BRL Working Paper Series No. 14

Public Versus Private Blockchains

Elias Strehle [1,*]

[1] Blockchain Research Lab, Max-Brauer-Allee 46, 22765 Hamburg, Germany
[*] Correspondence: strehle@blockchainresearchlab.org

Published: 30 Sep 2020

Abstract: Public blockchains like Bitcoin and Ethereum continue to have an exaggerated influence on the overall perception of blockchain technology. As a consequence, trustlessness is often presented as the central characteristic of blockchain: It is claimed that blockchain designers must assume that users do not trust each other and that there is no trusted third party. While this is arguably true for public blockchains, it is not a helpful perspective for private blockchains. Private blockchains can be highly efficient and effective when they act as a team player, operating alongside legal contracts, trust relationships, regulatory frameworks and trusted third parties.

Keywords: Blockchain; Enterprise Architecture

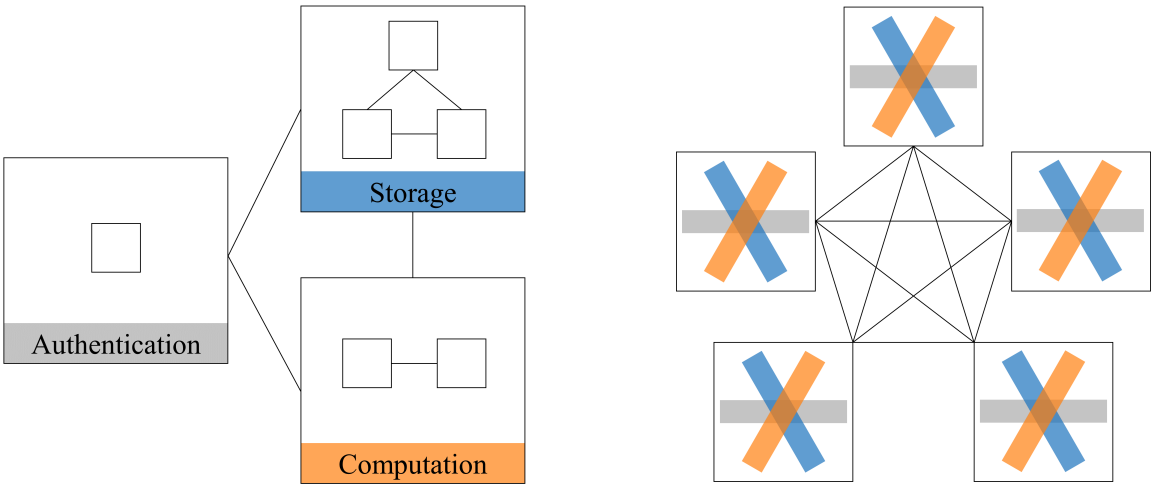
1 Introduction

Say "blockchain" and before long, someone will say "trust." Trust, or rather the lack of it, is one of the key concepts in explaining what blockchain is and what it does. Consider, for example, *The Economist*: "Simply put, [blockchain] is a machine for creating trust" (The Economist, 2015); a blockchain guide for business leaders published by the World Economic Forum: "If the actors/entities already know one another and trust one another, there is probably no need for blockchain" (Mulligan et al., 2018, p. 7); or an introductory book on blockchain: "The blockchain is trustless in the sense that a user does not need to trust the other party in a transaction, or a central intermediary, but does need to trust the system" (Swan, 2016, p. 2).

At the same time, two much-noticed corporate blockchain systems, TradeLens and FoodTrust, rely heavily on IBM as a central intermediary. Corporate blockchain implementations like Hyperledger Fabric, R3 Corda, or MultiChain allow users to circumvent the blockchain's consensus mechanism—one of the core components for building trust—in the interest of confidentiality. In fact, a study by Rauchs et al. (2019) finds that 77% of live blockchain systems do not implement multi-party consensus at all.

There seems to be a mismatch between the way blockchain technology is commonly described and the way enterprises actually use it. The main reason appears to be that the general perception of blockchain continues to be dominated by "trustless" public blockchains like Bitcoin and Ethereum. Enterprises, on the other hand, have mostly moved on to private blockchains, which are also referred to as enterprise, permissioned, or consortium blockchains.

