Part II: Blockchain and the Concept of Trust in Decentralized Futures
Chapter 4

BLOCKCHAIN AND THE CONCEPT OF TRUST IN DECENTRALIZED FUTURES

[1] Banveer Kaur Jhinger, Assistant Professor (Laws), University Institute of Law, Punjab University Regional Centre, Ludhiana

INTRODUCTION

Trust has long been the linchpin of social and economic systems and is traditionally embedded within centralized institutions such as banks, governments, and regulatory authorities. These entities function as intermediaries, thereby guaranteeing the integrity of transactions, contracts, and records (Le Quoc et al., 2025). However, the rise of digital infrastructure and the erosion of institutional legitimacyfueled by corruption, surveillance, and financial criseshas triggered a global trust deficit. Within this context, blockchain technology has emerged not merely as a tool for innovation but also as a radical proposition to reconceptualize trust itself. By distributing verification responsibilities across a decentralized network, blockchain challenges the necessity of a centralized authority and promises a system in which trust is encoded into algorithmic consensus and cryptographic security.

Originally designed as the underlying ledger for Bitcoin, the blockchain has rapidly evolved into a versatile infrastructure with applications across finance, governance, supply chains, and identity management. It reimagines trust not as a social relationship but as a technical protocol that is immutable, transparent, and verifiable by design (Lee et al., 2021). This shift raises profound questions: can technological systems truly replace the nuanced, contextual nature of human trust? What happens when trust becomes programmable? How do these transformations influence broader social contracts?As societies explore alternatives to hierarchical control and opaque institutions, blockchain is increasingly being positioned as a foundational layer for decentralized futures. However, techno-utopian promises are not without contradiction and critique, demanding a deeper interrogation of what trust means in a world being reshaped by code.

This chapter explores how blockchain technology reshapes the foundational concept of trust in contemporary digital societies, particularly in the context of decentralized systems. While trust has traditionally been anchored in institutions, such as governments, banks, legal systems, and

© 2025 Banveer Kaur Jhinger. Blockchain and the Concept of Trust in Decentralized Futures in Reframing Futures: Concepts and Challenges in a Rapidly Changing World. ISBN: 979-8-292-77050-3. pp. 130–145. Published by the Indian Institute of Industrial and Social Research.

intermediaries, blockchain proposes a radical shift by embedding trust within technological protocols, consensus algorithms, and cryptographic security. This transformation is not merely technical but also deeply conceptual, raising questions about authority, verification, reliability, and the nature of social contracts in an increasingly digitized and disintermediated world. By unpacking the philosophical, economic, and technological dimensions of this shift, this chapter investigates how blockchain challenges conventional understandings of trust and opens new avenues for imagining accountability and governance beyond centralized control. It also critically assesses the promises and pitfalls of decentralization, particularly in light of issues such as power asymmetries in protocol design, regulatory uncertainty, and the myth of neutrality in the code. Through this conceptual inquiry, the chapter intends to provide a framework for analyzing blockchain not just as a tool or market innovation, but also as a trust-generating infrastructure with far-reaching implications for institutional legitimacy, user agency, and democratic participation in the digital age.

CONCEPTUAL CLARIFICATION

Blockchain is a decentralized, distributed ledger technology that enables the secure, transparent, and tamper-resistant recording of transactions across a network. At its core, a blockchain is a chronologically ordered chain of blocks, each containing a set of data or transactions cryptographically linked to the previous one (Jimmy, 2024). This structure ensures that once data are recorded, they become extremely difficult to alter without consensus from the network, thereby fostering a novel mechanism for generating trust without centralized authorities. Originally conceptualized to support Bitcoin in 2008 by the pseudonymous Satoshi Nakamoto, blockchain emerged not just as an infrastructure for digital currency but also as a broader technological innovation that challenged traditional models of governance, recordkeeping, and institutional verification.

The origin of blockchain is deeply intertwined with the socio-technical context of the late 2000s, marked by the global financial crisis, deepening distrust in centralized financial institutions, and the growing influence of peer-to-peer technologies. Nakamoto's white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System,* introduced blockchain as a response to the double-spending problem in digital transactions without relying on a trusted third party (Biryukov & Tikhomirov, 2019). What set this system apart was its ability to achieve consensus among distributed actors through a process known as "proof-of-work," a computationally intensive mechanism that validates transactions and secures the network. While this initial implementation focused on financial exchange, the underlying ledger technology quickly captured attention across diverse fields from supply chains and identity verification to governance and data sharing. It has evolved from a cryptocurrency-specific protocol to a generalized technological paradigm. The launch of Ethereum in 2015 expanded the scope of blockchain by introducing programmable smart contracts, a self-executing code embedded within the blockchain that could automate complex interactions. This marked the transition from a simple ledger to a distributed computational platform, setting the stage for broader debates on decentralization, trust, and institutional change. In essence, blockchain's origin lies not only in technical ingenuity but also in a philosophical and political desire to reconfigure how trust is established and maintained in the digital age.

The concept of blockchain has evolved significantly since its inception, transforming from a niche cryptographic innovation into a foundational technology that reshapes our understanding of trust, authority, and decentralization. Initially introduced through the 2008 whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” by the pseudonymous Satoshi Nakamoto, blockchain technology was primarily envisioned as a solution to the double-spending problem in digital currencies, eliminating the need for centralized financial institutions by establishing a distributed, verifiable ledger. Blockchain was tightly coupled with the ethos of cypherpunk libertarianism, emphasizing individual sovereignty, resistance to state surveillance, and the dismantling of institutional monopolies over value and identity (Hossain et al., 2020). Beyond the confines of cryptocurrency, blockchain began to be framed as a "trust protocol" a system that could enable secure, tamper-resistant, and transparent interactions among mutually distrustful parties. This shift was particularly significant, as it reoriented the function of blockchain from a narrow technical tool to a broader socio-technical infrastructure. Ethereum, which was launched in 2015, marked a critical turning point in this evolution. By introducing smart contracts programmable agreements that execute autonomously when predefined conditions are met blockchain acquired a new dimension as a platform for decentralized applications (dApps). This opened the door to a range of uses, including supply chain transparency, identity verification, decentralized finance (DeFi), and governance systems.

