mol, 2002), and institutional analysis (Quinn, 2023).

ANT scholars tend to deemphasize discourse analysis. Latour challenges the notion that discourse is sufficient to explain reality, arguing that discourse is inseparable from material reality, as it is both shaped by and dependent on it (van Eeden, 2017, p. 3). However, Latour engages in discourse analysis in his empirical work. He views discourse as embedded in a larger network bounded by non-linguistic material objects. This is exemplified by his analysis of the failed Aramis rapid transport system in France (Latour, 1996). Latour analyzes official project documents, reports, and interviews with engineers, politicians, and stakeholders involved in the project, giving them a voice in a mock interrogation that he organizes. Where written material is not available, he compensates by giving a voice to the Aramis system itself, bringing it into discourse. This reflects Latour's material semiotics approach, in which objects are not merely passive entities but actively shape and destabilize socio-technological networks.

Material semiotics and poststructuralist discourse analysis (PDA) both reject fixed structures and essentialist categories, emphasizing relationality, contingency, and the co-construction of meaning and power through interactions between human and non-human actors. However, the materialist focus of ANT has been critiqued for overlooking systemic power structures embedded in the initial constitution of social settings (Roberts, 2012, pp. 26–29). This gap has led some scholars to integrate discourse analysis with ANT to examine how discourse and materiality co-construct power relations (Marres, 2007; van Eeden, 2017). Discourse shapes problematization, which is the process of defining social phenomena as deficient or in need of intervention, relative to an implied ideal state (Rose & Miller, 2017, p. 181). The understanding of this view of problematization aligns with Bacchi's "What's the Problem Represented to Be?" (WPR) approach, which examines how governance frameworks define issues as problems, shaping policy responses while constraining alternative perspectives. Expanding on poststructuralist discourse analysis, WPR emphasizes that problems do not pre-exist but are actively constructed through discourse (C. Bacchi & Goodwin, 2016, pp. 38–41).

Synthesis and Theory Application

I argue that ANT and Ostrom's IAD framework share a broad theoretical foundation, both rejecting top-down governance models and emphasizing how institutions emerge through interactions and negotiation. They share a non-hierarchical perspective, recognizing governance as adaptive and evolving rather than fixed. Both theories valorize the influence of rules, technologies, monitoring mechanisms, and biophysical conditions in shaping institutional outcomes

However, while Actor-Network Theory provides a powerful framework for analyzing the socio-technical assemblage of the United States cryptocurrency ecosystem, it also has notable limitations in addressing key aspects of trust formation and institutional stability required by the research goals. The strength of ANT is its ability to trace relationships between human and non-human actants, illustrating how trust emerges through interactions within the network. However, ANT does not differentiate between stable institutional arrangements and emergent networks (Murdoch, 1998, p. 362). This complicates the effort to understand how lasting structures of trust and governance solidify over time, creating a challenge in effectively addressing my second and third research objectives.

To address this limitation and provide structure to the research, I employ Elinor Ostrom's institutional framework. The framework provides a structural blueprint for the evaluation of institutional resilience over time. This blueprint comes in the form of a set of design principles for the establishment of resilient institutions, thereby identifying concrete institutional arrangements that promote stability (Ostrom, 2015, pp. 90–102). A major incentive for the reliance on this framework is the tools it provides for examining distributed self-governance (Shackelford & Myers, 2016, pp. 35–40). Furthermore, scholars have noted that cryptocurrencies share the main characteristics of the common-pool resources (CPR) that Ostrom studies: subtractability and non-excludability. Subtractability implies that the use or consumption of the resource by one actor reduces the amount available for others, whereas non-excludability dictates that it is very expensive to exclude consumers from using the resource (McGinnis, 2011, p. 174).

Consequently, I analyze the problematization of trust in the context of each of these design principles under the assumption that trust is the "glue" that enables institutional

persistence and stability in the ecosystem. My analysis utilizes the tools provided by IAD in conjunction with the relational lens of ANT to conceptualize how trust emerges, is translated, and becomes embedded within actor-networks, shaping the evolving institutional arrangements and the durability of the cryptocurrency ecosystem, while also acknowledging its continual fluidity and contingency.

However, neither ANT nor Ostrom's framework fully provides an empirical basis for understanding how discourse shapes institutional legitimacy, governance perceptions, and trust formation. To bridge this gap, I conclude each one of my examinations of Ostrom design principles by implementing PDA on the analyzed discourses. While ANT captures the relational and material dimensions of trust in governance, and IAD identifies concrete rule-based mechanisms for trust-enabled institutional resilience, PDA reveals how discourse legitimizes, destabilizes, or transforms governance structures to create that trust. Specifically, I use WPR analysis to shine a spotlight on the problematization of trust, the underlying norms and heuristics that shape it and the institutional results of how trust is shaped in the analyzed discourse.

Together, ANT, IAD, and WPR constitute a layered lens for analyzing how trust is problematized within the cryptocurrency ecosystem. This synthesis allows for a concerted examination of material-relational configurations and institutional design, through the analysis of discursive framings to provide a rich description of the assemblage and assess its prospects.

Chapter Four.

Research Methodology

My research examines the emergence of the cryptocurrency assemblage in the United States (U.S.). Yet, this does not imply that the U.S. is simply a case study for other countries facing similar economic disruptions. The U.S. market's size, diversity, and regulatory fragmentation, shaped by its federal system, create unique conditions. Additionally, major tech and financial institutions hold greater influence in the U.S. than in most other countries. However, as a dominant global economic actor and issuer of the world's primary reserve currency, the U.S. plays a leading role in shaping the trajectory of cryptocurrencies. Consequently, the development of the U.S. cryptocurrency ecosystem will have widespread global effects on market liquidity, stability, currency dynamics, and investor sentiment. As a result, U.S. policies will be a key force in shaping international cryptocurrency trends.

The primary set of documents analyzed in this study (see table 1 below) originates from a process initiated by the president of the United States via an executive order in March of 2022 in an effort to ensure responsible development of digital assets in the U.S. (Biden, 2022). The order led to nine policy reports and a complementary response from the Fed, including a request for public comment (RFC) (FED, 2022a). The call was a survey consisting of 22 open questions and obtained a total of 2,050 responses as of May 2023. About 50% of the responses were submitted by individuals. Other significant groups that responded to the survey were: academics (100), financial institutions (121), merchants (55), trade organizations (51), and consumer groups (32).

Public responses to the survey are taken at face value without assuming who these respondents are or any bias that they may have as a group. No assumptions are made as to their representation of public opinion in the broader public. Therefore, I use the term respondents, and refrain from referring to them as the general public. Readers may infer that they have a libertarian or at least a strongly liberal orientation, explaining their engagement with President Biden's Executive order, which calls for strong government intervention in a market of private currencies. Each respondent whose text was used has been identified with high probability as a real individual.

The texts were analyzed using the approach of poststructural discourse analysis (PDA) (Jacobs, 2019; Laclau & Mouffe, 1985). This methodology is apt for comprehending how collective action can be interpreted and understood consistently within the context of discourse. It studies the reciprocal relation between meaning and behavior. In the scope of this study' the reciprocal relationship is analyzed between meanings connected with trust and the behavior reflected by institutional design. By using PDA in a field abundant with innovation and new institutions, the deconstruction of language is key to understanding meanings related to trust.

Document Name	Reference
Ensuring Responsible Development of Digital Assets	(Biden, 2022)
Action Plan to Address Illicit Financing Risks of Digital Assets	(DOT, 2022)
2024 National Strategy for Combating Terrorist and Other Illicit Financing	(DOT, 2024)
Crypto-Assets: Implications for Consumers, Investors, and Businesses	(Treasury, 2022a)
The Future of Money and Payments	(Treasury, 2022b)
Stablecoins: Growth Potential and Impact on Banking	(FED, 2022b)
Money and Payments: The U.S. Dollar in the Age of Digital Transformation	(FED, 2022a)
Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments	(FED, 2023)
Public Policy Principles for Retail Central Bank Digital Currencies	(G7, 2021)
Technical Evaluation for a U.S. Central Bank Digital Currency System	(OSTP, 2022b)
Climate and Energy Implications of Crypto-Assets	(OSTP, 2022a)
FED RFC - Public Comments	(FED-comments, 2022)
OSTP – Public Comments	(OSTP-Responses-1, 2022)

Table 1 - List of Primary Sources for PDA

ANT extends the investigation beyond discourse to include material and technical aspects, recognizing that trust is shaped by both narratives and the infrastructures sustaining the ecosystem. This involves tracing relationships between human actors,

regulations, protocols, and technologies to map how trust is stabilized, contested, or disrupted. Some relationships are drawn from secondary sources such as news articles, laws, and official statements, which were cross verified but not analyzed discursively.

This paper takes a different approach from those that treat problems as objectively real and widely acknowledged. Instead, it adopts a poststructuralist perspective, viewing problems as constructed through stakeholders' network relations and reflected in policy discourse and public communications. (C. Bacchi & Goodwin, 2016, p. 39). This view is the basis for the analysis model "What's the problem represented to be?" (WPR) introduced by Carol Bacchi. WPR is a poststructural methodological framework designed primarily as a tool for analyzing discourse in public policy. It focuses on the construction of problematization by stakeholders (C. L. Bacchi, 2009). The framework prescribes that the analysis of problematization should follow six guiding questions that examine how a problem is represented, what assumptions underlie this representation, and how it has come about. They also address what is left unproblematic, what alternatives are excluded, and how the representation is maintained or contested (C. Bacchi & Goodwin, 2016, p. 20).

To address the problematization of trust in the cryptocurrency ecosystem, I focus on three of the WPR questions, adapting them to address the research goals:

- What is the problem of trust represented to be in the discourse by stakeholders of the cryptocurrency ecosystem?
- What deep-seated norms and heuristics underlie this representation of the problem?
- What are the discursive institutional effects of the representation of the "problem" regarding the constitution of institutions, and how do these institutional effects impact trust?

With these questions, I approach each text, reading it three times and encoding it with trust-related codes in Atlas.ti, a qualitative data analysis (QDA) software tool designed to help researchers systematically analyze large volumes of textual data. The reading pipeline consists of the following steps: First, I read the document thoroughly and summarize it. Second, I read it again and code the elements related to trust between actors in the ecosystem. Finally, I validate my coding by reading the document a third time and reviewing the coding output.

I conceptualize the codes used to capture trust in the analyzed policy documents, identifying passages that reflect trust relationships and categorizing them as "trust," "distrust," or "uncertain," with the latter indicating unresolved questions about trustworthiness. The five main codes, shown in Figure 1, are linked to the WPR questions. I hypothesize that risk and opportunity problematize trust: without them, there would be no need for trust, and it would not arise in the texts. As risk increases, trust declines and turns into distrust; as opportunity increases, trust grows and distrust lessens. This framing highlights the role of institutional change in enacting trust and distrust relationships. Norms and heuristics serve as the deep assumptions behind trust and distrust, and can be "made" or "unmade" through discourse. These processes define the logic of problematization and help address research question two. Institutions—formal and informal—such as CBDCs and decentralized governance, are both shaped by and shaping trust through discourse and mutual constitution of actants, a process Bacchi terms subjectification (C. L. Bacchi, 2009, pp. 49–53).

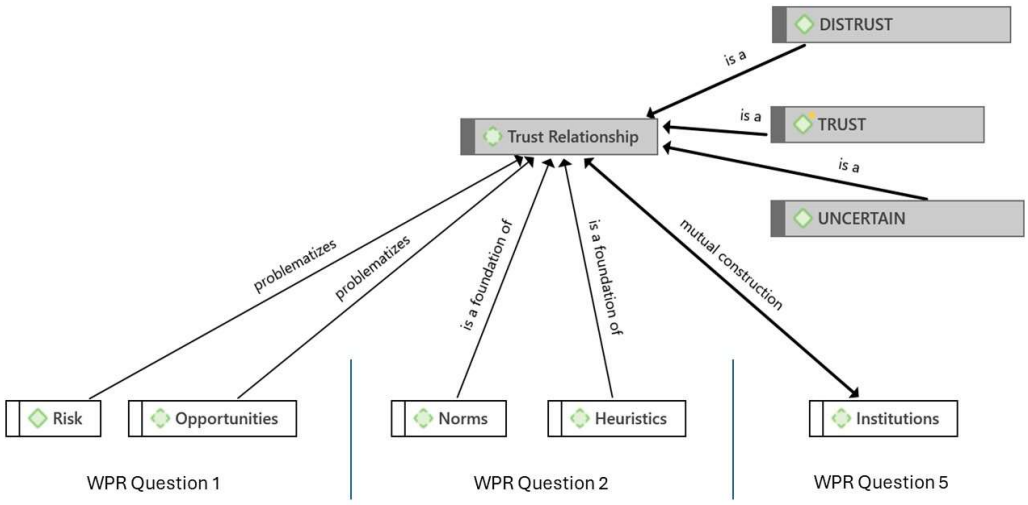

Figure 1 - The conceptualization of trust in terms of WPR (Atlas.ti)

I use computational methods to supplement my qualitative analysis in two main ways. First, to address the scale of my corpus of over 30,000 pages of responses, I used intentional coding with Atlas.ti's NLP algorithm, limited to specific categories aligned with my research questions (Atlas.ti, 2024). Automation enabled iterative sampling until saturation was reached—when additional responses no longer yielded new insights. Saturation was assessed using two criteria: "code-saturation," when the

codebook stabilized, and "meaning-saturation," when new data no longer changed the understanding of key issues (Hennink et al., 2017, pp. 591–597). The resulting sample was then subjected to in-depth manual analysis to extract trust dynamics.

The second goal of using NLP techniques was to support and improve the consistency of my manual analysis. Between readings, I generated three automated reference outputs: (1) named entity recognition (NER) to identify the actor network (Derczynski et al., 2015, pp. 2–3), (2) word2vec-based semantic word clouds (Derczynski et al., 2015, pp. 2–3) around trust-related terms to mark trust dynamics, and (3) sentiment analysis to detect dissenting or minority voices within response groups.

While the poststructural qualitative research that I am conducting is manual and involves deep reading of the material, NLP analysis of the documents and public responses help to solve the scale challenge in the corpus as well as augment the quality and consistency of my analysis. Recent experimentation in which qualitative research is augmented by natural language processing has yielded positive results, thereby enhancing quality and increasing the speed of analysis (Guetterman et al., 2018, pp. 2–10).

Chapter Five.

Clearly Defined Boundaries

The Cast of Actors

Ostrom's first design principle for enduring CPRs concerns clearly defined physical and social boundaries. In the small-scale CPRs she studied, she emphasized identifying both the appropriators and the geographic scope of rules. This emphasis on clear delineation is central to ensuring equitable access and effective governance of CPR arrangements:

> "Individuals or households who have rights to withdraw resource units from the CPR must be clearly defined, as must the boundaries of the CPR itself." (Ostrom, 2015, p. 90)

This part of the empirical analysis aims to introduce a topology of actors and uncover key issues in their construction, in the context related to the development and distribution of trust within the assemblage by integrating the concepts of subjectification from WPR analysis and translation from Actor-Network Theory. I will explore how actors are discursively shaped with specific identities and characteristics, and the roles that are attached to them in the context of trust.

The heterogeneity of actors in the management of large-scale CPR settings influences how boundaries are established and enforced. This diversity complicates the analysis of boundaries, as the varied roles of actors must be considered when determining the nature of control that stakeholders have over the resource and how that control is distributed (McGinnis & Ostrom, 1996, pp. 12–15). Considering these complexities, I argue that actor formation through the incorporation of roles into the analysis changes the understanding of boundaries as simple binary delineations, including or excluding potential stakeholders. Rather, the assignment of roles to actors determines the specific actions they can perform and relationships they can establish, thereby simultaneously including and excluding them in the assemblage. The resulting boundaries are therefore multi-dimensional and dynamic, being shaped by the roles and interactions of actors. These boundaries evolve based on the shifting responsibilities and relationships within

the ecosystem, reflecting an assemblage in which actors can be excluded from performing specific roles while being included in others.

Actants such as cryptocurrency miners, regulatory agencies, smart contracts, and cryptocurrency exchanges are shaped by evolving norms and institutional structures. Their identities form through discursive processes that define the assemblage and are organized into four main categories: the state, individuals, intermediaries, and digital assets. State actors fall into three groups: (1) the executive branch, led by the President and including departments reporting directly to the executive office, such as the Department of the Treasury and the Department of Justice; (2) the Federal Reserve, which operates with significant independence in monetary policy; and (3) regulatory agencies, which shape the regulatory framework while operating autonomously and advising the executive. The second actor category in the assemblage is individual stakeholders, distinguished by their relationship to financial systems, especially the divide between the general public and underserved individuals without access to basic services. The third category includes intermediaries such as traditional banks, cryptocurrency exchanges, and payment systems that facilitate the creation and management of digital assets. The fourth category consists of digital assets like Bitcoin, Ethereum, CBDCs, and stablecoins, along with the underlying technologies that support them, including distributed ledger technologies, cryptographic protocols, and consensus mechanisms such as Proof of Work and Proof of Stake.

Clear Boundaries, Enrollment and Trust

For actors to be successfully enrolled into the assemblage, they must have confidence that their interests are aligned with the overarching objectives of the network. This trust enables them to accept assigned roles and responsibilities, contributing to the formation of clear boundaries. Callon's concept of *interessement* explains this process: the focal actor aligns others' interests with the network to secure their participation (Callon, 1984, p. 206). When actors believe their involvement is beneficial, they commit to their roles, thereby reinforcing the assemblage. Clear role definitions foster trust by reducing uncertainty as actors know their responsibilities and can rely on others to fulfill theirs. This shared clarity mitigates the risk of boundary violations and resource exploitation (Ostrom, 2008, p. 7).

The relationship between trust and clear boundaries facilitated by successful enrollment is reciprocal. Trust establishes well-defined role boundaries, which in turn foster trust among actors. I conceptualize the trust in the overall goals of the assemblage and its capacity to achieve those goals as systemic trust, fostering confidence in the structure, processes, and relationships in the assemblage, leading to a reliable and stable ecosystem. Therefore, analyzing enrollment provides critical insights into how systemic trust is built among actors within the assemblage, as it reveals the dynamics and negotiations that establish clear roles and boundaries, which are essential for maintaining systemic trust.

State Enrollment

The presidential executive order serves as the foundation for my analysis, positioning the President as the primum movens (prime mover) in the creation of a United States cryptocurrency assemblage. I use the executive order and the document pursuant to section 4(b) of that order, issued by the DOT, to analyze how the state is enrolled into the assemblage. The question posed by the Office of the President regarding the future of money and payments in the age of digital assets focuses on how the vision of a stable and accessible ecosystem can be achieved through "responsible financial innovation":

"The United States has an interest in responsible financial innovation, expanding access to safe and affordable financial services, and reducing the cost of domestic and cross-border funds transfers and payments, including through the continued modernization of public payment systems." (Biden, 2022, p. 14143)

The formation of the ecosystem is contingent on what would be the policy regarding the future of money and payments that will best serve the "national interest" of the state (Biden, 2022, p. 14145) (Treasury, 2022b, p. 45). I contend that the formulation of national interest is the subject of the ANT obligatory passage point (OPP) that needs to be crossed for the assemblage to materialize. The OPP is a point or process that all actors in a network must pass through to achieve their individual or collective goals, effectively aligning their interests and creating a shared path toward the network's objectives (Callon, 1984, pp. 205–206). In this context, the Fed functions as the OPP by centralizing decision-making around the national interest, ensuring alignment among diverse actors in the assemblage.

Once the President designates national interest as a goal of the assemblage, he delegates the task of determining whether introducing a CBDC aligns with that interest to the Fed, effectively entrusting it with deciding how national interest can be best served:

"The Chairman of the Federal Reserve is also encouraged to evaluate the extent to which a United States CBDC, based on the potential design options, could enhance or impede the ability of monetary policy to function effectively as a critical macroeconomic stabilization tool" (Biden, 2022, p. 14146).

Here the President sets the Fed apart from the department of government by employing language that encourages rather than commands action. Consequently, the President positions the Fed as the indispensable OPP for the materialization of the ecosystem, enrolling it as a separate entity with an advocative link to the President and his government. Delegating cryptocurrency decisions to the Federal Reserve functions as *interessement* and enrollment into the crypto assemblage, though the Fed is already embedded in the monetary ecosystem through FedNow, which is a real-time, government-run payment system seen by some economists as a public alternative to cryptocurrency use cases (Smith, 2023). FedNow marks a policy shift, positioning The Federal Reserve as a lead actor in a domain once dominated by private innovation (Krause, 2024, p. 4).

According to ANT, the President himself must also be seen as an internal actor within the assemblage due to his role as the prime mover. The regulatory approach outlined in the policy section of the executive order assigns an external role to the state (Biden, 2022, p. 14144). In practice, The President's commitment to responsible financial innovation, financial inclusion, and payment system modernization signals that government is not merely an external regulator but an active participant in constituting and maintaining the assemblage—an intention underscored by the executive order's goal to launch a CBDC:

"A United States CBDC may have the potential to support efficient and low-cost transactions, particularly for cross-border funds transfers and payments, and to foster greater access to the financial system, with fewer of the risks posed by private sector-administered digital assets." (Biden, 2022, p. 14145)

Here the President launches a "sales pitch" to persuade potential actors that a CBDC will pose an alternative to high-risk private digital assets. The statement appears crafted

to appeal specifically to people with limited access to traditional financial systems, by emphasizing how a CBDC could offer a secure, cost-effective alternative to traditional fiat currencies and to private digital coins. By actively competing with cryptocurrencies on the speed, price and accessibility of transactions, the government departs from the role of an external, objective regulator and enters the assemblage.

Respondents to the RFC also position the executive branch and the Fed as internal actors, regardless of whether they support or oppose the introduction of a CBDC. A minority of respondents articulate a form of qualified or conditional trust in the state, indicating a willingness to accept state involvement contingent upon the fulfillment of specific conditions or circumstances.

"I think people still trust the government over anonymous blockchain however inaction can lead to losing people. I will not support anything but a government backed coin." (FED-comments, 2022, pp. 2–447)

The respondent frames the government as more trustworthy than "anonymous blockchain," citing the stability of state backing. However, this trust is conditional on effective action and sustained public confidence. The quote reflects reliance on norms of reciprocity and accountability, where trust must be earned through mutual exchange and alignment with public expectations, offering a consistent framework for assessing when trust is granted.

Based on the normative foundation, most respondents vehemently oppose the launch of a CBDC, arguing that the Fed itself should be abolished. Consequently, these respondents articulate concerns regarding potential government overreach, emphasizing that heightened involvement by the state could undermine the foundational norms of decentralization and autonomy in digital assets:

"What you should be doing is working on regulation to prevent the government from interfering with the use of assets by the consumers in our free republic. Until there is adequate regulation and reform, reining in the overreach and abuses that are ongoing, the thought of a Federalized digital currency is chilling at the very least." (FED-comments, 2022, pp. 4–29)

The reliance on government self-regulation reflects an expectation of insufficient government reciprocity and accountability. Terms like "chilling," together with

references to "overreach" and "abuses," frame the government as a threat to personal freedom, constructing it as an oppressive force within the assemblage. The phrase “free republic” encapsulates the tension between norms of individual autonomy and the structured governance required to ensure public good. By invoking this term, the respondent asserts that while freedom from government interference must be guaranteed, the government is expected to protect that freedom. This tension highlights the delicate balance between personal autonomy and the stability and security of the financial system, delineating a critical boundary within the assemblage.

While respondents who oppose government intervention in the form of a launch of CBDC acknowledge a role for the government in the assemblage, most completely exclude the Fed from any involvement, arguing for its abolition:

“It is my hope that we move away from fed control of the monetary supply. You seem to print money at will, undermining a currency’s actual value and you choose to do so purely for political purposes. You have proven to be ineffective. A mistake was made by Wilson one hundred years ago and it’s time to correct that mistake.” (FED-comments, 2022, pp. 4–103)

The statement positions the Fed and its control over money supply as a historical "mistake" rooted in President Wilson's policies. By invoking Wilson, the respondent invokes a conservative discourse that associates centralized financial authority with political manipulation and ineffective governance. Here the Fed is framed as an untrustworthy institution driven by ulterior motives rather than public or economic welfare.

In conclusion, the prevalent discourse on the roles of the government and the Fed suggests that they are not merely external regulators of a self-governing assemblage but are integral actors actively shaping governance and operational processes. The tension between calls for state accountability and fears of overreach highlights the dynamic and contested boundaries of the assemblage. The contested role of the Fed exemplifies the tension between Ostrom’s first principle, which emphasizes the importance of fixed boundaries and clearly defined roles, and the perspective which accommodates the fluidity and ongoing negotiation of actor relationships within a dynamic assemblage as theorized by ANT.

The Construction of Individual Actors

The global rise in financial literacy initiatives reflects a shift in how governments view individuals in financialized capitalist societies, where market logics dominate social and economic life (Santos, 2017, p. 410). Promoting financial literacy aligns with neo-liberal responsibilization, framing individuals as autonomous actors accountable for managing financial risks (Shamir, 2008, pp. 7–8). However, financial education theorists point to a tension between this expectation and the complexity of financial markets, arguing that true financial self-reliance is often unachievable. As a result, individuals are framed as both responsible and perpetually vulnerable (Willis, 2008, pp. 225–226).

The presidential executive order reflects this dominant trend in contemporary policy, referring to citizens as “consumers”. The exclusive use of the term "consumers" in the executive order indicates a particular economic perspective held by the administration, framing the role of individuals in the digital asset ecosystem primarily as economic agents. This choice persists in the documents published by DOT. In doing so, the government de-emphasizes other roles that individuals may have beyond consumerism, such as users, innovators, and members of society with a stake in the future of money and payments. However, The President and other government agencies emphasize the vulnerability of consumers, rather than their autonomy and ability to take responsibility for their actions. Consumers are presented as helpless, passive subjects in constant need of protection from market risks:

“*We must take strong steps to reduce the risks that digital assets could pose to consumers, investors, and business protections; financial stability and financial system integrity; combating and preventing crime and illicit finance; national security; the ability to exercise human rights; financial inclusion and equity; and climate change and pollution.*” (Biden, 2022, p. 14143)

Here consumer protection is one step required to mitigate risks posed by digital assets. The responsibility is owned by the government in its entirety and there is no indication in the executive order that consumers should have some of the responsibility of reducing this risk. Thus, consumers are not trusted by the government to be capable of aiding digital asset risk reduction.

The DOT reinforces this perspective, portraying consumers as actors primarily focused on engaging in financial transactions. The only instance in which DOT discusses consumer discretion is when it mentions that they have a choice of payment methods. DOT also addresses a special category of consumers - the vulnerable parts of society who are underserved in the traditional banking system and therefore, at a higher risk level in the context of the cryptocurrency ecosystem. The DOT prescribes an education system to address this special part of the population:

"Given significant interest of individual consumers, investors, and populations vulnerable to disparate impacts in crypto-assets, and the many non-traditional forms of projects and firms involved in crypto-asset activities, regulatory agencies should, as much as possible, issue guidance, interpretations, and rulemaking related to crypto-assets in plain language. Plain language guidance is that which is readily understandable by an audience of laypersons, technologists, and non-professional parties with interests in the topic." (Treasury, 2022a, p. 53)

The quote notes that unbanked and underbanked consumers are more likely to be less educated than others. The emphasis on plain language, fit for laypersons, demonstrates the problematization of financial inclusion as a literacy issue, suggesting that simplifying language is a necessary step to make financial services accessible to these groups. The vulnerability of these laypersons suggests that government plays a critical role in protecting consumers, ensuring that they are not only informed but also safeguarded within the financial system. Thus, two layers of consumers are "subjectified". Both groups need protection, the more vulnerable layer also requiring education about the risks involved in digital assets. This subjectification reflects an attempt to bridge the gap in financial inclusion by equipping vulnerable individuals with the tools to navigate both traditional and digital financial systems effectively.

