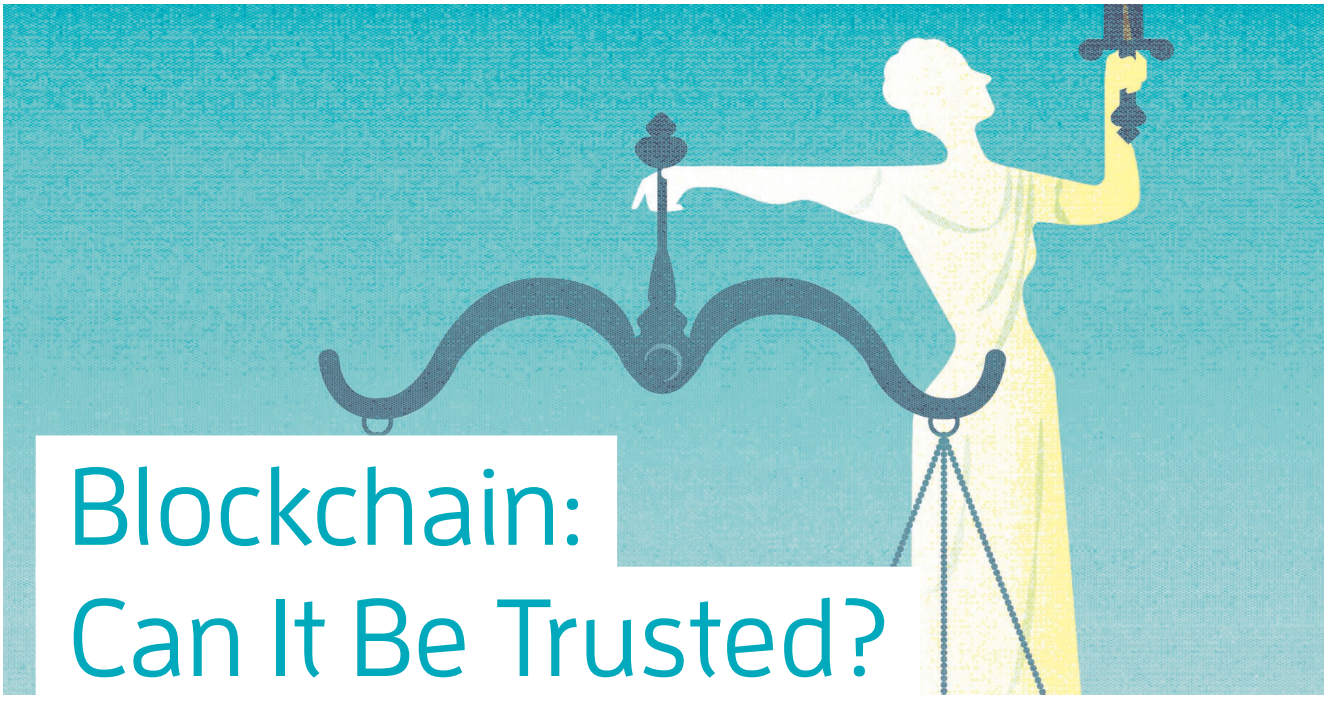

Blockchain: Can It Be Trusted?

Mohiuddin Ahmed, Edith Cowan University

Al-Sakib Khan Pathan, Independent University, Bangladesh

Blockchain technology claims to provide unparalleled security and data privacy, yet some vulnerabilities have recently been identified. In this article, we showcase the key advantages of blockchain technology and look at recent security breaches, critically analyzing its benefits while highlighting some resulting financial mishaps.

Blockchain was introduced by S. Nakamoto[1] for transactions involving cryptocurrency (also known as *Bitcoin*) in 2008. For Bitcoin, the concept of blockchain can be used as a public ledger to keep track of all transactions. Based on the effectiveness of blockchain in Bitcoin, this technology has been applied and is being integrated in a wide range of industries, such as finance, supply chain management, agriculture, and many others. Since the blockchain is able to digitize transactions efficiently, its technology is considered to make all types of transactions secure and transparent. Figure 1 reflects the key characteristics of blockchain technology. Although the recent literature extends these characteristics, the key characteristics remain the same.

