Column: Energy and Security

When Do We Need the Blockchain?

Deepak Puthal
Newcastle University

Saraju P. Mohanty
University of North Texas

Elias Kougianos
University of North Texas

Gautam Das
University of Texas at Arlington

The questions "When do we use the blockchain?" or "Where do we use the blockchain?" or "Why do we use the blockchain?" look simple, but these questions become complicated due to the increasing utilization of the blockchain. These days, it is being explored as a standard security solution. The blockchain has unique properties, and these are entirely different from other standard security or cryptography solutions. This article gives a summary of the uses of the blockchain, while answering the above three important questions.

The blockchain is being actively explored to ensure data and transaction security. Since it stores the transaction data permanently in a chain (i.e., a distributed ledger) and does not permit anyone to edit either the data or the chain after block acceptance, it provides tamperproof storage of historical data [1, 2]. Modifying the data after storing it in the chain of blocks is not permitted in the conventional, immutable blockchain. Each block stores the hash value of the previous block, so any modification to a block corrupts all of the following blocks in the chain [2]. Several applications required real-time auditing. In the social media use case, where users regularly update their data, the blockchain may not be appropriate for secure data storage. Any application that demands real-time auditing, or frequent modification of stored data should not use the blockchain for data storage. In the latest technologies, such as the Internet of Things (IoT), edge computing, and cloud computing deployed for several applications (e.g. Smart Healthcare, Smart City), there are always demands of both user and data privacy [2]. Also, social media applications need a certain level of user and data privacy. *Are these applications suitable to use the blockchain for data storage?* No, because of the blockchain technology's data transparency property. Any user in the network can visualize the data but cannot modify it, thus providing data integrity, but not data accessibility.

Establishing trust is an essential factor in any computing infrastructure. Trusted devices or users play the role of a central entity to verify all the transactions and system security. In contrast, one of the primary key features of the blockchain is to disregard the central trusted body and make the system decentralized. As a result, a scalable system with the presence of trusted peers in the network to is not easily adopted to the blockchain [3]. Similarly, the blockchain is developed for distributed networks where multiple peers in the network generate data packets or transactions. The blockchain is not a viable solution for a system

where only one or two devices create the data packets. A summary of deciding when we need a blockchain is shown in Figure 1 [1].

CHALLENGES OF BLOKCHAIN

Ther are always advantages and disadvantages to all new technologies developed for computer communications and computing technology, and they are very application-specific. Similarly, the blockchain has four key challenges specific to the application, namely scalability, throughput, latency, and size and bandwidth [2]. System applications requiring any of these properties should not use the blockhain directly. However, the blockchain could be programmed and improved to meet the specifications of the application. Along with these technical challenges, there are many research questions associated with the use of blockchain.

Is the blockchain for data or device?

The blockchain was initially developed for decentralized data security and storage. However, due to its broad adoption in several application domains and combination with other technologies, secure and trustworthy device deployment is vital in the blockchain [4].

Does the blockchain guarantee privacy?

The traditional blockchain was developed for the bitcoin and did not maintain data privacy. However, designing the blockchain for applications such as the IoT and edge computing should preserve user data privacy. One of the fundamental solutions is on-chain and off-chain data storage [5]. Instead of storing data in the chain, data could be stored in secure storage (in cloud, i.e., off-chain), and stored data references maintained in the distributed ledger (i.e., on-chain).