Drawing on the concepts of ANT, with the government as the prime actor engaging in translation, the problematization of the current landscape is framed as individuals lacking protection. This may be due to the complexities of the cryptocurrency landscape or because their exclusion from the traditional financial system propels them to digital assets. The government proposes training and protective measures as an interessement phase to encourage individuals to join the assemblage, thereby enrolling them as financially motivated, passive participants.

The Federal Reserve (FED) departs from government view of individuals in the cryptocurrency ecosystem. While still referring to the need to protect consumers, the Fed introduces other ways of naming individuals as the "public" and as "stakeholders". In addressing its role, assigned by the President, to deliberate on a potential United States CBDC, the Fed frames the public as collaborative partners in a broad consultation to shape the ecosystem:

"The Federal Reserve will seek input from a wide range of stakeholders that might use a CBDC or be affected by its introduction. This paper concludes with a request for public comment, the first step in a broad consultation that will also include targeted outreach and public forums."(FED, 2022a, p. 2)

The mention of "public forums" suggests a willingness to engage with the public within their own online communities, complementing the more structured approach of a formal request for public comment. This approach indicates an intention to actively seek and consider diverse perspectives rather than relying solely on centralized, controlled channels for input.

This analysis reveals significant tension in the subjectification of individual actors by the state within the discourse on the future of money and payments. In the context of boundaries: by positioning individuals primarily as consumers, the state limits the potential range of actions that could otherwise be open to them. This narrow subjectification delineates a boundary around individuals' roles, effectively framing them as actors to be enrolled for specific policy ends, rather than as autonomous economic participants. However, the Federal Reserve's positioning is more nuanced, reflecting a financialized perspective that assigns individuals a partially active role in managing their financial interests.

The Roles of Intermediation

In the traditional financial system, intermediation bridges capital suppliers and consumers, ensuring funds flow efficiently and securely. At the core of this system, intermediaries, particularly banks, act as custodians of financial ledgers. This role involves maintaining accurate transaction records and assessing creditworthiness to facilitate lending operations. Ancillary functions, including risk management, liquidity provisioning, and regulatory compliance, support and stabilize this foundational task,

enabling economic activity and promoting financial stability (Mishkin, 2007, pp. 208–211).

A defining characteristic of intermediation is its ability to create money through lending. In the fractional reserve system, banks retain a portion of deposits as reserves while lending the remainder, thereby expanding the money supply. Loans generate new deposits, amplifying the original monetary base and stimulating economic activity (Mishkin, 2007, p. 235). Even under the more recent ample reserves framework, where banks maintain higher reserve levels to ensure liquidity and stability, lending remains central to money creation (Copeland et al., 2024, pp. 27–28). In the United States, approximately 90% of the total money in circulation is created through these mechanisms (FED, 2024). This capacity for money creation is central to the business model of intermediaries, linking their revenue generation directly to their lending practices.

While traditional financial intermediaries have long been central to money creation and credit flow, the emergence of cryptocurrencies disrupt this traditional model by decentralizing ledger custodianship. The loss of custodianship challenges the role of intermediaries in creating credit supply. The DOT acknowledges that, in the contest of CBDC, the reduced deposits resulting from cryptocurrency adoption would limit the ability of intermediaries to create money. While this can be somewhat mitigated, the effect on the future of banking cannot be predicted (Treasury, 2022b, p. 41).

This dynamic extends beyond the introduction of CBDC. The same loss of custodianship occurs in any cryptocurrency-centric monetary system. Without this core function, intermediaries risk becoming peripheral actors in the financial system. In terms of ANT's moments of translation, the interessement of intermediaries to join the assemblage is undermined by their elimination as custodians of ledgers. The final statement in the quote demonstrates a lack of horizon for the role of intermediaries, challenging their very existence.

If a CBDC is introduced, the government is offering intermediaries an alternative foundation for a business model:

"Under this model, the Federal Reserve would issue and redeem U.S. CBDC, but the distribution of U.S. CBDC would be handled by intermediaries eligible for an account at the Federal Reserve and payment services would be managed by intermediaries and

other private sector participants. This would be similar to how paper currency is distributed through commercial banks. It also shares similarities to responsibilities surrounding noncash retail payments today: the intermediaries onboard provide customer support and manage payments. In addition, intermediaries would likely implement AML/CFT obligations, while relevant supervisors would monitor compliance with those obligations." (Treasury, 2022b, p. 23)

Thus, intermediaries are enrolled in the assemblage in a custodial role, framing them as facilitators rather than as active agents in the creation of new money. By omitting any reference to credit issuance or money creation, the statement redefines their role, emphasizing operational functions instead of active involvement in monetary processes. The comparison to cash distribution constructs a financial institution that acts as an arm of the FED, mainly tasked with auxiliary functions, including the implementation of federal anti-money laundering (AML) and combatting finance of terrorism (CFT) policies.

In response to the question of intermediaries in the RFC, proponents generally consider them entities that should conform to the regulatory standards of traditional financial institutions and be insured in the same manner as conventional banks. However, respondents remain silent on the role of intermediaries as creators of money. I posit that this is the result of the acceptance of intermediaries as custodians of their accounts and facilitators of money flow.

A significant number of respondents oppose the very existence of intermediaries, opting for decentralized models designed to avoid unnecessary control. Many of the respondents who oppose intermediaries also express skepticism or rejection of the concept of CBDC:

"There should be no intermediaries and no CBDC. Only Bitcoin should be used, and Bitcoin doesn't need any intermediaries because Bitcoin is decentralized." (FED-comments, 2022, pp. 1–298)

This framing implies that intermediaries are a necessary evil, required specifically to compensate for the inherent limitations of centralized systems like CBDC. In contrast, Bitcoin's decentralized model is presented as inherently self-sufficient, eliminating the need for intermediation.

Thus, the divergence between governmental efforts to integrate intermediaries within a regulated framework and public advocacy for decentralized ledgers reflects a critical tension in the future of financial intermediation. This tension underscores significant uncertainties surrounding the mechanisms by which credit creation and liquidity provisioning will be preserved. Applying the lens of Actor-Network Theory, intermediaries experience a diminished interessement, challenging their ability to remain integral actors within the financial assemblage. In parallel, the ambiguity surrounding their evolving functions risks undermining the foundational trust and cooperation emphasized in Ostrom's principles for robust institutional design. As centralized and decentralized financial models continue to develop, the capacity of intermediaries to adapt and redefine their roles will be central to their survival.

Translation of Digital Assets

Consistent with the theoretical framework of ANT, I conceptualize digital assets as actors within the assemblage that, like human actors, require translation to align their roles and interests with the broader network of actors. Within state discourse, digital assets are described in two distinct forms: (1) digital assets at large, referred to by the DOT as crypto-assets, and (2) digital assets as part of a regulated U.S. crypto ecosystem that includes a state-issued CBDC. In their unregulated form, digital assets are described, in the executive order, as introducing significant risks, such as their potential to enable illicit activities:

"Digital assets have facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity. The growing use of digital assets in financial activity heightens risks of crimes such as money laundering, terrorist and proliferation financing, fraud and theft schemes, and corruption." (Biden, 2022, p. 14149)

This statement problematizes digital assets by portraying them as tools for facilitating cybercrime and illicit financial activities, emphasizing the sophistication of these illicit activities. The term "sophisticated" emphasizes the complexity of these threats, implying that external intervention is necessary to address them. Additionally, the phrase "growing use" heightens the perceived urgency, framing the risks as rapidly escalating and demanding immediate attention.

Conversely, the state-regulated version of digital assets is constructed around CBDC, a digital asset that "*carries neither credit nor liquidity risk, and is therefore considered the safest form of money."* (FED, 2022a, p. 5). CBDC is envisioned to coexist and not replace other digital assets through features that enable intercommunication (OSTP, 2022b, p. 15) In this mode of digital assets the ecosystem is regulated and controlled by the state, through a federal framework.

In terms of ANT, digital assets are incorporated into the assemblage through translation, being problematized as dangerous and complex actors capable of enabling criminal activities. To successfully align their interests with the assemblage, the government proposes transforming them into well-regulated entities interoperating with the Fed through integration with the CBDC framework. This transformation enrolls digital assets as key actors in facilitating economic transactions within the United States.

Despite these efforts, public feedback indicates significant opposition to the launch of a CBDC, with many respondents also expressing concerns about over-regulation:

"Over regulation ... is pushing crypto innovation out of America and if digital assets threaten the CBDC, the CBDC could easily shut off access to it." (FED-comments, 2022, pp. 6–163)

This statement expresses distrust in the definition of roles prescribed by state discourse, highlighting a power dynamic in which the regulator wields disproportionate authority to shape roles and delineate boundaries within the assemblage. It constructs a narrative where excessive regulation and the dominance of a CBDC are pivotal forces, suggesting that concerns over free market competition may lead the regulator to leverage its power to drive innovation and digital assets out of the American cryptocurrency ecosystem in the future. The reference to over-regulation suggests that some regulation is acceptable, if it doesn't stifle innovation or lead to state overreach. It reflects an implicit agreement that digital assets should be translated into safe, regulated entities. However, excessive regulation and CBDC dominance risk shifting from stability to state control, undermining private actors and market dynamics.

Conclusion – WPR Analysis of Enrollment

The analysis of enrollment demonstrates that the boundaries within the U.S. cryptocurrency ecosystem are neither fixed nor binary. Rather, they are fluid and multi-dimensional, shaped by the dynamic roles and relationships among diverse actors. This is in line with ANT, where boundaries are understood as constructed and continually renegotiated through processes of translation and enrollment (Callon, 1998a, p. 262). The process of defining and renegotiating boundaries is deeply tied to trust, as the inclusion or exclusion of actants hinges on perceptions of their reliability, legitimacy, and alignment with the network's goals. This model of boundaries better reflects the discourse examined here by emphasizing clearly defined roles and identities rather than the rigid, static boundaries outlined by Ostrom as a design principle for robust ecosystems.

The problematization of trust in the context of actor roles produces a tension between government reliance on centralized regulatory frameworks and respondents' trust in decentralized free market mechanisms, while expecting the government to play a soft regulatory role. Government discourse frames trust as contingent upon its ability to protect consumers and uphold national security. This problematization positions the government and the Fed as the pivotal actor in ensuring stability and safeguarding the public through the introduction of CBDCs and regulatory oversight. In terms of ANT the president is positioning the state as the indispensable actor controlling the Fed decision as the obligatory passage point of the assemblage, a critical stage that all actors must pass through to achieve their goals (Callon, 1984, p. 204). In contrast, stakeholders problematize trust as emerging from the transparency inherent in decentralized digital assets. They express distrust in government interventions as illegitimate overreach, undermining freedom and innovation.

This tension of trust produces conflicting approaches to defining the identity of actors within the assemblage. Government narratives, guided by norms of institutional authority and national security as a common good, subjectify consumers as vulnerable actors ill-equipped to engage the complexities and risks of digital assets. Conversely, stakeholders, guided by norms of decentralization and actor autonomy, subjectify the government and the Federal Reserve as intrusive actors, questioning the legitimacy of their participation and framing them as threats to a self-regulating assemblage. The

clash between norms of centralized authority and national security versus decentralization and autonomy shapes institutional development as a negotiated response to conflicting expectations.

While exploring a potential CBDC, the Fed issued an RFC to solicit public input through three mechanisms: a call for comments, targeted outreach, and public forums. (FED, 2022a, p. 2). The call for comment is not only designed to gauge customer support for CBDC. Questions 15 to 22 in the Fed questionnaire ask the public for input on design consideration and specifics. By asking these questions the Fed is building a unique link in the assemblage that achieves a sense of co-enrolling of the digital assets into the assemblage (FED, 2022a, pp. 21–22). The questionnaire amounts to an immutable mobile device of mobilization designed to "bear on certain controversies and force dissenters into believing new facts and behaving in new ways" (Latour, 2012, p. 6). Thus, the combination of CBDC as a technological institution and the RFC as a democratic institution complement each other, forming an institutional response, by the state, designed to reconcile the clash of norms and foster a reciprocal positive effect on trust in the assemblage.

Chapter Six.

Collective Choice Arrangements

Governance in the Cryptocurrency Ecosystem

Governance refers to the frameworks and mechanisms developed to guide decision-making and establish rules within an ecosystem. These mechanisms must evolve to ensure that functions align with stakeholders' goals and policies (Hanisch et al., 2023, p. 2). Elinor Ostrom found that the capacity of stakeholders within an ecosystem to influence the ongoing practices of governance has a positive effect on the ecosystem's likelihood of thriving:

> "Most individuals affected by the operational rules can participate in modifying the operational rules." (Ostrom, 2015, p. 90)

This section begins by introducing Ostrom's conceptual framework for analyzing complex, self-organizing governance systems and extends it with a sociotechnical dimension to better understand software-embedded ecosystems. It then examines how decentralized governance structures rely on adaptability and stakeholder participation to foster resilience and trust, contrasting these approaches with the centralized models of traditional monetary systems. Next, I examine how trust in governance is problematized by the state and non-state actors, focusing on their degree of trust in decentralization. I contrast this problematization with how governance models are implemented in various cryptocurrency institutions, showing that cryptocurrencies and especially stablecoins are not necessarily more decentralized than the existing monetary system.

The resilience of robust CPR governance arrangements is attributed to their ability to adapt to changing conditions, enabling stakeholders to modify rules and strategies in response to evolving environmental, social, or economic conditions. In the absence of a central dominant actor dictating the rules, adaptable governance depends on the emergence of collective choice institutions (Ostrom, 2015, p. 93). This agility enables actors in a self-organized ecosystem to exercise three key capabilities:

- Stakeholders must be able to change the statutes that govern the CPR
- Stakeholders must be able to adjust parameters such as limits, rates and, fees.

- Organizational structures can be changed by common choice.

(Picht, 1987, p. 28)

The centralized governance structure of the incumbent monetary system, where government controls the rulemaking process, was already destabilized by what Cohen (2003, p. 6) called the deterritorialization of money. This process was initiated by the rise in capital mobility, wherein countries facing competition from abroad no longer monopolize rulemaking and parameter adjustment in their national monetary system. Deterritorialization has impacted internal monetary governance in the United States as well, despite its leadership role as the current issuer of the world's reserve currency (Bernanke, 2007). The erosion of monetary sovereignty created a demand for decentralized financial systems that operate independently of any single country's governance. Although many cryptocurrencies are not fully decentralized, they collectively represent a shift towards reducing the influence of national monetary authorities and promoting new forms of financial governance that can operate globally (Meyer & Hudon, 2019, p. 279).

To understand the governance dynamics within this emerging decentralized and deterritorialized financial landscape, I propose using Elinor Ostrom's three layers of institutional choice—operational, collective, and constitutional. Operational choices focus on the implementation of rules and the direct management of resources in the assemblage. Collective-choice decisions establish the rules and procedures that guide and regulate operational activities, focusing on how these rules are constructed and revised. At the highest level, constitutional choices define the foundational frameworks within which these decisions are made, shaping the fundamental principles of governance (McGinnis, 2011, p. 173). This layered framework highlights how different levels of rules are created, adapted, and institutionalized across different levels of governance. I argue that recognizing the processes shaping constitutional rules as the primary determinants of how the assemblage is governed highlights the need to valorize this highest level in the analysis, as it establishes the parameters for all other governance dynamics.

I argue that sociotechnical ecosystems introduce another classification dimension based on whether rules are enacted through statutes or software. Statutes are formal or informal rules set by stakeholders, while software rules are embedded in code by

programmers. Both are negotiated through discussion, debate, and consensus among engaged stakeholders. They are formalized via various mechanisms, such as voting, discussion platforms, or reputation systems. These negotiations produce constitutional and collective choices, implemented as either written rules or executable code. Importantly, code does not always enact operational level rules. Decision-support algorithms and artificial intelligence, such as those used to assess credit risk by generating operational choice rules.

Trust in the Constitution of Cryptocurrency Governance

The processes by which rules are developed and enacted form the foundation of governance. However, the effectiveness of these processes, measured by their capacity to cope with social dilemmas, depends on the trust they inspire among stakeholders (Ostrom, 2010a, p. 661). I define this trust as trust in governance, rooted in the belief that rules align with collective interests. Consequently, centralized trust in governance is the reliance on the concentration of rulemaking power in a central authority that is perceived to have the knowledge and fairness to execute governance as an exogenous force to the ecosystem in question (Ostrom, 2010a, p. 642). Centralized trust is founded on norms and heuristics of reliability, transparency, accountability, and the confidence that the source of trust has the agency to execute governance. By adhering to these norms and heuristics, the dominant actors of centralized ecosystems build and sustain trust, ensuring that their governance processes are regarded as legitimate and effective.

Conversely, decentralized trust in governance relies on the distribution of rulemaking power across a network of participants rather than centralizing it in a single authority. Trust in decentralized institutional rulemaking is founded on norms of checks and balances between various sources of trust and the democratic sovereignty of the majority. For both statutes and software, the perceived fairness of the process by which they are developed and implemented is essential. Fairness encompasses not only the outcomes but also the procedures used to reach those outcomes. Stakeholders are more likely to trust the system if they believe that the process is unbiased and accessible to all relevant actors. This perception of fairness is enhanced by consensus mechanisms that actively involve stakeholders in the rulemaking process. By ensuring that all voices have influence, the process becomes more inclusive, which in turn helps to achieve

outcomes that are viewed as equitable and legitimate (De Filippi et al., 2020, pp. 15–16).

In decentralized trust settings, the most prevalent method used for stakeholder participation in rulemaking is voting. Trust in the rulemaking process can be bolstered by integrating the process of rulemaking and the rules themselves onto a blockchain. This practice is known as "on-chain" governance. It is perceived as more inclusive and reliable because rules are immutable and can be executed automatically through code or smart contracts. However, on-chain governance also faces challenges related to scalability, security and limitations on the types of rules that can be automated (Werbach, 2018a, p. Location: 6832).

A foundational concept for trust in software rulemaking is the concept of open-source software. Open-source projects rely on collaborative work from a diverse group of developers who collectively shape the product and therefore have a crucial impact on the rules embedded in it. Voting is a crucial mechanism in this environment, enabling contributors and stakeholders to make democratic decisions about feature implementations, modifications, and project governance. Open-source projects trust the public at large by making all the code visible to developers and non-developers alike. Reciprocally, this built-in transparency encourages stakeholders to infer trust via scrutiny of the rulemaking process. Inferred trust in open-source communities is built on an aggregation of norms such as openness, transparency, collaboration, and adherence to quality standards. Several heuristics are also at play in this process, including experience, reputation, commitment and visibility (de Laat, 2010, pp. 329–337).

State Problematization of the Rulemaking Process

I regard the process that produces the corpus under investigation in this thesis as a process of rulemaking, as its role is to constitute policy and regulation. Therefore, the meta-discourse regarding the process initiated by the executive order must be considered in the analysis. The documents by the government and its agencies include a significant number of references to how the rules of cryptocurrency should be instituted in general, and specifically what the role of the government in the process is.

The executive order constructs a highly centralized assemblage in which the government is the sole actor responsible for rulemaking. In section 3 the president delegates his authority to an interagency process through which collective and operational choices will be made. A long list of dependent and semi-dependent bodies is provided in the context of the way rulemaking will be enacted. The order then goes on to assign tasks to these agencies, intended to help the president make decisions on the future of money and payments (Biden, 2022, pp. 14145–14146). The order further directs various agencies to produce a series of reports, including one from the DOT, tasked with providing recommendations for regulation and legislation to govern the ecosystem:

"The report shall also include policy recommendations, including potential regulatory and legislative actions, as appropriate, to protect United States consumers, investors, and businesses, and support expanding access to safe and affordable financial services." (Biden, 2022, p. 14147)

By limiting the role of other bodies to "policy recommendations", the president positions himself at the center of rulemaking, excluding other stakeholders. This "hub and spoke" approach to governance and rulemaking illustrates the president's perspective that his administration alone is capable of safeguarding U.S. national interests and consumer welfare.

As opposed to the President's centralized view, the DOT report builds on participatory processes embedded in the democratic institutions of the United States to include other stakeholders in the rulemaking process. The DOT issued a request for comment (RFC), casting other stakeholders as informants with the opportunity to provide input aimed at supporting the task of carrying out the mandate of the executive order:

"Treasury is requesting input from the public that will inform its work in carrying out its mandate under section 5(b)(i) of the Executive Order." (Federal Register, 2022, p. 40882)

While this broadens the scope of actors that can provide input to the task imposed on DOT, it falls short of allowing the public to participate in the acts of governance and rulemaking. They play a secondary role as "informants" in the government's centralized enterprise of rulemaking. There is no mention of how the positions of respondents will be taken under consideration. The DOT's perception of the outcome

of the RFC is conveyed in the resulting document in a highlighted section titled: "Listening to the Public":

"The data and insights shared through the RFC demonstrated a variety of views among commenters on the responsible development of digital assets, as well as on the implications for U.S. consumers, investors, and businesses. Commenters generally expressed their desire for action with respect to digital assets and supported the coordinated government approach pursued by the Administration." (Treasury, 2022a, p. 4)

Here, governance is problematized in the context of a voluntary RFC process that is inconclusive and therefore creates a challenge to the response of the government to public sentiment. The logical conclusion implied by the DOT is that the public is confused and willing to follow the centralized leadership of the government. Apart from the conclusion that respondents are willing to follow the government's lead, the DOT shows no sign of attempting to thoroughly analyze the results of the RFC.

The Fed issued its own RFC in its preparations to respond to the executive order regarding CBDC. However, in contrast to the informational role that the DOT discourse assigns to these comments, Fed discourse delegates veto power to the government and the public on the question of the introduction of a CBDC:

"The Federal Reserve will only take further steps toward developing a CBDC if research points to benefits for households, businesses, and the economy overall that exceed the downside risks, and indicates that CBDC is superior to alternative methods. Furthermore, the Federal Reserve would only pursue a CBDC in the context of broad public and cross-governmental support."

Although the Fed does not provide details on the mechanism used to measure public and cross-governmental support, this statement clearly decentralizes a major constitutional choice regarding the future of money in the United States and its rules of governance. Analysis of the questions in the RFC further strengthens this view, since many of them address constitutional and collective choices regarding matters related to rulemaking and governance. These questions include whether a CBDC should offer interest rates, and which types of firms should act as intermediaries in the future cryptocurrency ecosystem. It also includes an open question, asking respondents to

suggest design principles for CBDC. These design principles embody both formal and informal rules embedded in software code.

Since the RFC process ended, public opposition to a CBDC has grown, with several states initiating legal efforts to ban it. In response, Fed Chair Powell stated that any CBDC would require congressional approval (Hamilton, 2024a). I interpret this as the Fed's attempt to decentralize constitutional rulemaking by shifting the decision to elected representatives. Requiring congressional debate grounds the process in democratic legitimacy, moving authority from the executive and the Fed to a broader constituency. This also adds a federal dimension, incorporating both state and national perspectives into decisions about the future of money.

Public Problematization of Trust and Democracy

A substantial number of respondents approach the rulemaking issue through a lens of deep distrust toward the Fed, particularly regarding its policies and regulation of financial markets. The following example offers a representative, albeit moderate, illustration of this perspective:

"I don't take the Federal Reserve seriously enough to act in an ethical manner to 'regulate' financial instruments as it is. If the Federal Reserve was responsible, rates would be dictated by free markets." (FED-comments, 2022, p. 2/295).

The statement challenges the Fed's ethical credibility, framing it as a failure in performing its role as a regulator of financial markets. By contrasting the Fed's centralized authority with the perceived ethical superiority of free-market principles, it problematizes centralized regulation as inherently unethical. This discourse implicitly promotes the idea that ethical outcomes are more likely in decentralized, market-driven systems, disregarding the potential of unregulated systems to produce inequitable outcomes.

Others problematize centralized digital currencies in general by associating them with political risk and framing them as anti-democratic:

"The use of centralized digital currencies creates incredibly high political risks. In comparison with many decentralized alternatives, the CBDC as envisioned in the paper, does not allow users and holders to have a part in the governance of the protocol

or token. The CBDC must address governance just as any coin must do before its ICO or airdrop." (FED-comments, 2022, p. 6/550).

Here, the problem of trust in the Fed turns into a rejection of centralism as a norm. The respondent problematizes the absence of user involvement, drawing on decentralized finance norms to challenge the legitimacy of hierarchical governance structures. Ultimately, he asserts that the only way for Ostrom's design principle to be fulfilled is to construct a decentralized financial system.

While open-source cryptocurrency arrangements are not widely discussed by the public as solutions for the governance process, there is broad support for the openness of code in cryptocurrencies even if they are provided by the government. There are almost no negative references to open-source software as a basis for cryptocurrencies and it is often connected to the norms of agility, decentralization and security.

"In a decentralized emerging economy and the metaverse of technology coming, there should be no slow down with innovation and letting the people decide in an open-source manner." (FED-comments, 2022, pp. 5–367)

The phrase "letting the people decide in an open-source manner" associates the democratization of rulemaking with the development of open-source software. The respondent visualizes an assemblage in which rules are constituted through collaborative processes where stakeholders actively participate in decision-making, ensuring that governance structures are both transparent and inclusive. These principles align with foundational elements of decentralized governance, emphasizing fairness, accountability, and collective participation.

Most references to open-source software, in the context of CBDC, are positively correlated with verifiable trust:

"Build it on a bitcoin proof of work or proof of stake framework with an open-source software so that the public knows if the government is going back on their word." (FED-comments, 2022, pp. 5–587)

This statement constructs a discourse that intertwines trust, transparency, and accountability within the framework of decentralized governance. The reason given for developing an open-source CBDC is that this will enable scrutiny of government actions.

Individual respondents' vision of decentralized governance is not shared by the market leading cryptocurrency companies. Decentralized governance is mostly endorsed by smaller cryptocurrency providers and consortiums representing them. One such consortium is the Crypto Council for Innovation (CCI), a body representing innovative cryptocurrency tech companies which contends:

"Blockchain and smart contracts implemented via blockchain have the potential to transform the ability of individuals to influence the governance of companies and communities in which they participate." (OSTP-Responses-1, 2022, p. CCI–6)

This quote is indicative of the prevalent forward-looking language used to promote decentralization, featuring potential and possibilities rather than real achievements. It embodies the language of visionaries ushering in a more democratic future in which individuals are executing governance.

Conversely, the large commercial players in the cryptocurrency space do not emphasize decentralization. Their responses infrequently mention decentralization, and when they do, they adopt a neutral approach that positions decentralized finance as a potential advantage in the assemblage. A remark by Tether, the largest stablecoin provider worldwide with over 112 billion dollars in outstanding tokens, demonstrates the niche approach to decentralization as an experimental feature.