A blockchain is the accumulation of a series of blocks where each block stores data involved in a transaction. When the transaction occurs, it is stored in a block and added to the chain.[1] These blocks form a distributed database to store valuable information and form a blockchain. Since the blockchain contains shared databases, each of the participants in the blockchain has access to the same database. These databases are cryptographically secure to protect the integrity of the data. Adding any new blocks in the chain requires approval from each of the participants, making the data in the blockchain immutable. No intruder would be able to inject or delete any data from

Digital Object Identifier 10.1109/MC.2019.2922950
Date of current version: 9 April 2020

the blockchain. In terms of data security, the common cyberattacks like the denial-of-service (DoS) attack[2] and many others[3,4] do not have any significant effect if the data are stored using the blockchain. Therefore, this technology is being embraced at a rapid pace across a number of application domains. Now that we have this promising information in hand, let us learn about the effectiveness of blockchain, especially in the financial domain.

Blockchain technology is promising for financial organizations due to the unique characteristics discussed earlier. It could be helpful for those organizations considering the following aspects:

- Efficiency is increased because of transparent data records and the lack of intermediaries. The decentralized ledger system should reduce the period of settlement for any property purchase or sale, including the steps involved in each transaction.
- Data integrity is enhanced, which reduces the chance of potential financial loss. Since the records are immutable in the blockchain, it provides more accurate data with security for business operations and regular clients of any financial organization. Blockchain potentially reduces the risk of fraud and reflects an impeccable audit trail.
- Customer experience is improved through faster processing of information to set up new ventures. With blockchain, customers don't have to worry about using third parties to verify the legitimacy of any data and transaction.
- A higher availability of capital and reduced cost of business are offered. Blockchain has robust consensus mechanisms and smart contract options, which can optimize the time for a transaction to happen. This technology is also going to eliminate the administrative processing complexities associated with any account and third party, which would ease the capital flows for both clients and business owners.

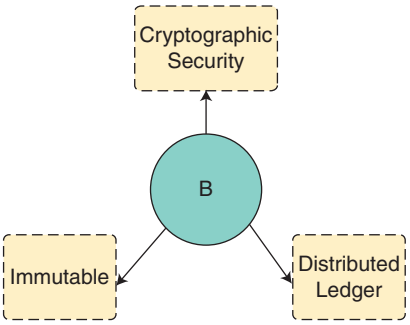

FIGURE 1. The key characteristics of blockchains.

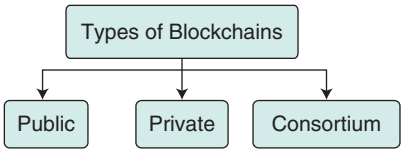

FIGURE 2. The different types of blockchains.

Despite showing great promise, recent discoveries suggest that there are some alarming security concerns with the widespread usage of blockchain in practice.[5] For example, the 51% attack or double-spend attack is quite common today.[10] In this attack, a miner or group of miners on a blockchain attempts to spend their cryptos on that blockchain twice. The attackers acquire control of a majority of the network's mining power and can easily defraud other blockminers in the network by sending them payments and then creating a dummy of the blockchain where the payments never really happened. In this article, we highlight some of the recent security issues and financial hazards that have occurred due to some vulnerabilities found in the technology.

BLOCKCHAIN TAXONOMY

In this section, we provide a taxonomy of blockchain and discuss the smart contracts that are blockchain's essential components.

Types of Blockchains

Figure 2 depicts three major types of blockchains, which are briefly described below.