Simultaneously, academic and policy discourses began to grapple with the implications of blockchain for institutional trust. Early techno-utopian narratives that portrayed blockchain as a “trustless” system one that obviates the need for trust by embedding it in code began to face critique. Scholars and practitioners increasingly recognize that blockchain does not eliminate trust, but rather *reconfigures* it by shifting it away from human institutions and towards algorithmic systems, cryptographic assurances, and community-based consensus mechanisms. This conceptual reconfiguration brought attention to the politics of decentralization, whose interests are served, who governs protocols, and how inclusion and exclusion are structured within these systems. By the early 2020s, blockchain's evolution was marked by an increased focus on its social, environmental, and ethical dimensions (Munir et al., 2022). Concerns about energy consumption, digital colonialism, and the concentration of power among protocol developers and miners spurred debates on the “decentralization paradox.” As blockchain entered new domains from public administration to the art world (via NFTs) the discourse evolved from one of the technical innovations to one deeply entangled with issues of governance, accountability, and social legitimacy. Today, blockchain represents not just a technical innovation but an evolving concept situated at the intersection of trust, decentralization, and digital sovereignty.

The conceptual terrain surrounding blockchain is interwoven with a variety of related terms, such as distributed ledger technology (DLT), decentralization, cryptography, and smart contracts, each bearing a specific meaning but often conflated in popular and academic discourse. At the heart of blockchain is DLT, which is a broader technological umbrella under which blockchain is implemented (Hamilton, 2019). Although all blockchains are distributed ledgers, not all distributed ledgers follow the blockchain’s specific architecture of cryptographically linked blocks. Understanding this distinction is critical to debates on scalability, energy efficiency, and institutional adoption.

Decentralization is another cornerstone term that must be unpacked. In common usage, decentralization implies the diffusion of power or authority away from the central entity. However, in the blockchain context, this concept operates on multiple axes: technical (node distribution), political (governance structures), and ideological (anti-authoritarian) (Atzori, 2017). Confusion often arises when decentralization is treated as absolute, whereas most blockchain systems today exist along a spectrum, from fully permissionless networks, such as Bitcoin, to permissioned enterprise platforms, such as Hyperledger. The degree and type of decentralization have direct implications for trust, transparency, and user agency; trustless trust is another oft-misunderstood term. Contrary to suggesting the absence of trust, this denotes a shift from interpersonal or institutional trust to protocol-based assurance. This is where cryptographic consensus mechanisms, such as proof-of-work or proof-of-stake, replace human arbiters with algorithmic enforcement. The distinction between traditional trust (in people or institutions) and protocol trust (in code and incentives) signals a paradigm shift in how reliability and accountability are conceptualized in digital economies.

Finally, smart contracts self-executing agreements coded into the blockchain are sometimes incorrectly equated with legal contracts. While they automate conditional logic, they lack the interpretive flexibility of law, and often raise questions about enforcement, fairness, and unintended consequences (Levy, 2017). Understanding how smart contracts relate to, but differ from, traditional contractual mechanisms is key to grappling with their role in decentralized governance; thus, clarifying these conceptual boundaries allows for a more rigorous analysis of how blockchain reconfigures foundational ideas such as trust, authority, and coordination in emerging socio-technical systems.

THEORETICAL FOUNDATIONS

The theoretical foundations of blockchain as a trust-generating mechanism lie at the intersection of cryptographic theory, distributed systems, institutional economics, and sociotechnical systems theory. At its core, blockchain technology operationalizes trust not through centralized authority, but through protocol-based consensus, creating what many scholars have termed "trustless trust" a condition where institutional or interpersonal trust is no longer required because validation is embedded in code and system architecture (Afzaal et al., 2022).A key theoretical contribution comes from the field of institutional economics, particularly Douglass North’s work on institutions as “rules of the game’ that structure human interaction. Blockchain can be viewed as a radical evolution of institutional design, and smart contracts and decentralized autonomous organizations (DAOs) are programmable institutions that enforce compliance through algorithmic codes rather than hierarchical enforcement. This rethinking of institutions draws on transaction cost economics (e.g., Oliver Williamson), which posits that trust and governance mechanisms exist primarily to reduce friction in economic exchanges. Blockchain reduces these frictions by automating verification and execution, thereby altering the cost-benefit equation of organizing activity within firms, markets, or networks.

Complementing these economic frameworks is sociotechnical systems theory, which examines how technological artifacts mediate social relations and institutional logic. Blockchain exemplifies what Bruno Latour and Actor-Network Theory (ANT) would describe as the reconfiguration of social trust into technical networks. In this framing, trust is not an emergent social norm but a distributed artifact a collectively maintained and cryptographically secured ledger that sustains itself through decentralized consensus mechanisms (K et al., 2023). Trust is no longer interpersonal or institutional but infrastructural, embedded within protocols that resist tampering, manipulation, or unilateral control, and also plays a foundational role, particularly in the design of consensus algorithms like Proof-of-Work (PoW) and Proof-of-Stake (PoS). These models align incentives among decentralized actors and ensure cooperation in a trust-minimized environment. In blockchain networks, game-theoretic mechanisms are used to manage Byzantine fault tolerance the ability of a system to function correctly even when some actors act maliciously or unreliably. These mechanisms mirror the logic of the mechanism design theory, in which rules and incentives are crafted such that rational actors lead to desirable outcomes without requiring moral trust.