Public blockchains like Bitcoin and Ethereum are indeed "trust machines," built to operate in the wild west of the world wide web. Public blockchains can be accessed by anyone and offer a degree of anonymity. Users have little reason to believe in each others' goodwill and often cannot rely on "off-chain" mechanisms (such as legal contracts) to protect themselves against fraud and abuse.



(a) Classic corporate system *(b) Public blockchain*

Figure 1: An illustration of entangled redundancy. System (a) illustrates a classic corporate system. It employs separation of concerns and has a low degree of redundancy. Separate parts of the system are responsible for authentication, data storage, and computation. The system is efficient and flexible but has a single point of failure in the central authentication component. Furthermore, an attacker can attempt to bypass individual components, e.g. to gain access to data storage without authentication. System (b) illustrates a public blockchain. Every part of the system redundantly performs all tasks in the system. All concerns are inextricably linked. There is no single point of control and it is not possible to bypass individual components. However, this comes at the cost of efficiency, confidentiality, and flexibility.

Private blockchains, by contrast, restrict access to a selected circle of persons and institutions. These tend to already maintain business relationships and operate within a framework of existing contracts, laws, and connected technical systems. For private blockchains, making trustlessness the overarching design principle is neither necessary nor useful.

Nonetheless, reduction of trust is often among the goals of a private blockchain system. It is therefore important to understand the advantages and disadvantages of trustlessness and how it can be selectively applied within a system. This paper details the trade-offs that come with the paradigm of trustlessness and its underlying design principles of redundancy and entanglement. Then it outlines a more balanced approach to designing private blockchains. The approach supplements the strengths of trustless blockchains with external trust mechanisms and the careful integration of trusted third parties. The result, hopefully, is a clearer view of what blockchain is and how enterprises can employ the technology to their advantage.

Public blockchains and the paradigm of trustlessness

On a public blockchain, anybody can register as a user and nobody can effectively censor anyone's activity in the system. This extraordinary openness has given rise to great hopes in how public blockchains and cryptocurrencies might change the world (see e.g. Tapscott and Tapscott, 2016). From a security perspective, however, uncompromising openness presents a unique challenge. Most technical systems rely heavily on perimeter security in the form of restricted access and firewalls. A completely open system by definition has no perimeter security. Anybody with the aim of harming the system can create an account—or a thousand accounts—and launch an attack from within. The gates are open.

An immediate consequence is that the system is only secure if it is secure from its own users. In

an open and disintermediated system, there is no basis for trust. The paradigm of trustlessness is unavoidable.

What characteristics of public blockchains ensure trustlessness? Trustlessness emerges from a design pattern which builds on two core ideas: redundancy and entanglement. For lack of a better term, it will be called entangled redundancy.

Redundancy is a well-established security principle. A commercial flight must be accompanied by at least two pilots. Banks observe a "four-eyes" principle when approving large credits. Distributed file systems store the same data on multiple nodes. On public blockchains like Bitcoin or Ethereum, redundancy is omnipresent. With the exception of mining, every node redundantly performs every computation in the system and every node redundantly stores every last byte of data. The goal is to avoid "single points of failure" or, more generally, prevent any minority of nodes from gaining control over any part of the system. Many of the strong security guarantees of blockchain systems—auditability, censorship-resistance, tamper-resistance—are immediate consequences of their all-embracing redundancy.

Entanglement describes how blockchains deliberately violate the design principle of "separation of concerns." The principle, introduced by Hürsch and Lopes (1995), recommends that a complex system be split into clearly separated components or layers, each of which deals with a single concern, such as process synchronization, failure recovery, or persistence. For instance, separation of concerns would imply that keeping nodes synchronized (a network issue), resolving conflicting transactions (a matter of business logic), and paying the system operators (a question of economic incentives) should be handled by different components. On a blockchain, all three tasks are covered by a single mechanism: the mining of new blocks. Mining is also performed redundantly by many agents, making it one example of how classic blockchains employ entangled redundancy.

Another example of how entangled redundancy permeates blockchain design is its authentication mechanism (Greenspan, 2018). Most other types of database separate authentication from interaction with the data. A user sends credentials to a central authorization component, which validates the credentials and grants the user a database connection. The user can then submit multiple transactions via the database connection without the need to re-authenticate every time. A blockchain, by contrast, entangles authentication and data interaction to dispense with the central authorization component: Every transaction must carry the digital signature of its creator to be able to authenticate itself. In addition, every node runs its own authorization component and redundantly checks that the signature is valid.