- *Public blockchains*: In this type, everyone can add a record to the block. Public blockchains contain any kind of data, a variety of nonrelated transactions that may or may not be financial. Today, public blockchains are used mostly for financial value exchange among multiple parties. For example, Ethereum is a distributed public blockchain network where miners try to earn Ether (a type of crypto token).
- *Private blockchains*: Only certain participants are allowed to write data in private blockchains. The key characteristics of private blockchains are performance and security. For example, when a company such as Paypal is required to securely store client information and financial transactions, the private blockchain

is superior in terms of performance compared to a public blockchain.
- *Consortium blockchains* (also known as *federated blockchains*): This type of blockchain has similar characteristics to private blockchains and can help multiple organizations with transactions and help maintain transparency among the involved parties. A consortium blockchain is synchronized to keep track of the transactions among the consortium members. Although this type of blockchain has relatively lower latency in transaction processing, it is not entirely decentralized.

Smart Contracts

A smart contract is a computer code that facilitates blockchain transactions. It is an entity of blockchain and an autonomous computer program that executes upon meeting specific conditions. In other words, smart contracts are the digital version of traditional economic contracts among different parties involved in any trade or business. Unlike traditional contracts, the blockchain-enabled smart contracts do not require any intermediaries to ensure the conditions are fulfilled. Figure 3 reflects the key benefits of smart contracts, which are briefly outlined below.

- *Accuracy*: Since there are no human intermediaries due to the executable codes, the system performs accurate transactions.
- *Autonomy*: Smart contracts can be developed by anyone.
- *Efficiency*: This is manifested due to the absence of multiple intermediaries.
- *Profitability*: Since human intermediaries are replaced by executable computer codes, the system is cost-effective.
- *Traceability*: Smart contracts provide a permanent record that facilitates audit and traceability, even if the original owner is no longer in business.

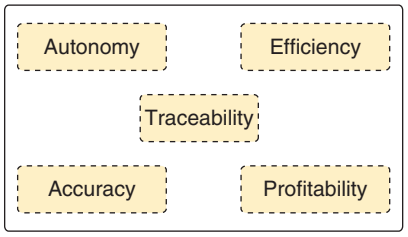

FIGURE 3. The benefits of smart contracts.

RECENT SECURITY BREACHES

Blockchain systems cannot ensure security even with such promising characteristics. Blockchain systems are vulnerable, and there is a tradeoff between scalability and security. To ensure the performance, security must be sacrificed. Although there are plenty of research works in scalable security, there is a significant lack of such research and development for the blockchain environment. As the blockchain-enabled system grows, for example, the number of users increases, or to facilitate services, the security is sometimes overlooked. Figure 4 shows that there is no one-size-fits-all blockchain solution,[7–9] and a comparison among the three different variants of blockchain systems is illustrated.

In this section, we highlight the recent issues with the usage of blockchain for financial organizations. However, the root cause of such disastrous situations is software vulnerability. A vulnerability can be an error in the code or a flaw in how it responds to certain requests. Among many, a common vulnerability that facilitates an attack is known as *Structured Query Language (SQL) Injection*. In certain websites, SQL can be used to search for keywords. Anyone with malicious

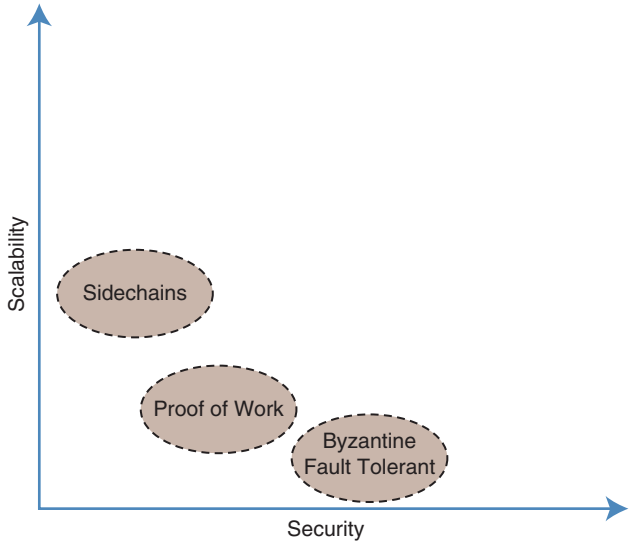

FIGURE 4. A comparison among three different variants of blockchain systems.

