frontiers
in Computer Science

HYPOTHESIS AND THEORY
published: 22 March 2021
doi: 10.3389/fcomp.2020.599406

Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology

Kelsie Nabben *

Blockchain Innovation Hub, RMIT University, Melbourne, VIC, Australia

The notion that blockchains offer decentralized, "trustless" guarantees of security through technology is a fundamental misconception held by many advocates. This misconception hampers participants from understanding the security differences between public and private blockchains and adopting blockchain technology in suitable contexts. This paper introduces the notion of "people security" to argue that blockchains hold inherent limitations in offering accurate security guarantees to people as participants in blockchain-based infrastructure, due to the differing nature of the threats to participants reliant on blockchain as secure digital infrastructure, as well as the technical limitations between different types of blockchain architecture. This paper applies a sociotechnical security framework to assess the social, software, and infrastructural layers of blockchain applications to reconceptualize "blockchain security" as "people security." A sociotechnical security analysis of existing macrosocial level blockchain systems surfaces discrepancies between the social, technical, and infrastructural layers of a blockchain network, the technical and governance decisions that characterize the network, and the expectations of, and threats to, participants using the network. The results identify a number of security and trust assumptions against various blockchain architectures, participants, and applications. Findings indicate that private blockchains have serious limitations for securing the interests of users in macrosocial contexts, due to their centralized nature. In contrast, public blockchains reveal trust and security shortcomings at the micro and meso-organizational levels, yet there is a lack of suitable desktop case studies by which to analyze sociotechnical security at the macrosocial level. These assumptions need to be further investigated and addressed in order for blockchain security to more accurately provide "people security".

Keywords: blockchain, security, socio-technical, design, trust, decentralization

OPEN ACCESS

Edited by:
Alex C. Ng,
La Trobe University, Australia

Reviewed by:
Shorouq Alansari,
University of Southam,
United Kingdom
Hassan Chizari,
University of Gloucestershire,
United Kingdom
Alan Colman,
Swinburne University of Technology,
Australia

Correspondence:
Kelsie Nabben
kelsie.nabben@rmit.edu.au

Specialty section:
This article was submitted to
Computer Security,
a section of the journal
Frontiers in Computer Science

Received: *27 August 2020*
Accepted: *23 December 2020*
Published: *22 March 2021*

Citation:
Nabben K (2021) Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology.
Front. Comput. Sci. 2:599406.
doi: 10.3389/fcomp.2020.599406

INTRODUCTION

Blockchain is forecast to be "future of financial and cybersecurity" and has the potential to "revolutionize applications and redefine the digital economy" (Singh and Singh, 2016; Underwood, 2016). Blockchains hold great promise to re-instate "trust" in society by enabling coordination without trust (Shahaab et al., 2020). If this is the case, then it is imperative to develop blockchains into functional, digital institutional infrastructure with transparent governance, security, and operational rules. Yet, it is rarely acknowledged that security and trust in blockchains are contextual, according to the type of blockchain architecture, the governance model, the needs of the participants using the system, and the context in which it is being applied. Beginning from the premise that blockchains are sociotechnical systems, this paper explores the question: “What security guarantees do different types of blockchain-based systems offer people?” The aim of this analysis is to apply a sociotechnical security approach to blockchains to clarify expectations, assumptions, and guarantees for those deploying and employing blockchains, in order to more accurately meet the expectations of participants in blockchain-based systems. By adopting a sociotechnical security analysis framework, this paper argues that both public and private blockchains have social, technical, and infrastructure layer security shortcomings. For private blockchains, these trust and security issues are evident in macrosocial (societal) applications. For public blockchains, security issues are present at the micro- (individual) and meso- (organizational) levels and unknown at the macrosocial level as there is a lack of suitable desktop case studies by which to analyze security in broader, social applications. Given the sociotechnical nature of blockchain-based systems, this sociotechnical security approach is termed “people security.” These findings are important as the sociotechnical trust and security gaps of different types of blockchains, across different applications are underexplored, despite the increasing prominence of blockchain-based systems in organizations and society.

Structure of the Paper

First, this paper defines blockchains as a sociotechnical construct and outlines the different types of blockchains and the traditional promises of “blockchain security.” Then, it adopts a sociotechnical security lens to frame “blockchain security” as “people security” and applies a sociotechnical security approach to both public blockchains and private blockchains (*Applying Sociotechnical Security to Blockchains Section*). Here, it becomes evident that both public and private blockchains still hold inherent trust and security limitations in terms of technical security, trust in social processes, and infrastructural dependencies. This paper finds that although public blockchains afford users with a greater participatory role in technical and governance processes, private blockchains are more commonly being adopted in contexts that require macrosocial coordination systems, resulting in inherent security limitations for participants through centralization (*Observations and Findings Section*). If blockchains are to become any closer to fulfilling their promise as “tools of trust” to offer more secure institutional infrastructures in society, a sociotechnical “people security” approach is essential (*In Code We Trust? The Limitations of Security in Blockchains Section*). Further research directions are then proposed to extend this study (*Conclusion and Further Directions Section*).

METHODOLOGY

This paper adopts a science and technology studies (STS) methodology to analyze blockchains as interdisciplinary sociotechnical systems that are co-constructed in relations between the technology itself and the “real-world” social processes, norms, and application in various forms of organizations (Singh, 2011). The approach is grounded in a social-constructivist view of security in sociotechnical systems, to reflect on the narrower technological determinist perspective which dominates much of the current discourse on blockchain security. Sociotechnical studies allow us to view cryptoeconomic organizing technologies as complex social systems that operate at three primary levels: the work systems level, the whole organization level, and the macrosocial system. Eric Trist first described sociotechnical systems, in the context of the coal mining industry, as microlevel work practices, meso-level organizational practices, and macro-level social systems (Trist, 1981). All three of these “multiscale” levels are apparent in the organizational capabilities of blockchains, in the actions of individual agents, the system level setting of objectives, and the structural, complex system level (Voshmgir and Zargham, 2019). Hayes suggests that blockchain-based cryptoeconomic systems should not be studied as money per se, but rather as systems that organize individuals through the radical disintermediation of institutions (Hayes, 2019). Thus, employing STS methods is a suitable approach to reveal the implicit and embedded technical, social, economic, and political assumptions and decisions that influence how blockchains are applied in social contexts (Bijker et al., 2012).

A sociotechnical security framework will be applied to analyze how understandings of blockchain security can evolve to consider “people security.” This framing broadens existing technical approaches to inspect the social layer (people and processes), software layer (code and applications), and the infrastructure layer (physical and technological infrastructure) (Li et al., 2018). This sociotechnical approach to blockchain security is termed “people security.” Through desk research, this study examines this approach by discussing various cases of both public and private blockchains.

Contributions

The Key Contributions of This Paper

i. Framing of blockchains as a sociotechnical construct and multiscale institutional infrastructure that operates at micro-, meso-, and macrosocial levels across different implementations.
ii. A sociotechnical analysis of the security attributes and limitations of blockchain security for people across various types of blockchains and blockchain applications, to expose the trust and security issues.
iii. An analysis of the security assumptions for participants across different types of blockchain applications, including possible future risks from blockchain automation and why blockchain may not be a desirable digital infrastructure in macrosocial contexts.

The innovation of public blockchains is the application of cryptoeconomic mechanisms to facilitate coordination at each level of a complex, sociotechnical digital system.

At the technical level, blockchains incorporate the encoding of economic game-theory mechanisms of byzantine fault tolerance and governance rules to enforce certain attributes, such as Sybil resistance, execute transactions, and perform certain functions as part of a broader system. At an organizational infrastructure level, blockchains are responsible for coordination within a system. At a macrosocial level, blockchains operate as a coordinating technology at the social, economic, and political level in society (Berg et al., 2019a).

BLOCKCHAINS AS A SOCIOTECHNICAL CONSTRUCT

Blockchain security in a cybersecurity sense tends to consider blockchains as a technical object of inquiry, when in fact they are a sociotechnical construct (Hayes, 2019). Blockchains enable transactions between participants in a network. They can be centrally issued and administrated ("permissioned" or "semi-permissioned"), such as private and consortium blockchains, or public and "permissionless". The key attributes of both public and private blockchains demonstrate the ways in which security is both a technical and a social consideration.

Different Types of Blockchains

Blockchain technologies can be divided into three broad categories. These distinctions are important for understanding the role of people in the system and how the system operates in the context in which it is applied.