"Moreover, decentralized smart contract-based markets can serve as a sort of sandbox where new forms of capital markets are created for lending, raising capital, and securitizing assets and companies. Controls around the size of projects in terms of value and volume of users can be monitored and controlled." (OSTP-Responses-1, 2022, p. Thether-3)

While portraying decentralization as an optional nascent feature, these companies readily embrace the idea that federal institutions will centrally regulate financial markets going forward. However, their view is not uniform. Tether envisions cryptocurrency regulation as specially tailored to the industry's unique characteristics. In their view, regulation should be a soft tool that provides oversight and guidance, considering the unknowns of innovation:

"... one of the key drivers of mass adoption includes the development of appropriate corresponding regulatory infrastructure which would incorporate the use of blockchain

technology, and legislation tailored to the industry rather than applied from existing frameworks. Legislative frameworks must take a risk-based approach while at the same time acknowledging the varying and unique nature of many of the incumbents' business models operating in this industry, in order to design approaches to supervision and regulatory guidance which is fair and effective." (OSTP-Responses-1, 2022, p. Tether-3)

The second largest global stablecoin provider is Circle, the issuer of USDC with over 34 billion dollars in outstanding tokens. Unlike Tether, Circle is based in the United States. While also subscribing to the idea of central government control, Circle favours enrolling cryptocurrency into the existing prudential governance framework controlling traditional financial markets.

"A strong regulatory framework with clear rules of the road would facilitate mass adoption of digital assets…Payment stablecoins should be brought into the prudential regulatory framework to best protect consumers and financial stability while allowing payments that have the reach, accessibility, and speed of the internet, without borders or boundaries." (OSTP-Responses-1, 2022, p. Circle-5).

Circle's emphasis on strength of the regulatory framework and the clarity of its rules, contradicts Tether's discourse on guidelines and flexibility in the face of innovation. Circle seeks strong, centralized governance, providing protection against unfair competition from companies with lesser regulation:

"As the United States and other countries take action to foster responsible innovation, companies without the same desire to be regulated will look for jurisdictions with lax regulation, oversight, and supervision. Not only do these companies pose a threat to consumers in the United States, they will compete with U.S. companies that are operating within its regulatory perimeter." (OSTP-Responses-1, 2022, p. Circle-5)

The notion of a "regulatory perimeter" in the statement constructs a clear boundary between regulated and unregulated spaces. It draws the line between good governance and lax governance and reveals a setting which has potential for exclusion and protectionism, terming it regulatory arbitrage. The regulatory perimeter is a centralized "walled Garden", controlled by regulation.

The prevalent conservative centralist leaning of cryptocurrency providers, regarding statutory governance, persists in the discourse surrounding software rules. Open-source software is not widely mentioned by large commercial players or the innovators in the cryptocurrency space. It is mostly mentioned as a technique to accelerate development and win the race between countries and firms to launch a dominant, transparent, and trustworthy digital cryptocurrency (FED-comments, 2022, pp. 8–655). These perspectives illustrate how major players in the cryptocurrency industry are constructing an assemblage defined by centralized regulatory frameworks tailored to their business models, while engaging in symbolic compliance with the industry's decentralization narrative.

Conclusion - WPR Analysis of Trust in Cryptocurrency Governance

Although major stablecoins use blockchain technology, they are not open-source and are centrally governed by corporate entities. Smaller providers like DAI and USDD offer open-source architectures, where governance token holders, who possess more currency, have more voting powers, creating a plutocratic bias. Other models grant voting rights based on contributors' qualifications and code maintenance, forming meritocracies (Linåker et al., 2019, p. 103). Both systems exclude parts of society and limit decentralization. Ultimately, rulemaking in open-source cryptocurrencies rests with a privileged group of maintainers or rich stakeholders, who control code changes through consensus-based voting schemes.

This results in a variety of centralized and hybrid offerings that provide a currency managed by private actors with varying degrees of decentralization in their governance models. This aligns with Ostrom's concept of polycentric ecosystems, environments in which rulemaking and governance are distributed across multiple autonomous yet interdependent and centralized decision-making entities (Ostrom, 2015, pp. 643–644). This structure allows for a variety of competing governance schemes, while necessitating cooperation to address overlapping issues effectively. Table 2 compares the discourse surrounding rulemaking mechanisms to their actual implementation in the cryptocurrency domain. The "public sentiment" column indicates the public's stance as it is reflected in responses to the RFC. A neutral sentiment typically indicates that public discourse about the institution is minimal. The next two columns indicate that, in

practice, the institutions that are more democratic are the ones that are least implemented.

Institution	Public sentiment	Participation	Implementation
Open Voting	Positive	Democratic	Low
Privileged Voting	Positive	Plutocratic	High
Informal Consensus	Neutral	Meritocratic	High
Corporate rulemaking	Neutral	Authoritarian	High
Proprietary Coding	Neutral	Authoritarian	High
Open-source coding	Positive	Meritocratic	High
Regulation by RFC	Negative	Democratic	Low

Table 2 - Cryptocurrency participation institutions

This analysis of discourse versus actual implementation reveals that respondents prefer a polycentric system of highly centralized non-democratic institutions to the democracy of one state-run solution.

The problem of trust in governance is represented by all parties as tightly linked to the degree of centralization in the rulemaking process. Many respondents view state intervention as an imposition of centralized governance, framing it as undemocratic and violating personal autonomy. The dominant discourse argues that cryptocurrencies provide a decentralized, democratic governance ecosystem that enhances individual autonomy and agency. This vision aligns with techno-anarchism, which champions self-sovereignty and trust systems grounded in the deterministic transparency of code rather than human discretion Swartz (2017, p. 90), describes techno-anarchism as leveraging decentralized technologies to disintermediate traditional power structures and establish governance through coded rules. Respondents echo this ethos, framing cryptocurrencies as a viable challenge to centralized control, represented by the Fed.

Respondents' distrust of the Fed is met asymmetrically by the Fed's trust in the public. Its move to grant veto power and involve the public in CBDC design reflects both a decentralization of constitutional rulemaking and an effort to build trust. This is an approach that Elinor Ostrom (2010a, p. 664) sees as key to resilient CPR systems. While institutional choice is anchored in democratic elections, the Fed extends public

influence further, allowing significant input at the constitutional and collective choice levels. Ultimately, Congress, which is elected by the people, holds the final say on the future of money and payments.

Cryptocurrency service providers, led by the top stablecoin companies, do not follow the trend towards decentralization, framing it as an experimental "niche" feature. While their assets are implemented on blockchain architecture, they are centrally managed on all levels of rulemaking. The discourse surrounding decentralization as an experimental feature reflects normative pressures from the cryptocurrency assemblage, where decentralization is idealized as a symbol of innovation and legitimacy. This conditional acceptance of decentralization is juxtaposed with efforts by providers to secure centralized regulatory frameworks that protect their operations from unfair competition and governance arbitrage across jurisdictions, while providing them with regulatory certainty. While some of them are asking for lenient, non-enforcing regulation that will accommodate technical innovation and financial freedom, most large providers prefer to become a part of the prudential governance scheme imposed on traditional financial firms.

In practice, a significant number of cryptocurrencies and most stablecoins are centralized in their rulemaking process. Even those who issue governance tokens and run on open-source software fall short of actual democratic governance. These solutions depend on plutocracy, bestowing more influence on wealthy token holders. Other currencies that create transparent rules through open-source code practice meritocracy by awarding influence based on technical know-how and reputation.

The interplay between norms and heuristics underlying the problematization of trust in governance emerges through the framing of centralization and decentralization as competing paradigms of legitimacy. Norms rooted in techno-anarchism, such as self-sovereignty, transparency, and trust in code, frame decentralization as both a technical and moral imperative. However, differing interpretations reveal a gap between the ideal and its practical implementation. Respondents equate decentralization with fairness and autonomy, while viewing centralization as coercive. State actors balance participatory measures with centralized control, and cryptocurrency firms, though promoting decentralization rhetorically, rely on centralized governance to meet regulatory needs.

The tension between actors' perspectives is a breeding ground for a variety of institutional developments addressing the consensus mechanisms that drive the rulemaking process. These varying approaches to consensus signal attempts to discover trustworthy governance in the assemblage. While decentralization is often framed as a pathway to fair governance, its implementation frequently falls short, giving way to centralized structures. This hybrid reality underscores the difficulty of balancing innovation with trust.

Chapter Seven.

Appropriation and Provisioning

Appropriation and Provisioning

Elinor Ostrom suggested that it is useful to separate common-pool resource availability issues into two broad categories: appropriation problems and provisioning problems. Appropriation is defined as the process by which actors come to possess, or otherwise utilize the resources from a shared resource system, while provisioning is the process by which actors invest resources to build and maintain the CPR (Ostrom, 2015, pp. 47–50). Analyzing these processes in field settings, she proposes the second design principle for a stable and thriving ecosystem:

> "Congruence between appropriation and provision rules and local conditions. Appropriation rules restricting time, place, technology, and/or quantity of resource units are related to local conditions and to provision rules requiring labor, material, and/or money." (Ostrom, 2015, p. 90)

This section suggests a definition of congruence in the context of cryptocurrencies and proposes the perception of stability and liquidity as qualitative measures by which this congruence can be qualitatively estimated. Next, I reveal diverging trust dynamics among actors in the assemblage regarding how stability and liquidity should be achieved, showing tension within each group of actors. I argue that this tension induces institutional innovation, leading to a reciprocal effect on trust.

The goal described by the term "congruence with local conditions" varies greatly in Ostrom's work, depending on factors such as ecology, social dynamics, economic conditions, and cultural norms. In discussing how to measure congruence, Epstein (2021) emphasizes the importance of uncovering the social and ecological mechanisms that underlie the problem to quantify or qualify congruence. In other words, one must analyze the congruence between appropriation or provisioning rules and the parameters that are contextually relevant to the problem at hand.

Applying Ostrom's framework to cryptocurrencies, appropriation refers to how users interact with and utilize the currency in circulation. It focuses on the operational mechanisms that enable stakeholders to use, transact, and hold the currency as a store of value. Provisioning, by contrast, governs the actions necessary to make the currency available for appropriation, including the rules for issuance, redemption, and the reserves that support its stability. Provisioning forms the foundation of a currency's reliability, ensuring its creation and backing maintain stability and trust. Without effective provisioning, crises will cause trust in the ecosystem to erode, compromising the currency's usability and long-term viability.

The key parameters that demonstrate the congruence between provisioning and the social and ecological mechanisms underlying the currency are its stability and liquidity. The existence of a currency as a store of value and unit of account depends on its ability to consistently reflect value over time. Stability, therefore, serves as a benchmark for assessing the alignment between provisioning rules and the specific variables that characterize cryptocurrencies. These "local" variables comprise the technological and economic characteristics and restrictions within the ecosystem, including the regulatory landscape, technologies, and governance structures constructed in the assemblage and ultimately realized in the ecosystem. In essence, local variables are the institutions perceived by stakeholders to be central to the currency's functionality.

In traditional ecosystems, central banks regulate the money supply to counteract inflation or deflation as needed (Ametrano, 2016, p. 6). In the cryptocurrency ecosystem, provisioning mechanisms serve a similar purpose, though they utilize a variety of mechanisms to maintain stability and liquidity. Congruence between provisioning and local variables must also account for liquidity, which ensures the currency functions effectively as a medium of exchange. Stability alone is insufficient if the currency cannot be exchanged for goods or other forms of money, which is socially constructed as a commodity distinguished by its infinite liquidity, which is grounded in the trust of all stakeholders in the currency issuer (Ingham, 2013, p. 54).

The subject of supply in cryptocurrencies is commonly identified with mining and staking mechanisms. These mechanisms govern the number of tokens circulating in the system, their creation, and how they are made available in the assemblage. However, mining and staking are protocols that determine the total supply algorithmically or, as

in the case of Bitcoin, impose a hard limit on the total supply. Hence, cryptocurrencies such as Bitcoin and Ethereum that rely on inflexible mechanisms of supply, do not provide a level of stability required to make them a trusted form of currency (Dodd, 2014, p. 368).

This section focuses on stablecoins as currencies that are intended to deliver the features of stable money. Stablecoins are tokens designed to be pegged to the value of an external base asset such as the dollar or gold. If the base asset is considered stable, the stablecoin assumes that trait while providing the advantages of cryptocurrency such as inexpensive payments and the ability to obviate traditional intermediation. The supply of coins in stablecoins does not follow the mining and staking models of unpegged cryptocurrencies. To preserve the peg, market-making devices adjust supply dynamically by creating demand when the price falls below the base asset and increasing supply when it rises above.

Stablecoins use various mechanisms to maintain liquidity and price stability. Some are backed by collateral, such as fiat currency or crypto assets, which issuers hold to redeem the stablecoin when needed. Others have no collateral, relying instead on dynamic methods to support their peg. The level of collateralization can vary from full, where all coins are backed by reserves, to partial or none, with fully collateralized coins offering greater security during market instability. Stablecoins also use different stabilization methods to manage price volatility. Some incentivize investors to adjust supply and demand to maintain the peg, while others rely on algorithmic protocols that create or reduce supply as needed. Algorithmic stablecoins often use a secondary token as a volatility buffer, with mechanisms like token auctions or supply burning to stabilize value. Many stablecoins blend these approaches, making them difficult to strictly categorize as collateralized or algorithmic. (Moin et al., 2019, pp. 4–9).

The Interaction between Supply and Trust

While monetary trust is often taken for granted, it becomes critical during crises, directly influencing the effectiveness of provisioning mechanisms. This was particularly evident during the period following the 2008 global financial crisis, known as “the age of quantitative easing”. During this time central banks, including the Fed, injected significant amounts of money into financial markets, shifting the balance between the availability of money and assets. Quantitative easing impacted monetary

trust by specifically reducing public confidence in central banks (Braun, 2016, pp. 1083–1084). This trend illustrates the link between money supply and public trust in the institutions that manage it.

Likewise, the institutional characteristics of stablecoin supply significantly influence the level of trust needed for their use as stores of value, units of account, and mediums of exchange. Even for fully collateralized stablecoin based on the underlying asset, trust is essential. In these cases, the primary trust required is in the issuer of the stablecoin. Stakeholders must trust that issuers will offer a transparent and accurate account of reserves, ensure the network remains operational, secure the underlying asset, employ market makers, and provide a reliable and prompt redemption process to turn stablecoin into the base asset. This basic layer of trust is required for all types of collateralization.

Deviations from the fully collateralized model, in which the coin is not fully backed by the base asset, necessitate additional layers of trust. When the base asset and the reserve assets differ, it is crucial to trust in the stability of the exchange rate between them and in the issuer's ability to manage fluctuations in this exchange rate. If the reserve asset is a crypto asset, trust must be extended to the specific characteristics of that crypto asset and the technology that underlies the institutional arrangement. The need for trust increases as the amount of collateral held in reserve decreases. For stablecoins that are not fully collateralized, actors must consider the possibility of bank runs and trust in ample reserves to withstand such a run. Alternatively, they need to trust that other players will not collectively rush to redeem their holdings all at once. This is social trust, rooted in the expectation that, as a community, stakeholders will act in a rational manner and will not make extreme decisions.

Trust tends to decrease as complexity increases. Stablecoin issuers often rely on methods to maintain price stability that can be difficult for most people to comprehend. In the case of a fully collateralized base asset identical to the peg, the exchange between the coin and the asset is straightforward and transparent. However, understanding the methods used in other cases demands a level of technological and economic expertise that exceeds the knowledge most stakeholders have. Trust in technologies and economic mechanisms without full understanding is based on norms and heuristics. Actants rely on established practices, regulatory oversight, and third-party validations as norms that signal reliability. Social proof, strong branding, and consistent user

experiences serve as heuristics that enable the confidence that stablecoins will remain pegged to their base asset and fulfill their monetary role. However, as the global financial crisis of 2008 has demonstrated, reliance on norms and heuristics alone increases risk as the financial and technological features become less intelligible (Awrey, 2011, pp. 293–294).

Individual Respondents' Problematization of Trust in Supply

In contrast to the complex map of trust required for various types of stablecoin reserve models, individual respondents' problematization of trust in cryptocurrency reserves is simpler, as reflected in the discussion involving CBDC. Given that government-backed stablecoins inherently command higher trust than privately issued coins, it follows a fortiori that the public will demand at least the same level of rigor from private stablecoins as is applied to CBDCs. Consequently, the discourse surrounding CBDC requirements sets a baseline for the expectations placed on private money. Notably, individual respondents do not distinguish between different types of stablecoin mechanisms or engage with the various design options available. This absence of differentiation persists despite several RFC questions that explicitly invite such a discussion.

Many respondents demonstrate a clear stance that stablecoins and CBDC must be backed by real assets, although they differ somewhat on the nature of these assets. A minority of responses view cryptocurrencies and especially bitcoin as a potential reserve for CBDC:

" Central Banks should return to a hard money standard, and put Bitcoin in their reserves, and via smart contract, a CBDC would be backed and redeemable in that Bitcoin collateral. "(FED-comments, 2022, p. 1/147)

This perspective highlights a tension, relevant to trust, as Bitcoin is called "hard money" but relies on electricity, network connectivity, and software. However, the term "hard money" has a more profound meaning, being identified with an ecosystem in which supply is based on an underlying physical asset limited in quantity. Paradoxically, this type of money favors the rich over public interest because its limited supply and deflationary nature increase the value of assets held by the rich while restricting credit

and economic flexibility, which disproportionately impacts lower-income individuals. (Ingham, 2013, p. 42)

Most respondents who address the question of collateralization take the hard money idea further, demanding that CBDC and stablecoins be backed by gold and silver, while vocalizing their distrust of the federal reserve in controlling market supply. A representative remark comes from a respondent answering a question about alternatives to CBDC:

"... replacing the Federal Reserve Notes with gold one - to - one with all outstanding credit and physical notes, then limiting the role of the Fed to verifying that banks do not extend credit without backing of gold. See papers by Pepperdine University Prof. George Reisman." (FED-comments, 2022, pp. 6–387)

The quote references George Reisman, a member of the Austrian school of economic thought and staunch advocate of laissez-faire capitalism, who proposes replacing the dollar with a gold-backed currency. Reisman's proposal encapsulates the tension, reflected in many responses, between advocating for economic freedom and imposing structural constraints to maintain monetary stability through a hard money regime.

Other respondents address the question of supply from the standpoint of liquidity provisioning. A significant portion of respondents consider liquidity essential, viewing any restriction on the free and fast access to money as a crisis:

"*A large part of bank runs, financial collapse, liquidity crises – is the unavailability or no access to money instantly."* (FED-comments, 2022, pp. 6–71)

The statement normalizes the idea that a significant cause of financial instability, including bank runs and liquidity shortages, is the lack of instant access to money. This deemphasizes broader systemic issues such as poor regulatory oversight, market speculation, or structural as potential causes of financial crises. The emphasis on instant access to money serves as a heuristic, offering reassurance by providing individuals with a perceived quick escape from financial uncertainty.

Some of the respondents cite liquidity pools as potential solutions to liquidity issues in a decentralized assemblage:

"Banks could have their own coins which would effectively be backed by CBDC and could allow people with bank accounts to stake their coins in a liquidity pool to earn interest. I think the only logical way to go is to go all the way and back CBDC and the dollar with Bitcoin so they hold equal value." (FED-comments, 2022, pp. 7–299)

A liquidity pool is a decentralized finance (DeFi) institution embedded in software, that locks funds in smart contracts to facilitate trading of digital assets. These pools pair a cryptocurrency token with an external token, allowing trades against pooled liquidity rather than traditional buyers and sellers. Liquidity providers invest in these pools, earning transaction fees and voting tokens. Automated market makers, which are essentially price stabilizing algorithms, use liquidity pools to set token prices algorithmically. Though potentially profitable, providing liquidity involves risks from volatility and supply-demand imbalances, which can outweigh returns. Many investors prefer to share risk with others through decentralized liquidity pools rather than rely on traditional financial institutions—even when those institutions are backed by Federal Reserve insurance. (Weingärtner et al., 2023, pp. 4–11).

These trends in individual preferences highlight a divergence between the norms of hard money reserves and those favoring instant access to funds. The norm of hard money is rooted in the goal of stability, tying currency to tangible assets like gold or Bitcoin to build trust through scarcity. By contrast, the norm of instant access prioritizes liquidity as a goal, focusing on ensuring funds are readily available to withdraw in times of crisis. Some respondents introduce liquidity pools as a decentralized solution to address the challenges of ensuring liquidity without relying on traditional financial institutions.

Financial Institutions' Problematization of Trust in Supply

The growing interest in decentralized liquidity solutions underscores the distrust in traditional financial intermediaries, even those insured by the Federal Government. However, these institutions problematize trust in the provisioning of money supply differently, viewing it as a competitive landscape where government, banks, and stablecoins vie for stakeholder trust. For these institutions, robustness in the wake of financial volatility becomes the critical competitive differentiator, particularly

considering the government's exploration of CBDC issuance. Table 3 highlights how traditional financial institutions problematize trust as a 3-way competition.

Competitive Relationship	Source	Representative Quote
CBDC - Banks	JP Morgan	*"First, a widely adopted CBDC could, over the long run, cannibalize bank deposits and therefore bank reserves. This would entrap liquidity that could otherwise be used to facilitate payments and meet regulatory liquidity requirements (e.g., the Liquidly Coverage Ratio) …, the FRB would likely have to counteract that dynamic by supplying additional reserves relative to what would now be considered the lowest comfortable level."* (FED-comments, 2022, pp. 9–407)
Banks - Stablecoins	HSBC	*". As the FRB noted in their October 2020 report on stablecoins, authorities agree on the need to apply supervisory and oversight capabilities and practices under the 'same business, same risk, same rules' principle."* (FED-comments, 2022, pp. 9–125)
CBDC - Stablecoins	League of Southeastern Credit Unions	*"This is where a CBDC could outcompete a privately issued stablecoin. The Federal Reserve has a theoretically infinite balance sheet and as such could guarantee the peg of any CBDC to the dollar. The Fed needs to be prepared to back this peg fully in order for this coin to compete with the already existing stablecoins."* (FED-comments, 2022, pp. 8–541)

Table 3- Competition triangle constructed by financial institutions

The three-way competition between CBDC, banks and stablecoins is constructed by most traditional financial institutions as a negative development. The emergence of these competitive products invokes a protectionist, fearful stature, calling for strict regulation by the state. The use of the term cannibalize invokes a sense of fierce competition. The use, by the HSBC Bank, of the fair play norm reflects the competitive concern, urging a level playing field. While these institutions acknowledge the emergence of digital money, they contend that they are best positioned to continue to supply it:

"Banks could issue stablecoins pari passu with bank deposits. Indeed, a recent Federal Reserve research paper concluded that under a framework in which stablecoins were backed by commercial bank deposits that were used for fractional reserve banking,

bank intermediation would not be disrupted, so long as "the treatment of stablecoin deposits [were] the same as non-stablecoin deposits in terms of the required reserve ratio, liquidity coverage and other regulatory and self-imposed risk limits." (FED-comments, 2022, pp. 9–146)

The BPI, a consortium of banks, introduces tokenized deposits—digital tokens backed by customer deposits within the existing fractional reserve system. These offer improved security and cheaper international transfers while preserving the traditional banking model. Though novel, the approach relies on the familiarity heuristic to build trust in established practices. To reinforce the status quo, the BPI warns that undermining banks' role in money supply could trigger a credit crisis.

Cryptocurrency solution providers construct the same competitive framework, but their view of this framework puts this competition in a positive light, emphasizing the importance of financial and technical innovation in constituting the ecosystem. A white paper written by one of the largest cryptocurrency exchanges contends that the supply of new private money is not different from the traditional system:

"Consider three of a stablecoin arrangement's core functions: (1) the creation and redemption of stablecoins, (2) transfers among users, and (3) storage of the stablecoins. Analogous functions could all be performed by a bank in the context of traditional payments.". (CoinBase, 2022, p. 19)

This remark emphasizes the similarity between traditional banking and cryptocurrency service providers. However, the main message is that while cryptocurrencies are similar to traditional money, the surrounding regulations should change to accommodate them. A popular trend voiced by the Crypto Council for Innovation, a consortium of digital asset makers and services, is that regulation should be focused on monitoring and reporting rather than the enforcement of rules (OSTP-Responses-1, 2022, p. CCI–28) .The reasoning underlying these claims is that regulation should not stand in the way of innovation even if it is to avoid financial harm (CoinBase, 2022, p. 36).

The perceived tension between regulation and innovation has led some cryptocurrency providers to attempt to self-regulate while not stifling innovation. One example of such initiatives is the establishment of Global Digital Finance Associations (GDF). Encompassing over 150 members, most of whom are cryptocurrency service providers, GDF is dedicated to the adoption of best practices for companies involved in the

cryptocurrency ecosystem. One of its main activities is the development of a comprehensive code of conduct to which its constituents may self-certify (GDF, 2024a). Part VI of the code addresses stablecoins, clearly prescribing regular auditing and mitigation if reserves fall below the necessary levels. However, it is vague about the necessary steps regarding algorithmic stablecoins. It prescribes that the algorithm must be validated regularly but warns that algorithmic stablecoins are susceptible to declining user trust, and may not withstand a run (GDF, 2024b, pp. 1–12) .

State Problematization of Trust in Cryptocurrency Supply

The United States government and the Federal Reserve consider the evolving cryptocurrency landscape as a regulatory vacuum, posing risks to the global demand for dollars:

"Fiat based stablecoin demand will largely be driven (or limited) by the underlying fiat currencies' characteristics. Stablecoins could affect demand for dollars globally. The magnitude and consequences of these changes depend on a range of factors, including the demand for stablecoins globally, assets backing stablecoins, and regulatory framework(s) applied to stablecoins in the United States and abroad." (Treasury, 2022b, p. 34)

This statement reflects a deep concern that the United States government is losing control over money supply, increasingly being subjected to external forces beyond its reach. The Treasury's acknowledgment that US regulation is just one of several determining factors alongside foreign regulatory frameworks and the characteristics of stablecoin-backed assets, emphasizes the distrust government has in its ability to maintain stability.

In his executive order the president emphasizes the need to protect financial stability in the United States and around the globe, citing the dangerous practices of some digital asset service providers and trading platforms. Hence, he proposes to investigate the idea of a United States digital currency (Biden, 2022, p. 14143). The DOT follows up with a declaration that CBDC will be a safe asset that would support stability in normal times:

"A well-designed CBDC should support financial stability. As with Treasury securities or reserve balances, a broadly available safe asset could crowd out private money creation. This could support financial stability in normal times …" (Treasury, 2022b, p. 40)

The statement employs a familiarity heuristic to promote CBDC as a natural extension of trusted financial instruments like Treasury securities and reserve balances. By associating the CBDC with these well-established and widely understood assets, it draws on the public's existing trust in state-backed tools to frame CBDC as equally safe and stabilizing.

The term "crowd out" implicitly positions the state as a competitor in the financial marketplace, directly challenging the private sector's role in money creation. This language acknowledges the inherent tension between the state's interventionist approach and the capitalist ideal of a free, self-regulating market. The introduction of a CBDC is framed as an active reconfiguration of the competitive landscape by offering a state-backed alternative to private digital currencies and other forms of private money.

While this underscores the stability and trust a CBDC could bring as a state-backed asset, it also reveals the potential for unintended consequences, outlined in the acknowledgment of the risks posed during periods of financial stress. If a CBDC is seen as the ultimate safe asset, it may attract large fund transfers during financial stress, draining liquidity from intermediaries and disrupting credit availability, raising borrowing costs for businesses and governments and destabilizing the financial system. (Treasury, 2022, p. 43).