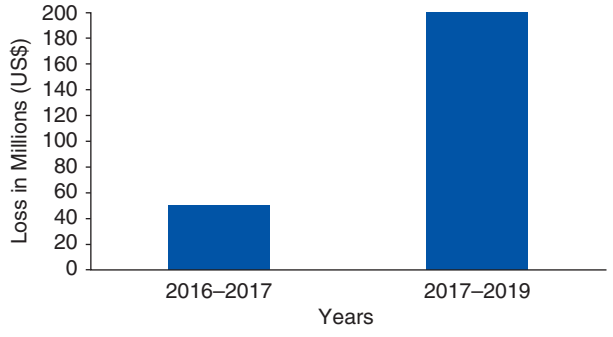

FIGURE 5. The recent financial losses due to smart contract vulnerabilities.

intensions can exploit this feature to create a query that contains SQL code. If the website is not properly protected, the search function will execute the malicious SQL query and potentially allow access to the database and provide control of the website to the cyber criminals.

Vulnerabilities exist in every type of software. Unfortunately, even the most popular operating system, Microsoft Windows, was open to the WannaCry attack.[6] It is alarming to note that one of the most popular web browsers, Firefox, had more than 100 vulnerabilities identified in each year since 2009. It is a reality that many software and web applications are developed within a tight time frame and do not have a foolproof process. In fact, developers often must prioritize meeting release deadlines rather than ensuring the security of the product. As a result, there might be vulnerabilities in the released product that cyber criminals can exploit.

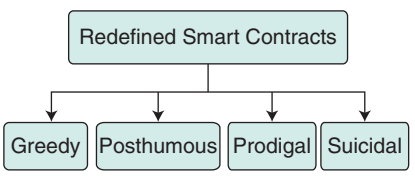

FIGURE 6. The four types of vulnerable smart contracts.[5]

In the context of smart contracts, web application and software vulnerabilities are of prime concern. Figure 5 shows the yearly financial loss due to such vulnerabilities. In 2016, US$50 million was stolen by exploiting the vulnerabilities of Ethereum blockchain.[5] A critical vulnerability was found for a subset of Ethereum wallets in November 2017 that cost US$150 million by making funds inaccessible.[5] Between 2017 and June 2019 (when this article was written), hackers embezzled approximately US$2 billion from financial institutions, based on what has been revealed publicly. There are many other unreported losses. Unfortunately, there are thousands of similar smart contracts on Ethereum that control wallets, tokens, and applications or hold funds.[5] The blockchain research community identified 34,200 vulnerable smart contracts to date. Among these, a set of 3,000 vulnerable contracts could be exploited by hackers to steal approximately US$6 million worth of cryptocurrency. Researchers have yet to define a security hole or vulnerability in a smart contract that can incur huge financial losses.

VULNERABLE SMART CONTRACTS

Smart contracts hosted on blockchains carry billions of dollars, approximately US$300 billion, and cannot be updated once deployed. Therefore, they become a lucrative target for cyber criminals and a potential risk for the financial institutions while having some benefits as discussed in the section "Blockchain Taxonomy." Recently, as discussed in Nikolíc et al.,[5] a blockchain research team built an analysis tool called MAIAN to identify vulnerabilities directly from the bytecode of Ethereum smart contracts, without requiring source code access. Figure 6 shows four different types of vulnerable smart contracts proposed in Nikolíc et al.[5] Here, we briefly describe them.