Public Blockchains

Public blockchains emphasize transparency and participation. The consensus of transactions is "decentralized," in that anyone can participate in validating transactions on the network, and the software code is publicly available or "open-source." Examples include Bitcoin and Ethereum.

The key attribute of public blockchain networks is that they pursue decentralization through cryptoeconomics, to ensure cooperation in a distributed network. In this case, decentralization refers to the characteristic of having no political center of control and no architectural central point-of-failure in the design of the software system (Buterin, 2017). The degree to which a blockchain is decentralized depends on design of the consensus algorithm, issuance of cryptoeconomic incentives, ownership of cryptographic "private keys," and governance of the network. Governance considerations include who can develop the software code, who can participate in the consensus mechanism, and who can take part in communal governance activities to maintain the network.

Consensus mechanisms are predominantly "Proof-of-Work" (PoW) or "Proof-of-Stake" (PoS).

Public blockchains can be applied to macrosocial coordination problems in society, due to their unique ability to provide decentralized consensus.

Private Blockchains

Private blockchains mean that membership to participate in validating transactions on the network is restricted to only include parties that are approved by a central administrator. Thus, private blockchains are centralized and operate more closely to a traditional database, than a complex, macrosocial coordination system. Transaction data is most often kept private.

Private blockchains often employ a "Proof-of-Authority" (PoA) consensus approach (Peng et al., 2020).

Private blockchains are often adopted in internal, business secure environments, such as access, authentication, and record keeping.

Consortium Blockchains

Consortium blockchains are comprised of known participants that are preapproved by a central authority to participate in consensus in a blockchain network. This "semi-permissioned" approach allows for a network to be distributed, or partly decentralized, while allowing for a degree of control over a network. Transaction data may be kept private.

Consortium blockchains can reach consensus *via* PoW, PoS, PoA, or others, such as delegated proof-of-stake, and more.

This type of blockchain may be used between known parties, in supply chain management, banking, or Internet of Things (IoT) applications.

Security in Different Types of Blockchains—Surfacing Assumptions

Blockchain security research is deeply focused on the technical attributes of security, which are under continuous development and improvement to strive toward the goal of offering stronger security guarantees to users (Karame and Androulaki, 2016; Li et al., 2020). All blockchains rely on secure software code to enable peer-to-peer transactions through the use of digital currency to offer security to users. A number of blockchain cybersecurity vulnerabilities remain under active investigation in the field of computer science (Lin and Liao et al., 2017; Chen et al., 2019; Zhang et al., 2019).

What security means for users of a blockchain network is different across different disciplines. While cybersecurity focuses on securing networks from threats, sociotechnical security focused on securing participants in the network.

Public blockchains are often referred to as decentralized, transparent, autonomous, immutable, and pseudonymous (Buterin, 2017). Transactions are executed by software code in "smart contracts" or rules that govern the network (Allen et al., 2019). According to the game theory of "cryptoeconomics," economic incentives align the interests of participants for cooperation within the network. Ownership of these cryptographically secure digital assets makes it very expensive to tamper with the network and prevent "double-spending" the same digital assets in the network, despite distributed computation of transactions (Berg et al., 2019b). The broader "consensus algorithms" that secure the network against cooption or "forking" of the ledger of transaction history *via* a 51% attack to control the network differ depending on the design of the particular blockchain network (Bach et al., 2018).

Thus, the fundamental threat which "blockchain security" protects against through technical characteristics and economic consensus mechanisms is centralization. The attribute of decentralization in public blockchains refers to freedom from relying on central intermediaries in its original interpretation from the cypherpunk culture and cryptoanarchic politics from which Bitcoin, the first fully functioning decentralized public blockchain, emerged (May, 1994).

In contrast, when information and validation on a blockchain is limited to certain parties, as with private and consortium blockchains, the privacy and security guarantees for users of that chain become very different. On private and permissioned blockchains, transactions can be censored through corruption or collusion, rules can be altered without the participation of users, and the administrator owns the digital assets of users if they hold the cryptographic "keys" to that data. Storage and computation may be distributed but the "nodes" (people that run software code) that validate transactions are known to other parties in the network and governance authority is not decentralized (Underwood, 2016). These design and governance attributes have critical security implications for the assumptions of people that participate in the network, if a blockchain is applied as a coordinating system in society, but still controlled by a central issuer and administrator.

Understanding the type of blockchain, who is being trusted, the needs of participants, and the context in which the blockchain is being applied is vital in reframing blockchain security in a sociotechnical setting.

APPLYING SOCIOTECHNICAL SECURITY TO BLOCKCHAINS

Sociotechnical security allows for a broader security analysis lens, encompassing the social, technical, and contextual aspects of a digital system. These aspects are integral to studying the security of blockchains as macrosocial infrastructure in society. This lens reframes "blockchain security" from referring to "decentralization from trusted third parties," to "people security", which considers the expectations and the needs of users as participants in blockchain-based systems.

A sociotechnical analysis is particularly valuable in analyzing blockchain systems in macrosocial contexts. People depend on "macrosocial" institutional infrastructure to govern society. As these institutions become digitized in the post-internet era, including through the adoption of blockchains, then blockchain design requires deliberate attention regarding the promises of decentralization and "trustless" security often given.

Governance in blockchain-based systems presents unique security challenges as it is encoded in the technical aspects of blockchain-based systems as governance rules are formalized in software code. The aim of governance in sociotechnical settings is to recognize the need to support flexible interactions among participants in the administration of network settings (Singh, 2011). While public blockchains encourage people to participate in software development, consensus mechanisms, and ongoing governance decisions: private blockchains generally maintain these governance functions centrally, reducing the role of people to that of "users", rather than participants. A sociotechnical lens to analyze governance in blockchains questions what is external, or "constituted of", and what is internal, or "constituted within", through interactions between administrators, technology, participants and other stakeholders in the network (Smith and Stirling, 2006).

More limited security frameworks that only focus on the technical components of a system do not fully address the challenges of participatory information systems, as they tend to disassociate people as "passive recipients of engineering decisions" instead of orienting the system around the expectations and needs of people (Goerzen et al., 2019). This is not to say that existing security practices are wrong, but rather that science and technology studies can further enhance security practices by drawing in an analysis of the social aspects of a system, especially in digital systems that operate in an institutional infrastructure role in society, such as blockchain.

Systems that are secure when used by people, known as "effective security", are complex and difficult to achieve because of gaps in the designer's awareness of user goals, threats, and behaviors in practice (Ferreira et al., 2014). Sociotechnical security offers a general approach to study the interacting layers of technical, social, and contextual aspects of security, by asking "who in the community participating in the network is in need of protection?", "what features can be exploited within this dynamic, human network—including technical as well as agency, governance, and influence?", "what are the external and internal threats to participants, including other participants?" and "who is responsible and accountable for securing participants in the network?" (Goerzen et al., 2019). If blockchains are to be applied as organizational and macrosocial structures, a sociotechnical understanding of blockchain security is required, to place the participants within the system as the referent focus of security. This can be referred to as "people security."

Security threats in sociotechnical systems relate to both intentional and nonintentional exploits. Latour refers to using a system outside of its anticipated context of use or application as "antiprograms" (Latour, 1990). These lenses require us to consider the expectations and intent of participants in the system. There are numerous frameworks by which to guide a sociotechnical analysis of blockchains. "Sociotechnical Attack Analysis" or "STEAL" is one example which supports both a formal technical analysis and a hypothetical deductive social analysis of a complex system (Ferreira et al., 2014). Rather than inventing a new security framework, the contribution of this paper is to apply a sociotechnical security approach to blockchains as macrosocial institutional technology.

The "people security" approach takes an existing sociotechnical security framework and applies it to blockchain, to investigate the role of people in both public and private blockchain instantiations. "People security" applies a simple, pre-existing three-layer sociotechnical security analysis to blockchains. This includes the social layer (people and processes), the software layer (code and applications), and the infrastructure layer (physical and technological infrastructure) (Li et al., 2018). The aim of this approach is to determine if a blockchain system can adapt to serve the security needs of users or furthermore investigate where and how people are reoriented from "users" to "participants" in certain blockchain architectures.

The next section of this paper applies a sociotechnical security analysis to blockchains to address how the social, technical, and infrastructural layers of the system are interconnected, with the aim of revealing assumptions about where and how blockchains are applied in relation to context, participant needs, and expectations.