Additionally, theories of networked governance and peer-to-peer (P2P) coordination, influenced by thinkers such as Yochai Benkler, provide insights into how blockchain reorganizes the production and verification of knowledge. Benkler's concept of "commons-based peer production" finds new relevance in blockchain, where distributed agents collectively maintain a ledger, verify transactions, and establish a consensus on truth without centralized oversight (Mezquita et al., 2022).Together, these theoretical strands help us understand blockchain not simply as a technological innovation but as a paradigmatic shift in how trust is produced, distributed, and sustained in a digitally mediated world. They reveal that blockchain is not the elimination of trust but its encoding into systems that presume adversarial conditions but still achieve cooperation, reliability, and legitimacy.

While the dominant narrative around blockchain technologies emphasizes their ability to replace traditional trust mechanisms with cryptographic certainty and code-based governance, a range of competing and complementary perspectives complicate this techno-optimistic view. At one end of the spectrum, the blockchain is hailed as a "trustless" system that eliminates the need for centralized intermediaries, such as banks, states, or corporations, by replacing human trust with algorithmic integrity. However, critical scholars argue that this portrayal oversimplifies the sociotechnical dimensions of trust (Nabben, 2021). Rather than eliminating trust, blockchain technologies redistribute and reconfigure trust into new actors such as developers, miners, protocol designers, and even opaque governance systems embedded in smart contracts. As Primavera De Filippi and Aaron Wright argue, blockchain does not eliminate trust; it shifts it from institutions to infrastructure, raising new questions about accountability, access, and control.Another perspective emerges from social systems theory and relational sociology, which view trust not as a vulnerability to be minimized through code, but as a social good that facilitates cooperation despite uncertainty. Niklas Luhmann, for instance, describes trust as a mechanism for reducing social complexity, and from this standpoint, blockchain's overengineering of predictability might actually constrain the generative ambiguity that trust entails in human interactions. From this view, blockchain may create rigid structures of conditionality that reduce the flexibility necessary for adaptive trust, especially in environments characterized by ambiguity, conflict, or moral negotiation, such as humanitarian aid, refugee governance, or indigenous land rights.

Meanwhile, from the perspectives of institutional economics and transaction cost theory, blockchain is seen as a complementary innovation that can augment existing institutions rather than render them obsolete (Bennet et al., 2024). Scholars like Elinor Ostrom and Oliver Williamson provide insights into how trust emerges within nested institutions and governance arrangements, suggesting that blockchain could serve as a supplementary layer of verification or record-keeping in complex institutional ecosystems, especially where formal enforcement is weak but social capital is high.Finally, perspectives from feminist and postcolonial theory challenge the universalism embedded in blockchain discourse, asking whose definitions of trust, autonomy, and decentralization are being operationalized. These frameworks point to the risks of epistemic and infrastructural colonialism, assuming that algorithmic decentralization is a universally desirable or liberatory goal. They emphasize that in many communities, trust is deeply contextual, culturally situated, and historically embedded in social relationships that cannot be fully codified into digital protocols.

The selection of a sociotechnical systems lens, enriched by institutional and trust theories, is critical for understanding the conceptual reconfiguration of trust in decentralized futures. Unlike earlier digital technologies that augment existing institutional arrangements, blockchain, as a distributed ledger system, operates by disintermediating traditional actors, such as banks, governments, and legal authorities, and replacing them with algorithmic consensus. This fundamental shift necessitates an analytical framework that can hold together the material-technical affordances of blockchain and the normative structures of trust and governance it challenges and reconstructs (Bennet et al., 2024).Institutional theory allows us to analyze how trust has historically been embedded in centralized structures through legitimacy, formal rules, and social contracts. By contrast, blockchain decentralizes the production and verification of truth, raising critical questions about how norms and trustworthiness are co-constructed when no single authority presides over interactions. Trust theory, particularly the distinction between interpersonal, institutional, and system trust, is essential to trace how blockchain attempts to relocate trust from human institutions to technical systems and what is potentially lost or gained in that shift.

Finally, a sociotechnical systems perspective is uniquely positioned to bridge the technical architecture of the blockchain with its sociopolitical consequences. It acknowledges that trust is not merely a function of protocol efficiency or encryption strength but is also shaped by user interpretations, power dynamics in protocol governance, and the broader cultural-political imaginaries of decentralization (John & Pam, 2018). This integrative approach is justified because it offers both descriptive and critical traction, which explains how blockchain-based trust systems function and enable inquiry into whose interests are embedded in their design and whose interests are marginalized. Thus, this tripartite lens is not only methodologically coherent but also essential to critically engage with the ideological and material reordering that blockchain technologies propose

DEBATES, GAPS, AND THEORETICAL CHALLENGES

At the heart of blockchain's promise lies a paradox: while it aims to eliminate the need for trust through algorithmic consensus, it simultaneously demands profound trust in the technology itself. This gives rise to one of the most fundamental tensions in blockchain discourse: the displacement of social trust from technological trust (Wang et al., 2022). The premise that trust can be "outsourced" to code and cryptography downplays the sociopolitical dimensions of trust-building, such as accountability, transparency, and human judgment. Critics argue that this techno-solutionism oversimplifies the nature of trust, reducing it to a function of verifiability and consensus protocols rather than a socially embedded relationship.

