Enterprise Blockchain Explained

By Stanton Heister

June 2022

What Is Blockchain

A blockchain is a chronologically ordered set of records stored on a decentralized (distributed) ledger. Blocks in the "chain" contain a set of transactions that are cryptographically linked to the previous block in the chain. A block is a list of transactions plus a block header. Blocks are linked together in the chain by the information contained in the block header.

The header contains:

- An algorithmically created cryptographic **hash** of the data in the block. A hash is a unique alphanumeric sequence and can be thought of as a "digital fingerprint."
- A **timestamp**
- The **hash** of the **previous block**

Linking a hash from block to block creates a chronologically linked chain. Figure 1 depicts how blocks are formed and linked in a blockchain. The very first block in a system is called the *genesis block* and begins the chain.

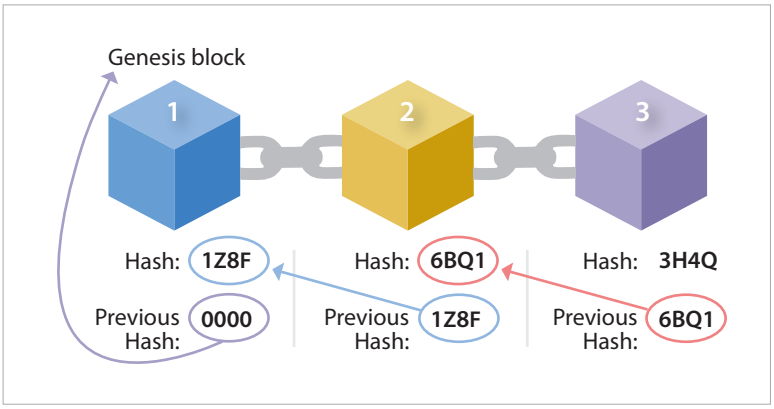


Figure 1: Blocks cryptographically linked.

Adapted from Simply Explained (2017).

Four fundamental characteristics of blockchains include:

- **Decentralization**—Records contained on ledgers within blocks are stored on a distributed network of computers called "nodes" rather than in one large central repository such as a bank or other third-party intermediary. In a distributed system, parties can transact directly without a central intermediary, which can save both time and costs. The images in Figure 2 represent how we can visualize computers all linked to a central point, a bank in this case (centralized), versus how a network of distributed computers operating in the cloud would interact.

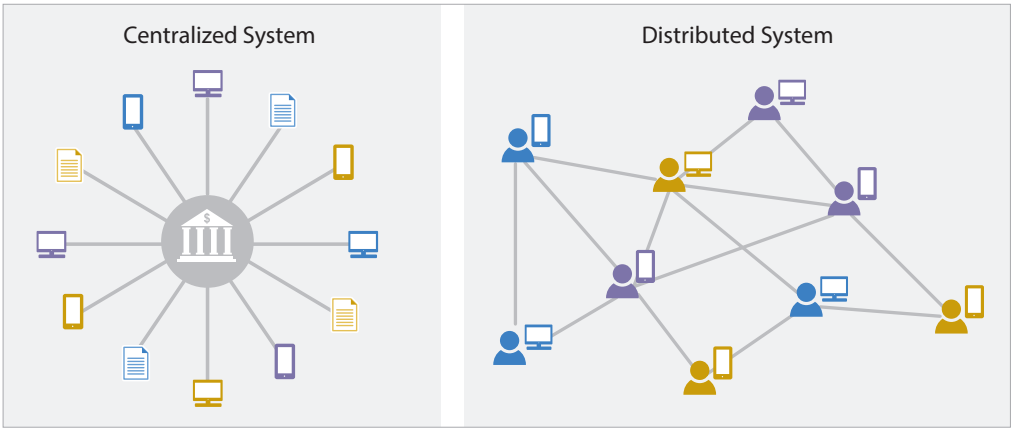
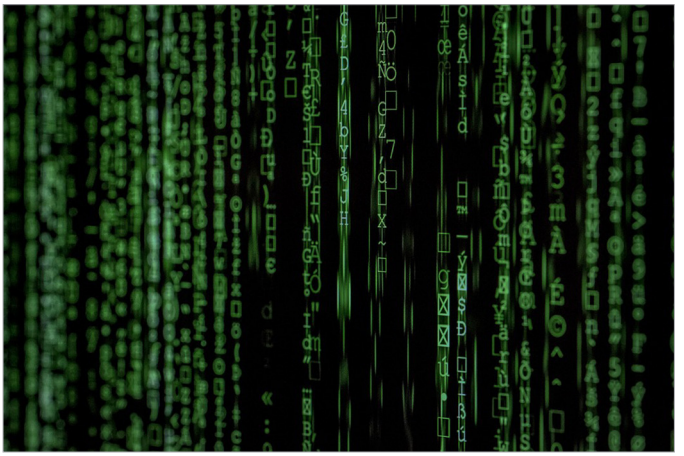