Entangled redundancy provides blockchain with the foundation for a comprehensive and resilient system of checks and balances. Every node can independently audit the system and verify that transactions "make sense" on all levels: as blobs of data in a peer-to-peer database, as economic transactions, and as a component in the system's incentive structure. Every user can see everything. Even the algorithms which use and create data on the blockchain are made transparent and auditable in the form of smart contracts. See Figure 1 for an illustration.

In total, this enables an all-embracing regime of "algorithmic self-policing" (Swan, 2016, p. vii). In a sense, public blockchains replace trust with security. They require no trust because the rules are strict, difficult to break, and almost impossible to break unnoticed. The result is an open and transparent system which is nonetheless secure and predictable for its users. However, the commitment to trustlessness comes at the cost of three desirable features: Efficiency, confidentiality, and flexibility.

Efficiency. The inefficiency of public blockchains is frequently pointed out. In comparison to other distributed database systems, public blockchains have low throughput capacity, high communication overhead, high storage requirements, and a high computational burden (Rauchs et al., 2018, Figure

11). Some inefficiencies, particularly those caused by Proof-of-Work consensus (Stoll et al., 2019), may be addressed in future implementations of public blockchains. Others are an immediate consequence of redundancy and can only be addressed by reducing the level of security. Only a node which redundantly performs all computations in the system and redundantly stores all the data is truly able to independently verify the state of the system. Thus, removing redundancy means giving up the security that comes with it.

Despite the inefficiency, Bitcoin and Ethereum are relatively lean systems that were built to run on a standard laptop. This is due to a number of self-imposed constraints which keep the number of transactions per second low and the computational burden of each transaction light. Corporate use cases which require a high number of transactions per second or high computational requirements may be unable to operate under similar constraints. Under these circumstances, it becomes important to consider where the security provided by redundancy is truly required and where it can be relinquished in the interest of efficiency.

Confidentiality. Rauchs et al. (2019, p. 51) find that one third of the discontinued corporate blockchain projects they investigated failed due to concerns about confidentiality and privacy. Even when legal issues are successfully addressed, enterprises may see too much transparency as a threat. Only command over scarce resources provides a competitive advantage (Carr, 2003). Access to data and algorithms can be a scarce resource, and in this case enterprises will be reluctant to open up. Advertising transparency as an end in itself is unlikely to convince them.

Unfortunately, reducing the transparency within a blockchain system can negatively impact its performance and security (Greenspan, 2018). The highest level of security is achieved when every user validates all transactions. But users can only validate what they can see. In the extreme case where data is shared only between two nodes and completely hidden from the rest of the system, a blockchain cannot provide more security than a direct connection between the two nodes. More generally, the parts of a transaction which are concealed from other users—for example through encryption or hashing—cannot be "understood" and therefore cannot be validated within the blockchain system.

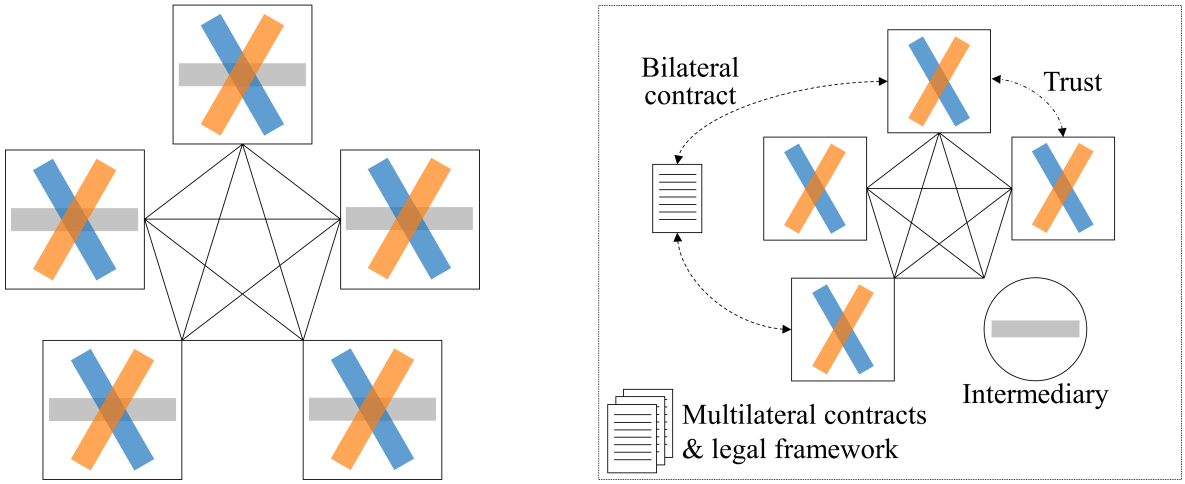
Flexibility. Trustlessness reduces the flexibility of a system on two levels. First, in a completely predictable system it is not possible to flexibly react to unforeseen circumstances. On Bitcoin, for example, it is impossible to retrieve coins which were accidentally sent to an unclaimed address. While such retrievals would be a useful and harmless feature in and of itself, malicious users could exploit the mechanism to revert legitimate transactions, thus making Bitcoin payments less predictable.