Another key controversy revolves around the myth of decentralization. Although blockchain is theoretically decentralized, in practice, many networks exhibit power concentrations. For instance, in proof-of-work blockchains such as Bitcoin, mining is dominated by a few major players because of the high costs of computational power and energy (Leonardos et al., 2020). Similarly, governance in blockchain ecosystems often remains opaque, with core developers, protocol founders, and venture capital investors wielding a disproportionate influence. This raises concerns about "decentralization theatre" decentralization theater, where the appearance of distributed authority masks new forms of centralization and elite capital, and further tensions emerge in the regulatory ambiguity surrounding blockchain applications. While some view technology as a tool to bypass restrictive state controls or financial gatekeeping, governments and international institutions are increasingly scrutinizing its use in illegal activities, money laundering, and financial fraud. The decentralized and pseudonymous nature of blockchain complicates regulatory oversight, raises questions about jurisdiction, consumer protection, and the enforceability of contracts. This legal gray zone undermines trust from institutional actors and the public alike.

Ethical controversies persist, particularly regarding the environmental costs of certain blockchain infrastructures. Bitcoin and Ethereum (pre-merger) have faced criticism for their massive energy consumption and ecological impact, sparking debates over the sustainability of decentralized consensus mechanisms (Tomatsu & Han, 2023). Moreover, the socioeconomic accessibility of blockchain is contested; while it promises inclusion, real-world applications often exclude those without technical literacy, digital infrastructure, or financial capital, and these tensions reveal that trust in blockchain is far from settled. Rather than a straightforward technological fix, blockchain emerges as a deeply contested terrain where ideals of decentralization, transparency, and autonomy are negotiated amid practical compromises, power asymmetries, and institutional pushback

While blockchain is often heralded as a revolutionary tool for decentralizing trust, critical perspectives challenge the technological determinism and utopianism surrounding it. One key critique arises from critical political economy and technological governance scholars, who argue that blockchain does not eliminate trust but rather reconfigures its locus, shifting it from centralized institutions to opaque algorithmic systems (He et al., 2019). They argue that this shift risks replacing one form of unaccountable authority (e.g., banks and states) with another (e.g., developers, miners, and platform owners), many of whom operate outside democratic oversight or regulatory transparency.

Critics also highlight the myth of decentralization. In practice, many blockchain systems are not truly decentralized. Mining processes are often dominated by a small number of actors or consortia, leading to what some scholars term “decentralized centralization.” This raises the question of who actually benefits from blockchain's promises? For marginalized populations, especially in the Global South, access to blockchain-based systems may be limited by infrastructure, digital literacy, or legal recognition, thereby reproducing existing inequalities under a new technological guise. Another line of critique targets the ideological underpinnings of blockchain, particularly its ties to libertarianism, techno-solutionism, and economic individualism (Allen et al., 2018). These ideological commitments often shape the types of problems that blockchain is designed to solve typically emphasizing efficiency, autonomy, and disintermediation while ignoring questions of justice, power asymmetries, and collective agency. Feminist technology scholars, for instance, point out how blockchain logic tends to prioritize formalized, binary, and rule-based systems of trust, neglecting the relational, affective, and embodied dimensions of how trust functions in social life.

Moreover, ecological and ethical critiques question the sustainability of blockchain, especially proof-of-work-based systems such as Bitcoin, which consume enormous amounts of energy. Environmental costs complicate the viability of blockchain as a tool for inclusive long-term systemic reform (Munir et al., 2022). Finally, scholars of law and regulation argue that blockchain's claim to be "trustless" and autonomous from institutional frameworks overlooks the embeddedness of technology in broader socio-legal contexts. Disputes, fraud, and unintended consequences still require human interpretation and institutional recourse, thus revealing the limits of purely code-based trust mechanisms.In sum, critical perspectives urge us to move beyond hype and interrogate who builds these systems, who benefits, and who bears the cost. They push for a more grounded and intersectional approach to evaluate the blockchain's potential in reshaping trust.

Despite a growing body of interdisciplinary research on blockchain and trust, several significant gaps remain in the literature (Chatziamanetoglou & Rantos, 2024). First, much of the discourse continues to be driven by techno-optimistic narratives that overstate the blockchain's capacity to solve trust-related challenges without sufficiently accounting for sociopolitical and contextual variables. While technical analyses of cryptographic mechanisms (e.g., consensus protocols and smart contracts) are robust, the social dynamics of trust, including informal practices, relational networks, and local governance structures, are often underexplored. This leads to an incomplete understanding of how trust is produced, maintained, or undermined in decentralized ecosystems.

Second, there is a dearth of empirical studies, especially longitudinal or ethnographic studies, that investigate blockchain implementation across diverse real-world contexts. Most case studies are concentrated on fintech or supply chain sectors in high-income countries, with limited attention paid to how trust operates in informal economies, rural contexts, or the Global South (Trivedi et al., 2021). This geographical and sectoral bias limits the applicability of current theories and risks by universalizing Western assumptions regarding trust, transparency, and authority. Third, the literature tends to frame blockchain as either inherently trustworthy because of its technological architecture, or as a trustless system where code replaces institutional mediation. This binary perspective overlooks hybrid arrangements in which blockchain coexists with legacy institutions, intermediaries, or cultural norms. Few studies have addressed how decentralized technologies are negotiated, resisted, or adapted within existing trust ecologies, such as community banking, informal land rights systems, or indigenous governance models.

Finally, insufficient attention has been paid to the *politics of design* in blockchain systems, including those that define trust parameters, set rules of governance, or benefit from the distribution of control (Crandall, 2019). The ideological underpinnings of blockchain development (libertarianism, techno-solutionism, or anti-statism) are seldom interrogated as potential biases shaping the affordances and limitations of trust in these systems, which calls for more pluralistic, interdisciplinary, and context-sensitive research agendas that engage critically with both promises and paradoxes of trust in blockchain-enabled futures.