PEOPLE SECURITY AND PUBLIC BLOCKCHAINS

Public blockchains remove the ability for central parties to unilaterally change the rules of the system to secure users against third-party interference. They do so by aligning economic incentives among participants to enable "trustless" interactions, whereby actors or "nodes" in a network can collaborate with others they do not know or trust. This is often referred to as "trustlessness" (Xinyi et al., 2018). The notion of blockchains as a trustless technology has been reinforced in numerous studies on blockchains, advocating for "code as law," whereby participants can collaborate with others that they do not know or trust according to the rules of the software code-governed network (Vidan and Lehdonvirta, 2019).

Trustlessness requires trust. Rather than a rhetoric of trustlessness, we must interrogate who is being trusted to design, deploy, and secure blockchain-based systems against the expectations of participants in that network. Blockchain security as a guarantee against the threat of centralization and a promise of trustlessness can be misleading.

In the first instance the rules of blockchain-based technology are a product of the context and beliefs in which they were developed and then applied. For example, the narrative of "trustlessness" is heavily embedded in the libertarian ideology and tech-utopian narratives that have informed the development of the technology (May, 1994). The development of peer-to-peer electronic cash emerged from the discourse and action of the "cypherpunks." This heterogeneous group of cryptography advocates, developers, and philosophers jointly participated in an online mailing list, administered by cryptoanarchists Timothy May, Eric Hughes, and John Gilmore (May, 1992; Hayes, 2019). This "technopolitics" heavily influences the ideology and security aspirations of public blockchains (Larkin, 2013).

In public blockchains, the ideology of trustlessness refers to the "cypherpunk philosophy of leveraging the economic cost of an attack on the network vs. the cost to use and maintain it, to preserve the autonomy of individuals that are reflected in cryptoeconomics consensus mechanisms" (Buterin, 2016). Trustlessness in not requiring third-party verification to execute transactions has been conflated with broader meanings of trust, which can create misleading assumptions regarding the capabilities of blockchains for users beyond the initial context (Chohan, 2019). Bitcoin, the initial "peer-to-peer electronic cash," is described by its inventor, the pseudonymous "Satoshi Nakamoto" as being "an electronic payment system based on cryptographic security instead of trust allowing any two willing parties to transact directly with each other without the need for a trusted third party" Nakamoto, (2009). From these origins, trustlessness is a normative property that represents what people *hope to achieve* with blockchain technology, rather than a security guarantee.

Trust between people is actually required on *an ongoing basis* between stakeholders in the "multi-sided" aspects of a blockchain-based system, including code development by developers, maintenance by miners, and participation by users. Trustlessness really refers to "trust minimization," as it is not possible for participants to maintain zero trust at every layer of the blockchain.

When blockchains are applied to manage macrosocial interactions that are responsible for the coordination of, and arbitration between, people in society, they function as institutions. The aim here is not to substitute human trust with computation but to offer trust guarantees through technical and social mechanisms, thus establishing "trustful" infrastructures (Nabben, 2020).

Public blockchains require trust between stakeholders in numerous ways. Coordination between software developers is necessary in each change to the software protocol code, such as issuance of a cryptocurrency (e.g., Initial Coin Offering) and network upgrades or "forks" (De Filippi and Loveluck, 2016). Similarly, the consensus mechanism that affords the system with "fault tolerance" depends on access to hardware "miners." Satoshi highlighted that it is computationally impractical for an attacker to change the public history of transactions "if honest nodes control a majority of CPU power" (2009). Yet, at the infrastructure layer, cryptocurrency hardware mining has become an extremely competitive industry across the manufacturing and supply chain, where innovation gains in computing power (such as the leap from GPU miners to ASIC miners) can "pre-mine" with increased hash rate to win more cryptocurrency-based block rewards, before releasing the technology to market (Grobys and Sapkota, 2020; Bitcoinera, 2018; Etherscan, 2021). According to a study by the University of Cambridge which analyzed the Internet Protocol (IP) addresses of Bitcoin miners, China controls 65% of the mining power or "hash rate," with the United States second at just over 7% (Cambridge Bitcoin Electricity Consumption Index, 2021). This means that collusion might influence the underlying record of transactions in forks or other governance disputes, thus demonstrating the need for trust in some actors in the network for blockchain security.

Transition from "proof-of-work" to "proof-of-stake" consensus is also a social coordination process. Proof-of-stake is the proposed solution to the risk of centralization of hardware miners in "Ethereum," the second largest blockchain by market capitalization. Yet, barriers to entry exist in the requirements to own substantial amounts of cryptocurrencies to "stake" in order to validate transactions and secure the blockchain and this process can be socially engineered. Cryptocurrency "whales" who own enough funds to move the market (such as initial team members of a project or hedge funds) can collude to dominate the staking market or "flash-crash" the market price of a cryptocurrency to endanger the security of the protocol. Another vulnerability of staking-based public blockchains is that trust can be allocated to "staking pool" infrastructure providers. These "staking-as-a-service" providers set up and maintain validator nodes for large proportions of some protocols, which forms points-of-failure if their systems or processes are compromised (Cong et al., 2020). In reality, blockchain technology can be compromised at the technical, software code, and social coordination layers in systems that are shaped by software engineers, social processes, and market forces.

Another limitation to "trustlessness" in public blockchain security is that the social layer of governance is still in open experimentation and is not yet, if at all, decentralized. This includes the invention of software-based governance via "Decentralized Autonomous Corporations" (DACs), later termed "Decentralized Autonomous Organizations" (DAOs) (Ethereum Foundation, 2014; Hsieh et al., 2018). The idea is not to replace trust with code but to provide accountability by making the rules of the system transparent through publicly available, open-source code (De Filippi et al., 2020). Yet, decentralized infrastructure does not necessarily lead to decentralization of influence within that infrastructure. "Any blockchain-based organization whose governance system relies mainly or exclusively on market dynamics is, therefore, ultimately bound to fail" (De Filippi, 2019). Despite technical sophistication, security through decentralization and trustlessness at the micro- and mesolevels in public blockchains is difficult to achieve due to social, technical, and infrastructural dependencies.

The next section explores a number of private blockchain case studies by applying a sociotechnical framework to investigate the social, software, and infrastructure layers of private blockchains in action at a macrosocial level, including which community participating in the network in need of protection; what features can be exploited within the network, and who is responsible and accountable for securing participants in the network. In contrast to public blockchains, permissioned blockchains are more readily being applied to macrosocial uses at a societal level on communities outside of software developers themselves, and thus this context has been chosen for the analysis of private blockchains as relevant to assess against the parameters of the sociotechnical "people security" approach.

Applying a Sociotechnical Security Analysis to Private Blockchain Networks

Private blockchains are prevalent in a number of real-world, macrosocial level applications across humanitarian, government, and corporate applications. Each case study below focuses on a use-case of blockchain as a macrosocial institutional infrastructure for coordinating goods, services, and people in society. Each example is then run through a sociotechnical analysis.

Humanitarian Case Study—Blockchain-Based Cash Voucher Assistance

Blockchains have been piloted in a number of humanitarian, not-for-profit organization use-cases at the macrosocial level, predicated on governing the most vulnerable. While some "humanitarian" oriented adoption is localized and organic, in response to hyperinflation and mistrust in government, like that of Venezuela, many cases are centrally issued by not-for-profit or aid organizations (Cifuentes, 2019; Kliber et al., 2019). One of the first high-profile humanitarian use-cases of blockchain is the World Food Programme's (WFP) "Building Blocks" project (World Food Programme, 2020). Blockchains were applied in the project as a ledger of transactions and settlement layer to transfer cash aid to Syrian refugees in a Jordanian refugee camp. The system is intended to "create more choice" for refugees to spend their cash aid at the supermarket (World Food Programme, 2020). The project received overwhelmingly positive coverage in the media (Juskalian, 2018; Apte, 2019; Awan and Nunhick, 2020). However, this blockchain-based system has a number of shortcomings which could equate to significant people security vulnerabilities for participants.

First, the community participating in the network in need of protection are Syrian refugees, who are a highly vulnerable population fleeing a civil war. Protection of identity is a necessity for this population (Gillespie et al., 2018). Yet, digital identities are being created that are permanently linked to biometric indicators which could then be hacked and traced back to family members or used as leverage to direct behaviors. Furthermore, biometric registrations are mandatory when receiving cash aid, making participation in the system mandatory and not voluntary.