Figure 2: Centralized versus distributed systems.

- Decentralized systems also eliminate what is sometimes referred to as a "honey pot" of data—where massive amounts of data are stored in one central location. This information can be very attractive for bad actors or cyber thieves to hack because of the potentially sensitive nature of the data stored in these systems, such as social security numbers or bank account information. Despite advances in software security, the number of cyber breaches is increasing. According to a recent report on data breaches, "The total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019" (RiskBased Security, Inc., 2021, p. 1). Users of centralized systems are at risk of their personal records becoming compromised, and every year millions of personal records, including names, emails, and passwords, have been subject to data breaches perpetrated by cyber hackers (RiskBased Security, Inc., 2021). Security is vastly improved in blockchain systems as blocks are stored over a decentralized set of nodes. This makes it extremely improbable for one entity to control a set of transactions because each block is stored on a distributed set of nodes, all of which must agree on each transaction's validity before it is committed to the chain (Heister & Yuthas, 2020).



Centralized data storage is vulnerable to hacking or other data breaches.

Photo courtsey Pixabay.

- **Immutability**—Once a transaction is recorded to a block and that block is cryptographically linked to the prior block, the transaction *cannot* be altered or deleted as with traditional databases. Traditional databases allow for four functions, where users or administrators can *create*, *read, update*, or *delete* a record. Blockchains are *append-only* systems, which means records can only be created or read but cannot be updated or deleted.
- **Security**—Computers or nodes in the system must come to a *consensus* that a transaction is valid. When that happens, the transaction is then committed to the block and can no longer be altered. This is fundamentally different than traditional systems where records can be recorded without prior validation that there is no other competing record. When a transaction takes place on the block, a consensus protocol is referenced to get the majority of the network to agree upon a single state transaction or change and then *tie* the current block of transactions to the previous block via a cryptographic *hash* (Zhang et al., 2019).
- The first consensus protocol, detailed in a 2008 white paper written by Satoshi Nakamoto (an unknown individual or set of individuals using that pseudonym) and used in many public blockchains like Bitcoin, Ethereum, and Litecoin, is known as proof of work (POW) or "mining." Because of the extreme energy use and poor transaction times of POW systems, other consensus protocols have arisen. The Ethereum blockchain is currently in the process of converting from POW to a "proof of stake" (POS) system that requires far less energy as consensus requires fewer nodes than a typical POW system. In POS systems, a finite number of nodes are chosen (e.g., fifty or one hundred) to validate transactions and create blocks. Proof of work blockchains can have an infinite number of miners participating in the validation and creation of blocks. Conversely, the Bitcoin POW network has hundreds of thousands of nodes participating in consensus. The country of Kazakhstan, a large participant in the crypto mining industry, has nearly 90,000 mining nodes which consume over 8 percent of the

country's energy (Volpicelli, 2022). Permissioned or private blockchains also employ different types of consensus strategies depending on the use case and solution. These networks differ from public systems where anyone can participate and view all transactions, and the network is governed by the entire community or set of node operators. In private blockchains, consensus can be achieved through a defined set of participants attaching cryptographic signatures to vote on what or if a transaction gets written onto the ledger. In all of these approaches, no single central authority arbitrates what is true or written onto the blockchain.