APPLICATION OR ILLUSTRATION

India's recent deployment of digital instruments, such as *e-RUPI*, a person- and purpose-specific digital voucher system, offers a compelling case of blockchain-mediated trust in public service delivery. Launched by the National Payments Corporation of India (NPCI) in 2021, e-RUPI was initially intended to streamline welfare distribution in sectors such as healthcare and vaccination programs (Bodó & Janssen, 2022). While not a cryptocurrency, e-RUPI integrates blockchain-inspired logic: it removes intermediaries, ensures traceability, and limits misuse. In doing so, it exemplifies how blockchain concepts can reconstruct trust between the state, service providers, and citizens, a relationship historically fraught with inefficiency, opacity, and corruption. Traditional welfare delivery in India has been riddled with challenges, such as "ghost beneficiaries," leakage, and misuse of funds. The process often involves multiple administrative layers, each of which becomes a potential site of delay, discretion, and rent seeking. The introduction of e-RUPI, a one-time SMS- or QR code-based payment system, transformedorms this experience. Beneficiaries receive a digital voucher directly linked to a specific service (e.g., vaccination at a private clinic), and service providers redeem the value without the need for a bank account or card. The design ensures that funds are utilized exactly as intended, reinforcing *programmatic trust* trust in the system and its logic–rather than in individual actors.

The embedded logic of smart contracts makes this model significant from a blockchain standpoint. Although not running on a fully public blockchain, such as Ethereum, e-RUPI adopts a *permissioned digital architecture* with fixed conditions and automated execution. This conditionality mirrors smart contracts in which outcomes are triggered only when predefined conditions are met (Singh et al., 2023). For example, the service provider receives payments only after the beneficiary verifies the service receipt. This minimizes the need for human mediation or post hoc audits, shifting trust away from discretionary institutional judgment toward programmable transparency and automatic enforcement.Moreover, e-RUPI also reconfigures the idea of *trustworthiness* in public-private collaborations. In India's often fragmented health ecosystem split between public dispensaries, private clinics, and third-party NGOs establishing trust across actors with competing incentives is difficult. By introducing a system in which payments are auto-validated and purpose-limited, blockchain principles can help build a common accountability structure. This is especially crucial in vaccine campaigns or maternal healthcare, where efficient and timely delivery can mean the difference between life and death.

Critically, the deployment of e-RUPI also reveals the limitations and contextual challenges of blockchain-driven decentralization. Unlike blockchain's ideal of radical openness and decentralization, e-RUPI operates within a highly centralized, state-regulated digital infrastructure. The central bank, the NPCI, and government ministries retain control over rules, implementation, and data (Schuler et al., 2024). Thus, the "decentralization" here is symbolic and conditional. Nevertheless, the system decentralizes *trust functions* it distributes the burden of verification and ensures that actors trust the logic of the system, rather than the institutions themselves–and illustrates how blockchain principles, such as automated execution, immutability, and transparency, can be adapted to real-world constraints, particularly in complex welfare ecosystems. Rather than replacing existing governance institutions, such systems *augment institutional trust* through digital architecture. It offers a model in which blockchain-inspired trust does not demand wholesale systemic overhaul but instead enhances targeted efficiency and accountability. In emerging economies such as India, such hybrid models may offer the most viable pathway toward decentralized trust, not through disruption but through calibrated transformation.

The case of blockchain-enabled land titling in Andhra Pradesh, India, provides fertile ground to reflect the theoretical implications of trust in decentralized technological systems. Classical trust theory in sociology and economics, particularly as articulated by scholars such as Niklas Luhmann and Anthony Giddens, posits trust as a mechanism that reduces social complexity and enables cooperation under uncertain conditions (Jonnalagadda et al., 2021). In traditional governance systems, institutional trust rooted in bureaucracies, legal systems, and social norms acts as a glue that binds individual and collective action. Blockchain challenges this assumption by relocating the trust locus from institutions to codes, algorithms, and distributed consensus.

This shift exemplifies what Primavera De Filippi and Aaron Wright describe as a move from "trust in institutions" to "trust in technology." Here, trust is not earned through human judgment or legitimacy but is mathematically ensured through cryptographic protocols and immutable records. However, this techno-centric vision of trust has certain limitations (Gresse & Linde, 2020). Blockchain's reliance on transparency and automated enforcement often abstracts the social and contextual dimensions of trust. For example, in land titling, while blockchain can reduce corruption and transaction fraud, it cannot address complex socio-legal disputes over customary land rights or informal tenure issues deeply embedded in local histories and power dynamics.From a critical theory lens, this raises the question: is blockchain creating a new kind of depoliticized trust, one that displaces human discretion with algorithmic authority? If so, it risks reinforcing techno-solutionism and sidestepping structural inequality. Postcolonial critiques further warn that such systems, designed largely in the Global North, may be ill-equipped to navigate the plural legal culture and governance ecologies of the Global South. Thus, while blockchain offers a reimagining of trust for decentralized futures, the theoretical reflection reveals that such a reimagining must be embedded within, not abstracted from, the sociopolitical realities of the contexts in which it operates.

CONTRIBUTION AND INNOVATION

Traditional models of trust have long been embedded in centralized institutions such as banks, governments, and corporations, where authority, regulation, and enforcement mechanisms guarantee legitimacy and reduce uncertainty. However, blockchain technology compels us to reconceptualize trust as a system-embedded, protocol-driven condition rather than an interpersonal or institutional phenomenon (Hossain et al., 2020). The novelty of blockchain lies not only in its technical design, but also in how it reshapes trust into an operational outcome of algorithmic consensus rather than a subjective social relation. This shift is radical: trust is no longer extended based on credibility or historical reputation but is "outsourced" to code and cryptographic mechanisms. This constitutes a paradigmatic reorientation, from *trust in people* to *trust in systems. The* key insight emerging is that blockchain does not eliminate trust; rather, it reconfigures its architecture. It transforms the *who* and *how* of trust into questions of *what rules*, *what codes*, and *what consensus protocols* can be collectively accepted. This new model introduces a form of "programmed trust," which paradoxically requires both absolute transparency (in the form of publicly auditable ledgers) and absolute opacity (in terms of users' anonymized identities). Such dualities challenge existing assumptions in both technological and sociological discourse.