- *Prodigal contracts*: Under any cyberattack, smart contracts usually return funds to the owners and past addresses. However, when a contract sends Ether to any arbitrary address, then the contract is called *prodigal*.
- *Suicidal contracts*: If a contract can be killed by any arbitrary account by executing the suicide function, the contract is then called *suicidal*.
- *Greedy contracts*: The contracts that remain alive and lock Ether indefinitely (worth millions of dollars for any organization using blockchain) are termed as *greedy*. These contracts cannot be released under any condition.
- *Posthumous contracts*: Once a contract is killed, the relevant codes and global variables are cleared from the blockchain. Therefore, any further execution is prevented. Still, these killed

contracts continue to receive transactions. These killed contracts that do not have any code and have nonzero Ether are termed as *posthumous*.

Blockchain is a recent trend that has the promise of better data integrity and security for a number of application domains.[7,8] Financial institutions are the pioneers in embracing this technology as blockchain started with the concept of bitcoins to facilitate financial transactions.[9] However, the recent vulnerabilities identified in the usage of smart contracts for blockchain has led to some doubt about the wide acceptance of blockchain technology. There are many other applications where the monetary value is superseded by other issues such as privacy (for example, health care records). In particular, if smart contracts for health-care domains are exploited by cyber criminals, the impact will be disastrous. The key insight of this article is not to discourage the usage of blockchain but point toward new research directions to design and develop a robust version of blockchain.

Any organization that plans to incorporate blockchain must answer the following questions:

- How do we design and develop secure smart contracts?
- How do we identify vulnerabilities in smart contracts?
- What are the mitigation strategies for zero-day vulnerabilities (in case they are exploited)? C

ABOUT THE AUTHORS

MOHIUDDIN AHMED is a lecturer of computing and security at Edith Cowan University, Perth, Australia. He is currently engaged in the Internet of Medical Things and blockchain research projects. Ahmed received a Ph.D. in computer science (cyber security and data analytics) from the University of New South Wales, Canberra, Australia. He is a Senior Member of the IEEE, Australian Computer Society, and Australian Information Security Association. Contact him at m.ahmed.au@ieee.org.

AL-SAKIB KHAN PATHAN is currently an adjunct professor at the Computer Science and Engineering Department, Independent University, Bangladesh. His research interests include wireless sensor networks, network security, cloud computing, and e-services technologies. Pathan received a Ph.D. in computer engineering from Kyung Hee University, South Korea. He is the editor-in-chief of *International Journal of Computers and Applications*. He is a Senior Member of the IEEE. Contact him at spathan@ieee.org.

REFERENCES

1. M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tut.*, vol. 21, no. 2, pp. 1676–1717, 2018. doi: 10.1109/COMST.2018.2886932.
2. M. Ahmed, "Thwarting DoS attacks: A framework for detection based on collective anomalies and clustering," *Computer*, vol. 50, no. 9, pp. 76–82, 2017. doi: 10.1109/MC.2017.3571051.
3. M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Future Gener. Comput. Syst.*, vol. 55, pp. 278–288, Feb. 2016. doi: 10.1016/j.future.2015.01.001.
4. M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016. doi: 10.1016/j.jnca.2015.11.016.
5. I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the greedy, prodigal, and suicidal contracts at scale," in *Proc. 34th Annual Computer Security Applications Conf. (ACSAC '18)*, 2018, pp. 653–663. doi: 10.1145/3274694.3274743.
6. S. Hsiao and D. Kao, "The static analysis of WannaCry ransomware," in *Proc. 20th Int. Conf. Advanced Communication Technology (ICACT)*, Feb. 2018, p. 1. doi: 10.23919/ICACT.2018.8323679.
7. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Daz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018. doi: 10.1016/j.future.2018.05.046.
8. T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32,979–33,001, May 2018. doi: 10.1109/ACCESS.2018.2842685.
9. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, May 2016. doi: 10.1109/ACCESS.2016.2566339.
10. C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," in *Proc. 5th Int. Conf. Dependable Systems and Their Applications (DSA)*, vol. 4. Piscataway, NJ: IEEE, Sept. 2018. pp. 15–24. doi: 10.1109/DSA.2018.00015.