- There are many different types of consensus mechanisms. Four of the more popular ways that blockchains reach consensus are: POW, POS, practical byzantine fault tolerance (PBFT), and delegated proof of stake (DPOS) (Xiaoqi et al., 2017). Although consensus is a key part of what makes blockchain technology unique, expanding on the topic is beyond the scope of this article. Readers are encouraged to further research blockchain consensus protocols (Xiao, et al., 2020) for a deeper understanding.
- The consensus and transaction block-building process prevents malicious attacks as *any* change in *any* block in the system will cause the hash value to change, which will break the chain, and that attempt to change the ledger will then be rejected.

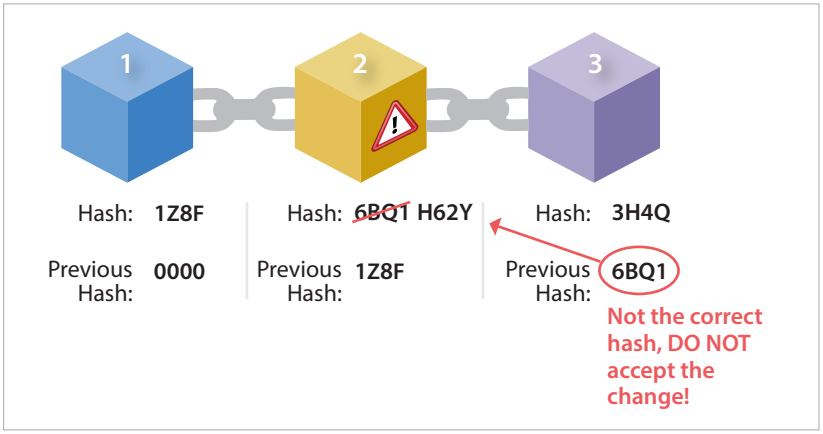


Figure 3: Broken chain.

Adapted from Simply Explained (2017).

- Figure 3 illustrates what happens when a bad actor attempts to break into one of the blocks and change the data in that block (block 2 in this case). We can see that by changing any data on the ledger within the block, the cryptographic hash is forced to *change*, and the chain will be broken. When the hash of any block changes, it will no longer be able to link with the next block, and the attempt to change the data will be rejected and voided by the system.

- **Transparency**—In public or permissionless systems such as Bitcoin or Ethereum, any user who has access can view recorded transactions on any block in the database. Once a record is committed to the database, it becomes visible to all. In private or permissioned systems, permissions are provided to individuals within the consortia of participants, and that permission system determines who can see which transactions. In these systems, even though permissions grant certain visibility, each participant in the system has the same set of agreed-upon transactions and can validate this at any time, thereby creating a single version of the "truth."

These four functions: **decentralization**, **immutability**, **security**, and **transparency**, create *trust* in the system without the need for any centralized authority. This makes blockchain or *distributed ledger technology* (DLT) unique and potentially disruptive for many industries. It should be understood that blockchain and DLT systems are rarely stand-alone solutions and are best suited when combined with other technology, systems, or networks. Architecturally, blockchains typically sit on top or beneath another set of technology and assist in performing transactions, tracking custody changes between parties, and providing immutability, which an underlying system would not otherwise possess. For example, system architects would likely not attempt to replace an enterprise resource planning (ERP) system with a blockchain solution. Rather, blockchain would sit on top of that system and manage transactions, track the movement of inventories, and improve security and transparency among trading partners.