Moreover, in decentralized blockchain ecosystems, trust becomes both dynamic and participatory. Actors are not passive recipients of institutional guarantees, but co-producers of the trust infrastructure itself, through mining, validating, voting on governance protocols, or even participating in decentralized autonomous organizations (DAOs). This participatory model opens up a democratic imaginary for trust, one that is mutable, contingent, and embedded in a networked social contract (Bellavitis et al., 2022). This presents an opportunity to rethink not only technological infrastructures but also social and political architectures of collaboration, accountability, and legitimacy.In emerging economies and postcolonial contexts often marked by institutional mistrust blockchain's promise is particularly potent. It offers an alternative trust scaffold, in which traditional systems have failed or been excluded. However, this innovation also introduces new asymmetries and risks that must be critically examined. As such, this chapter proposes a hybrid understanding of trust: one that bridges algorithmic verifiability with sociocultural legitimacy, reasserting the need for plural trust frameworks in the decentralized futures we imagine.

This chapter critically examines the interplay between blockchain technology and the reconfiguration of trust, particularly within decentralized systems. Drawing from technological, economic, and sociopolitical perspectives, we argue that blockchain does not merely serve as a technical protocol for recording transactions; rather, it embodies a new epistemology of trust that is programmable, transparent, and distributed (Bennet et al., 2024). Unlike traditional systems that centralize trust in institutions, such as banks, states, or corporations, blockchain enables trust to be embedded within the code itself, shifting authority from social hierarchies to algorithmic consensus. However, this shift is not without complexity or contradiction.Our central proposition is that blockchain engenders a “post-institutional trust paradigm,” wherein credibility is increasingly verified through decentralized, cryptographic processes rather than interpersonal or institutional relationships. This transformation is not purely technological but deeply conceptual trust is no longer rooted in historical reliability or reputation but in real-time validation and auditability. As such, blockchain presents both a rupture and a continuation: it disrupts long-standing mechanisms of trust while also extending the Enlightenment ideals of rational governance and traceability into the digital domain.

IMPLICATIONS AND FUTURE DIRECTIONS

This synthesis suggests that blockchain should be understood as a socio-technical imaginary a collective vision of a future organized around transparency, autonomy, and distributed agency. However, such imaginaries must be interrogated, as they risk obscuring issues of access, inequality, and governance opacity (Carter & Ubacht, 2018). Therefore, the proposition is not to romanticize blockchain but to foreground its dual capacity: it can decentralize power and democratize systems, but it can also reproduce exclusion under the guise of neutrality. Future research and design must account for these tensions, embedding ethical foresight into the very protocols that promise to reshape our notions of trust.The rise of blockchain technology compels a fundamental rethinking of how trust is theorized in the digital age. Traditional models of trust rooted in interpersonal relations, institutional authority, and state-backed legitimacy are increasingly inadequate for capturing the distributed, cryptographic, and often anonymous infrastructure that blockchain enables. Theoretically, blockchain signals a paradigm shift from relational trust to what may be termed protocol-based or algorithmic trust. This re-conceptualization challenges normative assumptions within fields such as economics, political science, and sociology, which have long treated trust as a social contract contingent on human actors and their reputations.

Moreover, blockchain decouples trust from centralized power structures, raising critical questions about post-institutional governance. By embedding trust within codes, consensus mechanisms, and smart contracts, blockchain reconfigures the locus of authority, suggesting new directions for theorizing sovereignty, legitimacy, and social coordination (De Filippi et al., 2024). This has significant implications for political theory, particularly around concepts such as decentralization, anarchism, and commons. Blockchain invites interdisciplinary theorization that draws from actor-network theory, assemblage theory, and systems theory, emphasizing how trust emerges from techno-social entanglements rather than stable institutional guarantees as well as the temporality and transparency of blockchain foregrounds as essential dimensions of trust. The immutable nature of distributed ledgers reorients trust toward the traceability of actions over time, shifting emphasis from future-oriented promises to past-verified behavior. This reorientation may necessitate new ethical frameworks to understand responsibility, consent, and accountability in automated systems. Finally, theoretical work on blockchain trust must grapple with its contradictions: how protocols can both enable radical openness and reproduce new forms of exclusion or opacity. As such, blockchain is not merely a technical innovation, but a conceptual frontier that compels scholars to rethink the foundations and futures of trust itself.

As blockchain technology matures, a rich landscape of research opportunities has emerged across disciplines. One critical area is the empirical assessment of how decentralized trust operates in diverse sociopolitical and cultural contexts (Danzi et al., 2020). Comparative studies of blockchain adoption in the Global South and the Global North can illuminate how trust is reconstituted in the absence of traditional intermediaries. Another promising avenue involves examining the unintended consequences of algorithmic governance, particularly how smart contracts and decentralized autonomous organizations (DAOs) may embed new asymmetries or biases under the guise of neutrality. Additionally, research on hybrid trust models, combining blockchain with conventional regulatory frameworks, can provide insights into more inclusive governance architectures. There is also a pressing need to explore the ethical questions surrounding data permanence, transparency, and consent in public ledgers. Interdisciplinary approaches that blend insights from economics, law, anthropology, and computer science can enrich the conceptual terrain and address normative questions regarding power, accountability, and justice in decentralized futures. Finally, longitudinal studies tracking the evolution of user trust in blockchain systems, especially during crises or systemic shocks, can provide invaluable insights into the resilience and limits of distributed trust infrastructure.