Second, a number of technical and social features can be exploited in the system. The system is inextricably linked in political and infrastructural contexts which may not be in the best interests of users. For example, the blockchain is centrally issued and administered by WFP and administrative access is afforded to a consortium of international aid organizations (Baah, 2020). This results in significant power asymmetries in terms of how the system operates, what data is recorded, where it is stored, who has permission to access the data, and for what purposes. The biometric iris scanners used are provided by a local Jordanian company, IrisGuard, meaning persistent, biometric digital identities of refugees are being stored locally. The UN Refugee Agency (UNHCR) has also used IrisGuard to register and store the irises of 2.5 million people on UNHCR's "Eyecloud" server, alongside other personal data for cross referencing (Zambrano et al., 2018). Once data is recorded, it is hackable, replicable, and vulnerable to technical or human exploitation (Verizon, 2020). The IrisGuard database and Eyecloud are also linked to Amman Bank ATMs in Jordan, where refugees can scan their eyes and withdraw cash. Numerous technical systems and levels of cybersecurity, as well as numerous permissions to access and correlate highly sensitive data, with little to no consent from participants persist throughout this system.

In this case, accountability falls on the humanitarian agencies who are responsible for ethically providing aid without establishing systemic vulnerabilities for recipients. Although the system may provide operational control and coordination efficiencies among aid agencies, this instantiation of the digital economy inextricably links the biometric digital identity of refugees with an immutable ledger, across numerous local and international databases. Here, blockchain is simply a database which is centrally issued and administered. This means that the system is not cryptographically secure and requires significant trust in the IT security of local companies and government agencies.

Similar private, blockchain-based applications in humanitarian contexts are being explored by UNICEF, Human Rights Foundation, International Federation of the Red Cross, and Oxfam (UNICEF Office of Innovation, 2020; Cuen, 2020; IFRC Innovation, 2018).

Government Case Study—Central Bank Digital Currencies

Blockchains are also gaining prominence in nation-state central bank digital currencies (CBDCs). The development of national CBDCs is underway in multiple countries, including Australia, Canada, and China (Bank of Canada, 2019; Reserve Bank of Australia, 2019; CNCEditor, 2020). Public blockchain platforms that enable digital currency, such as Bitcoin and Facebook's "Libra" platform, are perceived as competitors to nation-state central bank issued currency in the move for governments to issue their own central bank digital currency (Griffoli et al., 2018; Lagarde and Festival, 2018). Some of the justifications for CBDCs include financial inclusion of people in remote and marginalized regions and consumer protection as a low-cost interbank settlement layer. However, what Canada has coined the "road to digital currency" has been referred to in the case of China as "the road to digital unfreedom," with fears of state surveillance, as the system is designed in the interests of administrators, with centralized development, issuance, and governance (Qiang, 2019).

Digitization of entire nation-state monetary systems creates astounding data security vulnerabilities for populations. Significant concerns have been raised on the data security of government-led databases, as this sensitive national data creates a target for hackers from both the inside and the outside that could be exploited for geopolitical reasons (Schilling, 2019).

Unlike other digital asset platforms, CBDCs may not be voluntary for participants. As digital identity, value, and transactions are tied to citizenship, participation in CBDCs could be mandatory. The system is not intended to be decentralized or interoperable in order to circumvent the threat of centralization.

Furthermore, the myth of financial inclusion is predicated on access to proprietary computing devices and digital literacy, most of which is not within reach of the most vulnerable, who rely on the cash economy (Gopane, 2019). The aims of CBDCs are antithetical to the public blockchain ideology of decentralization. CBDCs will not offer anonymity, and the advantages of cash for users to avoid exposure to customer profiling or hacking will be lost in the transition to digital currency.

Of course, CBDCs are contextual, and the risks differ according to where and how the system is designed and issued (Killingland and Dahl, 2018). In general, the introduction of CDBCs could lead to disintermediation of the banking sector, trigger digital bank runs, and threaten banks' liquidity and business models (Sandner et al., 2020). Given the risks to participants in the network vs. the gains, CBDCs do not offer a positive macrosocial infrastructure that is private, decentralized, censorship resistant, or cost-saving and places a significant burden on the state to secure technical infrastructure and the data of citizens against geopolitical threats.

Corporate Case Study—Private Currency Platforms

Corporations are also able to leverage their user audience to issue blockchain-based platforms. In corporate situations blockchains are often applied internally, to perform a specific function in corporations and industry, such as transparent record keeping, as a tool for organizational efficiency, and cost-reduction (Carson et al., 2018). Here, blockchains are often private or permissioned networks, responsible for coordination of supply chain goods and record keeping between known, distributed parties. Examples include supply chain experimentation to ship and trace almonds from Australia to Germany and J.P. Morgan's "JPM Coin" for interbank settlement between institutional clients (Commonwealth Bank, 2018; Morgan, 2019). However, corporate blockchain-based currency platforms have also been proposed, such as the prominent case of Facebook's "Libra" blockchain (now re-branded to "Diem").

Facebook's Libra blockchain was proposed as a solution for global payments and financial inclusion. Through its own digital wallet called "Calibra," Facebook is aiming to capture the "super-app" trend by forming a digital ecosystem within its own services to capture customers. China has already digitized the majority of consumer payments through corporate giants Alibaba and Tencent "digital wallet" applications which account for 90 percent of the $17 trillion mobile payments' market in China in 2017 (CGAP, 2019). Due to Facebook's poor record on consumer protection and user privacy, alarms were raised by global data protection and privacy enforcement authorities (Dervishi et al., 2019). Libra raises significant concerns regarding the security of participants in the network.

When they made this announcement Libra was heavily criticized as competing against sovereign currencies and because of Facebook's record of consumer protection and privacy breaches. A number of "Libra Association" consortium members subsequently left, including PayPal, eBay, Mastercard, Stripe, and Visa (Marcus, 2019). A top Senate Banking Committee official stated that "we cannot allow giant companies to assert their power over critical public infrastructure. The largest banks and the largest tech companies do not act in the interest of working Americans, but in the interest of themselves and their investors" (Brown, 2019). This instantiation of privately owned and governed blockchain as a potentially global payment railway became a critical public infrastructure in society. Thus, security for users is paramount and yet it is lacking.

The revised Libra 2.0 promotes itself as secure, "built on blockchain technology and designed with security in mind" (Libra, 2020). Yet, it is not technically, socially, or infrastructurally robust against exploitation; governing members that buy-in to the Libra Association are responsible for validating transactions on the network (noting that this may be transitioned in the latter proposed version of Libra). While the privacy of participants was said to match that of existing cryptocurrencies, access to personally identifiable information *via* the Libra "digital wallet" (the local user interface that sends and receives transactions) has not been specified and may be accessible by Facebook and its affiliates. If Libra launches in 2022 as anticipated, it is expected to have a significant impact on the payments sector and the business modes of banks by offering a cheaper mean of cross-border remittance for consumers. Yet the broader implications of this lack of accountability or recourse for the security of users digital information and assets, remains opaque.

OBSERVATIONS AND FINDINGS

The trust and security guarantees of blockchains depend on the type of blockchain, the context in which it is applied, and the needs of participants. Blockchain security is dependent on how social and technical aspects of the system interact, the threat which participants believe they are optimizing against by using the system, who is trusted to fulfil certain functions in the system, and why a blockchain is being applied. Desk-based and case study investigations of the application of both public and private blockchains demonstrate that blockchains are fraught with security assumptions and shortcomings on the promise of system issuers toward system users at the social, software, and infrastructural levels.

There is a major discrepancy between the promise of "security," "decentralization," and "trustlessness" and the real threats, needs, and expectations of users. In private blockchains, security *via* decentralization is not an objective, as they are centrally administered by design and users do not have a participatory role in system design or governance. Yet, private blockchain architecture is most commonly being adopted in macrosocial contexts, where a public blockchain may be more suitable to afford privacy and security guarantees to users. In each private blockchain case described, threats are initiated and experienced by a number of stakeholders across the different technical and governance layers of the blockchain network with little accountability for the issuers who are responsible for designing, deploying, and governing the system. This is both an information asymmetry and a misalignment of incentives between system administrators and users.

Each private blockchain case study also reveals serious contextual gaps about the advantages of using a blockchain for the application and the security context and needs of the users of those systems. From these findings of the shortcomings of blockchain applications as a sociotechnical solution, the following table can be drawn as a simple tool for analysis of people security in blockchains. This framework was adapted from Goerzen et al.'s sociotechnical security framework analysis, which has been applied to social media systems (Goerzen et al., 2019), and Li et al.'s security requirements analysis for sociotechnical systems (Li et al., 2020).