This apparent tension, stemming from the potential for a CBDC to both strengthen and erode financial stability, has prompted proposals by the government and the Fed for two key institutional mechanisms to mitigate stability risk. The first proposal, which seeks to limit the amount of CBDC that any single entity can hold, addresses the risk associated with the perception of CBDC as the ultimate safe asset. By capping individual holdings, the government aims to prevent excessive accrual of CBDC during periods of financial instability by preventing uncontrolled transfers of funds from private intermediaries to the state-backed digital currency. The introduction of holding limits by the OSTP lists identity privacy as the only potential disadvantage of this feature (OSTP, 2022b, p. 38). This narrow view overlooks the social and trust

implications of restricting how much digital cash individuals can hold, a measure that directly limits financial freedoms. By introducing constraints on personal financial autonomy, the policy raises significant questions about the trade-offs between systemic stability and individual liberties.

The second proposed mechanism is the introduction of an interest-bearing CBDC. By allowing the Federal Reserve to adjust the interest rate on CBDC holdings, this approach would enable dynamic management of its attractiveness as an asset. However, the feature is presented by the OSTP under the technical title "Adjustments on Balances", embedding it within the technical capability of the Fed to directly adjust the balances in the accounts of actors (OSTP, 2022b, p. 40). The framing of an interest-bearing device with the ability of the Fed to interfere in account balances shifts the discourse incentivization and stability to government overreach, while remaining silent on what other motivations might drive such manipulations.

The introduction of a CBDC represents a significant shift in the government's approach to the cryptocurrency supply provisioning, transitioning from regulatory oversight to establishing a centralized mechanism for monetary control. To manage the potential systemic impacts of this shift, the government has proposed two institutional arrangements designed to calibrate its effects: one focused on limitations and the other on incentives. However, the discourse largely ignores the broader social implications of these mechanisms and their potential impact on systemic trust.

Conclusion – WPR analysis of Trust in Money Supply

This chapter posits that the congruence between money provisioning and local variables in the cryptocurrency assemblage can be measured by the perception of stability of the currency against a well-defined base asset, and its liquidity – the ease of converting it to other crypto assets or to fiat money. The entire body of discourse examined in this study tends to agree with the idea that these variables represent the level of congruence between money supply and local variables. Table 4 summarizes the problematization of money supply in the assemblage. Three distinct perspectives on currency provisioning emerge from the discourse: Traditional banking and government institutions view the fiat dollar as a stable reserve, grounded in high-quality liquid assets (HQLA) like securities, foreign commitments, and foreign currency. Many individual

respondents, however, express a preference for money backed by tangible hard assets such as gold and silver, valuing scarcity and physical reliability. Meanwhile, cryptocurrency providers advocate for market-driven solutions, suggesting that reserve systems should compete to gain stakeholder trust.

Actant	Supply Problematization	Preferred Collateral	Resulting institutions
Individuals	Liquidity Provisioning Distrust of Fractional reserves	Gold, Silver	Liquidity Pools
Traditional Financial Institutions	Unfair competition Regulatory Vacuum	Fiat Dollar	Tokenized deposits Uniform Regulation
Cryptocurrency companies	Distrust in Fractional Reserves Resilience Need for Innovation	A mixed variety to choose from, including algorithmic stablecoins	Government Monitoring Self-Regulation
State Agencies	System Resilience Regulatory Vacuum	Fiat Dollar Securities	Interest-bearing CBDC CBDC holding limits Restrictive Regulation

Table 4 - Cryptocurrency Supply problematization summary

Each of the four discourses highlights the tension between perspectives that are, to some extent, contradictory. These competing ideas and concepts trigger proposals for institutional development. The discourse of individual respondents often reflects distrust in the government and the fractional reserve system, favoring hard collateral for money and thereby increasing its scarcity. Conversely, many also stress the necessity of unlimited liquidity. This tension between norms underscores the significance of decentralized market-making mechanisms. The institutional result of this tension is the proposal of liquidity pools, self-organized institutions driven by technology that assure incentives for liquidity providers. The reciprocal effect is that liquidity pools reinforce social trust by demonstrating a working model of peer commitment based on mass participation.

In the discourse of traditional financial services, the tension that produces institutional results lies between the familiarity heuristic and the acknowledgement of progress. On one hand, the discourse emphasizes the familiarity with the incumbent fractional reserve system and its longstanding role in provisioning credit within the traditional

ecosystem. On the other hand, traditional service providers recognize the need for financial and technological innovation. In this context, innovation is viewed as an opportunity to restore trust in the traditional banking system and the fractional reserve system, which has been eroded by recent crises, particularly the 2008 GFC. The resulting institutional development emerges in the form of tokenized deposits, a stablecoin that is issued by banks based on actual customer deposits, thereby preserving fractional reserves. The discourse of cryptocurrency service providers reveals tension between trusting the free market to naturally differentiate successful supply schemes from failed ones, and the need to mitigate financial harm caused by irresponsible or criminal behavior of industry participants. This tension results in attempts by cryptocurrency service providers to self-regulate through the voluntary adoption of codes of conduct. Voluntary codes of conduct, in turn, influence adoption and trust in the services provided.

The idea of governments to issue CBDC is also a result of a clash between the understanding that cryptocurrencies compete with government-issued money and the realization that governments may not have the capabilities to enforce regulation on private money. The result is an attempt by the state to compete in the market by issuing CBDC, rather than regulate. To level the playing field and avoid runs on other assets, the government is considering adding interest to CBDC that can adjust its financial attractiveness and imposing limits on CBDC holdings as a last resort against bank runs. These institutional developments are, in effect, self-regulation as they limit state agencies' ability to compete in the ecosystem by imposing a price and limits on money supply. The United States is also working to regulate other players in the cryptocurrency ecosystem. In April 2024 senators Lummis and Gillibrand introduced a bill to the senate that imposes strict regulatory measures on stablecoin issuers, following calls by the Chairman of the Fed to do so (Lummis, 2024). The bill limits the type of assets that can be used as reserves, allowing only highly liquid dollar-denominated cash and securities. While falling short of mandating a 1:1 ratio between issued coins and reserves, it prohibits un-backed algorithmic stablecoins and imposes strict transparency requirements on the issuers (Lummis & Gillibrand, 2024). The bill also requires stablecoin issuers to be registered in the United States. In later comments the senators acknowledge that the largest stablecoin issuer (Tether) is not registered in the United States and is not subject to the regulation. They express their trust that consumers will

opt to use US registered stablecoins, implying that if Tether chooses to remain offshore it would be a bad business decision (Hamilton, 2024b).

I conclude that all four actors demonstrate internal debate around which cryptocurrency supply models are acceptable and how they should be governed. These disagreements result in an abundance of institutional innovation ranging from centralized government regulation to decentralized liquidity pools. The answer to the question: which of these institutions will prevail, will depend on a combination of regulation and free market dynamics. For Ostrom's design principle to be satisfied the prevailing institutions must provide stability and liquidity.

Chapter Eight.

Monitoring the Ecosystem

The Concept of Community Monitoring

Monitoring of common-pool resources refers to the ongoing process of extracting information from the CPR ecosystem, which is essential for identifying and responding to misuse or abuse of the resource (Slough et al., 2021, p. 2). Ferraro and Agrawal (2021, p. 4) identify three types of information extracted by the monitoring of common resource ecosystems: information about the state of the ecosystem is used to monitor its vital signs; information about the activities of actors in the ecosystem is used to identify rule violations by appropriators, and information about the actions of officials and authorities is used to point to governance problems and potential corruption. Ostrom contends that ecosystems in which monitoring is enacted by appropriators or an entity that is accountable to the appropriators tend to be more resilient. Thus, her fourth design principle for a thriving and stable CPR ecosystems:

> "Monitors, who actively audit CPR conditions and appropriator behavior, are accountable to the appropriators or are the appropriators." (Ostrom, 2015, p. 90).

This section introduces the concept of transparency as a fundamental norm and key indicator in the monitoring of a potential cryptocurrency ecosystem. It explores how transparency influences trust among stakeholders, drawing on Ostrom's principles and applying them to the unique challenges of digital ecosystems. The analysis utilizes PDA techniques to examine the discourse of state agencies, financial institutions, and private individuals, discovering the tensions between privacy, trust, and the prevention of illicit activities. By framing transparency as both a tool for governance and a potential source of mistrust, this section establishes the basis for understanding the institutional developments connected to transparency and their impact on trust.

The difference between Ostrom's view that monitoring arrangements must be accountable to appropriators and the analysis in this thesis is that the boundaries of the assemblage here are much broader and more inclusive than in the CPR ecosystems that she envisions. Ostrom views a common pooled resource as a self-governed entity supported by arrangements with an active, enforcing environment consisting of

government regulation and law enforcement. Consequently, she distinguishes between monitoring conducted by external forces and monitoring carried out by the appropriators. In the absence of external coercion, motivation to play by the rules depends on power dynamics within the assemblage. While power can still be inherently coercive, it can also be based on trust and reciprocity. The key factor in fostering such trust is what Ostrom calls "credible commitment", the assurance that an actant's promise to adhere to certain rules or agreements is trustworthy. When the commitment of an actant to adhere to the rules is perceived as credible, it motivates other actants to reciprocate by adhering to those same rules, thus maintaining governance and cooperation within the assemblage. Effective monitoring is a prerequisite to credible commitment, because it creates the knowledge that supports trustworthiness (Ostrom, 2015, pp. 44–45).

This thesis views all actors as endogenous appropriators within the cryptocurrency ecosystem, making it difficult to apply Ostrom's criteria for monitoring accountable to appropriators, rather than others. If all parties are appropriators, a new standard is needed to assess whether monitoring supports a robust CPR arrangement. I propose transparency as that standard, understood as a practical, utilitarian concept: the creation of a just and democratic informational environment where actants are informed enough to safeguard their interests and collaboratively manage the ecosystem (Fung, 2013, p. 184). Using transparency aligns with Ostrom's fourth principle by promoting accountability and inclusiveness. But simply making information available is insufficient. To be effective, transparency must offer information that matches the concerns of stakeholders, is accessible in clear and usable formats, and is actionable, allowing meaningful responses. When these conditions are met, transparency fosters trust in openness and honesty (Fung, 2013, pp. 190–204). Consequently, assessing transparency involves more than just measuring the amount of accessible information. It also requires developing criteria to evaluate how transparency is constructed by actants, and whether it is perceived as clear, equitable, and fair.

The Relationship Between Trust and Transparency

Trust and transparency both help ease concerns about the intentions of actants within the assemblage. Mutual scrutiny is often linked, by scholars, to correlate with a willingness to expose vulnerabilities to achieve goals or reduce risk. However, this

thesis defines trust as the willingness to cooperate despite vulnerability, without needing to verify others through monitoring. From this viewpoint, trust enables cooperation without transparency. Thus, trust and transparency can substitute for one another and are mutually suppressive. When one is strong, the other becomes less necessary. (Viola, 2021, pp. 26–27). According to Ida Koivisto (2022, pp. 15–16) truth is a mediating factor that shapes the relationship between trust and transparency. Depending on how much information is disclosed, trust and transparency can be either positively or negatively correlated. This dynamic is captured in her concept of the "truth-legitimacy trade-off", whereby transparency can enhance legitimacy and build trust, but excessive or raw disclosure may expose flaws and reduce trust. Contrary to the common belief that transparency promotes both truth and trust, Koivisto argues it tends to promote one at the expense of the other. As a result, stakeholders manage transparency strategically, based on their goals and the audience. (Koivisto, 2022, pp. 15–16).

The analysis of trust and transparency can also adopt the position that they are entirely independent of one another. Rather than regarding them as dependent, correlational, or negatively correlated, they can be examined as non-correlational interacting variables. Duke (2021, pp. 66–68) differentiates between two archetypes of transparency with different relationships to trust. Imposed transparency is characterized by the disclosure of information in response to coercion by one actant on another. Examples include the requirement of government by way of regulation to disclose personal information or the disclosure of information by government in response to public pressure. This type of transparency often arises in situations of conflict and distrust between actants. The second form is adopted transparency, the unsolicited voluntary disclosure by actants of information. Examples include private companies voluntarily sharing commercial information, and individuals sharing consumer experiences on public forums. Adopted transparency is related to the trust that the shared information will not be used by other actants to exploit the vulnerabilities of the disclosing actant, but on rational choice connected to the premise that non-disclosure could expose vulnerabilities to other threats. In these examples trust and transparency interact without a consistent causal direction.

By examining the components of imposed and adopted transparency as it is reflected in the discourse of Governments, regulatory agencies, individuals and financial

institutions, this chapter seeks to gain insights on the problematization of trust and its interaction with truth in the context of monitoring. Through the dual lens of imposed and adopted transparency, I elucidate how trust and truth are constructed, challenged, and maintained in the discourse. This analysis is material to the evaluation of the cryptocurrency assemblage in the context of Ostrom's fourth design principle.

Government Problematization of Verifiable Trust

The executive order on the Future of Money and Payments adopts a G7 document outlining a set of policy principles for its members as they pursue the establishment of a CBDC (Biden, 2022, p. 14150). The executive order is thus extended to include the policy guidelines specified in the G7 document. This document highlights transparency in two ways. Firstly, it emphasizes government transparency as its openness in disclosing policy and processes.

"CBDC might involve new responsibilities for authorities, enable new policy opportunities, and potentially bring entities in a CBDC ecosystem into contact with personal data. Appropriate transparency and accountability frameworks, for both public and private sector participants, are crucial." (G7, 2021, p. 7)

The document acknowledges that new policy opportunities arise with new responsibilities in the context of personal data. Government transparency is the mechanism by which the trade-off between new opportunities to realize policy and the responsibility to protect personal data can be communicated and justified. It is viewed as crucial for fostering trust.

In the government's version of the assemblage, stakeholders' disclosure of data, whether imposed or voluntary, is also referred to as transparency:

"CBDC may offer opportunities for greater transparency in payments including potentially better standards of identification and verification of transactions. However, depending on design choices, this may involve some reduction in user privacy." (G7, 2021, p. 21)

The president is offering two-way transparency, where the full disclosure by the public of its transaction data will be reciprocated by the government's disclosure of when and how the data is processed.

The G7 policy guideline regarding data privacy provides further assurances to the public in connection with the use of private data. It limits uses by the private and public sector to those grounded in legislature that addresses the proper purpose of data usage and the consent of stakeholders to that usage, under the principle that the minimal data required by law to achieve specific goals will be collected. The principle also covers transparent and ample securitization and safe storage of the data (G7, 2021, pp. 7–8)

The major reason for the requirement of personal data transparency, according to government policy documents, is to prevent illicit finance. Although government documents do not provide a precise definition of "illicit finance," the term covers a spectrum of illegal activities. In its initial action plan, the term is described symptomatically, focusing on three specific threats: money laundering, proliferation financing by nations evading sanctions, and terrorist funding (DOT, 2022, pp. 3–4). However, later descriptions show the term is fluid and evolves over time. A 2024 DOT report titled “National Strategy for Combating Terrorist and Other Illicit Financing” broadens the definition to include threats unrelated to national security or major crime:

Recent FATF reports examined corruption related to citizenship and residency by investment programs, highlighting how corrupt actors, tax evaders, and other criminals have exploited these programs to disguise their identities.” (DOT, 2024, p. 29)

The shift in scope of the term “illicit finance” is significant, considering the problematization, by government, of trust in the cryptocurrency assemblage as a question of balance between privacy and illicit finance prevention. As the scope of illicit finance is extended, greater stakeholder transparency is required to address the cases covered by the policy, thereby shifting the balance between illicit finance prevention and privacy:

“Jurisdictions must consider how to balance user trust and security with the need to counter illicit finance (such as the financing of terrorism and money-laundering and respect targeted financial sanctions).” (G7, 2021, p. 22)

This statement paradoxically places user security on both sides of the trade-off. However, the construction of security depends on how the "enemy" is problematized. When the enemy is external, such as criminal networks or terrorists, surveillance and enforcement are framed as necessary to protect the financial system, linking trust to the state’s ability to neutralize threats—even at the expense of privacy. When the enemy is

internal, like government overreach, security is constructed as the protection of privacy and autonomy. Through this dual framing, the President presents the trust trade-off as a matter of prioritization: minimizing systemic vulnerabilities or safeguarding individual liberties.

Government policy documents propose several solutions that may affect the balance between the prevention of illicit finance and privacy in case CBDC is introduced. These solutions also apply in a cryptocurrency ecosystem without CBDC. One approach is to limit the disclosure of user identities to a person's local service provider or to a dedicated entity in charge of user verification, limiting the distribution of identified private data by intermediation (G7, 2021, p. 22). Another strategy is tiering account holders or transactions to preserve anonymity for minor stakeholders and small transfers, allowing access for unverified users without undermining efforts against illicit finance (Treasury, 2022b, p. 26). Technologies like Zero Knowledge Proof and Multi-party Computation are proposed to hide user identities while enabling necessary data access. The government also seeks to clarify that private cryptocurrencies do not effectively protect identity or data, making a trusted central party the preferred solution for minimizing and securing data collection (OSTP, 2022b, pp. 20–22).

Financial Institutions – The intermediation Solution

Most responses from traditional as well as cryptocurrency centric financial service providers problematize the issue of monitoring as a matter of centralized government surveillance, raising concerns about the implications of such oversight. They emphasize that the role of trusted intermediaries is to prevent government possession of personal data, suggesting that anti money laundering and countering the financing of terrorism (AML/CFT) controls must remain in the hands of banks and financial institutions (FED-comments, 2022, p. 9:384). Some service providers issue dire warnings against government control of personalized data, exemplified by the Community Bankers Association's description of the government and financial regulators as hostile enemies who weaponize their authority:

"A recent and troubling example of the government/financial regulators inappropriately interfering with and imposing its priorities, was Operation Chokepoint. During this operation, the Department of Justice and the Federal Deposit Insurance

Corporation abused their powers and weaponized their authority to advance an ideological objective." (FED-comments, 2022, p. 9:76).

The reference to Operation Choke Point casts intermediaries as a shield between the private sector and state overreach. Launched by the DOJ in 2013 to combat financial fraud by targeting high-risk businesses, it also affected legal firms like payday lenders, sparking criticism of politically motivated interference. The Trump administration ended the program in 2017 (Stevenson, 2022, p. 360). While Operation Choke Point did not ask financial institutions to disclose personal data, it raises concerns about the potential implications of government access to such data. The operation's focus on regulating financial institutions and their relationships with businesses for ideological purposes raises the possibility that government can use personal data to enforce ideological policies on any stakeholder.

Despite the concern regarding government control and the violation of the arms-length relationship with intermediaries, most cryptocurrency service providers acknowledge their commitment to comply with regulatory requirements, emphasizing the voluntary nature of their compliance. While Tether is registered in the British Virgin Islands and Hong Kong where disclosure regulation is more lenient, they commit to proactive cooperation with United States regulators.

"Tether's dedication to fighting illicit actions in the realm of digital assets can best be demonstrated through our assistance in law enforcement investigations. Tether works closely with law enforcement partners to address cybercrimes and fraud. We also utilize chainalysis to identify scammers, investigate potential fraud, and report to relevant authorities." (OSTP-Responses-1, 2022, p. Tether: 2)

By mixing compliance and voluntary efforts, this quote demonstrates that the theoretical dichotomy between imposed transparency and adopted transparency can be ambiguous, rendering practical case studies a hybrid of these two modes. Cryptocurrency providers often exceed the legal and regulatory requirements set for them, voluntarily providing unsolicited information and doing so with greater frequency than mandated by regulatory authorities. Tether does this by maintaining a transparency page (Tether, 2024) that provides daily updates on its reserves, token distribution per platform and liquidity. This positions Tether as a cooperative and proactive actor within the digital asset ecosystem, aligning its legitimacy with its

dedication to combating illicit activities. Tether problematizes illicit actions as a primary threat to the integrity of digital assets. This framing positions Tether firmly on the side that prioritizes the external risk in the tradeoff constructed by the President. The reliance on terms like "identify scammers," "investigate potential fraud," and "report to relevant authorities" subtly establishes Tether an integral part of the apparatus of state overreach.

Respondents' Problematization – The Monitoring Tipping Point

The Federal Reserve raised the issue of balancing privacy and combating illicit activities as a question presented to respondents of the RFC regarding the potential introduction of a CBDC in the United States, phrasing it as follows:

"How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?" (FED, 2022a, p. 22)

The responses of private individuals do not indicate mistrust in the transparency of government and other federal agencies in their handling of users' private information. However, the most prominent theme across the responses is the concern and fear that CBDC will erode financial privacy by increasing government surveillance and control over financial transactions. Thus, government transparency is not being reciprocated by the public, despite being perceived as authentic. The most prevalent reason given for this asymmetry in the responses is that people distrust the government's will to limit illicit finance to large scale crime and terrorism:

"The removal of cash from our system will decimate the freedom of the middle and lower class. It will prevent you and your kids from doing one single odd cash job without the IRS tracking every single cent." (FED-comments, 2022, p. 5:134)

This statement positions cash not just as a medium of exchange but as a symbol of personal liberty, contrasting it with invasive government overreach. The phrase "decimate the freedom" conveys a sense of destruction, specifically of the middle and low classes who rely on the flexibility of cash as a means of social agency, allowing them to navigate economic systems on their own terms, sustain informal networks of trust, and participate in community-based exchanges that often fall outside institutional control. The perception that government surveillance is not only intended to prevent

large scale crimes is confirmed by the decision of the US government to lower the reporting thresholds from payment companies like PayPal to a volume of 600 US Dollars per year, per account. This move, by the government, is cited as an example of the potential for government surveillance, and the contempt that it provokes:

“Bad enough you can snoop through my account because it goes over 600 bucks from me getting money via PayPal, Venmo, cash app, etc.” (FED-comments, 2022, p. 1:251)

As a result, respondents place their trust in two alternatives to CBDC. First, despite government warnings that blockchains are not truly private, individual responders largely trust in the perceived anonymity of cryptocurrencies. Some of these responses openly state that illicit finance is of no concern when it comes to protecting privacy:

"Illicit activity will come with complete privacy, but should not deter open, permissionless usage. Instead, authorities should study Bitcoin’s blockchain to further understand transactional history to find those who use the technology for illicit purposes. Privacy is of utmost importance for a currency and requiring permission is unamerican." (FED-comments, 2022, p. 3:193)

This response emphasizes inclusion and freedom as the motivation to trust cryptocurrency anonymity. The requirement for permission to participate in the monetary system and to execute transactions is described as unamerican, positioning privacy as patriotic obligation. Government should adhere to that norm and seek illicit finance in the blockchain without compromising full privacy.

The other source of trust expressed by public individuals is the existing two-tier intermediated ecosystem:

“The current model works. People understand and accept that under legally defined situations the government has the right to access information on people's money. Bank accounts now are subject to IRS examination. Why should this change?” (FED-comments, 2022, p. 6:488)

The status quo bias heuristic is strong despite widespread mistrust in traditional financial institutions. Most respondents clearly prefer to maintain the current system, in which they can choose to conduct economic activity through the bank or keep it entirely confidential with cash.

Another powerful factor driving mistrust and fear is the availability heuristic. This mental shortcut relies on immediate examples that come to mind when evaluating an issue. A significant number of respondents invoke the example of social credit scores in China as a form of government surveillance that will evolve from direct centralized monitoring of financial activity (Liaropoulos, 2022, p. 132). A social credit score is a system of governance that attempts to rate the trustworthiness of actors in the ecosystem by scoring their financial activity. This system can be based on various data sources, including financial records, loan repayments, institutional compliance, and other financial actions. The prospect of social credit scores in the United States elevates fears to an emotional level.

"... a CBDC or cashless society creates a surveillance society where every purchase is potentially tracked and therefore no longer anonymous. This can be used by the government or third parties to monitor individual's spending habits, political affiliations, religious affiliations, leisure activities, and other spending. It creates the potential for a Chinese-style social credit score system that undermines our freedoms and liberties and even violates potential fourth amendment rights." (FED-comments, 2022, p. 8:511)

This statement not only expresses fear of government surveillance, but it also rejects transparency in general. The reference to potential violations of rights under the Fourth Amendment emphasizes the perceived threat to personal privacy and constitutional protections, by the government and third parties. The message is that financial monitoring is part of a larger scheme to monitor and control all aspects of human existence.

Respondents' problematization of the balance being struck by the state between the protection against illicit finance and personal liberties highlights a tipping point where the elimination of the ability of private individuals to perform transactions outside of the domain of state scrutiny. This is the point at which legitimacy turns into perceived overreach, transforming the state's role from protector to oppressor in the eyes of the public. Respondents emphasize the unique role of cash, not only as a medium of exchange but also as a vital component of informal economies, even though these economies function outside the law. The potential elimination of cash is viewed as a

threat to these informal networks, which support personal agency, community trust, and economic survival for many.

Conclusion – WPR analysis, problematizing a balance

In this chapter, I propose the concept of transparency to analyze the issue of monitoring in the cryptocurrency assemblage. Using transparency as a criterion involves not only the extent, but its nature and quality, which is contingent on the subjectification of the "enemy" and the nature of the threat that the monitoring is intended to address. While the state subjectifies external criminals and terrorists as the enemy, individual respondents frame the state actants as the adversary. Consequently, the analyzed discourses highlight monitoring as a tension between two competing norms of stakeholder security: protection from illicit activities and protection against government overreach. Each of the three discourses problematizes this tension with distinct emphases, as illustrated in Table 5.

The competing norms of security and autonomy underscore the delicate balance needed to maintain a resilient and inclusive ecosystem. In expressing this balance, stakeholder discourses use different scales to frame transparency in relation to privacy and other priorities. State discourse positions transparency on a scale emphasizing privacy versus illicit finance prevention, while financial institutions and individuals share a scale focused on privacy versus compliance. The latter discourses aim to minimize transparency to the extent necessary to meet regulatory requirements, while protecting their interests. For financial institutions, this involves maintaining trust with clients while fulfilling legal obligations. For individuals, it reflects a desire to protect autonomy and preserve anonymity.

Both the state and cryptocurrency-centric financial institutions practice adopted transparency by voluntarily exceeding mandated disclosure requirements. For the state, adopted transparency serves to demonstrate the legitimacy for its surveillance activity. Financial institutions, on the other hand, use adopted transparency to signal credibility and reinforce their role as trusted intermediaries in the eyes of the state and the public. In both cases, the balance between transparency and privacy is treated as negotiable, adjusted to achieve acceptable trade-offs. Conversely, individuals perceive transparency and privacy as fundamentally opposed, with a fixed and non-negotiable

boundary. For them, the perception of overreach undermines trust in other actants. Most respondents view cryptocurrencies as an institutional arrangement that reduces the need for transparency, allowing them to remain anonymous within the ecosystem. While some accept limited transparency with intermediaries, they strongly oppose extending it to government or regulators. This demand for anonymity is driven by fear and shaped by strong heuristics favoring the status quo, where cash transactions stay beyond legal reach.

Stakeholder	Problematization Scale	Adopted Transparency	Truth – Legitimacy Trade-off
State	Privacy – Illicit Finance Prevention	Yes	Truth
Financial Institutions	Privacy - Compliance	Yes	Balance
Individuals	Privacy - Compliance	No	Legitimacy

Table 5 - Monitoring tensions

The assumption that an ecosystem would align with Ostrom's 4th principle if private individuals were fully transparent holds only if the implications of the truth-legitimacy trade-off are overlooked. The recognition that too much transparency undermines trust must be a factor in the constitution of the ecosystem. Ignoring the trade-off between truth and legitimacy fails to account for the delicate balance required to maintain stakeholder trust while ensuring accountability. A stable assemblage must navigate this balance, recognizing that excessive transparency can erode the trust and resilience that Ostrom's principles seek to achieve.