The practical relevance of blockchain's trust architecture lies in its transformative potential across sectors, plagued by opacity, centralization, and inefficiency. In finance, smart contracts reduce dependency on intermediaries and enforce accountability through codes (Omar et al., 2022). In supply chains, blockchain ensures traceability and provenance, thereby enhancing consumer trust and regulatory compliance. Governance systems can adopt decentralized ledgers for transparent voting or public record-keeping, thus restoring citizen faith in institutions. Even humanitarian aid can be streamlined through verifiable, fraud-resistant digital identities and disbursement systems. For practitioners, technologists, policymakers, or social entrepreneurs, the ability to reimagine trust without centralized enforcement creates opportunities for innovation, inclusion, and resilience in a rapidly digitizing world.

CONCLUSION

The rise of blockchain technology has brought to the fore radical rethinking of trust in the digital age. Traditionally embedded in institutional frameworks, such as banks, governments, and legal systems, trust has long been predicated on hierarchical authority and centralized verification (Bennet et al., 2024). By contrast, blockchain decentralizes the architecture of trust and distributes verification across a peer-to-peer network, thereby challenging longstanding notions of credibility, authenticity, and authority. This chapter traces how the concept of trust is transformed within decentralized systems and examines the sociotechnical implications of this transformation across various domains, from finance to governance.

Conceptually, we clarified that blockchain is not merely a technological protocol but also a socio-political infrastructure, embedding values of transparency, immutability, and distributed consensus. We explored the evolution of trust from interpersonal and institutional models to algorithmic and protocol-based trust by situating blockchain within broader debates in information ethics, political economy, and technology (Hazarika & Shah, 2024). This shift has implications not just for transactional interactions but for the structure of collective belief systems and governance mechanisms.Theoretically, the chapter engaged with perspectives from economics, philosophy of technology, and critical media studies to analyze both the promises and pitfalls of decentralized trust. While some frameworks celebrate blockchain's potential to democratize access, reduce fraud, and disrupt exploitative intermediaries, others caution against introducing new forms of opacity, techno-determinism, and exclusion. We highlight the tension between the rhetoric of decentralization and the realities of technical complexity, energy-intensive infrastructure, and emergent power concentrations within blockchain ecosystems.

Through illustrative casessuch as decentralized finance (DeFi), digital identity verification systems, and blockchain-enabled voting, we examined how trust is operationalized and contested in practice. These cases underscore that the deployment of blockchain is never purely technical; it is deeply enmeshed in socio-political values, legal constraints, and cultural contexts. The chapter emphasized the importance of interrogating who gets to design trust systems, whose interests they serve, and how inclusive or exclusive these systems are ultimately (K et al., 2023).In synthesizing these insights, the chapter argued for a more critical and nuanced understanding of trust in decentralized futures, one that goes beyond technological optimism and engages with ethical, epistemological, and political dimensions. Blockchain may decentralize verification; however, it cannot automate trust as a social relationship. The future of decentralized systems must address this fundamental paradox. As we move forward, interdisciplinary inquiry and inclusive governance will be vital to ensuring that blockchain technologies are leveraged not just for innovation but also for justice, accountability, and genuinely democratic participation.

References

Afzaal, H., Gochhayat, S. P., Imran, M., & Janjua, M. U. (2022). Formal Modeling and Verification of a Blockchain-Based Crowdsourcing Consensus Protocol. *IEEE Access*, *10*, 8163–8183. https://doi.org/10.1109/access.2022.3141982

Allen, D. W. E., Berg, C., & Novak, M. (2018). Blockchain: an entangled political economy approach. *Journal of Public Finance and Public Choice*, *33*(2), 105–125. https://doi.org/10.1332/251569118x15282111163993

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5

Bellavitis, C., Fisch, C., & Momtaz, P. P. (2022). The rise of decentralized autonomous organizations (DAOs): a first empirical glimpse. *Venture Capital*, *25*(2), 187–203. https://doi.org/10.1080/13691066.2022.2116797

Bennet, D., Maria, L., Rahmania Az Zahra, A., & Putri Ayu Sanjaya, Y. (2024). Blockchain Technology: Revolutionizing Transactions in the Digital Age. *ADI Journal on Recent Innovation (AJRI)*, *5*(2), 194–199. https://doi.org/10.34306/ajri.v5i2.1065

Biryukov, A., & Tikhomirov, S. (2019, June 1). *Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis*. https://doi.org/10.1109/eurosp.2019.00022

Bodó, B., & Janssen, H. (2022). Maintaining trust in a technologized public sector. *Policy and Society*, *41*(3), 414–429. https://doi.org/10.1093/polsoc/puac019

Carter, L., & Ubacht, J. (2018). *Blockchain applications in government*. 1–2. https://doi.org/10.1145/3209281.3209329

Chatziamanetoglou, D., & Rantos, K. (2024). Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers*, *13*(3), 60. https://doi.org/10.3390/computers13030060

Crandall, J. (2019). Blockchains and the "Chains of Empire": Contextualizing Blockchain, Cryptocurrency, and Neoliberalism in Puerto Rico. *Design and Culture*, *11*(3), 279–300. https://doi.org/10.1080/17547075.2019.1673989

Danzi, P., Popovski, P., Kalor, A. E., Stefanovic, C., Nguyen, L. D., Hagelskjaer, A. K., & Sorensen, R. B. (2020). Communication Aspects of the Integration of Wireless IoT Devices with Distributed Ledger Technology. *IEEE Network*, *34*(1), 47–53. https://doi.org/10.1109/mnet.001.1900180

