The Blockchain as a Decentralized Security Framework

By Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Chi Yang

The blockchain is emerging as one of the most propitious and ingenious technologies of cybersecurity. In its germinal state, the technology has successfully replaced economic transaction systems in various organizations and has the potential to revamp heterogeneous business models in different industries. Although it promises a secure distributed framework to facilitate sharing, exchanging, and the integration of information across all users and third parties, it is important for the planners and decision makers to analyze it in depth for its suitability in their industry and business applications. The blockchain should be deployed only if it is applicable and provides security with better opportunities for obtaining increased revenue and reductions in cost. This article presents an overview of this technology for the realization of security across distributed parties in an impregnable and transparent way.

THE BLOCKCHAIN DEFINED

After the Internet, the blockchain is considered to be the next big revolutionizing technology, as it is reinventing the way we work and live. In 2008, the idea of the blockchain was first introduced by a researcher who implemented the digital cryptocurrency known as *bitcoin*. Essentially, the blockchain became an integral part of bitcoin's operation [1].

Digital Object Identifier 10.1109/MCE.2017.2776459
Date of publication: 8 February 2018

> After the Internet, the blockchain is considered to be the next big revolutionizing technology, as it is reinventing the way we work and live.

Numerous cryptocurrencies with very advanced features have come into existence since then, such as Ethereum, which introduces smart contracts [2]. The fundamental characteristics of the blockchain are shown in Figure 1.

For several decades, we have been dealing with information exchange and the transfer of money and other assets through online transactions via the Internet, where each of these transactions involved a trusted intermediary. These intermediaries are responsible for guaranteeing a secure exchange and are accountable in the event of any failures or security breaches. In a paradigm shift, the blockchain eliminates the need for any central authority between multiple parties executing financial and data transactions by using an incorruptible, immutable, and decentralized public ledger. This public ledger is a distributed

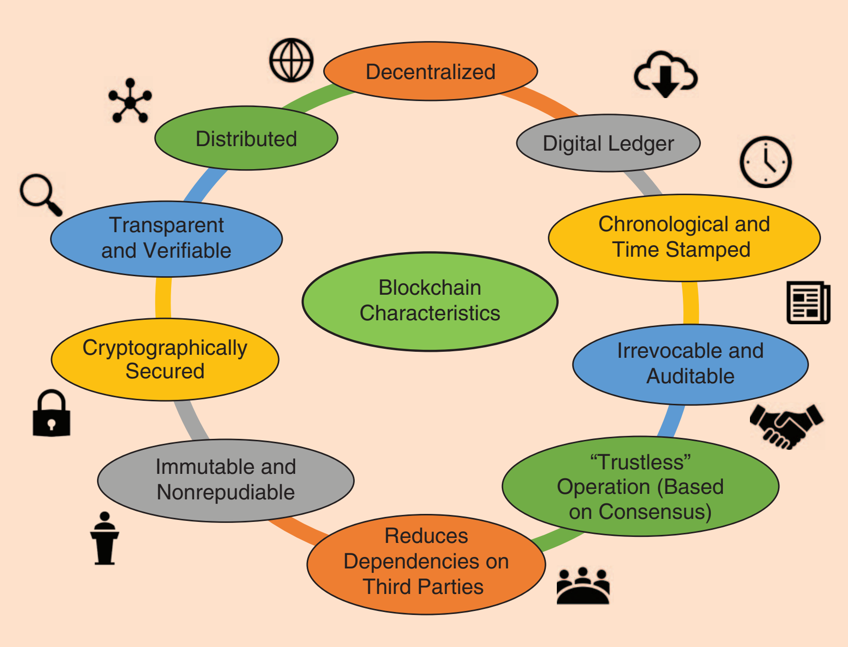
Decentralized
Digital Ledger
Chronological and Time Stamped
Irrevocable and Auditable
"Trustless" Operation (Based on Consensus)
Reduces Dependencies on Third Parties
Immutable and Nonrepudiable
Cryptographically Secured
Transparent and Verifiable
Distributed
Blockchain Characteristics