To facilitate the creation of a balance between truth and legitimacy three potential avenues for institutional development emerge: First, the rules of intermediation are being addressed to establish an institutional buffer that has access to stakeholder data but discloses only what is mandatory. This buffer serves as a defense layer against illicit finance, subjectifying intermediaries as trustees of sensitive information in the assemblage. Second, tiered monitoring has the potential to exclude small transactions or low-volume accounts from government scrutiny, thereby emulating the blind spot that government experiences with traditional cash. Finally, technologies must mature to manage information flows to the government without revealing personal data. One

such emerging solution is Zero Knowledge Proof (ZKP), which enables stakeholders to verify information—such as fund sources or user identities—without disclosing the underlying data.

In practice, these institutional arrangements have not matured to an operational level. While individuals are firmly committed to the complete anonymity of current cryptocurrency networks and the cash system, the government has focused its efforts on increasing surveillance rather than innovating ways to combat money laundering. This misalignment has contributed to known money laundering activities exceeding $30 billion in 2022. Although there was a decline in 2023, it is unclear whether this is due to effective measures, or if criminals and terrorists have found more sophisticated methods to hide their transactions (Chainalysis, 2024, pp. 4–8). While companies like Chainalysis are committed to monitoring blockchain-based cryptocurrencies, the stakeholders themselves have not undertaken to devise institutional arrangements that reward effective, trust-building transparency.

Chapter Nine.

Graduated Sanctions

The Double-Edged Sword of Sanctions

Sanctions are the consequences imposed on a stakeholder based on their behavior in relation to the codes of conduct established by the rules. While sanctions are commonly analyzed as punishment for non-compliance with institutional rules, they can materialize as positive consequences in the form of monetary incentives, reputation boosts, and operational advantages such as governance voting rights. This implies that stakeholders may be rewarded for cooperation as well as punished for breaking the rules. Sanctions are proven to affect the way that stakeholders deal with social dilemmas, the conflicts that stakeholders encounter between acting for the common good and making selfish choices (van Dijk et al., 2014, pp. 70–71). Ostrom contends that sanctions increase levels of cooperation and compliance within the ecosystem if they are proportional to the nature and impact of the behavior that they address. Thus, the proper design of sanctions has a direct effect on the resilience of a CPR ecosystem:

> "Appropriators who violate operational rules are likely to be assessed graduated sanctions (depending on the seriousness and context of the offense) by other appropriators, by officials accountable to these appropriators, or by both." (Ostrom, 2015, p. 90)

This section explores Ostrom's principle of graduated sanctions within the context of the cryptocurrency assemblage, emphasizing their implications for trust and cooperation. The empirical findings reveal a notable scarcity of references to sanctioning systems and a lack of institutional innovation in this area. An analysis of existing sanctioning practices underscores the predominance of state-driven punitive measures, suggesting a general acceptance among actants of a state-led sanctioning framework. The section concludes with a WPR analysis that examines the silence of actants on the issue of sanctions and proposes an alternative conceptualization of the sanctioning problem within the assemblage.

The emphasis on graduated sanctions reflects the understanding that penalties should be fair and proportionate. Punishments and rewards that are tailored to the offense are

often more effective than harsh penalties for minor offenses. However, sanctions can be counterproductive by encouraging stakeholders to treat compliance as a business decision rather than a moral one. This puts a price on non-compliance, making it a business decision rather than a moral decision rooted in social relationships. Sanctions can also erode interpersonal trust, shifting cooperation from reciprocity to fear. Their presence may signal that others are untrustworthy, fostering distrust and undermining cooperation. The utilitarian thinking that sanctions may induce, and the distrust that emerges with excessive sanctioning, work against cooperation rather than promoting it (van Dijk et al., 2014, pp. 71–74).

Werbach (2018a, Locations 4600–4687) argues that, like the effects of excessive sanctions, lack of sanctioning can foster utilitarian thinking and erode societal trust as well. Drawing parallels with the development of the Internet, he concludes that cryptocurrency governance structures, built on the premise that they define the law independently of state oversight, tend to disintegrate when the lack of obligation to the law transforms into a general lack of accountability. When the resulting actions transgress legal limits, the government finds ways to intervene, overcoming geographic and jurisdictional challenges, thereby making government sanctions a dominant component of the overall graduated sanctions system. This system includes a variety of measures including shaming, reputation manipulation and automated exclusion and blacklisting. Since this thesis regards the state and its agencies as equal participants in the assemblage, sanctioning by the state is considered a form of peer sanctioning in a CPR setting.

An alternative solution to measured, graduated sanctions could be the imposition of extremely harsh negative sanctions, severe enough to deter anyone from considering them as a viable course of action. However, this choice has encouraged stakeholders to evade sanctions by finding vulnerabilities in the monitoring scheme. Sanction evasion is often driven by the excessive costs of compliance or the perceived unfairness of the severity of sanctions, which can undermine the legitimacy of the sanctioning authority or the entire system (Mulder et al., 2009, p. 265).

Sanctions and Trust

Scholars often view sanctions as a fundamental aspect of the power dynamics between states and their stakeholders. However, the impact of this relationship on cooperation is not straightforward and can vary depending on the level and type of power exerted. Therefore, exerting more power does not necessarily lead to increased cooperation. Conversely, trust between stakeholders and government is positively related to cooperation, even in the most complex cases such as tax compliance, where the boundaries between legal and illegal behavior are often blurred. Reciprocal trust cultivates a synergistic tax climate between tax authorities and taxpayers, leading to voluntary compliance. Taxpayers pay their fair share because they trust that the government will use the funds to provide quality services, and government trusts taxpayers to report honestly (Wahl et al., 2010, pp. 384–386). Levi (2019, p. 362) defines a trustworthy government as having three characteristics: It does not generally renege on its promises, and if it does it makes its reasons known; it promotes equity and fairness; it delivers goods and services consistently. This type of trustworthiness correlates positively with compliance while reducing the motivation to evade or reject sanctions (van Dijk et al., 2014, p. 76).

In the context of the current study, the discussion of trust and the imposition of sanctions between government and its constituents is problematic on two fronts: First, government cannot be viewed as a single homogenous entity that commands trust. This can be illustrated by the fact that different branches of government command varying degrees of trust by society. In the United States local government commands the greatest trust whereas the executive branch and the legislature command low levels of trust (Jones, 2023). Consequently, if trust is to be analyzed as an enabler of a graduated sanctions regime, the variability in trust across different government branches must be considered. Second, I contend that the analysis of trust-power relationships extends beyond the interactions between governments and their constituents and is applicable to all relationships where sanctions are involved. In relationships where power dynamics are less pronounced, trust compensates for the absence of coercive mechanisms. Without a clearly defined authority, trustor and trustee must forge a relationship of mutual trust to ensure cooperation. In these contexts, formal or informal sanctions are only effective if they are perceived as fair and just by both sides, and if both agree that their implementation is mutually beneficial. This is very much relevant to cryptocurrencies, where in addition to the coercive powers of the state, sanctions can

be imposed by the public, by financial institutions and by automated rules embedded in software.

Problematization of Sanctions by Respondents

Respondents' reference to sanctioning is sparse in the primary corpus examined in the thesis. However, red lines are demarcated by individuals regarding the types of negative sanctions that are unacceptable and the norms of trust that they invoke in connection with sanctions. In considering the prospect of a CBDC, respondents reject the possibility that the state will be able to freeze their accounts and exclude them from the financial system. The following quote describes sanctions that are unacceptable.

"The federal reserve will be able to: freeze anyone's account, seize anyone's money, block any transaction, etc."(FED-comments, 2022, p. 5:321)

This comment is directed specifically at the FED as a source of mistrust, while other comments target the government in general:

"Giving the government the power to suspend someone's ability to spend money freely, or a business's ability to receive payments. Imagine the tyranny this could bring if suddenly this CBDC was to be used this way at a mass scale. Imagine creating a system that could automatically reward people who voted one way or another and punished those who didn't." (FED-comments, 2022, p. 2:61)

The statement reflects fear of both positive and negative state sanctions, portraying the government as powerful, malevolent, and capable of oppression. The word "tyranny" evokes authoritarianism and abuse of power, sharply contrasting with government documents that frame control as protection. Like much of the private discourse, it shows strong resistance to the idea of government-administered sanctions influencing public behavior. Some respondents note that even if current intentions are benign, a future shift toward misuse is seen as inevitable:

While that may not be its initial intent, it is impossible to imagine a future where a centralized governing body does not try to exert control over the users of the currency whether through monetary policy means, or direct action against them. (FED-comments, 2022, p. 12:388)

Here, the phrase "impossible to imagine" constructs a discourse of inevitability, portraying centralized governance as doomed to failure. The statement implies that even if the government's initial intentions are benign, the fragility of the political system makes it likely that future governments will use their sanctioning power to exert control by way of manipulating people's money. The association of the government and the FED with the concept of centralization reveals a deep-rooted heuristic, equating the power of the state with centralization, thereby ignoring the underlying democratic process as the basis for state authority. This unrelenting stance is not universally shared among all the respondents. Some of them do recognize the power and legitimacy of the United States Government to sanction. However, this reluctant willingness is contingent upon the condition that due process is observed:

"It is critical that CBDCs… are never used to freeze assets without due process through the US court systems." (FED-comments, 2022, p. 8:13)

The invocation of due process reflects the norm that basic rights must be respected to prevent potential abuses of power by the government or the FED, emphasizing distrust toward these branches of the government. Due process implies that a person is entitled to prior notice, an opportunity to be heard, and the right to a neutral decision maker as conditions to the imposition of sanctions. The use of the term "through the court system" suggests that substantive due process is demanded. This type of due process is a legal principle that protects certain fundamental rights from government control, putting the decision in the hands of the judicial system. It goes beyond the requirement that the government follows fair procedures, ensuring court involvement in the enactment of governance (Resnik & Hershkoff, 2023, pp. 614–617).

Graduated Negative Sanctions in Practice

Apart from the resistance by the public to sanctions by the government without due process, trust in graduated sanctions is not problematized in any of the discourses examined in this thesis. Neither governmental bodies, regulatory agencies, nor financial institutions have directly problematized the punitive measures intended to regulate cryptocurrency-related transgressions. Additionally, the texts do not address the numerous positive incentives inherent in the cryptocurrency ecosystem, such as

rewards for staking, mining, transaction verification, and investment in liquidity pools. Nevertheless, a graduated negative sanctions regime has developed as part of the existing ecosystem. Table 6 outlines the types of sanctions imposed in practice, in order of severity, and actual examples of their implementation. The examples are sanctions with a predominantly punitive character, as opposed to those aimed at public protection or financial remediation.

Sanction	Applied by	Example	Date
Reputational Harm	Public	The Tether stablecoin faced a massive loss of trust for claiming to be backed by 1:1 reserves without agreeing to audits.	2018
Suspension of Accounts	Crypto firms	Binance Freezes Stolen Cryptocurrency Assets Worth $11.8 million in kidnapping scheme, blocks criminals' access to funds.	2023
Fines	Regulatory Agencies (state)	BitMEX was fined $100 million by the CFTC for failing to implement proper anti-money laundering procedures.	2021
Delisting from Exchanges	Crypto firms	Tornado Cash plummets 56% after Binance says it is delisting the token for not meeting listing standards.	2023
Asset Forfeiture	Government And regulatory agencies (state)	US Confiscates $400M: DOJ administers forfeiture judgment Against Onecoin for money laundering	2020
Court Imposed Civil Penalties	Courts (State)	Ripple Labs was sued by the SEC for failing to comply with AML/KYC procedures while facilitating money transfers.	2015
Imprisonment	Courts (State)	Ross Ulbricht, founder of Silk Road, was sentenced to life in prison for operating a marketplace that facilitated the execution of illegal transactions.	2014

Table 6 - Sanctions Hierarchy

This table shows the hierarchy of punitive measures, with civil penalties and imprisonment requiring substantive due process, highlighting the state's dominance in imposing severe sanctions. However, the disintermediated nature of the crypto ecosystem complicates this structure, as financial institutions often operate beyond traditional regulatory and geographic boundaries. This limits governments' ability to enforce compliance, as seen in the 2015 Ripple case. Ripple was fined $950,000 for KYC and AML violations. The case led some firms to boost compliance, while others

moved operations abroad, citing government overreach. This shift helped establish countries like Switzerland as crypto-friendly hubs. (J. Epstein, 2017).

Another limitation stems from the challenge of applying laws meant for centralized systems to decentralized platforms, where accountability is distributed. Legal frameworks often fail to address those who enable illegal activity without directly committing it, as seen in the harsh sentencing of Ross Ulbricht, who was subjected to the most severe punishment in the history of crypto-related cases. Ross Ulbricht, founder of Silk Road, a darknet marketplace that used bitcoin to trade illegal drugs and other illicit goods, was sentenced to life in prison without parole. He was convicted under the charge of operating a continuing criminal enterprise, known as the Kingpin Statute. This law, typically used against leaders of major organized crime operations, carries a minimum sentence of 20 years, and is one of the most serious drug-related charges in U.S. law. Although Ulbricht did not personally sell drugs, he was punished for creating and running the platform that enabled illegal activity. His sentence sparked widespread criticism for being excessive given that he was a non-violent, first-time offender. His clemency petition, now the largest active one with over 600,000 signatures, is supported by legal experts, civil rights advocates, libertarians, privacy activists, and politicians including Robert F. Kennedy Jr. and Donald Trump (Ulbricht, 2024). In a speech on May 25th, 2024, Donald Trump vowed to commute Ross Ulbricht's sentence on his first day in office, a move widely seen as an effort to appeal to Libertarian voters (Schaefer, 2024). Although the push for Ulbricht's release is primarily driven by the libertarian movement in the United States, many draw comparisons between Ulbricht's sentence and that of Sam Bankman-Fried, the former CEO of the failed cryptocurrency exchange FTX, who was sentenced to 25 years for defrauding investors and customers of over $8 billion in losses. Critics argue that, given the scale of Bankman-Fried's fraud compared to the fact that Ulbricht did not steal money, it is Bankman-Fried who deserves a life sentence rather than Ulbricht (Buchwald, 2024).

WPR Analysis of Sanctions Problematization

The problem of trust in sanctioning represented by respondents is the fear that centralized authorities will misuse their sanctioning powers to freeze accounts and exclude individuals from the assemblage. This representation is underpinned by norms

that equate centralized power with risks of authoritarian overreach and erosion of individual financial autonomy. The main effect is the weakening of trust in centralized institutions by framing them as untrustworthy and challenging their legitimacy and authority in the administration of sanctions.

The scarcity of references to sanctioning in the corpus prompts an inquiry into the silences surrounding this issue, using WPR's fourth question:

"What is left unproblematic in this problem representation? Where are the silences? Can the 'problem' be conceptualized differently?"(C. Bacchi & Goodwin, 2016, p. 20)

Unlike other controversial issues covered in this study, where the Fed, DOT, and the OSTP actively seek public input to provoke debate, the lack of discourse problematizing trust in sanctions indicates acceptance by the state institutions, of the existing graduated sanctions system. In the traditional financial ecosystem, the government implements procedural due process to sanction transgressors by imposing fines, seizing assets and ordering banks to freeze accounts. Many public comments call for removing sanctioning powers from the executive and regulatory agencies, arguing that harsh penalties should be handled by the judiciary through substantive due process. This reflects a shift away from the current system and signals distrust in the executive and regulatory branches to administer sanctions fairly. The argument that the current democratic system does not ensure that future governments will apply sound moral principles signals a deep distrust of both the democratic system itself and in the broader society.

The entrustment of the judicial system with the administration of severe sanctions is not unlimited. As demonstrated by the Ross Ulbricht case, public reaction to the perceived severity of sanctions can evolve into a powerful political movement, capable of challenging the legitimacy of the judicial system and prompting calls for remediation at the highest levels. This underscores respondents' preference for imposing harsher sanctions on those who steal from constituents of the assemblage over those who facilitate broader criminal activities, contrasting the judicial view that clearly prioritizes the broader societal impact of the crimes.

I argue that the sparse problematization of negative sanctions by all discourses is closely linked to the underdevelopment of new institutions designed to enforce punitive measures. Despite the potential for significant institutional and technological

innovations in this area, few have been explored or implemented. Thus, sanctions such as on-chain automated fines, which could be enforced through smart contracts and penalties for attempted transaction falsification remain theoretical. Similarly, the concept of decentralized exclusion hearings, where stakeholders could vote to exclude bad actors from the network, has not yet been seriously proposed. These alternative solutions lead to the answer to the last part of the WPR question: "*Can the 'problem' be conceptualized differently?"* By conceptualizing the problem as a systemic issue of how the monopoly over violence should evolve with distributed governance policies, discourse could have challenged the centralized structure of sanctioning rather than adapting the assemblage to fit within them.

This lack of institutional development contrasts with the automatic reward systems that were built into the cryptocurrency ecosystem by design. Stakeholders get rewarded for a variety of actions including the validation of transactions, currency mining, and provision of credit and liquidity. I argue that this discrepancy is not due to an objective difference between positive and negative sanctions, but rather to the subjective nature of human decision-making. People are not yet, and may never be, ready to delegate punitive decisions to machines. The reluctance to automate such decisions stems from a prevailing conjecture that subjectivism, empathy, and moral reasoning play crucial roles in determining appropriate sanctions. The actants not only wish to leave these decisions in the hands of humans, but they also want these humans to be legal professionals whose responsibility is to be impartial and fair.

Chapter Ten.

Conflict Resolution

The Role of Conflict Resolution

The sixth design principle proposed by Ostrom, characterizing robust CPR arrangements, is the availability of conflict resolution mechanisms in the ecosystem:

> "Appropriators and their officials have rapid access to low-cost local arenas to resolve conflicts among appropriators or between appropriators and officials." (Ostrom, 2015, p. 90)

This section examines the discourse surrounding trust in conflict resolution systems, focusing on the interplay between remediation as a conflict resolution mechanism and immutability as a conflict mitigation feature. I show that, while immutability is adopted as a foundational norm in decentralized systems, it is limited by the acknowledgment that the solution of some conflicts requires human reasoning and morals, thereby inhibiting the development of a truly no-party trust assemblage.

Ostrom considers conflicts among appropriators a significant threat to the resilience of CPR arrangements (Ostrom, 2015, p. 86).While robust institutional rules can convey the feeling that they are unambiguous, in practice rules need to be interpreted to apply to new situations and infractions. Appropriators of a common resource require assurance that they have recourse when such new situations occur (Werbach, 2018a, Location 3036). Thus, every institutional arrangement must have conflict resolution mechanisms to endure (Ostrom, 2015, pp. 100–101). I contend that the issue of conflicts can be addressed not only by way of resolution but also through proactive prevention. If the goal is to minimize ongoing conflict, mitigation is a critical component in achieving this objective. Under that assumption, Ostrom's sixth design principle should therefore be restated as: *Institutional arrangements should be established to prevent conflicts among appropriators and provide low-cost arenas for resolving them when they arise*. Consequently, I introduce the concept of conflict resiliency, which encompasses both conflict resolution and mitigation as the capacity of the ecosystem to withstand conflict.

In the monetary ecosystem most disputes stem from the asynchronous nature of economic activity, meaning that payment and delivery of goods or services do not occur simultaneously. Instead, various payment models and terms are used to facilitate transactions, depending on factors such as industry practices, consumer preferences, and technological capabilities. The last two decades of the twentieth century featured accelerated growth in asynchronous activity based on credit. Between 1984 and 2002, the share of credit card usage alone grew from 6% of purchases to 34% (Morriss & Korosec, 2005, p. 2). This growth put credit card companies at the forefront of dispute resolution in credit card transactions. These companies have established dispute resolution processes, making them the first line of arbitration in transaction conflicts (Morriss & Korosec, 2005, pp. 56–65).

In other sectors of the ecosystem, a variety of dispute resolution methods have been used, ranging from legal measures and litigation to online dispute resolution (ODR) solutions provided by payment providers. ODR services are increasingly gaining recognition and standing in the traditional legal system (Hanriot, 2016, pp. 5–7). These measures are complemented by various mitigation methods that contribute to the prevention of disputes. Escrow services protect users from infractions by holding funds until the agreed-upon terms are fulfilled. Additionally, reputation systems are used to ensure that bad actors do not command the trust of potential counterparts in smaller internet transactions (Pieńkowski, 2011, p. 97). Technological solutions in the areas of anti-fraud and cybersecurity are also increasingly being used to mitigate risk of crime (Uddin et al., 2020, pp. 248–249).

In the cryptocurrency ecosystem blockchain technology plays a significant role in reducing the risk of conflicts by introducing mechanisms that enhance trustworthiness. The underlying blockchain infrastructure, with its decentralized and immutable ledger, guarantees that all transactions are securely recorded and resistant to tampering. The use of cryptographic security provides assurance that transactions are legitimate and have not been compromised. Thus, blockchain reduces the likelihood of conflicts by providing a transparent and final record of transactions, which helps prevent disputes and fosters smoother interactions within financial ecosystems (Werbach, 2018a, Location 3108).

Trust and Conflict Resolution

According to the definition of trust used in this thesis, engaging in asynchronous financial transactions involves the voluntary exposure of the vulnerability of the creditor, as the party reimbursed later in the transaction. For instance, if a merchant delivers goods or services prior to receiving payment, they expose their vulnerability to the risk of non-payment. If this risk materializes, the consequence is financial harm. Consequently, parties must have trust in the capacity of the assemblage to enforce the agreements that underlie transactions. In traditional conflict resolution, enforcement is often based on law or social relations. However, in blockchain-based environments, trust takes on a different form, grounded in the determinism of technology. This shift introduces the concept of "no-party trust," where reliance is placed on the technological system itself to ensure procedural certainty and enforce agreements without intermediaries or centralized authority. Smart contracts, for example, automate the enforcement of agreements, allowing parties to engage in transactions without relying on personal or institutional trust (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019, pp. 252–254).

This reliance on technology enables transactions in environments where traditional trust mechanisms are unavailable, offering a form of assurance grounded in the predictable execution of agreements. By shifting the basis of enforcement to a decentralized framework, these systems facilitate economic exchanges that would otherwise be hindered by the lack of legal or relational recourse, ensuring that obligations are met without requiring direct trust between the parties involved.

Problematization of Trust in Conflict Resolution

In its technical evaluation of a United States CBDC, the Office of Science and Technology Policy (OSTP) identifies eighteen design choices for a potential CBDC, two of which pertain to conflict resilience: remediation and programmable money. This thesis considers these design choices as institutional components within the assemblage. The design choices of remediation and programmable money are key to building conflict resiliency in the context of a United States CBDC, and cryptocurrency in general. Remediation focuses on mechanisms to rectify transaction errors by amending the ledger or applying compensatory transactions, thereby acting as a conflict

resolution mechanism. Programmable money enables the embedding of conditions or rules into transactions, allowing for automated enforcement of predefined agreements. This functionality helps mitigate conflicts through the introduction of enhanced transactional certainty.

The OSTP lists the goals of remediation, constructing them as conflict resolution mechanisms.

"We assume a CBDC system will be required to facilitate remediation, so that persons or entities can conduct activities such as recovering accounts, voiding transactions, ordering restitution, and conducting recovery and resolution activities." (OSTP, 2022b, p. 22)

The assumption of necessity acts as a heuristic, establishing remediation as the default solution for transaction disputes within a CBDC system. It presumes that remediation is essential to the operation of financial ecosystems, leaving alternative approaches unexplored. By presenting remediation as fundamental to a functional monetary ecosystem, this heuristic encourages its adoption as the standard for resolving transaction-related disputes.

To underline the necessity, the OSTP document goes on to supply a straightforward real-world illustration. This is the only explicit example presented by the OSTP document. I interpret the use of an example as a special effort to ensure that any reader comprehends remediation as a fundamental feature of monetary systems:

"For example, if Alice mistakenly pays Bob $100, an on-ledger remediation approach could simply void that transaction, leaving Alice and Bob the way they were before the transaction." (OSTP, 2022b, p. 22)

OSTP's decision to use a real-world example in the context of remediation demonstrates a deliberate emphasis on simplicity, aiming to make the concept of remediation accessible and universally understood, while keeping silent about more complex cases, such as fraud and cybercrimes. The next logical step, taken by the discourse, is to conclude that the necessity of remediation entails a centralized assemblage, where the government and intermediaries hold the authority to manipulate transactions (OSTP, 2022b, p. 23).

Additionally, remediation requires infrastructure capable of accommodating manipulation of ledger entries. However, blockchain technology, by design, lacks the mechanisms required for such interventions. As a result, OSTP proposes the implementation of remediation using off-chain transactions. The reliance on this type of remediation is designed to nullify transactions by entering new ledger entries that have the opposite effect of the problematic transaction, thereby nullifying it. However, OSTP admits that the critical issue in this case is how such a process would be governed (OSTP, 2022b, p. 23)

The discourse is silent regarding how centralized governance may undermine core benefits of digital assets like noncustodial wallets and offline transactions. Centralized remediation introduces delays, jurisdictional hurdles, and intermediaries that disrupt blockchain's promise of seamless, automated cross-border payments. As a result, OSTP's vision for dispute resolution mirrors traditional currency systems, relying on intermediaries and negating the very advantages digital assets are meant to provide.

As opposed to the discourse of the OSTP, conflict resolution is rarely mentioned by financial institutions and individual responders. This silence suggests that traditional conflict resolution is often taken for granted as a safety net to other forms of conflict resiliency governance methods. However, this overlooks the distinct challenges inherent in decentralized systems, where conventional safety nets, such as centralized arbitration or legal recourse, are insufficiently effective.

Problematization of Trust in Conflict Mitigation

A search in the coding of the comments of responders reveals that, whereas remediation is not mentioned even once in the responses, immutability shows up as a norm over 80 times. Almost all occurrences of the immutability concept are positive in sentiment, and position it as an established norm for respondents. As an example, a private citizen provides the following response to the question of CBDC resilience:

"A hack of the private ledger would give bad actors complete control. Using a public open source immutable protocol would give maximum security to our financial system." (FED-comments, 2022, p. 5/28)

This statement presents a comprehensive risk model for private ledgers, highlighting the threat posed by bad actors and the potential impact of losing control to such entities. Private ledgers are portrayed as inherently vulnerable, while public ledgers are characterized as nearly invincible, being associated with maximum security.

Immutability as a norm is also adopted by financial institutions. In response to a question about design principles to be considered by the federal reserve when designing digital currencies, MAG, a body representing merchants, clearly preferred immutability in connection with the prevention of fraud. The following is a characteristic invocation of the immutability norm in this context:

"A well-designed CBDC also could lower U.S. payment fraud. Leveraging the immutable ledger technology employed by cryptocurrencies, CBDCs can be resilient to payment fraud, especially if existing authentication and security features are embedded into the transfer process from the outset." (FED-comments, 2022, p. 9/263).

The statement identifies the same risk as does the discourse of respondents, invoking the blockchain principle of permanent and tamper-proof records through the term "immutable ledger". However, it overlooks potential challenges, such as governance issues, disputes requiring remediation, or systemic risk that could arise from centralizing control over an ostensibly immutable ledger.

Over the last decade, several conflict mitigation methods have emerged within the cryptocurrency ecosystem to build trust and reduce transaction risks. One widely used approach is the reliance on recommender systems and reputation scores to assess the credibility of potential transaction counterparts. Studies have shown that the reputation of e-commerce vendors is strongly correlated with consumers' purchasing decisions (Saxborn et al., 2024, p. 88). This use of reputation systems is not limited to consumers; lending organizations also leverage credit ratings to mitigate lender default risks. While reputation systems focus on preventing transactions from occurring with untrustworthy parties, the use of escrow services can mitigate conflict during the transaction process. Escrow services offered by major cryptocurrency exchanges and by specialized Escrow startups are used in transactions between buyers and untrusted sellers to ensure compliance with the agreed terms of the deal. The escrow service holds the funds paid until the transaction has been successfully completed or reversed. In the case of the

exchange of goods for cryptocurrency, funds are retained by a trusted third party until the buyer either accepts the purchase or exercises their right to return the goods.