For corporate blockchains, a narrow focus on predictability can prove fatal, for instance when a court demands that data be erased but the blockchain's tamper-resistance makes it very difficult or even impossible to do so.

Second, a trustless system is difficult to fix or improve. A high degree of entanglement means that everything is connected and small changes may have unforeseen consequences. The resulting difficulties are illustrated by Ethereum's ongoing struggle to replace Proof-of-Work mining with something less wasteful. Since mining serves many purposes simultaneously, improving how it is done has proved to be an overwhelming task.[1]

For cryptocurrency, blockchain's first application, a lack of flexibility is arguably less important. While the technical details of the implementations have changed, the working principle has essentially remained the same since Nakamoto (2008) implicitly defined what a cryptocurrency should be. Classic blockchains have proved highly resistant to fundamental change, and users who demanded alterations were often asked more or less kindly to go and build their own blockchain. The same ap-

[1] For details, see https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.



(a) Public, trustless blockchain *(b) Blockchain as a team player*

Figure 2: Comparison of a trustless blockchain and blockchain as a team player. Blockchain (a) was developed with trustlessness as the overarching design principle. No trust is assumed among users and no third parties are allowed to perform services on the blockchain. Blockchain (b) is embedded in a wider context of existing trust relationships, legal contracts, and law. Furthermore, selected functions on the blockchain are performed by an intermediary instead of the users. While blockchain (b) is "less trustless" than blockchain (a), it enables higher levels of efficiency, confidentiality, and flexibility.

proach will not work for enterprises. A high degree of entanglement can make it difficult to adjust the system to evolved business practices, re-negotiated contracts, or new laws. At worst, the blockchain will be rendered obsolete because it cannot adapt to changing requirements and circumstances.

In conclusion, public and trustless blockchains strive for unbreakable security, complete transparency, and maximum predictability at the cost of efficiency, confidentiality, and flexibility. Their design reflects a deep suspicion of third parties and the fact that a completely open and fairly anonymous internet application cannot rely on any external factors, such as trust, to keep their users from abusing or attacking the system.

A new perspective

The paradigm of trustlessness is neither good nor bad in itself, in the same way that trust is not a yes-or-no issue. On public blockchains, however, the commitment to trustlessness is absolute, since there is no other way of keeping the system secure.

The designer of a corporate blockchain, on the other hand, is not in the same position as early blockchain inventors like Satoshi Nakamoto or Vitalik Buterin. For her, public blockchains continue to be a source of inspiration, but she has the freedom to re-evaluate their design choices.

The private blockchain implementation Hyperledger Fabric, for example, sacrifices some security for efficiency with its lean consensus algorithms, and some transparency for confidentiality with its access control features and private channels (Androulaki et al., 2018). Other technologies follow a similar path.

On a conceptual level, two shifts of perspective reveal how private blockchains can employ other mechanism alongside trustlessness: View blockchain as a team player, and embrace intermediation, but on your own terms.

Blockchain is a team player. Corporate blockchains cannot and usually should not handle all aspects of a business use case on their own. In this regard, it is helpful to view blockchain as a tool for the mitigation of transaction risk.

Transactions can fail for many reasons: misunderstanding, malfunction, incompetence, fraud. Enterprises rely on a wide range of tools to reduce transaction risk, the most important one arguably being the legal contract. Other mechanisms include trust, reputation, and law. Blockchain is a new tool. It can offer powerful support when transaction risk stems from unreliable data, a lack of transparency, or unpredictable technical systems. It can also be an efficient and secure alternative for certain trust-based interactions and paper-based contracts.