FIGURE 1. The pivotal characteristics of a blockchain.

database that is shared across all of the network participants. It is a tamper-proof, cryptographically secured, and permanent record of all of the transactions that ever took place among the participants. They can view the transactions related to them anytime they want, but once validated and added to the blockchain, the transactions can be neither deleted nor modified, which makes the blockchain immutable and irreversible. Each transaction is verified by the participants via means of predefined validation and consensus mechanisms without affirmation or authentication by any central authority. This not only reduces the cost but also eliminates the chances of information loss due to a single point of failure, because ledger copies are synchronized across all of the participants. Thus, in addition to its salient features, which include immutability, validation, decentralization, and transparency, the blockchain promises to provide privacy and security at any given time. Figure 2 demonstrates the difference between a centralized execution of transactions and a decentralized blockchain system.

The concept of the software-defined perimeter is also receiving a lot of attention by establishing a secure channel before communication [3], where it also works with a centralized controller [4], [5]. There is a large number of current research areas, such as the cloud [6], the Internet of Things (IoT) [7], edge computing [5], and big data [7], which can directly apply the blockchain to eliminate centralized controller entities. Consequently, the blockchain will benefit several emerging applications, including smart cities, banking, and the Internet of Vehicles [8], [9].

THE BLOCKCHAIN: HOW DOES IT WORK?

Consider a system of N users across a network sharing information and performing exchanges of assets. Instead of relying on an intermediary among them, they agree on a protocol called a *consensus algorithm*, which enables the establishment of mutual trust and allows for the validation of transactions on a peer-to-peer basis. Thus, the building blocks of a blockchain-based system include the network participants, a consensus protocol, such as proof of work, cryptographic hashes, and digital signatures.

> Each transaction is verified by the participants via means of predefined validation and consensus mechanisms without affirmation or authentication by any central authority.

The network participants can be individuals, organizations, or institutions sharing a copy of the ledger containing their valid transactions in a sequential order. The ledger is composed of a sequence of blocks, as shown in Figure 3, linked together by their hash values in chronological order to maintain data integrity and timeliness. Each block consists of a set of transactions digitally signed by the owner and verified by the rest of the participants before being added to the block. The features of the blockchain include the following.

- *Digital signatures*: Participants wishing to execute a transaction will broadcast it across the network. The

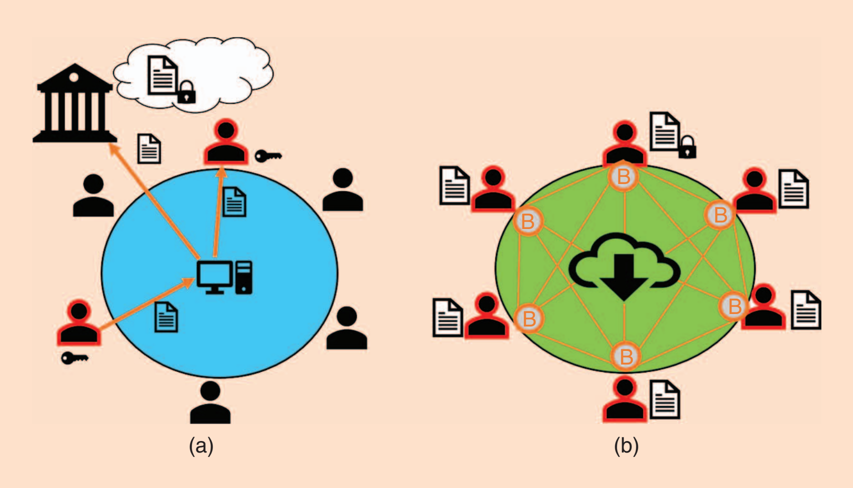

FIGURE 2. The (a) centralized system with intermediaries versus a (b) decentralized blockchain system.