While enabling transactions between untrusting parties, even in cross border deals, these services require a neutral third party to operationalize trust. The arrangement suffers from two major limitations connected to trust: first, the trusted third party must be neutral and honest. And second, it must be capable of competent arbitration or be trusted by both parties to be able to carry out the arbitration in a complex business setting. To counter the latter limitation some escrow services partner with specialized arbitrators and allow the parties to bring in their own arbitration service. Escrow.com offers governance of a process that involves arbitration services by members of the American Arbitration Association and other specialized companies (Escrow.com, 2024).

In cryptocurrency ecosystems, the challenge of ensuring an honest arbitrator is addressed through a technological framework that leverages the cryptographic capabilities of cryptocurrency infrastructures to facilitate multi-signature (multisig) transactions. This solution requires the buyer to deposit the funds into a multisig wallet shared with a seller and an arbitrator. The funds may be withdrawn only when two of the three owners sign a transaction that either completes the transfer or refunds the buyer. Multisig solutions reduce the amount of thin trust required in the third party because the arbitrator does not have control of the funds at any point in time. However, the risk of collusion between a party and the arbitrator persists, as does the risk of choosing an arbitrator that is incompetent to make the right choice.

The quest to eliminate a trusted third party in financial transactions produced the innovation of smart contracts that are pieces of programmed code that is stored and executed on a blockchain network. They operate based on predefined rules agreed upon by the involved parties. These rules trigger the execution of financial operations on the blockchain when certain terms are satisfied. Smart contracts work through a combination of cryptographic principles and decentralized consensus mechanisms. When parties initiate a transaction involving a smart contract, the code is deployed onto the blockchain. Upon deployment, the smart contract becomes immutable, meaning its code cannot be altered once recorded on the blockchain. Smart contract awaits input or triggers from external sources, such as specific events or data feeds. When these

conditions are met, the contract self-executes, autonomously carrying out the terms of the agreement. One of the weaknesses of smart contracts is their reliance on trustworthy data sources that feed real-life events into the system. This limits the scope of use cases, that can be covered, to those that can deliver machine-verifiable ontology. Companies, such as Chainlink, specialize in delivering reliable data to blockchains to feed smart contracts. They boast a variety of use cases from financial services to insurance and climate based smart contracts.

Immutable technology enforces contracts by making parties trust technologically defined rules and the technology itself. This willingness to be vulnerable to technology replaces the willingness to become vulnerable to the counterpart of the deal, thereby creating the possibility of low friction and even anonymous interaction. This trust is seen as a new type of "no-party" trust (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019, pp. 260–262).

While the OSTP list the decision to allow programmability as a technical design option of CBDC, this feature is linked to innovation and not to mitigation (OSTP, 2022b, p. 32).

In its analysis of the positive and negative aspects of smart contracts OSTP is mostly negative, stating that smart contracts may introduce systemic risk due to the interdependence that is likely to develop between contracts in the system which can cause unexpected feedback loops. The most notable objection that OSTP raises is that the immutability of smart contracts may reduce financial protections for consumers, thereby countering the purpose of smart contracts:

"Programmability might introduce challenges for stopping code execution in response to bankruptcy, recovery and resolution, or other court prescribed activities. The smart code execution is driven by standard external inputs and may have additional challenges for adjusting or accommodating "extraordinary" events such as bankruptcy or receivership, which could lead to violations of laws or regulations." (OSTP, 2022b, p. 33)

The discourse assumes that smart code execution is primarily driven by standard external inputs, suggesting an inherent reliance on predefined conditions and rules. This assumption implicitly frames programmability as inadequate for addressing dynamic, unforeseen circumstances, where legal or institutional discretion is necessary. The lack

of adaptability is problematized, casting doubt on the suitability of programmable systems for real-world financial ecosystems.

The disposition of respondents regarding smart contracts is almost entirely positive. Most herald the possibility of mitigating risk with smart contracts. (FED-comments, 2022, p. 6/122) However, a minority of respondents echo the OSTP in questioning the practicality of smart contracts and their ability to replace the writing and interpretation of contracts:

"Smart contracts tend to be anything but smart and are generally a solution in search of a problem. The vast majority of contract disputes take place due to conflicting interpretations—which no computer can definitively solve" (OSTP-Responses-1, 2022, p. 239).

The statement challenges the utility of smart contracts, labelling them as "not smart" It emphasizes the indispensability of humans in the process of conflict resolution and rejects the value of deterministic software in actual field settings.

As for financial institutions, including HSBC, Mastercard, JP Morgan, and Paypal, an analysis of all references to programmable money and smart contracts revealed positivity across the board, with JP Morgan pointing out that the potential of programmable money comes with a risk of eroding consumer confidence in the stability of value of a potential digital currency. The advantages of programmable money presented by institutions include the reduction of money laundering and fraud, replacing escrow services at a lower cost and the opportunity of developing innovative financial services. As is the position of most private respondents, there is a notable absence of reference to remediation outside of the scope of smart contracts (FED-comments, 2022, p. 9).

Thus, the question posed by OSTP regarding the type of remediation mechanism to be used in CBDC is largely ignored by all non-state respondents. All other actants in the assemblage, including digital assets themselves, tend to pre-mitigate fraud and error in the cryptocurrency ecosystem, rather than building institutions for remediation and restitution.

Conclusion – Applying WPR to Conflict Resolution

The 2016 DAO incident in the Ethereum ecosystem highlighted the tension between immutability and community governance in decentralized systems. The DAO, a smart contract-based investment fund, was hacked due to a loophole, resulting in the loss of a third of its funds. In response, Ethereum founder Vitalik Buterin proposed reversing the hack by altering the blockchain, a move adopted through a vote weighted by token holdings. This rollback split the community and led to the creation of two cryptocurrencies: Ether and Ether Classic. Debates following the fork revealed deep disagreements about the morality of immutability, with some framing blockchain as a social construct subject to democratic values, while others grounded their reasoning in legal frameworks like U.S. law. Although later incidents, such as the 2017 Parity wallet bug that froze $150 million in Ether, caused significant losses, no further remediation efforts were made. This marked a return to technological determinism, reinforcing immutability as a central principle. However, the incident proved that immutability is not absolute and can be reversed by human intervention. The DAO incident represents a central theme in the problematization of remediation versus immutability.

The government's problematization of trust in the cryptocurrency ecosystem, as reflected in the OSTP discourse, focuses on remediation as the central issue. OSTP assumes that a functional financial system must include mechanisms to rectify errors and settle disputes through corrective actions, such as voiding transactions or conducting restitution. It uses a strong necessity heuristic to impress the fact that the ecosystem must have the ability to roll back transactions. The OSTP positions remediation as essential to trust, operationalizing it as through centralized and permissioned governance structures. However, this problematization largely overlooks the challenges that remediation-based systems pose to financial certainty and overall trust as they render settled transactions contingent and undermine their finality.

In contrast, other stakeholders problematize trust through the lens of resilience, focusing on the ability of the system to inherently prevent conflicts. This perspective highlights mechanisms like reputation systems, programmable money and smart contracts, which are designed to minimize dependence on centralized remediation by reducing the need for human intermediaries in conflict resolution. This sentiment is

based on distrust in the current centrally controlled, intermediated ecosystem. Unlike the government, their discourse prioritizes the prevention of disputes over post-transaction corrections, framing resilience by immutability as the foundation for a sustainable and trust-generating ecosystem.

The rise of immutability as a dominant norm in the discourse of respondents is founded on the original idea of Nakamoto that it is a fundamental ingredient needed to create a "trustless" assemblage (Nelms et al., 2018, p. 21). This contrasts the government's reliance on mutability as the incumbent, well-established and self-evident norm that lies at the foundation of conflict resolution in monetary systems. Challenging mutability with its opposite gives rise to a completely new normative framework featuring technological determinism, finality of transactions, efficiency, and moral neutrality. This framework of norms reduces the need for human intervention in arbitration and resolution of conflict.

While these two positions are discursive binary opposites, institutional development and specifically the use of escrow services and the vote connected to the DAO incident indicates that analyzing them as mutually exclusive is not sufficient for understanding the complexities of trust and governance in blockchain ecosystems. These examples illustrate how elements of mutability and immutability can coexist within hybrid governance models, reflecting the need for both technological guarantees and human oversight in addressing disputes and maintaining trust. The technological implementation of digital money on blockchain does not ensure immutability, which depends on social and institutional constructions that make up the relations within the assemblage. For instance, if institutional arrangements were such that a vote by stakeholders to create transaction the negates a ledger entry, the immutability of the ecosystem would be compromised despite its blockchain-based implementation. However, while escrow services have become an increasingly prevalent feature in cryptocurrency ecosystems, voting for remediation has not emerged as a mainstream practice. This illustrates the fluid and transient nature of institutional structures in the emergent assemblage.

Chapter Eleven.

Ecosystem Autonomy

External Constraints

Elinor Ostrom argues that, for CPR ecosystems to thrive, the appropriators must have enough freedom from central authorities to design their own institutions and devise the rules by which they are governed. She describes several cases in which government intervention negatively impacted the resilience of CPR systems, citing the inability of external authorities to cater to the particularities of local settings (Ostrom, 2015, pp. 173–176). This has led her to formulate her seventh design principle:

> "The rights of appropriators to devise their own institutions are not challenged by external governmental authorities." (Ostrom, 2015, p. 90)

However, as Ostrom acknowledges, alongside the successes of autonomous CPR arrangements there are numerous examples in which autonomous self-governance has broken down under external pressures, especially in settings that feature large internal power imbalances (Dietz et al., 2003, p. 1908). Power imbalances often result in selfish behavior and free riding, which are further intensified by the scale and diversity of some CPR ecosystems. This can lead to intervention by external authorities, ranging from total takeover of governance to limited involvement guided by respect for local rules (Keohane & Ostrom, 1994, pp. 72–76). The 2008 financial crisis illustrates how self-governance can break down in large heterogeneous systems where power is unequally distributed and actors prioritize short-term gains over stability (Rajan, 2019, pp. 208–209). In response to the crisis, Congress passed the Dodd-Frank Act, a sweeping law designed to enhance financial stability and protect consumers. It established regulatory bodies to monitor systemic risk, restricted high-risk investments, and imposed strict reporting and transparency requirements on financial institutions (McLaughlin et al., 2020, pp. 5–8). This hybrid governance approach, where external authorities intervene while respecting market dynamics, reflects the idea that large scale self-governed systems may need to be balanced by external scrutiny.

By considering the state as endogenous to the cryptocurrency assemblage, its role shifts from that of an external regulating entity to an internal set of actors with powers to

regulate and enforce certain aspects of the ecosystem. The extent and nature of this power is the result of the network of relationships in the assemblage. However, this approach does not produce an entirely autonomous ecosystem. There are external forces that may potentially constrain the ability of internal actors to freely establish their own institutions; foreign governments and international organizations play a significant role in shaping the regulatory environment for cryptocurrencies, even if they are not part of the domestic regulatory framework. Organizations like the Financial Action Task Force (FATF) establish standards that influence the design of cryptocurrency institutions by setting compulsory guidelines for implementing measures to combat money laundering and terrorist financing, thus shaping the framework in which cryptocurrency development occurs (Carruthers & Arslan, 2019, pp. 529–530). While dominant governments significantly shape the policies and standards of these organizations, the latter maintain a notable degree of autonomy due to the principal-agent relationships that exist between the organizations and their constituents (Broome & Seabrooke, 2012, p. 3). By presenting their policies as "best practice" international organizations enable governments to frame compatible internal policies as compliance with external international standards (Broome & Seabrooke, 2012, p. 7).

In accordance with the conceptualization of actants as described by ANT, I categorize international organizations and foreign governments as exogenous to the U.S. cryptocurrency assemblage, as their interests are not directly translated into roles and responsibilities within the network. While they exert significant influence, they remain external because they do not actively participate in the internal processes that shape the U.S. cryptocurrency ecosystem. Instead, their influence is mediated through intermediaries, such as international agreements or guidelines, which are later interpreted and applied by internal actors. Despite the formal autonomy of international organizations, the United States retains significant influence by leveraging its historical role in constructing and managing the liberal international order. Since World War II, it has shaped a unipolar system aligned with its interests. However, this dominance is increasingly contested due to internal decline and rising demands for multipolarity. The 2008 financial crisis further undermined confidence in the existing order, prompting calls for systemic reform.

Autonomy and Trust in U.S. Leadership

I argue that the autonomy of the assemblage is dependent on trust in U.S. leadership, defined as the confidence in the nation's capacity to influence international regulatory frameworks, align foreign governments with these standards, and maintain the status of the U.S. Dollar as a global reserve currency and unit of account. The foundations of this leadership extend beyond government agencies and regulators; it encompasses the private sector and corporate entities as integral components of the state's capacity, rendering them part of the leadership mechanism. Consequently, U.S. leadership should be viewed as a feature of the entire assemblage, where public and private actants, including the U.S. dollar, collectively contribute to exerting regulatory influence on both domestic and international stages. When trust in this leadership is strong, internal stakeholders are confident that the United States can set global and domestic standards, ensuring its autonomy from external influence.

Conversely, when trust in U.S. leadership erodes, internal stakeholders may seek guidance and authority from foreign states and international organizations. This reliance on outside entities undermines the autonomy of the domestic ecosystem, limiting its capacity to develop self-governance. The erosion of trust in U.S. leadership can lead to reliance on external entities across all actants within the assemblage, as the government relies on international standards to promote its internal agenda in the assemblage. While this increases its capacity to set internal rules, it compels the government to align with global norms, thereby diminishing the ability of the ecosystem to craft independent, localized institutions. Financial firms and private actors, unconvinced of the U.S. government's ability to set and maintain global regulatory standards, may seek more favorable environments in jurisdictions that allow greater regulatory leniency. This behavior constrains the ability to set rigid rules in the assemblage that significantly diverge from international standards and practices. The investments that private entities make in relocating away from the reach of United States regulations, signify the confidence that the United States is unlikely to successfully impose its rigid standards on other jurisdictions and international organizations. This dynamic reflects a shift in the ecosystem's regulatory power away from the local level and towards international influence, further reducing autonomy. If one assumes that the United States can exert total leadership, thereby homogenizing the regulatory landscape, there would be no incentive for actors to pursue relocation.

Government Problematization of U.S. Leadership

In the objectives part of the executive order's policy section, the President declares the goals of the United States with respect to its global leadership position. Each of the objectives begins with the term "We must…", conveying a sense of urgency to respond to advances in digital and distributed ledger technology for financial services. Reinforcing U.S. leadership is one of the six goals.

"We must reinforce United States leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets." (Biden, 2022, p. 14144)

The description of the goal continues by outlining the logic that drives U.S. leadership, based on two foundations: First, The United States must lead the global financial system to set standards that *"Promote: democratic values; the rule of law; privacy; the protection of consumers, investors, and businesses; and interoperability with digital platforms, legacy architecture, and international payment systems."* This establishes the role of the United States as the entity responsible not only for the smooth operation of the financial system but also for its sound moral values and fairness. The second foundation underlying U.S. Leadership logic is the special national security and economic benefits that the United States reaps from the central role of the U.S. Dollar and its financial institutions in the global financial system:

"The United States derives significant economic and national security benefits from the central role that the United States dollar and United States financial institutions and markets play in the global financial system. Continued United States leadership in the global financial system will sustain United States financial power and promote United States economic interests." (Biden, 2022, p. 14144)

The statement links the role of the U.S. dollar directly to national security, suggesting that the dominance of the dollar is not just about economics, but about protecting national sovereignty and maintaining security. The repetition of "United States" normalizes the nation as the focal point of importance, emphasizing that its leadership and dominance in the global financial system are both natural and necessary for economic stability and security. This emphasis on United States centrality implicitly marginalizes global equity and the interests of other nations.

While the president seeks to maintain this centrality, he acknowledges the need for international cooperation, reflecting the tension between autonomy and dependence on multilateral institutions to ensure a level playing field that it cannot fully enforce:

"Technology-driven financial innovation is frequently cross-border and therefore requires international cooperation among public authorities. This cooperation is critical to maintaining high regulatory standards and a level playing field." (Biden, 2022, p. 14149)

The statement positions international cooperation as an imposed limitation, stemming from the cross-border nature of technological innovation, rather than an opportunity to collaborate. This framing downplays the potential for international collaboration as a positive and productive opportunity for shared progress. It portrays cooperation as a necessary response to mitigate risks and impose U.S. regulatory standards.

A further key objective, designated by the President, is the ability to impose sanctions on foreign nationals and countries that violate U.S. laws by engaging in illicit activities, including money laundering and terrorism financing. (Biden, 2022, p. 14144). The identification of sanctions as a necessary control demonstrates that the United States government works under the assumption that, if it is to be a global leader, it must retain the power of coercion in the global arena.

The president goes on to construct a comprehensive risk model based on threat, vulnerability, impact, and mitigation to assess how potential threats could exploit vulnerabilities causing harm (impact). He then identifies mitigations to reduce or prevent the risk:

"Illicit actors, including the perpetrators of ransomware incidents and other cybercrime, often launder and cash out of their illicit proceeds using digital asset service providers in jurisdictions that have not yet effectively implemented the international standards set by the inter-governmental Financial Action Task Force (FATF) .... When digital assets are abused or used in illicit ways, or undermine national security, it is in the national interest to take actions to mitigate these illicit finance and national security risks through regulation, oversight, law enforcement action, or use of other United States Government authorities." (Biden, 2022, p. 14144)

The risk model presents national security as a central norm, threatened by illicit use of digital assets. It frames security as a collective U.S. interest, linking global financial stability to compliance with U.S.-aligned regulations. Illicit actors in non-compliant jurisdictions, especially those ignoring FATF standards, are portrayed as threats requiring strong U.S. leadership. This reinforces a global power dynamic where security concerns justify extending U.S. regulatory influence. However, the text's alignment with FATF standards creates tension, as the FATF now includes countries like Russia and China (Pavlidis, 2021, p. 7).

To balance between the risk posed by the irresponsible jurisdictions and the imperative of building operational payment systems, The Office of Science and Technology Policy (OSTP) proposes an institutional arrangement based on technical interoperability, framing it as an "arms-length" relationship between ecosystems:

"Here, interoperability is not the same as integration, as the former refers to systems that can talk to each other, while the latter refers to more direct access to other systems." (OSTP, 2022b, p. 15)

While integration allows software to access the data of remote systems, interoperability refers to the ability of systems to communicate and exchange information while remaining separate and independent. Thus, each system retains control over its own processes, rules, and data, but can share or communicate with other systems using common standards or protocols. Trust in an interoperable system is more conditional and localized than trust in integration. Actors rely on the agreed protocols to ensure transactions are carried out with integrity and consistency rather than relying on remote systems.

The design choice considered by the OSTP is whether to build a "more" or "less" interoperable CBDC. A central inhibiting factor to increasing the level of interoperability is the need to align governance and standards:

"...governance and standards alignment can provide a key roadblock to more interoperability. A less technically interoperable CBDC system may not have to deal with as many obstacles to achieve high functionality as expected." (OSTP, 2022b, p. 16)

The OSTP's cautious approach to interoperability underscores the trade-off between maintaining control and embracing the benefits of interconnectedness with entities that do not fall in line with United States standards. The limited conditional trust in external actors, not enrolled in the cryptocurrency assemblage, drives the design and creation of interoperability institutions. Reciprocally, the emergence of interoperability as an institutional arrangement shapes trust by making it more conditional and localized. Trust in remote, foreign entities is replaced by trust in protocols that define the boundaries of remote relationships.

Non-Governmental Problematization of U.S. Leadership

Despite the morally questionable, self-serving interoperability considerations advanced by the President, individual respondents do not challenge the motivations behind the norms of U.S. financial leadership or the central role of the U.S. dollar. A minority of the respondents argue that maintaining U.S. leadership is dependent on being attentive to external trends and policies of other countries:

"If other nations with stable central banks issue CBDC then United States has no choice but to join the band to stay competitive and keep dollar as dominant currency for trade and commerce. United States rather lead the pack then lag. Early bird gets to define the rules of the game." (FED-comments, 2022, p. 4/33)

This statement underscores the limits of US leadership, arguing that, to maintain its leadership role, the United States is compelled to "join the band". The statement portrays the U.S. as both an agent and a subject in the global financial order. While it has the capacity to lead, it must comply with global trends. The tension between agency and contingency represents an intricate power dynamic where leadership is not derived from unilateral actions, but from a policy based on the consideration of the objectives of others.

Nevertheless, most individual respondents adopt a more simplistic view, asserting that the United States must unilaterally exercise its financial leadership, rather than falling in line with global trends as is exemplified in the following response to the question of how foreign government decisions should influence those of the United States:

"They shouldn't. We are a sovereign nation and the world leader. The world will accommodate the United States and our vast economy. We should never act to accommodate other nations. They should act to accommodate our economy."

In this context, world order is portrayed as absolute and uncontested, with the United States depicted not only as a global leader but as a dominant force vested with agency and power. This implies that the assemblage is fully autonomous, wielding the power to influence others to align with its internal decisions. Like many similar responses the statement overlooks the complexities of global governance and any interdependencies between the assemblage and external actors.

To emphasize autonomy, a significant number of responses invoke an old parenting heuristic encouraging children to think for themselves and not jump off a bridge just because their friends did:

"We shouldn't let countries with less freedom convince us to have less freedom and privacy. Just because one country jumps off the CBDC dystopia bridge doesn't mean we have to." (FED-comments, 2022, p. 1/130)

This statement also invokes an availability heuristic, suggesting that following the examples of countries with less freedom and privacy leads to dystopian scenarios. This sentiment appears in numerous other quotes which explicitly name China as the culprit that leads the race to launch a CBDC (FED-comments, 2022, p. 2/53). Respondents advocating for full U.S. economic autonomy ignore the digital euro and the ECB's progress, focusing instead on China's authoritarianism as a fear-based justification. This absence suggests a preference for a simplified, polarized narrative over engaging with global complexity. As a result, the discourse offers no institutional proposals and reflects distrust not only in foreign actors but also in the U.S. itself to sustain global leadership.

The traditional banking sector is fully in line with the cautious approach to competition by other countries, suggesting that the Fed should carefully observe the decisions and policies of other nations before deciding. The following comment by Mastercard is representative of this sentiment:

"The Federal Reserve should monitor the decisions by other OECD nations and evaluate whether the development of a U.S. CBDC would be important to maintaining

the preeminence of the U.S. financial system and sustaining the role of the U.S. dollar as the world's reserve currency." (FED-comments, 2022, p. 9/25)

The statement acknowledges the influence of other OECD nations, positioning them as significant actors whose decisions shape the considerations of the Fed. However, this influence is contextualized within a competitive framework where the U.S. seeks to preserve its financial pre-eminence. The statement's focus on OECD nations reflects a prioritization of actors whose decisions align with shared economic and governance principles, while implicitly positioning economies such as Russia and China as less relevant to a U.S. decision.

Some traditional financial institutions argue that trust in U.S. leadership is rooted in structural factors rather than specific decisions. The Bank Policy Institute highlights the norms and heuristics that underpin this trust. The strength and scale of the economy, combined with the stability of its financial markets, foster confidence in the centrality and reliability of the United States as an actor in the global arena. Additionally, the ease of converting U.S. dollars to other currencies and the liquidity of U.S. Treasury securities serve as practical decision-making shortcuts for global market participants (FED-comments, 2022, p. 9/164). This attribution of trust to structural factors, though shaped by the inherent opposition by banks to a potential CBDC launch due to concerns over disintermediation, supports the view of some individual respondents that the United States should preserve its independence in decision-making and resist influence from other nations.

This rationale is also picked up by senior Fed economists in a document titled "Implications of a U.S. CBDC for International Payments and the Role of the Dollar". The document addresses the influence of the potential decisions by other countries on the international role of the Dollar. It concludes that even if foreign governments were to make decisions threatening the central role of the Dollar, the United States will have time to react due to the slow nature of the change.

"The driving factors for the popularity of dollar assets as store of value are based on the ample supply and liquid market for U.S. Treasuries and other debt and the long-standing stability of the U.S. economy and political system. If other jurisdictions were to provide similar conditions, then the dollar could lose out to these currencies. These trends, however, move slowly." (Flemming & Judson, 2024).

The statement constructs the dollar's dominance through a rational lens, tied to the structural advantages of the U.S. financial system and political stability. By focusing solely on economic factors such as liquidity and market size, it marginalizes the potential role of ethical leadership and geopolitical context in sustaining the dollar's pre-eminence. This omission downplays how values-driven governance might influence systemic trust, instead framing the U.S. role in global finance as contingent on its performance, rather than as a product of its legal and moral authority.

WPR analysis of Autonomy in the Global Arena

The problem of trust in the cryptocurrency ecosystem, as represented in the discourse, centers on the erosion of confidence in U.S. global leadership. While there is consensus on the necessity of U.S. leadership, there is divergence in perspectives on whether it can be maintained. A weakening of confidence in the ability of the United States to set global standards drives internal stakeholders to turn to foreign governments and international organizations or, in some cases, to move operations to jurisdictions offering more regulatory leniency. While the government is constructing this question as a dilemma, all other discourses are in consensus that the decisions of others should not automatically dictate the policies of the United States. Some stakeholders, particularly traditional financial institutions, argue that while the U.S. should monitor global trends, it should use these observations to inform its own independent strategy rather than necessarily complying.

The representation of the problem is underpinned by deep-seated norms and heuristics that emphasize the historical and structural dominance of U.S. leadership. Trust in U.S. leadership is tied to the unipolar order in which the United States is world hegemon. U.S. leadership is normalized as essential, not only for financial stability and security but also for the preferred status of the United States. Justification for this normalization is rooted in the norms of democracy and the rule of law, reinforced by structural factors like the historical scale and stability of the U.S. economy. Additionally, this trust is shaped by historic heuristics, by which the post-World War II dominance is framed as a cornerstone of global stability and embeds the recognition that U.S. leadership is both natural and necessary. This framing is further reinforced by contrasting American liberal leadership with perceived authoritarian threats, particularly China’s CBDC development, which is presented as a danger to freedom and privacy.

The balance between the autonomy of the United States and its leadership role in international payment systems has led to the valorization of interoperability—a technical, arm's-length institutional arrangement designed for interconnectivity with external systems while minimizing the need to place trust in foreign jurisdictions. This is achieved by shifting trust to the protocols that define the rules of interaction. I argue that the United States model of participation in the effort to provide solutions for the global payment system by the BIS Innovation Hub constitutes a form of "political interoperability". This model transfers trust from the BIS Innovation Hub itself to carefully defined operational protocols between the Federal Reserve, the BIS, and other central banks, ensuring that the United States retains control over its participation in shaping the future of finance. This institutional arrangement is specifically designed by the Federal Reserve to preserve U.S. sovereignty while allowing for the close monitoring of global trends and the continued assertion of its leadership in global finance.

Chapter Twelve.

Conclusions

Reframing Society

When Simmel conceptualized trust in money at the turn of the twentieth century, asserting that it extends beyond interpersonal trust to become a claim on society, he depicted that society as a community obligated to uphold that claim. However, it seems that Simmel himself understood that the term "community" is insufficient to capture the object of trust that enables money to perform its functions, perhaps feeling the need to dissect it further by referring to it as a socio-political system (Simmel et al., 2011, p. 177). I propose that the emergence of cryptocurrencies shifts these dissection efforts toward perceiving society not as a socio-political construct, but as a socio-technical assemblage.