Second/Third Generation Blockchains

One key development to the blockchain ecosystem was when it transitioned from the first-generation blockchains like Bitcoin to second-generation blockchains like Ethereum and those that have followed. The Bitcoin blockchain, described in Satoshi Nakamoto's 2008 white paper, was innovative and groundbreaking (Nakamoto, 2008). The Bitcoin blockchain created the first working system that eliminated the need for intermediaries for the transfer of cryptocurrencies. Second-generation blockchains such as Ethereum are what computer scientists refer to as "Turing complete." They enable a much more robust set of code execution. For example, the Ethereum blockchain allows rules to be written in any way that can be expressed by computer code, which enables the writing and execution of smart contracts (Wang, 2017). According to Cong and He (2017), "Smart contracts are digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution." In essence, smart contracts are agreements that contain if-then logic. For example, if flooding is reported, then an insurance payment will be sent.

Smart contracts can facilitate and enforce agreements between one or more parties in an automated fashion, thereby speeding the processing of systems and ensuring accuracy. For example, globalization has transformed the way companies procure, process, and produce goods, and as a result, global supply chains have become complex and have increased the number of intermediaries to settle transactions. When we reduce or even eliminate intermediaries and the number of transactions

Second-generation blockchains, such as Ethereum, allow more flexible and robust code execution than do first-generation blockchains, such as Bitcoin.

Photo courtesy Unsplash.

through the use of smart contracts, efficiencies improve in turn. Supply chains are often fraught with transaction fees, as each intermediary takes some percent (of the value) of the transaction. Even if it is a small fraction of the price of the goods processed, when spread across several intermediaries, these costs add up, and frictions put a drag on the global economy. Blockchain solutions enable goods to be tracked and moved end-to-end via information collection enabled by smart input mechanisms such as radio frequency identification (RFID) tags, beacons, or other sensors and processed in real-time, where both buyers and sellers receive information about the movement of goods and financial settlement along the way (Cong & He, 2017).

Additionally, the decentralization and elimination of costly intermediaries that blockchain provides could result in major impacts on companies and economies in the developing world. Eliminating costly fees helps small businesses compete with industry giants, which could have a significant and positive effect on the global economy (Gupta, V., 2017).

Figure 4 illustrates a simple process flow that might exist within an enterprise supply chain network or consortia. It highlights how transactions and assets can be driven digitally by smart contracts and how visibility in the system is enhanced. A system like this improves speed and reduces cost. A blockchain network such as this also enables retailers to identify a set of bad products and trace those products back to the source in seconds rather than weeks.

