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 itself, 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 integration of information across all the users and third parties, it is important for the planners and decision-makers to analyse 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 in obtaining increased revenue and reductions in cost. This article presents an overview of this technology for 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 blockchain was first introduced by a researcher who implemented the digital cryptocurrency known as bitcoin, where the blockchain is an integral part of its working [1]. Numerous cryptocurrencies with much advanced features have come into existence since then, such as the Ethereum which introduces smart contracts [2]. The fundamental characteristics of the blockchain are illustrated in Figure 1.

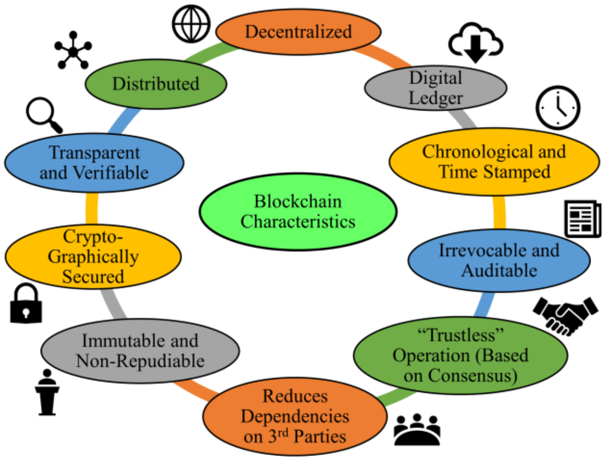
Decentralized
Digital Ledger
Chronological and Time Stamped
Irrevocable and Auditable
"Trustless" Operation (Based on Consensus)
Reduces Dependencies on 3rd Parties
Immutable and Non-Repudiable
Crypto-Graphically Secured
Transparent and Verifiable
Distributed
Blockchain Characteristics

FIGURE 1. Pivotal characteristics of blockchain.

For several decades, we have been dealing with information exchange, and transferral of money and other assets through online transactions via the Internet, where each of these transactions involved a trusted intermediary. These intermediaries are responsible to guarantee a secure exchange and are accountable in case of any failures or security breaches. In a paradigm shift, the blockchain eliminates the need of 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 database that is shared across all the network participants. It is a tamper-proof, cryptographically secured, and permanent record of all 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 neither be deleted nor modified, which makes the blockchain immutable and irreversible. Each transaction is verified by the participants by means of pre-defined 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, since ledger copies are synchronized across all 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 all points in time. Figure 2 demonstrates the difference between centralized execution of transactions and the decentralized blockchain system.

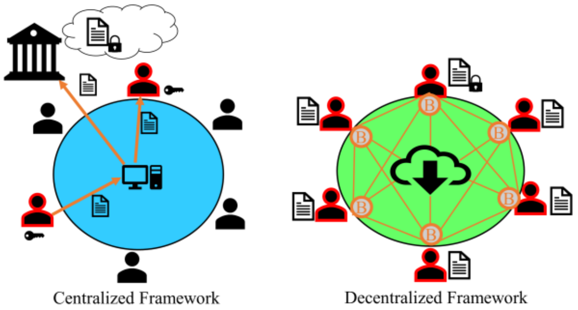

FIGURE 2**.** Centralized systems with intermediaries versus decentralized blockchain systems.

The concept of 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 controler [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 Bigdata [7], which can directly apply the blockchain to eliminate centralized controller entities. Consequently, the blockchain will benifit several emerging applications including smart cities, banking, and the Internet of Vehicles (IoV) [8, 9].

THE BLOCKCHAIN - HOW DOES IT WORK?

Consider a system of '*N*' users across a network sharing information and performing exchange of assets. Instead of relying on an intermediary among them, they agree on a protocol called a *consensus algorithm*, which enables them to establish mutual trust and allows for validating the 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*.

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. Some features of the blockchain are now discussed.

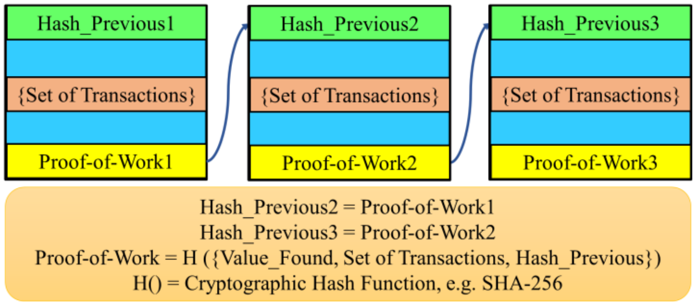
Hash_Previous1
Hash_Previous2
Hash_Previous3
{Set of Transactions}
{Set of Transactions}
{Set of Transactions}
Proof-of-Work1
Proof-of-Work2
Proof-of-Work3
Hash_Previous2 = Proof-of-Work1
Hash_Previous3 = Proof-of-Work2
Proof-of-Work = H ({Value_Found, Set of Transactions, Hash_Previous})
H() = Cryptographic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

FIGURE 3**.** Structure of the chained blocks.

Digital Signatures: Participants wishing to execute a transaction, broadcast it across the network. This transaction is digitally signed by the owner by repeated hashing of the public key for source authentication and then broadcast for verification by other nodes.

Consensus: Since the blockchain revolves completely 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, each participant starts finding the appropriate proof-of-work.

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.