At the same time, blockchain designers should dare to rely on contracts, trust, reputation, and law where justified (compare Figure 2). This will lighten the burden placed on the blockchain and go a long way towards offering sufficient levels of efficiency, confidentiality, and flexibility. A blockchain does not have to replace all existing contracts with smart contracts and thus provide all "social contexts within which [legal] contracts operate, and the complex ways in which people use them" (Levy, 2017, p. 1). It does not have to disregard existing trust relationships and ignore that "while both trust and security are mechanisms for reducing complexity and making life more manageable, trust enables people to act in a richly complex world, whereas security reduces the richness and complexity" (Nissenbaum, 2004, p. 179). It does not have to emulate Bitcoin's deep suspicion of public and financial institutions and attempt to solve "trust problems" which its users see as unproblematic (Golumbia, 2016). A good corporate blockchain is a team player. Many applications will benefit from a blockchain, but few should be moved entirely onto one.

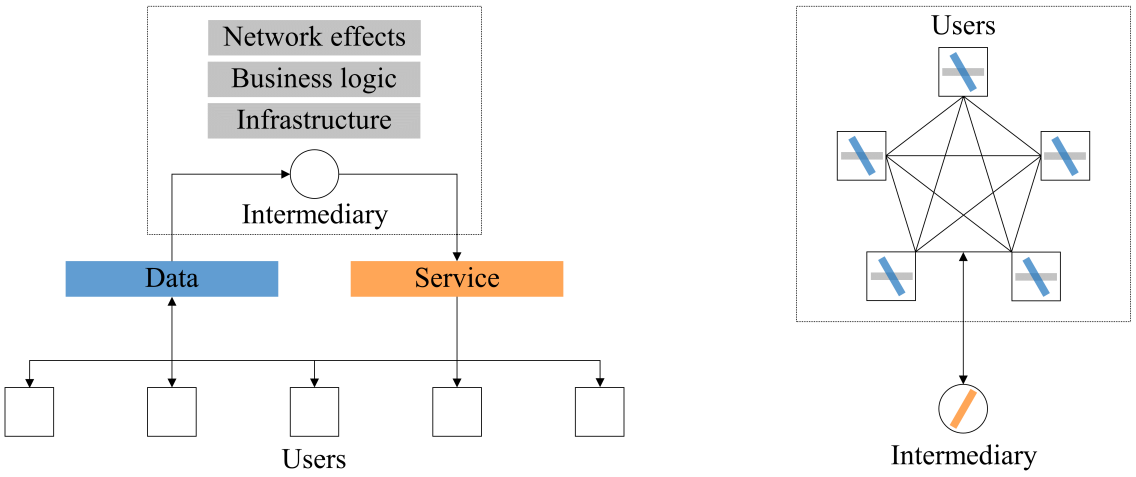
As a concrete example of blockchain as a team player, consider a system which implements tamper-resistance not through the usual technical measures but through legal contracts. In this approach, users are free to modify data on the blockchain, but in doing so leave behind indelible tamper evidence which is visible to every user. The users negotiate a legal contract which defines the circumstances under which modifications to data on the blockchain are permitted. The tamper evidence guarantees that a breach of contract is easy to detect and claim, the legal contract ensures that the system remains flexible in case of unforeseen circumstances or new laws.

Intermediation, on your own terms. Blockchains and third parties are often presented as natural opponents. But few would say that intermediation is a problem in itself. Intermediaries provide useful services. They only become a problem when they demand excessive fees, thwart competition, and generally make themselves irreplaceable, e.g. by gaining control over data, processes, technical infrastructure, and networks. Harmful intermediaries erect technological barriers to entry for competitors, who might otherwise provide better and cheaper services.

Blockchains can lower these technological barriers for entry. They allow their users to keep an eye on their data, define their own processes, operate the infrastructure on their own and build a network without a powerful intermediary at its center. While intermediaries can still act as a trusted third party on the blockchain and perform useful services, the power relationship between intermediaries and users is turned on its head. Figure 3 illustrates the idea.

Such user-controlled blockchains with intermediaries also hold great potential for the privatization of public services. With a blockchain, public institutions can provide the playing field and set the rules for private contractors. The system remains under the control of the public institution while the services performed within the system are privatized. This makes privatization more competitive and more transparent.