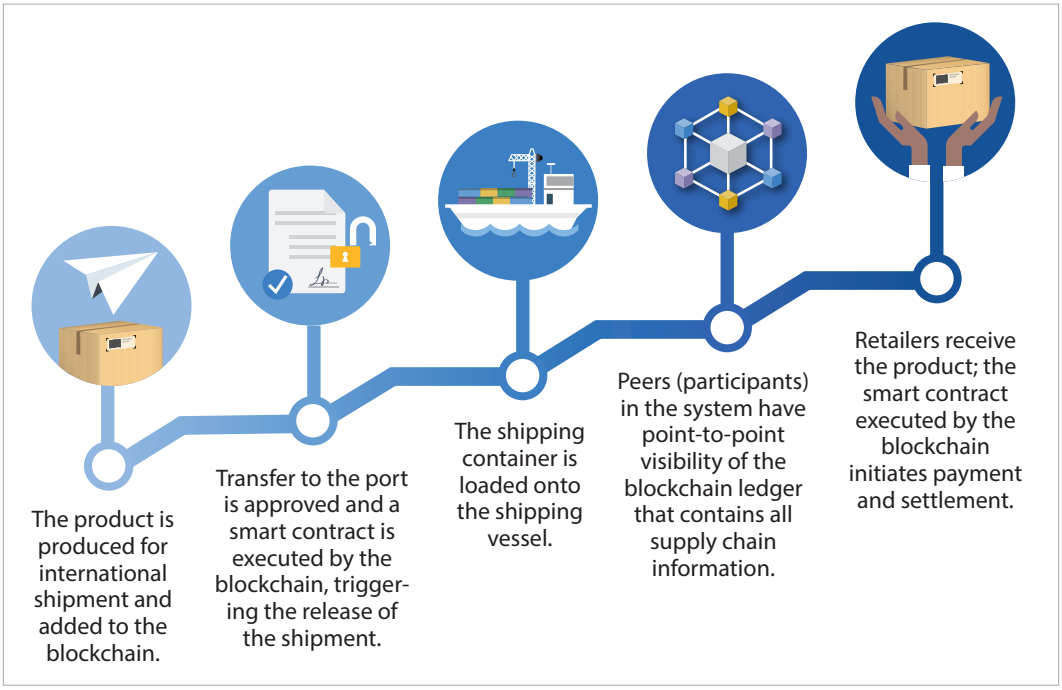


Figure 4: Global supply chain flow.

Adapted from Hewett and Deshmukh (2019).

Enterprise Blockchain

Private or permissioned blockchains are often referred to as *enterprise blockchain systems*. Enterprise blockchains have a defined set of participants that govern the system. In these permissioned blockchains, users are known entities and possess some level of permission to participate in the network. Permissions are defined upfront by members of the network or consortia and enable or constrict members' respective permissions to view or write data to the network. This is why enterprise blockchains are sometimes referred to as a "team sport" where members of the consortia have to agree to share data, coordinate processes, and allow others to help define the rules.

Anonymity and pseudonymity are also features of blockchains, especially public or permissionless systems, which attract some users. A distinction should be made between completely anonymous and pseudonymous. Someone who is anonymous is able to operate or speak in a way that makes them unidentifiable. Someone who is pseudonymous operates or speaks in a way in which they can be identified, but their identification shields who they actually are (Anonymity vs. Pseudonymity In Crypto, 2021). Because of the limited number of participants and the use of permissioning, enterprise blockchains are less anonymous than public or permissionless blockchains. This is not necessarily an undesirable feature, as anonymity in private chains is much less important, and the level of transaction visibility is determined by permissions that are predetermined and agreed to by the members of the consortia.

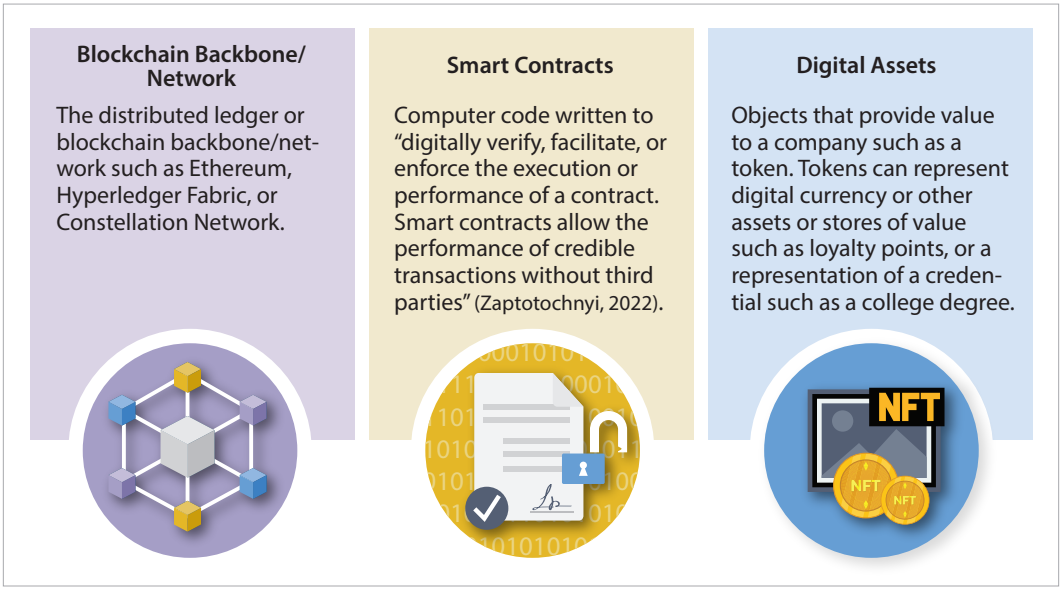


Figure 5: Key elements on which enterprise blockchains depend.