Cryptographic Hashes: When a proof-of-work is found by a participant, the block is broadcast to all participants, which 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 above intrinsic features as an integral part of the blockchain's working, it promises *data immutability*, *data integrity*, *data authentication and validation*, *decentralization and data transparency*, thus guarantying 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 utilizing public and private keys of the nodes.

APPLICATIONS OF THE BLOCKCHAIN

The promising features of blockchain are disrupting multiple industries attracted towards this technology, but it is important to analyse their suitability to the needs of each industry. It is a revolution but not a panacea for all the business needs. If only 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 on a third party.

(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. For time-sensitive applications, the blockchain is not appropriate as it takes time for a block to be accepted in the chain. In the case of bitcoin, this time is approximately 10 minutes.

Data in the distributed public ledger is immune to any tampering as it is highly encrypted using advanced cryptography, hence the technology finds applications in cyber security. It eliminates the usage of centralized devices in the IoT and other forms of networking. Therefore, devices connected could update software, manage bugs and communicated 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 healthcare with the Internet of Medical Things (IoMT) or the Internet of Health Things (IoHT) to provide security, privacy, and effective insurance processing [11].

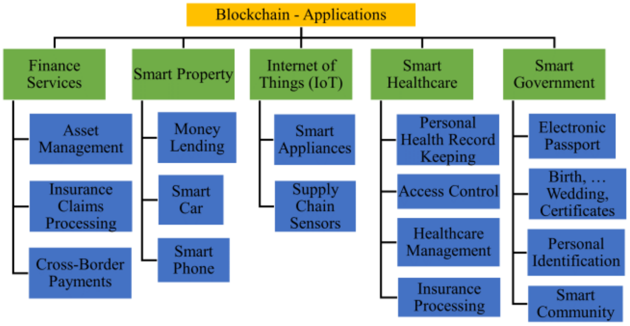

FIGURE 4**.** Potential applications of the blockchain.

CONCLUSIONS

The blockchain is an effective solution of 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, at the same time, ensures 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.

ABOUT THE AUTHORS

Deepak Puthal (deepak.puthal@uts.edu.au) is a Lecturer (Assistant Professor) in the Faculty of Engineering and IT at University of Technology Sydney (UTS), Australia. His research interests include cyber security, Internet of Things, distributed computing, and Big Data Analytics. He has a Ph.D. degree in Computer Science and Information Systems from UTS, Australia. He received IEEE Distinguished Doctoral Dissertation Award for Excellence in STC on Smart Computing for the year 2017. He is an author of 30 peer reviewed research articles. He is serving as 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 IT at University of Technology Sydney, Australia. Her research interest includes Vehicular networks, Information security and cloud computing.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the University of North Texas. Prof. Mohanty's research is in Smart Electronic Systems which has been funded by National Science Foundations, Semiconductor Corporation, and US Air Force. He authored 220 research articles, 3 books, and invented 4 US patents. His Google Scholar h-index is 28 and i10-index is 82. He is the EiC of the IEEE Consumer Electronics Magazine. He serves as the Chair of Technical Committee on VLSI, IEEE Computer Society. More about him is available at: http://www.smohanty.org.

Elias Kougianos (eliask@unt.edu) is Professor in Engineering Technology at the University of North Texas. He obtained his Ph.D. in electrical engineering from Louisiana State University in 1997. He is author or co-author of over 120 peer-reviewed journal and conference publications. He is a senior member of IEEE.

Chi Yang (chiyangit@gmail.com) received his Ph.D. in computer science at the University of Technology, Sydney (UTS), Australia. He is a research Fellow in the Unitec Institution of Technology, Auckland, New Zealand. His major research interests include WSN, IoT, Big Data Processing, Could Computing, parallel & distributed computing, privacy & security and XML data streams.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system.", https://bitcoin.org/bitcoin.pdf, Last visited 11 Nov 2017.

[2] P. Bailis, A. Narayanan, A. Miller, and S. Han, "Research for practice: cryptocurrencies, blockchains, and smart contracts; hardware for deep learning", *Communications of the ACM*, Vol. 60, No. 5, 2017, pp. 48-51.

[3] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building Security Perimeters to Protect Network Systems Against Cyber Threats", *IEEE Consumer Electronics Magazine*, Vol. 6, No. 4, 2017, pp. 24-27.

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

[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 Transactions on Big Data*, 2017, In Press.

[6] C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, “Big-Sensing-Data Curation for the Cloud is Coming”, *IEEE Consumer Electronics Magazine*, Vol. 6, No. 4, 2017, pp. 48-56.

[7] D. Puthal, R. Ranjan, S. Nepal, and J. Chen, “IoT and Big Data: An Architecture with Data Flow and Security Issues”, in *Proc. of the 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 Consumer Electronics Magazine*, Vol. 5, No. 3, 2016. pp. 60-70.

[9] D. Puthal, Z. H. Mir, F. Filali, and H. Menouar, “Cross-layer architecture for congestion control in Vehicular Ad-hoc Networks”, in *Proc. of the International Conference on Connected Vehicles and Expo*, 2013, pp. 887-892.

[10] Elio-David Di Iorio, 17 Blockchain Applications That Are Transforming Society, https://blockgeeks.com/guides/blockchain-applications/, Last visited 3rd November, 2017.

[11] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Healthcare”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 8, Issue 1, January 2018, pp. xx-yy.