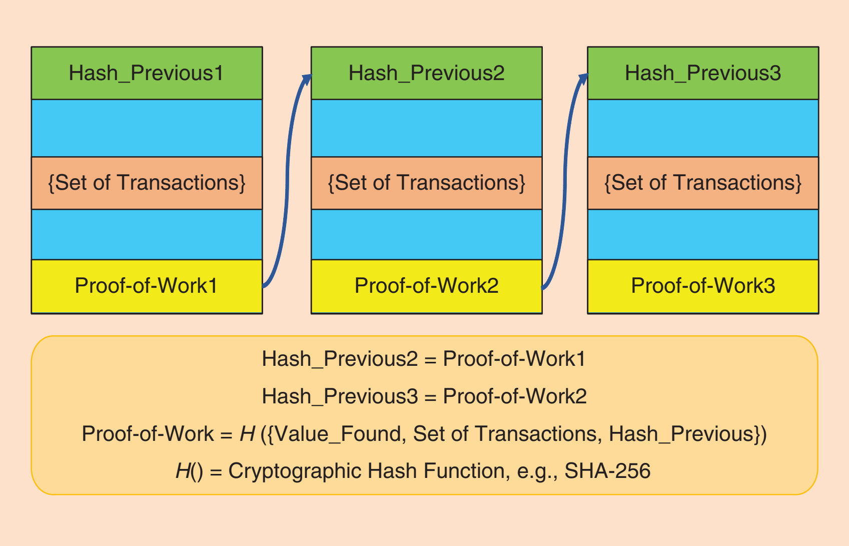
Hash_Previous1
{Set of Transactions}
Proof-of-Work1
Hash_Previous2
{Set of Transactions}
Proof-of-Work2
Hash_Previous3
{Set of Transactions}
Proof-of-Work3
Hash_Previous2 = Proof-of-Work1
Hash_Previous3 = Proof-of-Work2
Proof-of-Work = H ({Value_Found, Set of Transactions, Hash_Previous})
H() = Cryptographic Hash Function, e.g., SHA-256

FIGURE 3. The structure of the chained blocks. SHA: secure hash algorithm.

transaction owner digitally signs it by repeatedly hashing the public key for source authentication and then broadcasting the transaction for verification by other nodes.

- *Consensus*: Because the blockchain completely revolves around decentralization, there is no trusted third party responsible for secure storage and management of data or accountability in case of any security breaches. All participants collect these transactions into a new block and start working on the consensus protocol to identify the validation of the transaction. If the consensus is based on proof of work, then each participant starts finding the one that is appropriate.
- *Proof of work*: It is the value searched from a pool of values making the cryptographic hash value of the block begin with *N* number of zeros. This is to render greater security plus an opportunity to win some reward points, thus providing an incentive for a participant to perform this proof-of-work calculation.

The building blocks of a blockchain-based system include the network participants, a consensus protocol, such as proof of work, cryptographic hashes, and digital signatures.

- *Cryptographic hashes*: When a proof of work is found by a participant, the block is broadcast to all participants, who accept it by adding to their blockchain after computing a cryptographic hash, such as SHA-256 for the block, to be used as the Hash_Previous for the next block (Figure 3). The longest chain is the trusted one and added to the blockchain when participants receive multiple blocks simultaneously.

With the preceding intrinsic features acting as an integral part of the blockchain's operation, it promises data immutability, data integrity, data authentication and validation, decentralization, and data transparency, thus guaranteeing data security across distributed systems. The blockchain is immutable. The records can be altered only if more than 51% of the nodes are under the control of hackers, which is unsustainable. The technology is autonomous, and it maintains the anonymity of the sender and receiver in the transaction by using public and private keys of the nodes.

APPLICATIONS OF THE BLOCKCHAIN

The promising features of blockchain technology are enticing to multiple industries, but it is important to analyze the suitability of blockchains with regard to the needs of each industry. It is a revolution but not a panacea for all business needs. Only if the following situations arise can organizations consider deploying a blockchain-oriented security solution.

1) A group of people or multiple parties frequently generate transactions dependent upon a third party.