De Filippi, P., Mannan, M., & Reijers, W. (2024). *Blockchain Governance*. Massachusetts Institute Of Technology. https://doi.org/10.7551/mitpress/14994.001.0001

Gresse, W. G., & Linde, B. J. (2020). The anticipatory psychological contract of management graduates: Validating a psychological contract expectations questionnaire. *South African Journal of Economic and Management Sciences*, *23*(1). https://doi.org/10.4102/sajems.v23i1.3285

Hamilton, M. (2019). Blockchain distributed ledger technology: An introduction and focus on smart contracts. *Journal of Corporate Accounting &amp; Finance*, *31*(2), 7–12. https://doi.org/10.1002/jcaf.22421

Hazarika, A., & Shah, M. (2024). Blockchain-based Distributed AI Models: Trust in AI model sharing. *International Journal of Science and Research Archive*, *13*(2), 3493–3498. https://doi.org/10.30574/ijsra.2024.13.2.2598

He, S., Tang, Q., Wu, C. Q., & Shen, X. (2019). Decentralizing IoT Management Systems Using Blockchain for Censorship Resistance. *IEEE Transactions on Industrial Informatics*, *16*(1), 715–727. https://doi.org/10.1109/tii.2019.2939797

Hossain, M. P., Rahaman, M. A., Saju, S. A., Khaled, M., Roy, S., & Biswas, M. (2020). *Vehicle Registration and Information Management using Blockchain based Distributed Ledger from Bangladesh Perspective*. 900–903. https://doi.org/10.1109/tensymp50017.2020.9230781

Jimmy, F. (2024). Enhancing Data Security in Financial Institutions with Blockchain Technology. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *5*(1), 424–437. https://doi.org/10.60087/jaigs.v5i1.217

John, T., & Pam, M. (2018). Complex Adaptive Blockchain Governance. *MATEC Web of Conferences*, *223*, 01010. https://doi.org/10.1051/matecconf/201822301010

Jonnalagadda, I., Stock, R., & Misquitta, K. (2021). TITLING AS A CONTESTED PROCESS: Conditional Land Rights and Subaltern Citizenship in South India. *International Journal of Urban and Regional Research*, *45*(3), 458–476. https://doi.org/10.1111/1468-2427.13002

K, D. K., B, P. S., Hj, S., G, V., P, S., & N, D. (2023). Comparative Analysis of Transaction Speed and Throughput in Blockchain and Hashgraph: A Performance Study for Distributed Ledger Technologies. *Journal of Machine and Computing*, 497–504. https://doi.org/10.53759/7669/jmc202303041

Le Quoc, D., Nguyen Quoc, H., & Nguyen Van, H. (2025). Evaluating the influence of digital financial inclusion on financial crises and economic cycles: a Bayesian logistic regression insight. *Journal of Financial Regulation and Compliance*, *33*(2), 280–301. https://doi.org/10.1108/jfrc-10-2024-0206

Lee, M., Ijsselsteijn, W., & Frank, L. (2021). Brokerbot: A Cryptocurrency Chatbot in the Social-technical Gap of Trust. *Computer Supported Cooperative Work (CSCW)*, *30*(1), 79–117. https://doi.org/10.1007/s10606-021-09392-6

Leonardos, N., Leonardos, S., & Piliouras, G. (2020). *Oceanic Games: Centralization Risks and Incentives in Blockchain Mining* (pp. 183–199). Springer. https://doi.org/10.1007/978-3-030-37110-4_13

Levy, K. E. C. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, *3*, 1–15. https://doi.org/10.17351/ests2017.107

Mezquita, Y., Corchado, J. M., Gil-González, A. B., Martín Del Rey, A., & Prieto, J. (2022). Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. *Energies*, *15*(9), 3046. https://doi.org/10.3390/en15093046

Munir, M. A., Hasan, M., Uzair Ayub, H. M., Hussain, A., Sultan, M., Imran, S., Masood, T., Shahbaz, M. A., Habib, M. S., Salman, C. A., Mujtaba, M. A., Akhtar, M. S., & Qamar, A. (2022). Blockchain Adoption for Sustainable Supply Chain Management: Economic, Environmental, and Social Perspectives. *Frontiers in Energy Research, 10*. https://doi.org/10.3389/fenrg.2022.899632

Nabben, K. (2021). Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology. *Frontiers in Computer Science, 2*. https://doi.org/10.3389/fcomp.2020.599406

Omar, I. A., Hasan, H. R., Omar, M., Jayaraman, R., Debe, M. S., & Salah, K. (2022). Supply Chain Inventory Sharing Using Ethereum Blockchain and Smart Contracts. *IEEE Access*, *10*, 2345–2356. https://doi.org/10.1109/access.2021.3139829

Schuler, K., Schär, F., & Cloots, A. S. (2024). On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance. *Journal of Financial Regulation*, *10*(2), 213–242. https://doi.org/10.1093/jfr/fjad014

Singh, A., Rani, R., Ganesh, A., Patil, R. R., Pippal, S. K., & Kumar, S. (2023). Secure Voting Website Using Ethereum and Smart Contracts. *Applied System Innovation*, *6*(4), 70. https://doi.org/10.3390/asi6040070

Tomatsu, Y., & Han, W. (2023). Bitcoin and Renewable Energy Mining: A Survey. *Blockchains*, *1*(2), 90–110. https://doi.org/10.3390/blockchains1020007

Trivedi, S., Mehta, K., & Sharma, R. (2021). Systematic Literature Review on Application of Blockchain Technology in E-Finance and Financial Services. *Journal of Technology Management &amp; Innovation*, *16*(3), 89–102. https://doi.org/10.4067/s0718-27242021000300089

Wang, W., Du, L., & Yu, Y. (2022). Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-12412-0