Trust, but Verify: Applications and Limitations of the "People Security" Model

Buterin defined trust as "assumptions about the behavior of others," of which one dimension of failure is how badly the system would fail if this assumption is not met (Buterin, 2020). The security concern about a misalignment of assumptions between system designer and user is "how badly will the system fail if the security assumption of the user is violated?" In the cases outlined above, the results of a system failure, such as leaked identity or loss of digital assets, could be severely damaging to the referent user of community in need of security within the system.

The above analysis outlines technical and social security limitations in both public and private blockchains, as well as considering the context in which blockchain is applied and the participants in the system. When users are not entitled to participate in the governance of the system, their security can more easily be compromised.

In public blockchains, the role of people in participating in the network is threefold. People are invited to participate in developing the open-source code of the network, people are needed to secure the network by validating transactions and maintaining their software through the consensus mechanism of mining in proof-of-work or staking in proof-of-stake, and people are able to govern the network by participating in community discussions, voicing proposals, and voting on movements. Although not completely "decentralized," "trustless," or secure, user participation in the function and governance of the network enables new types of macrosocial institutional digital infrastructure, in which sociotechnical security is a consideration.

In contrast, private and permissioned blockchains in social coordination contexts position people as "users," with less agency, authority, or transparency over how the system functions, in comparison to those responsible for designing, issuing, and administrating the system. There is little to no role for participation in developing, securing, or governing the network. This limits the ability of private blockchains to offer people security to users of the system through the unique cryptoeconomic attributes evident in public blockchains of decentralization and trust minimization.

In an anomaly about how and why blockchains are being applied; private blockchains, are being applied in numerous macrosocial applications despite not offering new or novel security affordances, whilst public blockchains are not being as readily adopted as broader social, coordination systems, despite their unique socio-technical security attributes. Thus, this analysis has been limited in its ability to assess the socio-technical security outcomes of public blockchains as there are few known cases of public blockchains that are open, freely accessible, permissionless, and decentralized that operate in macrosocial environments in society, outside of the software developer communities in which they are developed. Experimentation with public blockchains and "Decentralized Autonomous Organizations" may be a suitable area for further exploration of sociotechnical security research.

The main limitation of this analysis is its use of a desk-based research method. In future, this approach could be extended to include ethnographic field-research in order to understand the contexts, needs, and expectations of participants in these systems, in order to observe and establish more accurate findings about people security in these particular cases.

IN CODE WE TRUST? THE LIMITATIONS OF SECURITY IN BLOCKCHAINS

Blockchains are a sociotechnical construct, and as such, blockchain security is not only about network security, rather we must also consider participants in the network. Both public and private blockchains possess sociotechnical security vulnerabilities at the social, software, and infrastructure layers. Citizens of public blockchain-based macrosocial digital institutions are warned: "there is no proven linear-causal relationship between decentralization in technical systems and equitable practices socially, politically or economically" (O'Dwyer, 2016). There is, however, a transition of trust from existing institutions, towards the designers and governors of public blockchain infrastructure. Meanwhile, private and semi-permissioned blockchain-based systems are similar to many other web-based technologies in that they are invisible infrastructures, which operate behind user interfaces (Star, 1999). This means that unless the software code that governs the system is open-source *and* participants know how to audit (or read) code, they do not know how it has been designed to work. Thus, many applications of blockchain systems in the real world are permissioned and oftentimes typify the threat of centralization by codifying dependence on private actors.

At the software level, blockchain security can be compromised by vulnerabilities in the code itself. Examples include privacy limitations through upgrades to the core cryptographic primitives, traceability and monitoring of pseudonymous public key addresses, network monitoring through traffic analysis, and increasingly sophisticated blockchain analytics services which deanonymize actors in the network (Troncoso et al., 2017). Furthermore, people's digital assets are also vulnerable through shortcomings in blockchain code, such as the infamous "DAO" hack in which around $60 million (at the time) was stolen from a "decentralized, automated" smart contract which allowed for double withdrawals because a single line of code was not in the correct order (Dhillon et al., 2017). The pursuit of decentralization also places significant onus on people to manage their own "private keys," or cryptographic passwords, through secure storage (Least Authority, 2020). A number of other crucial technical issues remain unresolved in the proposal for the latest version of Ethereum at the time of writing, which is predicted to become the largest public blockchain by market capitalization and users upon launch.

At the social level, social processes continue to enable and restrict both public and private blockchain applications. Regulation remains an ongoing ambiguity for participants in blockchain systems. As a "polycentric enterprise" comprised of participants, network validators, and exchanges, public blockchains are subject to a variety of governance restrictions, depending on jurisdiction (Alston et al., 2020). Shortcomings also exist in the asymmetries in the surrounding context of how and where blockchains are deployed. Most cryptocurrency Initial Coin Offerings (ICOs) project launches have come out of the United States, but people from around the world invest at their own risk, with little to no legal recourse in the event of loss. The Library Law of Congress notes that one of the most common government responses to cryptocurrency is to issue warnings about investing. "Such warnings, mostly issued by central banks, are largely designed to educate the citizenry about the difference between actual currencies, which are issued and guaranteed by the state, and cryptocurrencies, which are not" Library of Congress Law, (2018). ICOs have been regulated in numerous countries due to the risk to retail investors of investing in a volatile assets with no stable underlying value—highlighting digital illiteracy in establishing realistic expectations of what blockchain is and does.

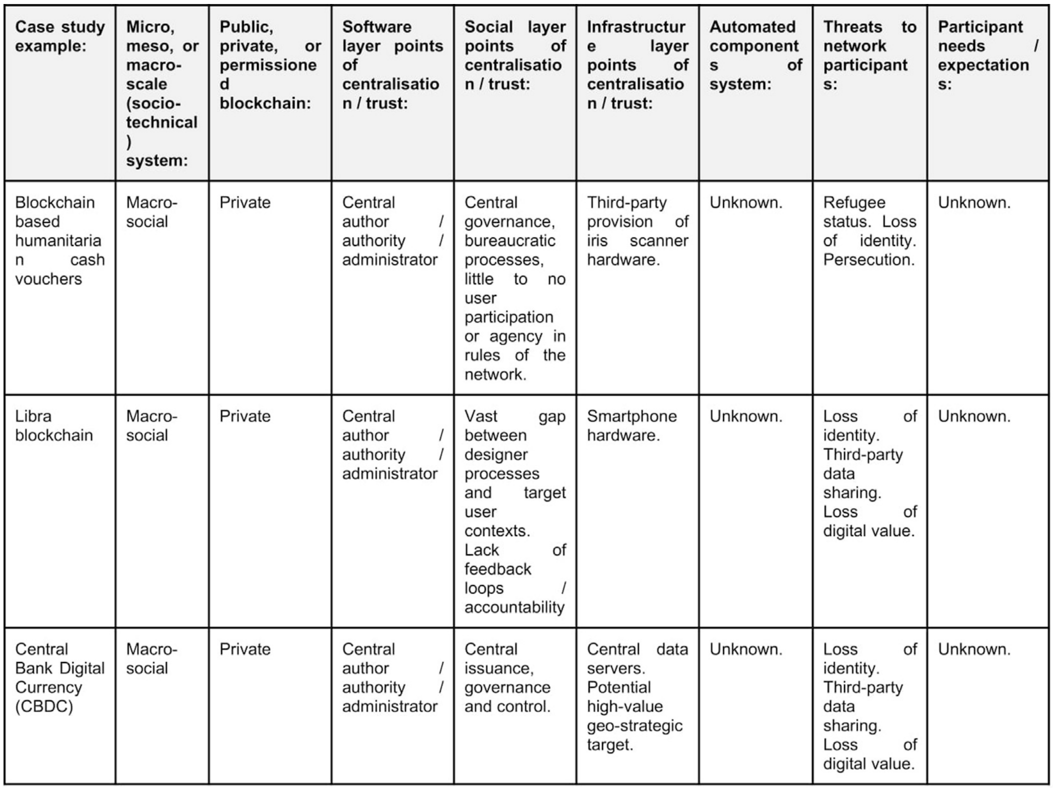
In terms of governance, centralization exists at multiple intersections in blockchain-based infrastructures. In private blockchains, issuance and administration of blockchain-based networks are often synonymous with network ownership and control. In public blockchain, early espoused ideologies of blockchain being decentralized to create freedom and choice for individuals created security assumptions for participants. Yet, tokens are often owned by a concentration of actors and software and governance decisions are often made by a small group of people.