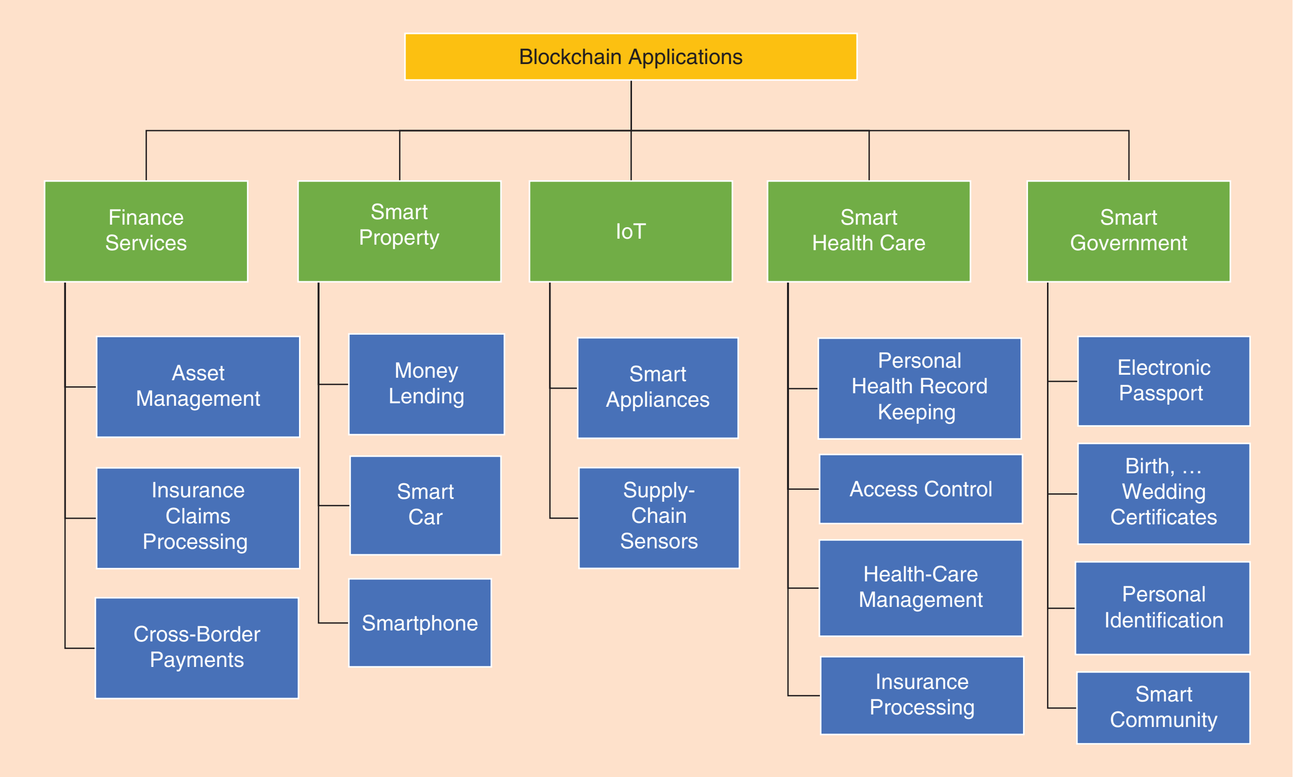

FIGURE 4. The potential applications of a blockchain.

2) The third party cannot be trusted, and the authenticity of transactions is questionable.
3) The validation of transactions is a priority, and, thus, an enhanced system rendering data authenticity and integrity is important.
4) Data integrity over confidentiality and processing performance is important. However, for time-sensitive applications, the blockchain is not appropriate, as the transfer duration is lengthy for a block that needs to be accepted into the chain. In the case of bitcoin, this process lasts approximately 10 min.