There are three key elements on which enterprise blockchains depend (see Figure 5):

- The distributed ledger or blockchain backbone/network such as Ethereum, Hyperledger Fabric, or Constellation Network.
- Smart contracts: Computer code written to "digitally verify, facilitate or enforce the execution or performance of a *contract*. Smart contracts allow the performance of credible transactions without third parties" (Zaptotochnyi, 2022).
- Digital assets: Objects that provide value to a company, such as a token. Tokens can represent digital currency or other assets or stores of value such as loyalty points or a representation of a credential such as a college degree.

The presence of these three elements enables groups of companies, known as consortia, to set up systems and processes to digitally conduct business with speed and efficiency in the absence of a central authority.

Enterprise blockchains do not require the vast amounts of processing power as other public chains do because they have many fewer nodes participating in the consensus and validation process. Consensus also tends to be reached faster, as there are far fewer nodes on a network to form a consensus. This is important because it also allows for the growth of the network and for quickly processing large numbers of transactions via improved scalability and throughput—problems that plague many public blockchain systems. Scalability is the capability of a blockchain network to increase the speed of transactions and the throughput needed by the network to decrease the processing time for transactions on the network. "The higher a network's scalability, the more efficiently it can send transactions and process different types of data. Scalability is one of the three main characteristics of a mature blockchain network, with the other two being decentralization and security" (Crypto glossary,

n.d., S section, para. 8). For organizations within an enterprise network, these are important factors.

An example of an enterprise network or consortia is Tradelens—a blockchain platform jointly developed by Maersk and IBM using Hyperledger Fabric as its underlying blockchain technology. It is a collection of supply chain partners that includes cargo owners, transportation carriers, freight forwarders, logistics providers, ports and terminals, customs agencies, and others. The Tradelens blockchain enables the efficient, transparent, and secure exchange of information that resides within the logistics system, which results in greater collaboration, trust, and cost savings across the global supply chain. According to ("Trade Made Easy," 2020), the Tradelens organization claims the digitization and exchange of data enabled by the blockchain solution could improve efficiencies by 15 percent resulting in a $1.8 trillion revenue increase in 2020 and a $5.2 trillion revenue increase per year by 2050.

Summary

Blockchain solutions make use of groundbreaking technology that has the potential to impact and even disrupt many industries. Its underlying architecture can be implemented to improve or replace legacy systems used by corporations, government entities, etc. These solutions also reduce frictions in economic systems that can cause inefficiencies and time delays and increase costs. Companies that ignore the potential system improvements that blockchain solutions provide may find themselves at a competitive disadvantage and may potentially find their very viability at risk. For these reasons, it is important for business executives to become knowledgeable about the possibilities blockchain and distributed ledger technologies (DLT) provide.

Blockchain and DLT have matured to the point where resources are becoming more abundant and thorough. Readers interested in researching more about blockchain can visit sources such as the Hyperledger Foundation, the Global Business Blockchain Council, or a recent whitepaper generated by a working group sponsored by the state of California which identifies several areas where the technology could be of use in the coming years (California Blockchain Working Group, 2020).

Bibliography

Anonymity vs. pseudonymity in Crypto. (2021, May 17). Cryptopedia. https://www.gemini.com/cryptopedia/anonymity-vs-pseudonymity-basic-differences

California Blockchain Working Group. (2020). *Blockchain in California: A roadmap*. https://www.govops.ca.gov/wp-content/uploads/sites/11/2021/06/BWG-Final-Report-2020-July1.pdf

Cong, L. W., & He, Z. (2017). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754–1797.