At the infrastructure layer, significant security issues exist in the hardware and infrastructure dependencies of blockchains. This includes reliable internet connectivity, which forms the basis of the underlying infrastructure which blockchain networks are dependent upon. Although much development was funded by The Defense Advanced Research Projects Agency (DARPA), the internet began with a vision of creating a "decentralized commons" that was coopted by private and commercial interests (Berners-Lee, 2000). Yet, the centralization of information, ownership, and influence on the internet reveals significant limitations in the assumption that the blockchain digital economy can be decentralized, because it is dependent on the existing infrastructure of the internet. The same is true of hardware dependencies, such as mobile phones and computer hardware.

Blockchain Evolution and Security Concerns—Looking Ahead

As blockchain holds a potentially significant trajectory in critical economic and governance infrastructure in society, "people security" offers a critical lens for both designers and users for transparent, voluntary participation in systems that clarify design assumptions and the context in which they are applied.

Pursuing people security could also help to reveal design assumptions and user needs as functions within blockchain-based systems become more automated. "Because artificial intelligence is about the automation of cognitive processes, and blockchain is the automation of transactions, there are specific scenarios where both technologies can be combined. A blockchain network can provide a decentralized platform to support some advanced AI capabilities" (Marechaux, 2019). Automation of certain rules and functions by combining them with other emerging technologies such as artificial intelligence (AI) has the potential to semiautonomously govern interactions based on how the system is encoded through smart contracts, DAOs, and machines—thus lessening the agency of participants (Salah et al., 2019). Suggested use-cases for automated blockchains include data marketplaces, explainable AI, and the Internet of Things (IoT) (Dinh and Thai, 2018). While blockchains may enable *more* decentralized instantiations of AI, the *assumption* is that this is decentralized and therefore secure, without always considering those assumptions apply to the human participants in the network. In such cases, trust is reallocated from existing institutions to semi-autonomous digital



Case study example:	Micro, meso, or macro-scale (socio-technical) system:	Public, private, or permissioned blockchain:	Software layer points of centralisation / trust:	Social layer points of centralisation / trust:	Infrastructure layer points of centralisation / trust:	Automated components of system:	Threats to network participants:	Participant needs / expectations:
Blockchain based humanitarian cash vouchers	Macro-social	Private	Central author / authority / administrator	Central governance, bureaucratic processes, little to no user participation or agency in rules of the network.	Third-party provision of iris scanner hardware.	Unknown.	Refugee status. Loss of identity. Persecution.	Unknown.
Libra blockchain	Macro-social	Private	Central author / authority / administrator	Vast gap between designer processes and target user contexts. Lack of feedback loops / accountability	Smartphone hardware.	Unknown.	Loss of identity. Third-party data sharing. Loss of digital value.	Unknown.
Central Bank Digital Currency (CBDC)	Macro-social	Private	Central author / authority / administrator	Central issuance, governance and control.	Central data servers. Potential high-value geo-strategic target.	Unknown.	Loss of identity. Third-party data sharing. Loss of digital value.	Unknown.

FIGURE 1 | "People security" analysis framework, applied to blockchain case studies.

agents to act on behalf of people, weakening the barrier between the rules of the digital world and the physical world, yet software code is subjective and reflects assumptions about behavior in the real world that are contained in theoretical models of the system designer (Leveson, 2012). Therefore, surfacing where and how automation is occurring in a system through transparent code is a crucial first step to minimizing complexity to apply a people security approach. Further analysis is required into the effects of automation on people security.

In some circumstances, blockchains may not be a desirable macrosocial infrastructure to afford security to people at all, due to the fundamental assumptions that shape the attributes of blockchain-based systems. Some of the values that blockchains institute, such as immutable records of data, have the potential to conflict with privacy, legal frameworks, and data norms. Other peer-to-peer protocols offer a different ontology which is not based on rational, economic self-interest and individualism. By contrast, the Holochain team encourages a "post-blockchain," "agent-centric," cryptographically secure data infrastructure which does not require digital tokens for data sharing, access, storage, and verification of public data (Harris-Braun et al., 2018). Similarly, Dat protocol offers data hosting through an "append-only" protocol that runs on a distributed, peer-to-peer network of computers that can work offline or with poor connectivity, whereby the original uploader can add or modify data while keeping a full record of history and cryptographic keys are often shared for collective governance of digital assets (Dat Protocol, 2019). The fundamental assumptions of decentralization, trustlessness, immutability, and security that undergird blockchain systems must be made explicit in order to assess the suitability of the protocol by potential users and carefully consider the needs, trade-offs, and consequences for participants.

CONCLUSION AND FURTHER DIRECTIONS

As a tool, blockchains possess unique, cryptoeconomic properties that are useful for some applications. As an organizational infrastructure, blockchains enable some decentralization by reallocating trust to other parties. Blockchains are a macrosocial coordinating technology in society, with interlinked technical and social functions, including automation, oracles, smart contracts, voting, and digital currency. When applied to macrosocial coordination problems, it is imperative to analyze blockchain security as "people security" to more accurately assess the type of blockchain and the context of the application against the social, software, and infrastructure requirements of participants using the system. If blockchains are to be applied as institutions, we need the best institutions possible for society.

There are no blanket security guarantees afforded by blockchains. Blockchain technology possesses different attributes and varying levels of security for people participating in a system, depending on the design decisions, issuance, administration, and context in which it is applied. This research paper finds that there are a number of security and trust issues that need to be addressed in both public and private blockchains, especially as centralized, private blockchains which limit the autonomy of users are most commonly being employed in macrosocial contexts. In uncovering the assumptions regarding the promises and expectations of both public and private blockchains, it is clear that blockchain security, in its current form, has significant security limitations for people.

While blockchain-based networks are distributed, users must understand that both public and private blockchains are far from decentralized. This sociotechnical analysis of "blockchain security" as "people security" can support system designers and participants to clarify expectations, assumptions, and guarantees when deploying and employing these tools as systems in order to acknowledge user expectations and communicate realistic security guarantees.

Further research emerging from this study includes the application of the people security framework to different use-cases for deeper sociotechnical security analysis of specific blockchain implementations and user groups, further comparability of different blockchain designs to analyze the people security trade-offs implementations, an interdisciplinary investigation into people security in macrosocial applications of public blockchains, and a security investigation into the social outcomes of automated functions within blockchain-based systems.

AUTHOR CONTRIBUTIONS

KN is the sole author of this work.

REFERENCES

Allen, D. W. E., Lane, A. M., and Poblet, M. (2019). The governance of blockchain dispute resolution. *Social Sci. Res. Netw.* doi:10.2139/ssrn.3334674

Alston, E., Law, W., Murtazashvili, I., and Weiss, M. B. H. (2020). "Can permissionless blockchains avoid governance and the law?" Available at: http://dx.doi.org/10.2139/ssrn.3676761.

Apte, P. (2019). *"How blockchain is bringing Food security to refugees"*, dell technologies. Available at: https://www.delltechnologies.com/en-us/perspectives/how-blockchain-is-bringing-food-security-to-refugees/ (Accessed August 14, 2020).

Awan, F., and Nunhick, S. (2020). Governing blocks: building interagency consensus to coordinate humanitarian aid. *The Journal of Science Policy and Governance.* 16 (2). doi:10.38126/jspg160201

Baah, B. (2020). Humanitarian cash and voucher assistance in Jordan: a gateway to mobile financial services. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/01/Jordan_Mobile_Money_CVA_Case_Study_Web_Spreads.pdf (Accessed August 14, 2020).

Bach, L. M., Mihaljevic, B., and Zagar, M. (2018). "Comparative analysis of blockchain consensus algorithms," in 2018 41st international Convention on Information and communication technology, Electronics and microelectronics (MIPRO), 1545–1550. doi:10.23919/MIPRO.2018.8400278

Bank of Canada (2019). *The road to digital money*. Ottawa, ON: Bank of Canada. Available at: https://www.bankofcanada.ca/2019/04/the-road-to-digital-money/ (Accessed August 08, 2020).

Berg, C., Davidson, S., and Potts, J. (2019a). Blockchain technology as economic infrastructure: revisiting the electronic markets hypothesis. *Front. Blockchain.* 2. doi:10.3389/fbloc.2019.00022

Berg, C., Davidson, S., and Potts, J. (2019b). *Understanding the blockchain economy: an introduction to institutional cryptoeconomics*. Ottawa, NO: Edward Elgar Publishing.