Consider the following example of a blockchain with an intermediary. A consortium of enterprises stores information about transactions on a mutually operated blockchain. While users can only see



(a) Intermediation without blockchain

(b) Intermediation with blockchain

Figure 3: A blockchain can limit the power of an intermediary. In both situations, the intermediary performs a useful service. In situation (a), however, the intermediary is also in control of the corresponding infrastructure, business logic, and network effects. This results in technical barriers to entry and effectively reduces competition for the service provided by the intermediary. In situation (b), the users remain in control by operating a shared blockchain system. The intermediary can still perform the service but can no longer erect technical barriers to entry.

their own data, one intermediary has access to all information on the blockchain. It acts as an arbitrator who intervenes when a conflict arises between two users. The act of arbitration is likely to require expert knowledge and human judgment, for instance to determine legal responsibility and negotiate reimbursements. Consequently, the intermediary must be trusted. The service performed by the intermediary is indispensable—but the intermediary itself is not. The consortium can switch to a competing arbitrator at any time without the need to re-collect data, re-invent processes, re-build technical infrastructure, and re-create network effects. One could even imagine a marketplace for arbitration on the blockchain.

Conclusion

Celebrating the launch of the Ethereum blockchain in 2015, the blockchain author and investor William Mougayar demanded: "We need to learn how to apply what the blockchain gives us."[2] But enterprises are not in the business of doing justice to a technology. Blockchain developers need to learn how to apply the technology to corporate use cases. The resulting blockchains may have little in common with pioneer blockchains like Bitcoin or Ethereum, because they carefully balance security and efficiency, transparency and confidentiality, predictability and flexibility.

The uncompromising design of public blockchains is still too often presented as the ideal to which all blockchains should aspire. Absence of trust among users and the removal of third parties are postulated as essential characteristics of any "real" blockchain.

But above all, a corporate blockchain must be useful. A useful blockchain is sufficiently flexible to deal with the intricacies of complex and ever-changing business requirements. It falls back on legal contracts where it makes sense. It relies on trust, reputation, and existing legal frameworks where justified. It integrates intermediaries without giving up control. Usefulness, not trustlessness, should be the overarching design principle for corporate blockchains.

[2] https://blog.ethereum.org/2015/05/24/the-business-imperative-behind-the-ethereum-vision/.

References

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., and Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18)*, pp. 1–15, Porto, PT. ACM Press. https://doi.org/10.1145/3190508.3190538.

Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review*, (May 2003).

Golumbia, D. (2016). *The Politics of Bitcoin: Software as Right-Wing Extremism*. University of Minnesota Press, Minneapolis, MN, first edition.

Greenspan, G. (2018). Where blockchains add real value. *Innovations: Technology, Governance, Globalization*, 12(1–2):58–69. https://doi.org/10.1162/inov_a_00267.

Hürsch, W. L. and Lopes, C. V. (1995). Separation of concerns. Working paper, College of Computer Science, Northeastern University.

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.

Mulligan, C., Scott, J. Z., Warren, S., and Rangaswami, J. P. (2018). Blockchain beyond the hype: A practical framework for business leaders. Whitepaper, World Economic Forum.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Whitepaper. Retrieved May 27, 2020, from https://bitcoin.org/bitcoin.pdf.

Nissenbaum, H. (2004). Will security enhance trust online, or supplant it? In Kramer, R. M. and Cook, K. S. (eds.), *Trust and Distrust in Organizations: Dilemmas and Approaches*, volume 7 of *Russell Sage Foundation Series on Trust*, chapter 7. Russell Sage Foundation.

Rauchs, M., Blandin, A., Bear, K., and McKeon, S. (2019). 2nd global enterprise blockchain benchmarking study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3461765.

Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K., and Zhang, B. (2018). Distributed ledger technology systems: A conceptual framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3230013.

Stoll, C., Klaaßen, L., and Gallersdörfer, U. (2019). The carbon footprint of Bitcoin. *Joule*, 3(7):1647–1661.

Swan, M. (2016). *Blockchain: Blueprint for a New Economy*. O'Reilly UK Ltd., first edition.

Tapscott, D. and Tapscott, A. (2016). *Blockchain revolution : how the technology behind bitcoin is changing money, business, and the world*. Portfolio, New York, first edition.

The Economist (2015). The trust machine: The promise of blockchain. *The Economist*.