Crypto glossary. (n.d.). *Cryptopedia*. https://www.gemini.com/cryptopedia/glossary

Deloitte. (2020). *Deloitte's 2020 global blockchain survey: A new age of digital assets*. Deloitte Insights. https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf

Disparte, D. (2019, May 20). Why enterprise blockchain projects fail. *Forbes*. https://www.forbes.com/sites/dantedisparte/2019/05/20/why-enterprise-blockchain-projects-fail/?sh=2d271c7a4b96

GBBC. (n.d.). Global Blockchain Business Council. https://gbbcouncil.org/

Gupta, M. (2017). *Blockchain for dummies, 2nd IBM limited edition*. John Wiley & Sons.

Heister, S., & Yuthas, K. (2020). The blockchain and how it can influence conceptions of the self. *Technology in Society*, *60*. https://www.sciencedirect.com/science/article/abs/pii/S0160791X19301745

Hewett, N., & Deshmukh, S. (2019, April 25). 3 ways blockchain can revolutionize global supply chains. *World Economic Forum*. https://www.weforum.org/agenda/2019/04/3-ways-blockchain-global-supply-chains/

Hofer, L. (2019, April 23). DAG vs. blockchain–Technologies for different use cases. *ICO.li*. https://www.ico.li/dag-vs-blockchain/

Hurder, S. (2020, March 02). Why enterprise blockchains fail: No economic incentives. *Coindesk*. https://www.coindesk.com/why-enterprise-blockchains-fail-no-economic-incentives

Hyperledger Foundation. (2022). https://www.hyperledger.org/

Lee, A. (2019, April 28). How to position blockchain platforms to increase adoption. *LinkedIn*. https://www.linkedin.com/pulse/how-position-blockchain-platforms-increase-adoption-adrian-lee/

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. *Bitcoin.org*. https://bitcoin.org/bitcoin.pdf

RiskBased Security, Inc. (2021). *RiskBased security. 2020 Year End Report Data Breach QuickView*. https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

Simply Explained. (2017, November 13). How does a blockchain work–Simply explained [Video]. *YouTube*. https://www.youtube.com/watch?v=SSo_EIwHSd4

Trade Made Easy. (2020). *Tradelens*. https://www.tradelens.com/

Volpicelli, G. M. (2022, January 12). As Kazakhstan descends into chaos, crypto miners are at a loss. *Wired*. https://www.wired.com/story/kazakhstan-cryptocurrency-mining-unrest-energy/

Wang, K. (2017, July 6). Ethereum: Turing-completeness and rich statefulness explained. *Hackernoon*. https://hackernoon.com/ethereum-turing-completeness-and-rich-statefulness-explained-e650db7fc1fb

World Economic Forum. (2020). *Global Standards Mapping Initiative: An overview of blockchain technical standards*. http://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf

World Economic Forum. (2020). *Inclusive deployment of blockchain for supply Chains: A Framework for blockchain interoperability*. http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

Xiaoqi, L., Peng, J., Ting, C., Xiapu, L., & Qiaoyan, W. (2017). A survey on the security of blockchain systems. *Future Generation of Computer Systems*, *107*. https://doi.org/10.1016/j.future.2017.08.020

Xiao, Y., Zhang, N., Lou, W., & Hou, T. (2020). *A survey of distributed consensus protocols for blockchain networks*. Virginia Polytechnic Institute and State University, Washington University. https://doi.org/10.48550/arXiv.1904.04098

Zaptotochnyi, A. (2022, April 11). What are smart contracts? *Blockgeeks*.

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computer Survey*, *52*(3). https://doi.org/10.1145/3316481

About the Author

Dr. Stanton Heister's education includes a BS in business administration from the University of Michigan, an MBA from the University of Portland, and a doctorate in business administration with a focus on international business from Argosy University. Dr. Heister currently teaches in the School of Business at Portland State University and has taught many different courses in the management and leadership area, as well as the following Blockchain courses: Blockchain Fundamentals, Blockchain for Business, Blockchain for Business Lab, Emerging Topics in Blockchain, and Blockchain and Exponential Technologies.

Dr. Heister has published several papers in the area of blockchain and distributed ledger technology and cowrote a chapter titled "How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity," which was included in the book *Blockchain Potential in AI*.