Thus, while Simmel's notion of money as a claim on society remains intact, the analytical tools used to examine the composition of that society require revision. Instead of framing society solely as a system of political and social structures, the analytical emphasis now shifts toward a distributed network of hybrid formations, where political authority, algorithmic governance, and decentralized economic actants are deeply entangled in sustaining monetary legitimacy**.**

In this sense, the introduction of cryptocurrencies is not a fundamental change in the composition of the social system. Society has always been a socio-technical construct, with money historically embedded in technological infrastructures, from early tally sticks and metal coins to modern digital banking systems. However, the abundance of technology shifts attention toward the increasing importance and agency of non-human actors in the production of trust.

To support this shift in emphasis, I use Actor-Network Theory (ANT) and the Institutional Analysis and Development (IAD) framework to examine how cryptocurrencies reshape the socio-technical assemblage underpinning money's

legitimacy. ANT captures the fluid, relational nature of money but lacks a clear model for how trust solidifies into durable institutions. In contrast, IAD offers a structured view of institutional resilience but overlooks the dynamic social and technical mediations highlighted by ANT.

Since decentralized financial institutions are neither entirely stable nor purely emergent, a synthesis of these perspectives is necessary, integrating IAD's structured institutional analysis with ANT's attention to ever-evolving sociotechnical configurations. However, such a synthesis between two disparate ontological approaches is theoretically and practically problematic. In seeking to reconcile the two approaches, I have attempted to navigate the tension between analyzing the ecosystem as a nascent ever-unstable assemblage and the view that the cryptocurrency ecosystem is an evolutionary phase of an established, longstanding monetary system. Additionally, this thesis aims to strike a balance between ANT's purely descriptive approach, which prioritizes allowing the network to articulate its own dynamics, and the need for an explanatory framework that accounts for how trust becomes problematized and negotiated within the assemblage

Building on this theoretical synthesis, the remainder of this chapter revisits the research questions outlined in the introduction, synthesizing the empirical findings to produce analytical insights. First, I examine the constitution of the assemblage and its structural characteristics, outlining the key actants and institutional arrangements that shape its formation. Next, I explore the dynamics of trust, analyzing how trust is problematized within the assemblage and identifying the patterns that emerge in response. In doing so, I assess the interplay between trust and institutional development, demonstrating how these evolving mechanisms serve as the foundation that binds the assemblage together. Finally, I consider the implications of these findings for the long-term stability of the cryptocurrency ecosystem, evaluating whether its discursive construction fosters resilience or fragility. The chapter concludes with reflections on the theoretical frameworks employed in this study, discussing their contributions and potential refinements for future research of this type.

The Constitution and Structure of the U.S. Cryptocurrency Assemblage

On the 5th of November 2024 Donald Trump was re-elected as President of the United States, a development met with explicit satisfaction of the leaders in the cryptocurrency industry who contributed hundreds of millions of dollars to his campaign. The cryptocurrency industry also boasts its role in the election of 274 "pro-crypto" lawmakers to Congress (Schouten, 2024). While "pro-crypto" policies lack a precise definition, they generally emphasize free-market ideals, decentralization, and a "laissez-faire" approach to financial and monetary innovation aimed at advancing the industry. In announcing his pro-crypto agenda, Trump pledged to make the United States a "Bitcoin superpower" (Kruesil, 2024). This vision suggests that, rather than issuing a CBDC or developing a national digital asset ecosystem, the President intends to assert dominance in the global cryptocurrency ecosystem. Consequently, his statement invites a critical examination of whether a U.S. cryptocurrency assemblage truly exists, as its existence is fundamental to justifying its analysis.

Ostrom presumes the existence of CPR ecosystems, treating them as an ontological reality to be analyzed. Conversely, ANT questions the existence of an assemblage, conceptualizing it as an epistemological construct, collectively constituted through ongoing processes of social construction, which is termed translation. If this translation process is weak or fails, the assemblage may dissolve, highlighting its contingent and dynamic nature. Based on this theoretical approach, the discourse analyzed in this thesis demonstrates that the existence of a U.S. cryptocurrency assemblage must be affirmed. The structure of the U.S. cryptocurrency assemblage is constituted through a dynamic network of actants, institutional arrangements, and negotiated roles, as evidenced in the ongoing translation processes captured in the corpus.

The discourse begins with the U.S. President, who positions himself as the prime actant and initiates translation, mobilizing others into the assemblage. Actants are onboarded through ongoing processes of problematization, interessement, and enrollment, forming a dynamic network. Individuals are framed both as vulnerable consumers and empowered partners with agency in design. Intermediaries are enrolled as state collaborators focused on facilitating transactions, rather than creating money or credit as in the traditional financial system. Their role remains open to negotiation as they pursue new business models and redefine their responsibilities.

The role of the state is negotiated through translation, leading to its fragmentation into four actants: the government, the Federal Reserve, regulatory agencies, and the judiciary. This fragmentation, evident in the corpus and necessary for analysis, reflects Callon's (1998b, pp. 16–19) concept of disentanglement, which avoids treating the state as a singular actor. Respondents illustrate this by rejecting the FED while affirming the judiciary's role in stabilizing the assemblage within socially recognized boundaries.

Despite the sentiment of many responders that the state has no business intervening in a global borderless market, the boundaries of the United States cryptocurrency assemblage are distinctly evident within the analyzed discourse. Commercial actants express their dilemma of either maintaining compliance with U.S. regulatory agencies or withdrawing from U.S. regulatory oversight. Other actants seek the protection of state actants from fraud and unfair competition, by establishing strong spatial and relational ties with actants in the U.S. cryptocurrency assemblage. However, these boundaries are neither rigid nor binary, but remain fluid and role-contingent, shifting as actants negotiate their positions within the assemblage. Role contingency refers to the conditional inclusion of an entity within a boundary, determined by the specific function it performs. As a result, actants may be simultaneously included in certain capacities and excluded in others. This is evident in the contrasting roles assigned to regulatory agencies, which are internalized for sanctioning rogue actants but excluded from monitoring them. Such tensions render the binary distinction between the state as either endogenous or exogenous increasingly untenable, as its role is continuously negotiated through interaction. An analysis grounded in Ostrom's seven design principles indicates that state actants frequently transcend the position of external regulators and should be conceptualized as endogenous components of the assemblage.

Intertwined with the mobilization of actants, the assemblage, a set of institutional arrangements emerge, designed to operationalize the collective vision of a functioning ecosystem. These are assemblages that function as socio-technical mechanisms, integrating technological, normative, and organizational components to perform specific functions and regulate behavior within the ecosystem. While these institutional arrangements are not unique to the U.S. cryptocurrency assemblage, their operational rules emerge through the ongoing negotiation and translation processes that shape the U.S. cryptocurrency assemblage.

Some institutional arrangements are socially transformed as they become translated within the assemblage. This is apparent in the attempt to create a role for traditional bank deposits and avoid disintermediation. The resulting arrangement, described in Chapter Seven, is the adaptation of traditional bank accounts through the tokenization of deposits on a blockchain, combining conventional banking with blockchain security and efficiency. This adaptation enables banks to maintain their role as financial intermediaries and continue supplying liquidity to the market. Other institutional arrangements are eliminated in the translation process. This is exemplified by the rejection of algorithmic stablecoins evidenced in the Lummis-Gillibrand bill referenced in Chapter Seven. This bipartisan legislative response to stablecoin failures signals a broad consensus within the assemblage, fostering a balance between innovation and risk mitigation. Retail CBDC is another example, widely rejected by non-state discourse and framed by state actants as contingent on the support of constituents.

These cases illustrate how institutional arrangements within the U.S. cryptocurrency assemblage discursively emerge or disintegrate through negotiation and adaptation, rather than being imposed as static structures. Ostrom perceives this as a crucial process of rulemaking that adapts institutions to local conditions as outlined in Chapter Six. From an ANT perspective, these institutions operate as actants, engaging in the network through translation processes that continuously reshape them. Thus, both ANT and Ostrom reject static institutional structures, emphasizing instead the dynamic, iterative processes through which institutions are shaped, maintained, or transformed by ongoing interactions among actants.

Trust Dynamics in Hybrid Institutions

Researchers across various disciplines characterize the impact of blockchain technology as a disruptive shift in the fundamental dynamics of trust. The transition is described as a shift from trusting intermediaries to reduce risk and manage trust, to trust in digital systems and algorithms (Fenwick & Vermeulen, 2019, p. 11). Others view this technology as an enabler of trust in the outcomes of institutions without the need for trust in the participants of these institutions. This is achieved through blockchain's ability to ensure institutional reliability via deterministic computation, allowing trust in institutional outcomes without necessitating trust in the individual participants (Davidson et al., 2017, p. 5; Werbach, 2018a, Location 891).

The current empirical investigation into the discourses of actors provides a constructivist affirmation to the ontological and theoretical claims made by De Filippi et al. (2020, pp. 7–8), that the subjects of trust and distrust in the context of cryptocurrencies, are socio-technological assemblages, referred to as blockchain-based networks or solutions. However, as the findings reveal, not all the institutional arrangements in the context of cryptocurrencies are blockchain-based. This is exemplified by the institutional arrangement of Zero-Knowledge-Proof (ZKP) discussed in Chapter eight. This arrangement is potentially a critical solution to the problem of the balance between the need to prevent crime and the right to privacy. Although ZKP relies on cryptography, it operates independently of blockchain technology. Furthermore, some institutional arrangements that incorporate blockchain cannot be considered blockchain centric. A case in point is blockchain-based voting, where blockchain assures the integrity of the vote, but the institutional framework primarily revolves around voter identification and representation rules that are organizational rather than technological in nature.

De Filippi et al. distinguish between trust and confidence, following sociological interpretations by Luhmann (2000, p. 3), by which trust involves a willingness to expose vulnerability and the expectation that others will act in one's best interest, whereas confidence is based on predictability and perceived stability. Blockchain enhances confidence through deterministic computation, reducing reliance on trust. I contend that this distinction is problematic because the willingness to expose vulnerability, which is central to the definition of trust, also characterizes confidence in practice. Both trust and confidence influence the degree to which actants are willing to accept risk, making the distinction less useful for analyzing trust dynamics. This is evident in the empirical findings, where no minimal threshold of confidence was identified as a prerequisite for institutional arrangements to be deemed acceptable.

Given this analysis, trust remains a disposition to willingly expose vulnerabilities with the goal of potential benefits or risk mitigation. It is a trust in hybrid assemblages of human and technological components with varying levels of predictability. This predictability does not correlate with the amount of human versus technological agency in the assemblage. For instance, the U.S. judicial system is an institution that is mostly human in its composition, yet it is perceived as highly predictable and trustworthy due to established legal precedents and the rule of law. The framework of due process,

trusted by respondents, fosters a sentiment of certainty and trust in a fair outcome as demonstrated in Chapter Nine. In contrast, algorithmic stablecoins, which are technologically driven and operate with minimal human intervention, exemplify an institution that, despite its reliance on deterministic smart contracts and autonomous mechanisms, remains untrustworthy in the minds of actants. The collapses of TerraUSD and other algorithmic stablecoins demonstrate that even highly automated financial mechanisms can fail when affected by unforeseen market behaviors, and vulnerabilities in code. These failures contribute to the development of heuristics that foster mistrust in technology.

Given that the level of automation, and the resulting immutability, is not a determining factor in the trust and acceptance of institutional innovation, this prompts a deeper examination of the norms and heuristics that shape the institutional arrangements. Empirical evidence highlights human discretion in critical decision-making processes as a key factor in fostering trust, ultimately shaping institutional outcomes. Human backstops that enable intervention, particularly in times of crisis, are key in the institutional landscape around governance, conflict resolution, monitoring, and sanctioning. In these areas, where automation has the highest impact, the human factor is inserted at the end of the process to override potential vulnerabilities due to over-automation. This is exemplified by the DAO crisis where it was proven that even the foundational immutability of blockchain can be negated by humans when called for. In the context of the sensitive subject of sanctioning, the involvement of courts and due process ensures that penalties are not purely algorithmic but reflect broader considerations of fairness and proportionality. A notable exception to this arises from the extreme distrust of the FED, promoting the will of many individuals to impose a hard-coded limit on money supply in the form of tangible backing to a potential CBDC and other stablecoins.

While immutability does not foster trust or certainty, trust in decentralization is integral to shaping institutional arrangements in the assemblage. As a norm, it underpins the formation of liquidity pools, zero-knowledge proofs, governance by voting, and transaction validation, all of which have gained wide consensus. These mechanisms align with the prevailing discourse favoring reduced reliance on centralized institutions and the distribution of authority across a network. By preventing single points of control, decentralization mitigates risks associated with arbitrary decision-making.

Trust in majority decision-making emerges from a heuristic that prioritizes collective, independent governance over centralized authority. Decentralization is not just a feature of blockchain: it is a governance architecture, also apparent in the RFC process described in Chapter Two. The FED decision to make CBDC contingent on public support is one of decentralization's off-chain forms.

The prioritization of decentralization, however, does not imply a commitment to democratic governance, nor does the empirical evidence suggest that democracy itself is a primary driver of trust in institutional arrangements. While decentralization ensures that decision-making power is dispersed, it does not guarantee equal participation or collective control. Most cryptocurrency governance models examined in the assemblage operate under structures that privilege financial stake or technical expertise over broad democratic participation. Furthermore, the preference of many respondents to trust corporate governance over state control amounts to rejection of the democratic system in favor of corporate authoritarianism.

Respondents' discourse indicates that trust in governance does not stem from open participation but from perceptions of resilience, stability, and self-interest. One of the clearest examples of the rejection of democratic governance as a source of trust is the preference for stablecoins over CBDCs. Despite being issued by private corporations with centralized governance structures and profit-driven motives, stablecoins are still perceived as more trustworthy than a government-backed CBDC. The preference for stablecoins is not rooted in democracy but rather in market-driven competition. Respondents prefer to be free to choose between various non-democratic solutions over the democratic accountability of public money. This reinforces the notion that there is a disconnect between the democratic system of the United States and the respondents' framing of the state as a coercive actor that operates against public interests.

These trust-driven dynamics develop within a broad context of general distrust, as outlined in Chapter Five. Respondents distrust state institutions, particularly the Federal Reserve, viewing them as coercive actors. The government frames the public as helpless consumers needing protection while problematizing trust in decentralized finance as a risk to stability and security. Financial institutions face skepticism from both regulators and responders as all sides navigate the prospect of disintermediation. This mutual distrust amplifies key tensions described in the context of each of Ostrom's

seven principles, including the conflict between decentralization versus state control, privacy versus financial surveillance, and liquidity versus stability.

Discourse analysis suggests that trust emerges from institutional responses to these perceived tensions between various competing actant expectations. Mitigating the tensions requires institutional mechanisms that either balance or disrupt them to foster trust. Some institutional arrangements seek to balance between the extremes of the tension, carefully crafting an enforceable compromise that is acceptable across the assemblage. This is exemplified by tiered monitoring, discussed in Chapter eight, in which the right of government to use surveillance is dependent on transaction amount limits or activity thresholds of the transacting parties. This allows the government to mitigate illicit finance while preserving the privacy of most individuals.

Other institutional arrangements seek to disrupt the tension by innovation that discovers a non-zero-sum solution to the tension. Liquidity pools disrupt the liquidity–stability tension, described in Chapter Six, by reducing the central reserve requirements that are crucial for the stability of a monetary system. This institutional arrangement increases liquidity by allowing decentralized participation in reserve allocation, while enhancing stability by distributing risk across a broader network of liquidity providers rather than depending on a centralized point of failure.

To conclude, trust in specific norms drives the institutional development that addresses the tensions arising in the problematization of the assemblage. These institutional innovations either balance competing demands or disrupt tensions by introducing new solutions that reconfigure the trust dynamics within the system. By resolving or reshaping these tensions, institutional innovation shapes actants' perceptions of the assemblage and influences which norms and heuristics take precedence. This reciprocal relationship between trust and institutional development underscores how evolving governance structures and technological innovation continuously redefine the landscape of the assemblage. As the legitimacy of institutions evolves, it reinforces or challenges existing trust heuristics, thereby shaping the trajectory of future innovations and governance norms.

Implications for Long-Term Stability

Elinor Ostrom's research focuses on analyzing the success or failure of CPR arrangements. However, she does not explicitly provide a precise definition of what constitutes this success that she terms "long-enduring CPR arrangements". This terminology implies a forensic approach, where success can only be recognized in hindsight (Ostrom, 2015, pp. 27–28). While the term: "long enduring" may suggest stability, Ostrom does not equate success with permanence. Rather, she emphasizes institutional agility in the face of changing conditions as a factor in the endurance of ecosystems (Ostrom, 2015, p. 93).

This perspective aligns with ANT's concept of ongoing translation, where assemblages must continuously renegotiate relationships to remain viable (Callon, 1984, p. 224). Viability does not mean stability but rather a continuous process of punctualisation, by which institutional arrangements temporarily bind together to form coherent actant while remaining susceptible to change and contestation. This binding becomes apparent when the actant is perceived in terms of its functions rather than its internal mechanisms (Law, 1992, pp. 5–6). I contend that the punctualisation of the U.S. cryptocurrency assemblage will be established as long as it is accepted by actants as a monetary system that manages digital coins, used as units of account, a store of value, and a medium of exchange. At that point, its role as financial infrastructure will be taken for granted, with its internal complexities black-boxed into a singular, accepted system (Latour, 1987, pp. 122–123).

Despite the growth of cryptocurrency in the United States, this temporary and contingent state of stability has not been achieved. Cryptocurrency adoption has yet to reach a level where its role as a monetary system is taken for granted. Questions regarding its legal classification, institutional legitimacy, and long-term viability remain prevalent, impeding it from becoming a practical currency. Without a widely accepted and enduring framework, that aligns a critical mass of actants, the U.S. cryptocurrency assemblage remains an evolving and contested space rather than a fully punctualised network.

ANT emphasizes the dynamic binding of humans and non-humans into what is termed the "means to produce the social", that function as mediators and intermediaries within a network. Mediators actively transform and shape interactions, while intermediaries

produce deterministic outputs without altering relations in the assemblage. These means are constructed actants in the assemblage, serving as the "glue" that binds the assemblage together. Mediators contribute to the durability of the network, constantly maintaining its relationships by adapting them to changing conditions. In contrast, intermediaries stabilize these relationships by producing black boxes that render complex processes well-defined through their inputs and outputs, making them appear self-evident and unquestionable. These constructions are not pre-existing actors who link up to constitute an assemblage. They are a transient product of the ongoing translation taking place within the assemblage (Latour, 2005, p. 42).

I equate the institutional arrangements described in this thesis with Latour's "means to produce the social". However, I found it difficult to separate them into mediators and intermediaries without rendering my analysis very difficult to comprehend due to the high level of detailed deconstruction required. I believe that this type of deconstruction can be very useful in understanding why human trust requires certain elements to be stable intermediaries, while depending on the continuing contestation and contingency of others. On the macro level, the reliance on ongoing flux is evident in the areas where discourse emphasizes the need for competition. This is particularly apparent in the discourse regarding competition between different forms of stablecoins, where diversity and continuous innovation foster trust by ensuring that stakeholders can shift between alternatives when necessary.

A survey level view of institutional development in the context of Ostrom's seven design principles reveals a mixed level of contribution to the durability of the assemblage based on the amount and quality of the innovation and adaptation taking place in the analyzed discourses. While some design principles exhibit institutional diversity and an effort to bridge the tensions, others lag. The tension between privacy and surveillance discussed in the context of monitoring remains unresolved and almost unaddressed. Technological solutions, such as ZKP are not mature. There is a lack of alignment between actants that manifests in the unwillingness of respondents to compromise on privacy. Graduated sanctions and conflict resolution also lack innovative social and technical solutions. Instead, they fall back on institutional arrangements from the traditional financial ecosystem. These fallbacks are often highly centralized and impractical in the context of digital coins, suffering from several impediments; Boundary issues weaken enforcement beyond U.S. jurisdiction,

imbalanced human-technological roles reduce trust in both efficiency and fairness, and over-reliance on centralized authority clashes with the decentralized ethos, eroding institutional trust.

The discourses reveal two distinct forms of distrust: interpersonal distrust, exemplified in the profound skepticism toward the Federal Reserve and financial institutions, while institutional distrust which is evident in the rejection of algorithmic stablecoins and central bank digital currencies. However, much of this distrust does not work to weaken the durability or the stability of the assemblage. Blockchain itself is a prime example: originating from distrust in centralized governance and intermediation, it establishes an alternative solution for the verification of transactions. Thus, it establishes an institutional infrastructure that enhances stability through deterministic protocols and increases durability by enabling continuous adaptation of governance without reliance on any single authority.

The abundance of institutional development in the U.S. cryptocurrency assemblage suggests that its long-term stability and durability rely on its capacity to institutionalize ongoing tensions rather than resolve them. However, institutional development is not sufficient; this movement must be directed toward achieving the goal of creating an ecosystem that functions as an alternative to traditional money. The current trajectory shows that while institutional arrangements are evolving, they remain fragmented. Institutional developments around the enablement of stablecoins, including CBDC, are a significant move in the direction of the goal, while anonymization of transactions and transacting entities can prove to become an impediment to full scale adoption of digital coins as money.

The critical determinant of whether institutional development will move toward the goal of using cryptocurrencies as money is the degree of alignment among actors within the assemblage. President Biden's interventionist approach, promoting CBDC to address exclusion and intermediation, revealed low actor alignment. In contrast, Trump's pro-crypto stance has strengthened alignment by emphasizing autonomy, deregulation, and positioning cryptocurrencies as alternatives to traditional finance. This shift reconfigures relationships and moves the assemblage closer to establishing cryptocurrencies as money.

Towards a New Theoretical Approach

A new theoretical framework must be capable of tracing how governance emerges and assessing the durability of the institutions it produces. This requires moving beyond ANT's descriptive orientation by incorporating tools for analyzing institutional resilience, while retaining ANT's emphasis on the fluid and relational nature of socio-technical systems. Governance, in this view, is not static but continuously co-produced by human and non-human actants.

The phrase "problematization of trust" captures this duality. Problematization reflects ANT's focus on ongoing negotiation, contestation, and shifting associations, while trust signals a stable outcome as the objective. However, trust is not always extended to fixed structures; it can also be placed in contingency, adaptability, and the capacity for change. In this sense, trust is both the outcome of institutional stabilization and a dynamic process shaped by continuous interaction.

Both Elinor Ostrom and the founders of ANT, despite their differing ontologies, recognize this tension. Together, their insights point toward the need for a new theoretical perspective that can account for the co-emergence of governance and trust within large scale, nascent socio-technical assemblages.

Bibliography

Allen, D. W. E., & Potts, J. (2016). How innovation commons contribute to discovering and developing new technologies. *International Journal of the Commons*, *10*(2). https://doi.org/10.18352/ijc.644

Ametrano, F. M. (2016). *Hayek Money: The Cryptocurrency Price Stability Solution* (SSRN Scholarly Paper 2425270). https://doi.org/10.2139/ssrn.2425270

Atlas.ti. (2024). *Intentional AI Coding—ATLAS.ti 24 Windows – User Manual*. https://manuals.atlasti.com/Win/en/manual/SearchAndCode/IntentionalAICoding.html

Auer, R., Farag, M., Lewrick, U., Orazem, L., & Zoss, M. (2023). *Banking in the Shadow of Bitcoin? The Institutional Adoption of Cryptocurrencies* (SSRN Scholarly Paper 4416784). https://doi.org/10.2139/ssrn.4416784

Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., & Shin, H. S. (2021). *Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier* (SSRN Scholarly Paper 3922836). https://doi.org/10.2139/ssrn.3922836

Awrey, D. (2011). *Complexity, Innovation and the Regulation of Modern Financial Markets* (SSRN Scholarly Paper 1916649). https://doi.org/10.2139/ssrn.1916649

Bacchi, C., & Goodwin, S. (2016). *Poststructural Policy Analysis: A Guide to Practice*. Springer.

Bacchi, C. L. (2009). *Analysing Policy: What's the Problem Represented to Be?* Pearson.

Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications*, *4*(1), Article 1. https://doi.org/10.1057/s41599-018-0065-0

Bekemeier, F. (2021). *The Institutionalization of Cryptoassets and Decentralized Financial Markets* (SSRN Scholarly Paper 3899162). https://doi.org/10.2139/ssrn.3899162

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom / Yochai Benkler.* (1st ed.). Yale University Press. https://doi.org/10.12987/9780300127232

Bernanke, B. S. (2007, March 2). *Globalization and Monetary Policy*. Board of Governors of the Federal Reserve System. https://www.federalreserve.gov/newsevents/speech/bernanke20070302a.htm

Biden, G. (2022). Ensuring Responsible Development of Digital Assets. *Federal Register*, *Federal Register*(87), 14143–14152.

Bloor, D. (1976). *Knowledge and Social Imagery*. Routledge & K. Paul.

Bodó, B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, *23*(9), 2668–2690. https://doi.org/10.1177/1461444820939922

Bordo, M. D. (2021). *Central Bank Digital Currency in Historical Perspective: Another Crossroad in Monetary History* (Working Paper 29171). National Bureau of Economic Research. https://doi.org/10.3386/w29171

Braun, B. (2016). Speaking to the people? Money, trust, and central bank legitimacy in the age of quantitative easing. *Review of International Political Economy*, *23*(6), 1064–1092. https://doi.org/10.1080/09692290.2016.1252415

Brekke, J. K. (2021). Hacker-engineers and Their Economies: The Political Economy of Decentralised Networks and 'Cryptoeconomics.' *New Political Economy*, *26*(4), 646–659. https://doi.org/10.1080/13563467.2020.1806223

Broome, A., & Seabrooke, L. (2012). Seeing like an International Organisation. *New Political Economy*, *17*(1), 1–16. https://doi.org/10.1080/13563467.2011.569019

Brown, M. B. (2015). Politicizing science: Conceptions of politics in science and technology studies. *Social Studies of Science*, *45*(1), 3–30. https://doi.org/10.1177/0306312714556694

Buchwald, E. (2024, March 28). *March 28 2024: Sam Bankman-Fried sentencing | CNN Business*. CNN. https://www.cnn.com/business/live-news/sam-bankman-fried-sentencing-03-28-24/index.html

Callon, M. (1984). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. *Sociological Review*, *32*(1), 196–233. https://doi.org/10.1111/j.1467-954x.1984.tb00113.x

Callon, M. (1998a). An essay on framing and overflowing: Economic externalities revisited by sociology. *The Sociological Review*, *46*(S1), 244–269. https://doi.org/10.1111/j.1467-954X.1998.tb03477.x

Callon, M. (1998b). Introduction: The embeddedness of economic markets in economics. *The Sociological Review*, *46*(S1), 1–57. https://doi.org/10.1111/j.1467-954X.1998.tb03468.x

Callon, M. (1999). Actor-Network Theory—The Market Test. *The Sociological Review*, *47*(1_suppl), 181–195. https://doi.org/10.1111/j.1467-954X.1999.tb03488.x

Carruthers, B. G., & Arslan, M. (2019). Sovereignty, Law, and Money: New Developments. *Annual Review of Law and Social Science*, *15*(Volume 15, 2019), 521–538. https://doi.org/10.1146/annurev-lawsocsci-101518-042625

Chainalysis. (2024, July). *Money Laundering and Cryptocurrency*.