Data in the distributed public ledger is immune to any tampering, as it is highly encrypted using advanced cryptography. The technology therefore finds applications in cybersecurity. It eliminates the usage of centralized devices in the IoT and other forms of networking, so connected devices can update software, manage bugs, and communicate directly. The technology provides a new way of managing trust and can be effectively applied in insurance and domains like finance, as presented in Figure 4 [10]. It eliminates the involvement of a third party; hence, it is finding effective utilization in private transport and ride sharing. It is envisioned that the blockchain can have significant applications in smart health care with the Internet of Medical Things or the Internet of Health Things to provide security, privacy, and effective insurance processing [11].

CONCLUSION

The blockchain is an effective solution for the centuries-old consensus problem. Using cryptography (hashes and digital signatures) and a system that rewards participants, the winner of a cryptographic lottery reaps the rewards while ensuring the validity of the entire ledger. At the same time, the blockchain is not a universal solution to any problem having to do with transaction verification and security. Its implementation must be adopted only after careful examination of the requirements of the application. The impact of the blockchain in modern society is disruptive, and the consequences of its widespread adoption are still unknown.

> Data in the distributed public ledger is immune to any tampering, as it is highly encrypted using advanced cryptography.

ABOUT THE AUTHORS

Deepak Puthal (deepak.puthal@uts.edu.au) earned his Ph.D. degree in computer science and information systems from the University of Technology Sydney (UTS). He is a lecturer (assistant professor) in the Faculty of Engineering and Information Technology at UTS. He received the IEEE Distinguished Doctoral Dissertation Award for Excellence in Special Technical Community on Smart Computing for the year 2017. He is an associate editor of *IEEE Consumer Electronics Magazine*.

Nisha Malik (nisha.malik@student.uts.edu.au) is a Ph.D. student in the Faculty of Engineering and information technology at the University of Technology Sydney, Australia. Her research interests include vehicular networks, information security, and cloud computing.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a professor at the University of North Texas, Denton. He has authored 250 research articles and three books and holds four U.S. patents. His Google Scholar h-index is 28 and i10-index is 83. He is the editor-in-chief of *IEEE Consumer Electronics Magazine* and serves as the chair of the IEEE Computer Society Technical Committee on Very Large Scale Integration.

Elias Kougianos (eliask@unt.edu) earned his Ph.D. degree in electrical engineering from Louisiana State University, Baton Rouge, in 1997. He is a professor in engineering technology at the University of North Texas, Denton. He is the author or coauthor of more than 120 peer-reviewed journal and conference publications.

Chi Yang (chiyangit@gmail.com) earned his Ph.D. degree in computer science at the University of Technology Sydney, Australia. He is a research fellow at the Unitec Institution of Technology, Auckland, New Zealand. His research interests include wireless sensor networks, the Internet of Things, big data processing, cloud computing, parallel and distributed computing, privacy and security, and extensible markup language data streams.

REFERENCES

[1] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] P. Bailis, A. Narayanan, A. Miller, and S. Han, "Research for practice: Cryptocurrencies, blockchains, and smart contracts; hardware for deep learning," *Commun. ACM*, vol. 60, no. 5, pp. 48–51, 2017.

[3] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyber threats," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 24–27, 2017.

[4] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, 2016.

[5] D. Puthal, X. Wu, S. Nepal, R. Ranjan, and J. Chen, "SEEN: A selective encryption method to ensure confidentiality for big sensing data streams," *IEEE Trans. Big Data*, vol. PP, no. 99, pp. 1, 2017.

[6] C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, "Big-sensing-data curation for the cloud is coming," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 48–56, 2017.

[7] D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and big data: An architecture with data flow and security issues," in *Proc. Cloud Infrastructures, Services, and IoT Systems for Smart Cities*, 2017, pp. 243–252.

[8] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, 2016.

[9] D. Puthal, Z. H. Mir, F. Filali, and H. Menouar, "Cross-layer architecture for congestion control in vehicular ad-hoc networks," in *Proc. Int. Conf. Connected Vehicles and Expo*, 2013, pp. 887–892.

[10] BlockGeeks. (2017). 17 blockchain applications that are transforming society. [Online]. Available: https://blockgeeks.com/guides/blockchain-applications/

[11] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything you wanted to know about smart healthcare," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 18–28, 2018.