Berners-Lee, T (2000). Weaving the Web: The original design and ultimate destiny of the World Wide Web. New York: Harper Business.

Bijker, W. E., Hughes, T. P., and Pinch, T. (2012). *The social construction of technological systems*. Anniversary Edition. Cambridge, MA: The MIT Press. Available at: https://mitpress.mit.edu/books/social-construction-technological-systems-anniversary-edition (Accessed August 07, 2020).

Bitcoinera (2018). Are we decentralized yet? Available at: https://bitcoinera.app/arewedecentralizedyet/ (Accessed August 15, 2020).

Brown, S. (2019). "Brown: federal Reserve must protect economy and consumers from Facebook's monopoly money | U.S. Senator sherrod Brown of Ohio. Available at: https://www.brown.senate.gov/newsroom/press/release/brown-federal-reserve-must-protect-economy-and-consumers-from-facebooks-monopoly-money (Accessed August 16, 2020).

Buterin, V. (2016). *"A proof of stake design philosophy,"* medium. Available at: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51 (Accessed August 16, 2020).

Buterin, V. (2017). *"The meaning of decentralization,"* medium. Available at: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (Accessed June 12, 2020).

Buterin, V. (2020). *"Trust models."*, Vitalik.ca. Available at: https://vitalik.ca/general/2020/08/20/trust.html (Accessed November 30, 2020).

Cambridge Bitcoin Electricity Consumption Index (2021). Cambridge bitcoin electricity consumption Index (CBECI). Available at: https://cbeci.org/mining_map (Accessed August 16, 2020).

Carson, B., Romanelli, G., and Zhumaev, A. (2018). *The strategic business value of the blockchain market*. Sydney, Australia: McKinsey. Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value (Accessed August 08, 2020).

CGAP (2019). China: a digital payments revolution, Washington DC: CGAP (Consultative Group to Assist the Poor). Available at: https://www.cgap.org/research/publication/china-digital-payments-revolution (Accessed August 16, 2020).

Chen, H., Pendleton, M., Njilla, L., and Xu, S. (2019). A survey on Ethereum systems security: vulnerabilities, attacks and defenses. Available at: http://arxiv.org/abs/1908.04507 (Accessed August 08, 2020).

Chohan, U. W. (2019). "Are cryptocurrencies truly trustless?," in *Cryptofinance and mechanisms of exchange: the Making of virtual currency*. Editors S. Goutte, K. Guesmi, and S. Saadi (Cham, CH: Springer International Publishing), 77–89.

Cifuentes, A. F. (2019). Bitcoin in troubled economies: the potential of cryptocurrencies in Argentina and Venezuela. *Lat. Am. Law Rev.*, 99–116. doi:10.29263/lar03.2019.05

CNCEditor (2020). "*State media sheds light on China's central bank digital currency.*" China Banking News. Available at: http://www.chinabankingnews.com/2020/04/24/state-media-highlights-regtech-functions-controlled-anonymity-of-chinas-central-bank-digital-currency/ (Accessed August 14, 2020).

Commonwealth Bank (2018). Commonwealth Bank completes new blockchain-enabled global trade experiment. Available at: https://www.commbank.com.au/content/shared/newsroom/2018/07/commonwealth-bank-completes-new-blockchain-enabled-global-trade- (Accessed August 16, 2020).

Cong, L. W., He, Z., and Li, J. (2020). Decentralized mining in centralized pools. *Rev. Financ. Stud.* doi:10.1093/rfs/hhaa040

ConsenSys (2019). "Blockchain for NGOs: project unblocked cash case study," *ConsenSys*. Available at: https://consensys.net/blockchain-use-cases/social-impact/project-unblocked-cash-case-study/ (Accessed August 08, 2020).

Cuen, L. (2020). "Human rights foundation funds bitcoin privacy tools despite 'Coin Mixing' Legal Stigma", Coin Desk, New York, [Online]. Available at: http://www.coindesk.com/human-rights-foundation-bitcoin-privacy-tools-developer-fund (Accessed January 2021).

Dat Protocol (2019). how Dat works. Available at: https://datprotocol.github.io/how-dat-works/ (Accessed August 16, 2020).

De Filippi, P. (2019). Blockchain technology and decentralized governance: the pitfalls of a trustless dream. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524352 (Accessed July 08, 2020). doi:10.2139/ssrn.3524352

De Filippi, P., and Loveluck, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. *Social Sci. Res. netw.* 5 (4). doi:10.14763/2016.3.427

De Filippi, P., Mannan, M., and Reijers, W. (2020). Blockchain as a confidence machine: the problem of trust and challenges of governance. *Technol. Soc.* 62, 101284. doi:10.1016/j.techsoc.2020.101284

Dervishi, B., Falk, A., Therrien, D., Bonane, M. O., Buttarelli, G., Denham, E., et al. (2019). Joint statement on global privacy expectations of the Libra network. Available at: https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf (Accessed August 14, 2020).

Dhillon, V., Metcalf, D., and Hooper, M. (2017). "*The DAO hacked*," in blockchain enabled applications: Understand the blockchain Ecosystem and How to Make it *work for you*. Berkeley, CA: Apress. doi:10.1007/978-1-4842-3081-7_6

Dinh, T. N., and Thai, M. T. (2018). AI and blockchain: a disruptive integration. *Computer.* 51 (9), 48–53. doi:10.1109/MC.2018.3620971

Ethereum Foundation (2014). DAOs, DACs, DAs and more: an incomplete terminology guide. Available at: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ (Accessed August 08, 2020).

Etherscan, n. d. (2021). *"Top 25 miners by blocks | etherscan,"* Ethereum (ETH) blockchain explorer. Available at: http://etherscan.io/stat/miner?range=7&blocktype=blocks (Accessed August 15, 2020).

Ferreira, A., Huynen, J. L., Koenig, V., and Lenzini, G. (2014). "A conceptual framework to study socio-technical security," in Human Aspects of information security,Privacy, and Trust. Cham, 318–329. doi:10.1007/978-3-319-07620-1_28

Gillespie, M., Osseiran, S., and Cheesman, M. (2018). Syrian refugees and the digital passage to europe: smartphone infrastructures and affordances. *Soc. Media Soc.* 4 (1), 205630511876444. doi:10.1177/2056305118764440

Goerzen, M., Watkins, E. A., and Lim, G. (2019). "Entanglements and exploits: sociotechnical security as an analytic framework," in 9th {USENIX} workshop on free and open communications on the internet ({FOCI} 19)

Gopane, T. J. (2019). "An enquiry into digital inequality implications for central bank digital currency," in 2019 IST-africa week conference (IST-Africa), 1–9. doi:10.23919/ISTAFRICA.2019.8764838

Griffoli, T. M., Peria, M. S. M., Agur, I., Ari, A., Kiff, J., Popescu, A., et al. (2018). *Casting light on central bank digital currencies*. Washington DC: International Monetary Fund. Available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233 (Accessed August 14, 2020).

Grobys, K., and Sapkota, N. (2020). Predicting cryptocurrency defaults. *Appl. Econ.* 52, 5060–5076. doi:10.1080/00036846.2020.1752903

Harris-Braun, E., Luck, N., and Brock, A. (2018). Holochain scalable agent-centric distributed computing DRAFT (ALPHA 1) - 2/15/2018. [Online]. Available at: https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf (Accessed January, 2021).

Hayes, A. (2019). The socio-technological lives of bitcoin. *Theor. Cult. Soc.* 36 (4), 49–72. doi:10.1177/0263276419826218

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., and Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *J Org Design.* 7 (1), 14. doi:10.1186/s41469-018-0038-1

IFRC Innovation (2018). IFRC blockchain application wins global islamic finance competition. *IFRC Innovation.* Available at: http://media.ifrc.org/innovation/2018/02/12/ifrc-blockchain-application-wins-global-islamic-finance-competition/ (Accessed August 08, 2020).

Juskalian, R. (2018). "*Inside the Jordan refugee camp that runs on blockchain,"* MIT Technology Review. Available at: https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/ (Accessed August 14, 2020).

Karame, G. O., and Androulaki, E. (2016). *Bitcoin and blockchain security.* Norwood, MA:Artech House.

Killingland, M., and Dahl, L. B. (2018). "Central bank digital currencies – fad or the future? : a framework for country level assessment of central bank digital currencies" Available at: https://openaccess.nhh.no/nhh-xmlui/handle/11250/2586746 (Accessed August 14, 2020).