Cohen, B. J. (2003). *Monetary Governance in a World of Regional Currencies*. https://escholarship.org/uc/item/3h33v4v3

CoinBase. (2022, July). *Stablecoins: Coinbase Whitepaper*.

Collins, H. M., & Yearley, S. (2010). 10. Epistemological Chicken. In A. Pickering (Ed.), *Science as Practice and Culture* (pp. 301–326). University of Chicago Press. https://doi.org/10.7208/9780226668208-011

Copeland, A. M., Duffie, D., & Yang, Y. (David). (2024). *Reserves Were Not So Ample After All ** (SSRN Scholarly Paper 4185217). Social Science Research Network. https://doi.org/10.2139/ssrn.4185217

Cunha, P. R., Melo, P., & Sebastião, H. (2021). From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution. *Future Internet*, *13*(7), Article 7. https://doi.org/10.3390/fi13070165

Dacin, M. T., Goodstein, J., & Scott, W. R. (2002). Institutional Theory and Institutional Change: Introduction to the Special Research Forum. *The Academy of Management Journal*, *45*(1), 45–56. https://doi.org/10.2307/3069284

Davidson, S., De Filippi, P., & Potts, J. (2017). *Blockchains and the Economic Institutions of Capitalism* (SSRN Scholarly Paper 3221527). Social Science Research Network. https://papers.ssrn.com/abstract=3221527

Davidson, S., Filippi, P. D., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639–658. https://doi.org/10.1017/S1744137417000200

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284. https://doi.org/10.1016/j.techsoc.2020.101284

de Laat, P. B. (2010). How can contributors to open-source communities be trusted? On the assumption, inference, and substitution of trust. *Ethics and Information Technology*, *12*(4), 327–341. https://doi.org/10.1007/s10676-010-9230-x

Derczynski, L., Maynard, D., Rizzo, G., van Erp, M., Gorrell, G., Troncy, R., Petrak, J., & Bontcheva, K. (2015). Analysis of named entity recognition and linking for tweets. *Information Processing & Management*, *51*(2), 32–49. https://doi.org/10.1016/j.ipm.2014.10.006

Dietz, T., Ostrom, E., & Stern, P. C. (2003). The Struggle to Govern the Commons. *Science*, *302*(5652), 1907–1912. https://doi.org/10.1126/science.1091015

Dimaggio, P. J., & Powell, W. W. (2004). Chapter 4 THE IRON CAGE REVISITED: INSTITUTIONAL ISOMORPHISM AND COLLECTIVE RATIONALITY IN ORGANIZATIONAL FIELDS. In F. Dobbin (Ed.), *The New Economic Sociology* (pp. 111–134). Princeton University Press. https://doi.org/10.1515/9780691229270-005

Dodd, N. (2014). *The social life of money / Nigel Dodd., Social life of money*. Princeton University Press. http://elib.openu.ac.il/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=786583&site=ehost-live&ebv=EB&ppid=pp_Cover

Dodd, N. (2018). The Social Life of Bitcoin. *Theory, Culture & Society*, *35*(3), 35–56. https://doi.org/10.1177/0263276417746464

DOT. (2022). *Action Plan to Address Illicit Financing Risks of Digital Assets*.

DOT. (2024, May 1). *2024 National Strategy for Combating Terrorist and Other Illicit Financing*.

Duke, S. A. (2021). The dynamics of imposed transparency and its role in deep social conflicts. In *Trust and Transparency in an Age of Surveillance* (pp. 65–84). Routledge. https://library.oapen.org/bitstream/handle/20.500.12657/51387/9781000488425.pdf?sequence=1#page=78

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. J. (2019). Smart Contracts: Reducing Risks in Economic Exchange with No-Party Trust? *European Journal of Risk Regulation*, *10*(2), 245–262. https://doi.org/10.1017/err.2019.37

Epstein, G. (2021, April 21). *Chapter 2A: The Congruence Principle – The In Common Podcast*. https://www.incommonpodcast.org/chapter-2a-the-congruence-principle/

Epstein, J. (2017, September 10). What Switzerland's 'Crypto Valley' tells us about the state of blockchain. *VentureBeat*. https://venturebeat.com/business/what-switzerlands-crypto-valley-tells-us-about-the-state-of-blockchain/

Escrow.com. (2024). *Escrow Disputes—Escrow.com*. https://www.escrow.com/learn-more/how-escrow-works/escrow-dispute

Fantacci, L., & Gobbi, L. (2021). Stablecoins, Central Bank Digital Currencies and US Dollar Hegemony: The Geopolitical Stake of Innovations in Money and Payments. *Accounting, Economics, and Law: A Convivium*. https://doi.org/10.1515/ael-2020-0053

FED. (2022a). *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*.

FED. (2022b, January). *Stablecoins: Growth Potential and Impact on Banking*.

FED. (2023, April 1). *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*. https://www.federalreserve.gov/publications/money-and-payments-summary-of-public-comment.htm

FED. (2024). *Federal Reserve Board—Money Stock Measures—H.6—October 22, 2024*. Money Stock Measures - H.6 Release. https://www.federalreserve.gov/releases/h6/current/default.htm

FED-comments. (2022). *FED RFC - Public Comments*. https://www.federalreserve.gov/cbdc-public-comments.htm

Federal Register. (2022, July 8). *Vol. 87, No. 130*.

Fenwick, M., & Vermeulen, E. P. (2019). Technology and corporate governance: Blockchain, crypto, and artificial intelligence. *Tex. J. Bus. L.*, *48*, 1.

Ferraro, P. J., & Agrawal, A. (2021). Synthesizing evidence in sustainability science through harmonized experiments: Community monitoring in common pool resources. *Proceedings of the National Academy of Sciences*, *118*(29), e2106489118. https://doi.org/10.1073/pnas.2106489118

Ferré, F. (1995). *Philosophy of Technology*. University of Georgia Press.

Flemming, J., & Judson, R. (2024). *Implications of a U.S. CBDC for International Payments and the Role of the Dollar*. https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-a-u-s-cbdc-for-international-payments-and-the-role-of-the-dollar-20240216.html

Fung, A. (2013). Infotopia: Unleashing the Democratic Power of Transparency*. *Politics & Society*, *41*(2), 183–212. https://doi.org/10.1177/0032329213483107

G7. (2021, October 1). *Public Policy Principles for Retail Central Bank Digital Currencies*.

GDF. (2024a). *GDF Code*. GDF. https://www.gdf.io/code/

GDF. (2024b). *GDF Principles for Stablecoins*.

Golumbia, D. (2015). *Bitcoin as Politics: Distributed Right-Wing Extremism* (SSRN Scholarly Paper 2589890). https://doi.org/10.2139/ssrn.2589890

Golumbia, D., & Justice, G. (2024). *Cyberlibertarianism: The Right-Wing Politics of Digital Technology* (1st ed). University of Minnesota Press.

Gorton, G. B., & Zhang, J. (2023). *Bank Runs During Crypto Winter* (SSRN Scholarly Paper 4447703). https://doi.org/10.2139/ssrn.4447703

Guetterman, T. C., Chang, T., DeJonckheere, M., Basu, T., Scruggs, E., & Vydiswaran, V. G. V. (2018). Augmenting Qualitative Text Analysis with Natural Language Processing: Methodological Study. *Journal of Medical Internet Research*, *20*(6), e9702. https://doi.org/10.2196/jmir.9702

Hall, P. A., & Taylor, R. C. R. (1996). Political Science and the Three New Institutionalisms. *Political Studies*, *44*(5), 936–957. https://doi.org/10.1111/j.1467-9248.1996.tb00343.x

Hamilton, J. (2024a, March 8). *U.S. Fed Chair Powell Says "Nowhere Near" Pursuing CBDC, Won't Spy on Americans*. CoinDesk. https://www.coindesk.com/policy/2024/03/07/us-fed-chair-powell-says-nowhere-near-pursuing-cbdc-wont-spy-on-americans

Hamilton, J. (2024b, April 18). *Sen. Lummis: It'll Pay to "Choose Circle Over Tether" Under U.S. Stablecoin Proposal*. https://www.coindesk.com/policy/2024/04/18/sen-lummis-itll-pay-to-choose-circle-over-tether-under-us-stablecoin-proposal/

Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research*, *162*, 113777. https://doi.org/10.1016/j.jbusres.2023.113777

Hanriot, M. (2016). *Online Dispute Resolution (ODR) as a Solution to Cross Border Consumer Disputes: The Enforcement of Outcomes* (SSRN Scholarly Paper 2811195). https://papers.ssrn.com/abstract=2811195

Hayes, A. (2019). The Socio-Technological Lives of Bitcoin. *Theory, Culture & Society*, *36*(4), 49–72. https://doi.org/10.1177/0263276419826218

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough? *Qualitative Health Research*, *27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Hodgson, G. M. (2006). What Are Institutions? *Journal of Economic Issues*, *40*(1), 1–25. https://doi.org/10.1080/00213624.2006.11506879

Humphreys, L. (2005). Reframing Social Groups, Closure, and Stabilization in the Social Construction of Technology. *Social Epistemology*, *19*(2–3), 231–253. https://doi.org/10.1080/02691720500145449

Ikenberry, G. J. (2011). *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (Vol. 141). Princeton University Press. https://doi.org/10.2307/j.ctt7rjt2

Ingham, G. (2013). *The Nature of Money*. John Wiley & Sons.

Jacobs, T. (2019). Poststructuralist discourse theory as an independent paradigm for studying institutions: Towards a new definition of 'discursive construction' in institutional analysis. *Contemporary Political Theory*, *18*(3), 379–401. https://doi.org/10.1057/s41296-018-0279-3

Jain, G., Shrivastava, A., Paul, J., & Batra, R. (2022). Blockchain for SME Clusters: An Ideation using the Framework of Ostrom Commons Governance. *Information Systems Frontiers*, *24*(4), 1125–1143. https://doi.org/10.1007/s10796-022-10288-z

Jasanoff, S. (2004a). Ordering Knowledge, Ordering Society. In *States of Knowledge*. Routledge.

Jasanoff, S. (2004b). *States of Knowledge: The Co-Production of Science and the Social Order*. Routledge.

Jevons, W. S. (1875). *Money and the Mechanism of Exchange*. D. Appleton.

Jones, J. M. (2023, October 13). *Americans Trust Local Government Most, Congress Least*. Gallup.Com. https://news.gallup.com/poll/512651/americans-trust-local-government-congress-least.aspx

Jordahl, H. (2007). *Inequality and Trust* (SSRN Scholarly Paper 1012786). https://doi.org/10.2139/ssrn.1012786

Keohane, R. O., & Ostrom, E. (1994). *Local Commons and Global Interdependence*. SAGE.

Keynes, J. M. (1930). *A Treatise on Money*. Harcourt, Brace.

Knapp, G. F. (1924). *The State Theory of Money*. MsMillan and Company Limited. https://ideas.repec.org//b/hay/hetboo/knapp1924.html

Koivisto, I. (2022). *The Transparency Paradox*. Oxford University Press.

Korczynski, M. (2000). The Political Economy of Trust. *Journal of Management Studies*, *37*(1). https://doi.org/10.1111/1467-6486.00170

Kruesil, K. (2024, July 28). *Trump calls for US to be 'crypto capital of the planet' in appeal to Nashville bitcoin conference | AP News*. https://apnews.com/article/donald-trump-bitcoin-cryptocurrency-stockpile-6f1314f5e99bbf47cc3ee6fc6178588d

Laclau, E., & Mouffe, C. (1985). *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. Verso.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press.

Latour, B. (1990). Technology is society made durable. *The Sociological Review*, *38*(S1), 103–131.

Latour, B. (1996). *Aramis, or The Love of Technology*. Harvard University Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory / Bruno Latour*. Oxford University Press.

Latour, B. (2012). Visualisation and Cognition: Drawing Things Together. *AVANT. Pismo Awangardy Filozoficzno-Naukowej*, *3*, 207–257.

Latour, B., & Woolgar, S. (1986). *Laboratory Life: The Construction of Scientific Facts*. Princeton University Press.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5*(4), 379–393. https://doi.org/10.1007/BF01059830

Law, J. (2004). *After Method: Mess in Social Science Research*. Routledge. https://doi.org/10.4324/9780203481141

Levi, M. (2019). Trustworthy Government and Legitimating Beliefs. *Nomos*, *61*, 362–384.

Levi, M., & Stoker, L. (2000). Political Trust and Trustworthiness. *Annual Review of Political Science*, *3*(1), 475–507. https://doi.org/10.1146/annurev.polisci.3.1.475

Liaropoulos, A. (2022). Digital Authoritarianism 'Made in China': Installing a Digital Dystopia. *National Security and the Future*, *23*(1), 124–139. https://doi.org/10.37458/nstf.23.1.7

Linåker, J., Regnell, B., & Damian, D. (2019). A Community Strategy Framework – How to obtain influence on requirements in meritocratic open source software communities? *Information and Software Technology*, *112*, 102–114. https://doi.org/10.1016/j.infsof.2019.04.010

Luhmann, N. (2000). *Familiarity, Confidence, Trust: Problems and Alternatives*. https://www.semanticscholar.org/paper/Familiarity%2C-Confidence%2C-Trust%3A-Problems-and-Luhmann/a5ae78f779284090b9cadb9c5b05501c223f9c23

Lummis, C. (2024, April). Lummis, Gillibrand Introduce Bipartisan Landmark Legislation to Create Regulatory Framework for Stablecoins » Senator Cynthia Lummis. *Senator Cynthia Lummis*. https://www.lummis.senate.gov/press-releases/lummis-gillibrand-introduce-bipartisan-landmark-legislation-to-create-regulatory-framework-for-stablecoins/

Lummis, & Gillibrand. (2024, April). *Lummis-Gillibrand Payment Stablecoin Act of 2024*.

Marres, N. (2007). The Issues Deserve More Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy. *Social Studies of Science*, *37*(5), 759–780. https://doi.org/10.1177/0306312706077367

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. *Social Semiotics*, *23*(2), 261–277. https://doi.org/10.1080/10350330.2013.777594

McGinnis. (2011). An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework. *Policy Studies Journal*, *39*(1), 169–183. https://doi.org/10.1111/j.1541-0072.2010.00401.x

McGinnis, M., & Ostrom, E. (1996). Design principles for local and global commons. *The International Political Economy and International Institutions*, *2*, 465–493.

McLaughlin, P. A., Sherouse, O., Febrizio, M., & King, M. S. (2020). *Is Dodd-Frank the Biggest Law Ever?* (SSRN Scholarly Paper 3664165). https://doi.org/10.2139/ssrn.3664165

Meyer, C., & Hudon, M. (2019). Money and the Commons: An Investigation of Complementary Currencies and Their Ethical Implications. *Journal of Business Ethics*, *160*(1), 277–292. https://doi.org/10.1007/s10551-018-3923-1

Milkroad. (2023). *Stablecoins Market Cap: Stablecoin Charts & Historical Data*. Milk Road. https://milkroad.com/stablecoins/

Mishkin, F. S. (2007). *The Economics of Money, Banking, and Financial Markets*. Pearson Addison Wesley.

Mitchell-Innes, A. (1914). The Credit Theory of Money. *Banking Law Journal*, *31*, 151–168.

Moin, A., Sirer, E. G., & Sekniqi, K. (2019). *A Classification Framework for Stablecoin Designs* (arXiv:1910.10098). arXiv. https://doi.org/10.48550/arXiv.1910.10098

Mol, A. (2002). *The Body Multiple: Ontology in Medical Practice*. Duke University Press.

Morriss, A. P., & Korosec, J. A. (2005). *Private Dispute Resolution in the Card Context: Structure, Reputation, and Incentives* (SSRN Scholarly Paper 735283). https://doi.org/10.2139/ssrn.735283

Mulder, L. B., Verboon, P., & De Cremer, D. (2009). Sanctions and moral judgments: The moderating effect of sanction severity and trust in authorities. *European Journal of Social Psychology*, *39*(2), 255–269. https://doi.org/10.1002/ejsp.506

Murdoch, J. (1998). The spaces of actor-network theory. *Geoforum*, *29*(4), 357–374. https://doi.org/10.1016/S0016-7185(98)00011-6

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nelms, T. C., Maurer, B., Swartz, L., & Mainwaring, S. (2018). Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. *Theory, Culture & Society*, *35*(3), 13–33. https://doi.org/10.1177/0263276417746466

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge University Press.

North, D. C., & Weingast, B. R. (1989). Constitutions and Commitment: The Evolution of Institutions Governing Public Choice in Seventeenth-Century England. *The Journal of Economic History*, *49*(4), 803–832. https://doi.org/10.1017/S0022050700009451

OSTP. (2022a, September 9). *CLIMATE AND ENERGY IMPLICATIONS OF CRYPTO-ASSETS*. US Government.

OSTP. (2022b, September 16). *TECHNICAL EVALUATION FOR A U.S. CENTRAL BANK DIGITAL CURRENCY SYSTEM*. US Government.

OSTP-Responses-1. (2022). *OSTP - Public Comments*. https://www.regulations.gov/document/TREAS-DO-2022-0014-0001

Ostrom. (2015). *Governing the commons: The evolution of institutions for collective action / Elinor Ostrom. [electronic resource]* (Canto classics edition.., Canto Classics). University Press.

Ostrom, E. (1998). A Behavioral Approach to the Rational Choice Theory of Collective Action: Presidential Address, American Political Science Association, 1997. *The American Political Science Review*, *92*(1), 1–22. https://doi.org/10.2307/2585925

Ostrom, E. (2002). Chapter 24 Common-pool resources and institutions: Toward a revised theory. In *Handbook of Agricultural Economics* (Vol. 2, pp. 1315–1339). Elsevier. https://doi.org/10.1016/S1574-0072(02)10006-5

Ostrom, E. (2008). *Design Principles of Robust Property-Rights Institutions: What Have We Learned?* (SSRN Scholarly Paper 1304708). Social Science Research Network. https://papers.ssrn.com/abstract=1304708

Ostrom, E. (2009). *Understanding Institutional Diversity*. Princeton University Press.

Ostrom, E. (2010a). Beyond Markets and States: Polycentric Governance of Complex Economic Systems. *The American Economic Review*, *100*(3), 641–672.

Ostrom, E. (2010b). Polycentric systems for coping with collective action and global environmental change. *Global Environmental Change*, *20*(4), 550–557. https://doi.org/10.1016/j.gloenvcha.2010.07.004

Ostrom, Tiebout, C. M., & Warren, R. (1961). The Organization of Government in Metropolitan Areas: A Theoretical Inquiry. *The American Political Science Review*, *55*(4), 831–842. https://doi.org/10.2307/1952530

Pavlidis, G. (2021). Financial action task force and the fight against money laundering and the financing of terrorism. *Journal of Financial Crime*, *28*(3), 765–773. https://doi.org/10.1108/JFC-09-2019-0124

Picht, C. (1987). Common property regimes in Swiss alpine meadows. *A Conference on Advances in Comparative Institutional Analysis at the Inter-University Center of Postgraduate Studies, October*, 19–23.

Pieńkowski, D. (2011). A Holistic Framework for Trust in Online Transactions. *International Journal of …*. https://www.academia.edu/2339938/A_Holistic_Framework_for_Trust_in_Online_Transactions

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004

Poteete, A. R. (2010). *Working together [electronic resource]: Collective action, the commons, and multiple methods in practice / Amy R. Poteete, Marco A. Janssen, Elinor Ostrom.* (Course Book.). Princeton University Press.

Prasad, E. S. (2023). *The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance*. Belknap Press.

Quinn, Ú. (2023). *Exploring the Use of Actor-Network-Theory as a Means of Analysing Complex Organisational Networks: An Irish Case Study* (SSRN Scholarly Paper 4865219). Social Science Research Network. https://doi.org/10.2139/ssrn.4865219

Rajan, R. (2019). *The Third Pillar: How Markets and the State Leave the Community Behind*. Penguin.

Resnik, J., & Hershkoff, H. (2023). *Constraining and Licensing Arbitrariness: The Stakes in Debates about Substantive-Procedural Due Process*. https://openyls.law.yale.edu/handle/20.500.13051/18398

Roberts, J. M. (2012). Poststructuralism against poststructuralism: Actor-network theory, organizations and economic markets. *European Journal of Social Theory*, *15*(1), 35–53. https://doi.org/10.1177/1368431011423573

Rose, N., & Miller, P. (2017). Political power beyond the state: Problematics of government. In *Foucault and law* (pp. 191–224). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315094021-9/political-power-beyond-state-problematics-government-nikolas-rose-peter-miller

Roth, F. (2009). The effect of the financial crisis on systemic trust. *Intereconomics*, *44*(4), 203–208. https://doi.org/10.1007/s10272-009-0296-9

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2021). When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. *Sage Open*, *11*(1), 21582440211002526. https://doi.org/10.1177/21582440211002526

Rozas, D., Tenorio-Fornés, A., & Hassan, S. (2021). Analysis of the Potentials of Blockchain for the Governance of Global Digital Commons. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.577680

Rule, S. (2023, February 6). *You're Still Early: An Objective Look At Bitcoin Adoption*. Bitcoin Magazine - Bitcoin News, Articles and Expert Insights. https://bitcoinmagazine.com/markets/an-objective-look-at-bitcoin-adoption

Santos, A. C. (2017). Cultivating the self-reliant and responsible individual: The material culture of financial literacy. *New Political Economy*, *22*(4), 410–422. https://doi.org/10.1080/13563467.2017.1259302

Saxborn, M., Pan, Y., & Said, A. (2024). Trust Through Recommendation in E-commerce. *Proceedings of the 2024 Conference on Human Information Interaction and Retrieval*, 87–96. https://doi.org/10.1145/3627508.3638294

Schaefer, P. (2024, May 25). *Trump pledges to commute sentence of Silk Road founder Ross Ulbricht if elected*. POLITICO. https://www.politico.com/news/2024/05/25/trump-commute-ross-ulbricht-sentence-libertarian-convention-00160025

Schouten, F. (2024, November 17). *The crypto industry plowed tens of millions into the election. Now, it's looking for a return on that investment | CNN Politics*. CNN. https://www.cnn.com/2024/11/17/politics/crypto-industry-donald-trump-reelection/index.html

Scott, W. R. (2008). *Institutions and Organizations: Ideas and Interests*. SAGE.

Shackelford, S., & Myers, S. (2016). *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace* (SSRN Scholarly Paper 2874090). https://doi.org/10.2139/ssrn.2874090

Shamir, R. (2008). The Age of Responsibilization: On Market-Embedded Morality. *Economy and Society - ECON SOC*, *37*, 1–19. https://doi.org/10.1080/03085140701760833

Simmel, G. (2004). *The Philosophy of Money*. Psychology Press.

Simmel, G., Frisby, D., Bottomore, T., & Lemert, C. (2011). *The Philosophy of Money*. Routledge. https://doi.org/10.4324/9780203828298

Slough, T., Rubenson, D., Levy, R., Alpizar Rodriguez, F., Bernedo del Carpio, M., Buntaine, M. T., Christensen, D., Cooperman, A., Eisenbarth, S., Ferraro, P. J., Graham, L., Hartman, A. C., Kopas, J., McLarty, S., Rigterink, A. S., Samii, C., Seim, B., Urpelainen, J., & Zhang, B. (2021). Adoption of community monitoring improves common pool resource management across contexts. *Proceedings of the National Academy of Sciences*, *118*(29), e2015367118. https://doi.org/10.1073/pnas.2015367118

Sousa, A., Calçada, E., Rodrigues, P., & Borges, A. (2022). Cryptocurrency adoption: A systematic literature review and bibliometric analysis. *EuroMed Journal of Business*, *17*. https://doi.org/10.1108/EMJB-01-2022-0003

Stern, P. C. (2011). Design principles for global commons: Natural resources and emerging technologies. *International Journal of the Commons*, *5*(2). https://doi.org/10.18352/ijc.305

Stevenson, D. D. (2022). *Operation Choke Point: Myths and Reality* (SSRN Scholarly Paper 4292272). https://doi.org/10.2139/ssrn.4292272

Strange, S. (2016). *Casino capitalism / Susan Strange ; with a new introduction by Matthew Watson.* Manchester University Press.

Swartz, L. (2017). Blockchain dreams: Imagining techno-economic alternatives after Bitcoin. *Another Economy Is Possible: Culture and Economy in a Time of Crisis*, *1*.

Tether. (2024). *Transparency* [Financial institutions]. Tether Trasparency. https://tether.to/en/transparency/?tab=usdt

Treasury. (2022a). *Crypto-Assets: Implications for Consumers, Investors, and Businesses*.

Treasury. (2022b). *The Future of Money and Payments*. cbdc

Uddin, Md. H., Ali, Md. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, *22*(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

Ulbricht. (2024). *THE OFFICIAL WEBSITE FOR ROSS ULBRICHT*. Free Ross. https://freeross.org/

Uslaner, E. M. (2010). Trust and the Economic Crisis of 2008. *Corporate Reputation Review*, *13*(2), 110–123. https://doi.org/10.1057/crr.2010.8

van Dijk, E., Mulder, L. B., & de Kwaadsteniet, E. W. (2014). For the common good? The use of sanctions in social dilemmas. In *Reward and punishment in social dilemmas* (pp. 70–84). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199300730.003.0005

van Eeden, P. (2017). Materializing discourse analysis with James, Schmitt and Latour. *Palgrave Communications*, *3*(1), 1–19. https://doi.org/10.1057/palcomms.2017.39

Vaz, J., & Brown, K. (2019). *Are Cryptocurrencies a More Equitable Form of Money?* (SSRN Scholarly Paper 3358670). https://doi.org/10.2139/ssrn.3358670

vbuterin. (2016, June 17). *Personal statement regarding the fork* [Reddit Post]. R/Ethereum. www.reddit.com/r/ethereum/comments/4oj7ql/personal_statement_regarding_the_fork/

Viola, L. A. (2021). The limits of transparency as a tool for regulating surveillance: A comparative study of the United States, United Kingdom, and Germany. In *Trust and Transparency in an Age of Surveillance* (pp. 21–46). Routledge. https://library.oapen.org/bitstream/handle/20.500.12657/51387/9781000488425.pdf?sequence=1#page=34

Wahl, I., Kastlunger, B., & Kirchler, E. (2010). Trust in Authorities and Power to Enforce Tax Compliance: An Empirical Analysis of the "Slippery Slope Framework." *Law & Policy*, *32*(4), 383–406. https://doi.org/10.1111/j.1467-9930.2010.00327.x

Weingärtner, T., Fasser, F., Reis Sá da Costa, P., & Farkas, W. (2023). Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. *Journal of Risk and Financial Management*, *16*(10), Article 10. https://doi.org/10.3390/jrfm16100454

Werbach, K. (2018a). *The Blockchain and the New Architecture of Trust*. MIT Press.

Werbach, K. (2018b). *The Siren Song: Algorithmic Governance By Blockchain* (SSRN Scholarly Paper 3578610). https://papers.ssrn.com/abstract=3578610

Willis, L. E. (2008). *Against Financial Literacy Education* (SSRN Scholarly Paper 1105384). Social Science Research Network. https://papers.ssrn.com/abstract=1105384

Yan, W., & Zhou, W. (2023). Is blockchain a cure for peer-to-peer lending? *Annals of Operations Research*, *321*(1), 693–716. https://doi.org/10.1007/s10479-022-05108-1

Zelizer, V. A. R. (2010). *Economic lives: How culture shapes the economy / Viviana A. Zelizer.* (Course Book). University Press. https://doi.org/10.1515/9781400836253