Kliber, A., Marszałek, P., Musiałkowska, I., and Świerczyńska, K. (2019). Bitcoin: safe haven, hedge or diversifier? Perception of bitcoin in the context of a country's economic situation—a stochastic volatility approach. *Phys. Stat. Mech. Appl.* 524, 246–257. doi:10.1016/j.physa.2019.04.145

Lagarde, C., and Festival, I. M. D. S. F. (2018). Winds of change: the case for new digital currency.*IMF*. Available at: https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency (Accessed August 14, 2020).

Larkin, B. (2013). The politics and poetics of infrastructure. *Annu. Rev. Anthropol.* 42 (1), 327–343. doi:10.1146/annurev-anthro-092412-155522

Latour, B. (1990). Technology is society made durable. *Sociol. Rev.* 38 (S1), 103–131. doi:10.1111/j.1467-954x.1990.tb03350.x

Least Authority (2020). Ethereum 2.0 specifications security audit report Ethereum foundation. Available at: https://leastauthority.com/static/publications/LeastAuthority-Ethereum-2.0-Specifications-Audit-Report.pdf. (Accessed August 16, 2020).

Leveson, N. (2012). *Engineering a safer world: systems thinking applied to safety.* Cambridge, MA: The MIT Press.

Li, T., Horkoff, J., and Mylopoulos, J. (2018). Holistic security requirements analysis for socio-technical systems. *Software Syst. Model.* 17, 1253–1285. doi:10.1007/s10270-016-0560-y

Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generat. Comput. Syst.* 107, 841–853. doi:10.1016/j.future.2017.08.020

Libra, n. d. (2020). "Libra | A new global payment system," *Libra.org*. Available at: https://libra.org/en-US/ (Accessed August 14, 2020).

Library of Congress Law (2018). *Regulation of cryptocurrency around the world.* Available at: https://www.loc.gov/law/help/cryptocurrency/world-survey.php (Accessed August 16, 2020).

Lin, I. C., and Liao, T. C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* 19–5. doi:10.6633/IJNS.201709.19(5).01

Marcus, D. (2019). Hearing before the United States senate committee on banking, housing, and urban affairs: testimony of david marcus. Available at: https://www.banking.senate.gov/imo/media/doc/Marcus%20Testimony%207-16-19.pdf (Accessed August 14, 2020).

Marechaux, J. L. (2019). Towards advanced artificial intelligence using blockchain technologies—IEEE blockchain initiative. Available at: https://blockchain.ieee.org/technicalbriefs/march-2019/towards-advanced-artificial-intelligence-using-blockchain-technologies (Accessed August 16, 2020).

May, T. C. (1994). Cyphernomicon. Available at: https://web.archive.org/web/20110607130638/http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html (Accessed August 15, 2020).

May, T. C. (1992). The crypto anarchist manifesto. Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html (Accessed August 15, 2020).

Morgan, J. P. (2019). *J.P. Morgan creates digital Coin for payments.* Available at: https://www.jpmorgan.com/global/news/digital-coin-payments (Accessed August 16, 2020).

Nabben, K. (2020). "*Trustless approaches to digital infrastructure in the crisis of COVID-19 Australia's newest COVID app. Home-grown surveillance technologies and what to do about it," social science research network.* Rochester, NY. doi:10.2139/ssrn.3579220SSRN Scholarly Paper ID 3579220

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf (Accessed February 1, 2020).

O'Dwyer, R. (2016). "Blockchains and their pitfalls," in *Ours to Hack and to Own.* Editors Trebor Scholz and Nathan Schneider. (New York City: OR Books), pp. 228–232.

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., and Shimizu, S. (2020). Privacy preservation in permissionless blockchain: a survey. *Digital Commun. Networks.* doi:10.1016/j.dcan.2020.05.008

Qiang, X. (2019). President XI's surveillance state. *J. Democr.* 30 (1), 53–67. doi:10.1353/jod.2019.0004

Reserve Bank of Australia (2019). Submission to the senate select committee on financial technology and regulatory technology. Available at: https://www.rba.gov.au/publications/submissions/payments-system/financial-and-regulatory-technology/index.html (Accessed August 14, 2020).

Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. (2019). Blockchain for AI: review and open research challenges. *IEEE Access*. 7, 10127–10149. doi:10.1109/ACCESS.2018.2890507

Sandner, P., Schulden, P., Grale, L., and Grobe, J. (2020). "The digital programmable euro, Libra and CBDC: implications for European banks," in Conference: EBA policy research workshop: new technologies in the banking sector, impacts, risks, and opportunities. Available at: https://www.researchgate.net/publication/343334690_The_Digital_Programmable_Euro_LibrL_and_CBDC_Implications_for_European_Banks (Accessed August 16, 2020).

Schilling, L. (2019). "Risks involved with CBDCs: on cash, privacy, and information centralization," in conference: reinventing bretton woods: dialogue of the continents 2019 hamburg, ResearchGate. doi:10.13140/RG.2.2.30645.22248

Shahaab, A., Maude, R., Hewage, C., and Khan, I. (2020). Blockchain: a panacea for trust challenges in public services? a socio-technical perspective. *J. Br. Blockchain Assoc.* 3 (2), 6. doi:10.31585/jbba-3-2-(6 Available at: https://www.researchgate.net/publication/343307094_Blockchain_A_Panacea_for_Trust_Challenges_In_Public_Services_A_Socio-technical_Perspective (Accessed November 30, 2020).

Singh, M. P. (2011). "Governing sociotechnical systems," in 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology 1. doi:10.1109/WI-IAT.2011.288

Singh, S., and Singh, N. (2016). "Blockchain: future of financial and cyber security," in 2016 2nd International Conference on contemporary Computing and informatics IC3I, 463–467. doi:10.1109/IC3I.2016.7918009

Smith, A., and Stirling, A. (2006). "Moving inside or outside? Positioning the governance of sociotechnical systems", Science and Technology Policy Research, *SPRU electronic working paper series*, Brighton, England: University of Sussex. Paper No. 148.

Star, S. L. (1999). The ethnography of infrastructure. *Am. Behav. Sci.* 43 (3), 377–391. doi:10.1177/00027649921955326

Trist, E. L. (1981). The evolution of socio-technical systems: a conceptual framework and an action research program. Occasional Paper No. 2, Toronto, ON, Canada: Ontario Quality of Working Life Centre.

Troncoso, C., Isaakidis, M., Danezis, G., and Halpin, H. (2017). "Systematizing decentralization and privacy: lessons from 15 Years of research and deployments," in Proceedings on privacy enhancing technologies, 302–329. Available at: https://arxiv.org/abs/1704.08065 (Accessed June 12, 2020).

Underwood, S. (2016). Blockchain beyond bitcoin. *Commun. ACM.* 59 (11), 15–17. doi:10.1145/2994581

UNICEF Office of Innovation (2020). UNICEF funding opportunity for blockchain startups. Available at: https://www.unicef.org/innovation/applyBlockchainCrypto (Accessed August 08, 2020).

Verizon (2020). "2020 data breach investigations report," *verizon enterprise*. Available at: https://enterprise.verizon.com/resources/reports/dbir/ (Accessed August 15, 2020).

Vidan, G., and Lehdonvirta, V. (2019). Mine the gap: bitcoin and the maintenance of trustlessness, *New Media Soc.* 21 (1), 42–59. doi:10.1177/1461444818786220

Voshmgir, S., and Zargham, M. (2019). Foundations of cryptoeconomic Systems," *Cryptoeconomics working paper series*, 1. Vienna University of Economics–1.

World Food Programme (2020). Building blocks | WFP innovation. Available at: https://innovation.wfp.org/project/building-blocks (Accessed August 08, 2020).

Xinyi, Y., Yi, Z., and He, Y. (2018). "Technical characteristics and model of blockchain," in 2018 10th international Conference on communication Software and networks (ICCSN), 562–566. doi:10.1109/ICCSN.2018.8488289

Zambrano, R., Young, A., and Verhulst, S. (2018). "Case study: connecting refugees to aid through blockchain enabled ID management: world Food Programme's building blocks". Available at: https://www.irisguard.com/media/laglvgzk/building-blocks-case-study.pdf (Accessed August 13, 2020).

Zhang, R., Xue, R., and Liu, L. (2019). *"Security and privacy on blockchain,"* ArXiv190307602 Cs. Available at: http://arxiv.org/abs/1903.07602 (Accessed August 08, 2020).

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.