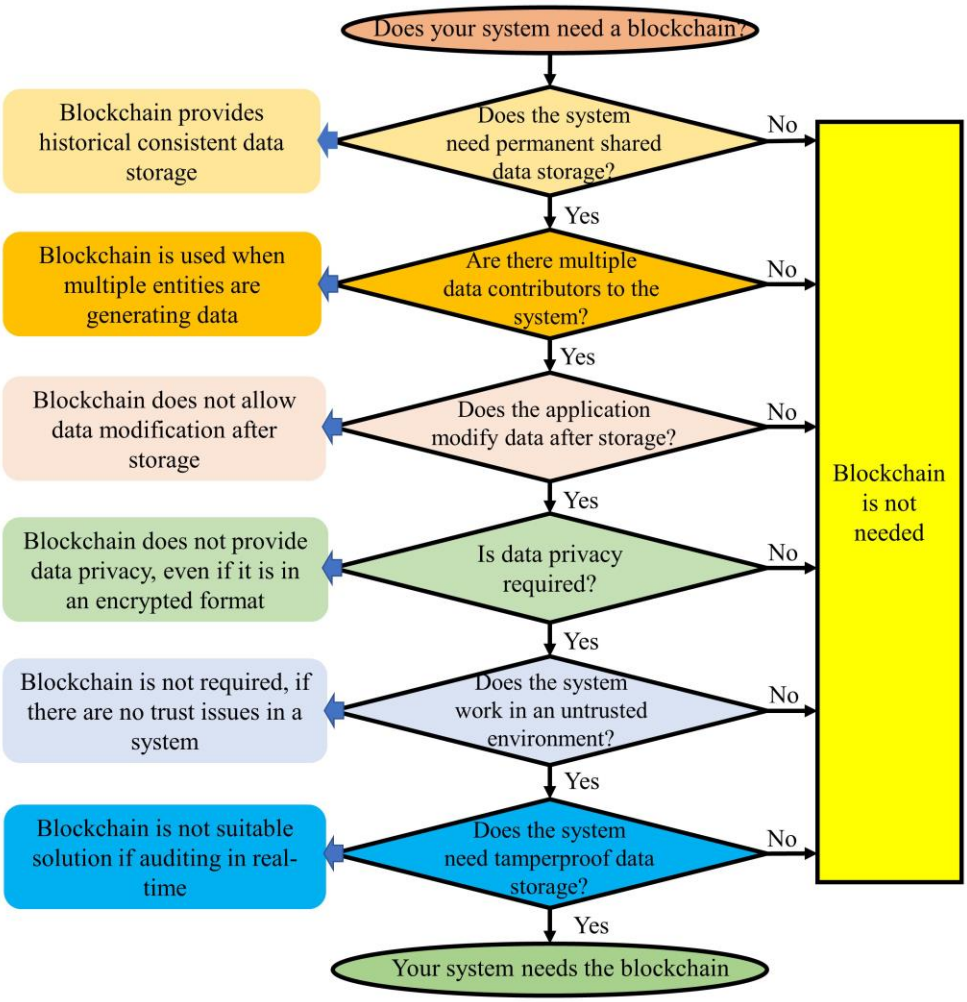

Figure 1: Steps to evaluate the use of blockchain [1].

Is the blockchain suitable for the IoT?

Conventional blockchain consensus requires a massive amount of computational resources, energy, and time for the mining, which is impossible for any kind of IoT application, because of resource constrained devices used for IoT system deployment [4, 6]. The blockchain could be used for IoT applications, but it needs

to be redeveloped based on IoT application requirements.

Blockchain: Is it prone to quantum computer atatcks?

There is no perfect answer to this question because there is no quantum computer available to do the testing [7]. However, data cannot be altered or tampered after stored in the chain, even by a quantum computer. Blocks in the chain are interconnected with the previous block's hash value, so any modification in the block content will corrupt the whole chain.

BLOCKCHAIN SECURITY THREATS

There are three crucial stages in the blockchain process, namely mining, networking, and smart contract, where there are very high possibilities of potential cyber threats to compromise the overall system (see Figure 2).

Threats in Mining:

A distributed consensus mechanism is an underlying property of the blockchain to maintain mutual trust.

Selfish Mining: In "Selfish Mining", a dishonest miner acts like a trusted miner but does not publish the mining outcome to the network [8]. A selfish miner attempts to confuse the other trusted miners to spend their resources for no rewards.

Block-withholding attack: The Block-withholding attack is possible when a dishonest miner discards the blocks and never published them until the right time to release them [9].

>50% attack: The blockchain is designed with a strong assumption, i.e., honest nodes control the network. When an intruder controls more than 50% of network users, then this type of attack is possible.

Threats in Networks:

The blockchain is designed for purely decentralized and peer-to-peer networks, where individual peers run blockchain algorithm(s) for data communications.

Distributed Denial of Service attacks (DDoS): It is difficult for an attacker to launch DDoS attack in a blockchain network compared to conventional client-server systems. Still, the attacker has possibilities of launching a DDoS attack in both the network and application layers. The DDoS attack at the network layer consumes all the network bandwidth to block the actual blocks, whereas at the application layer the attack disables the server by consuming all its resources.

Sybil attack: This refers to one attacker with multiple identities. In peer-to-peer blockchain networks, the attacker creates multiple identities to participate in the mining process. Then, ultimately it leads to the ">50% attack" in the mining process.

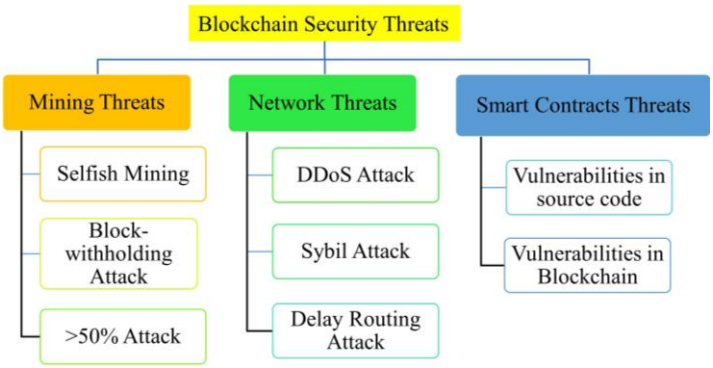

Figure 2: Security threats of blockchain.

Delay Attack: In this attack, the attacker interrupts the transmission of blocks, within the peers of the network. The attacker attacks the routing path to capture blocks and halt them for some time (20-30 minutes) and transmit them to the miner after a delay. As a result, miners waste their resources without getting the current block information.

Smart Contract threats:

A smart contract is a script, which is executed automatically when satisfying certain conditions. 'Ethereum' is a blockchain platform specifically designed for smart contract implementation [10].

Vulnerabilities in Sourcecode: Vulnerabilities in the sourcecode is a major flaw in any software-based solution and so with the smart contract.

Vulnerabilities in Blockchain: The user sends transactions to invoke the preprogrammed smart

contract, but it is not always ensured that the smart contract runs in the same state when other transactions may be calling the same smart contract. This bug is known as Transaction-Ordering Dependence, and this affects up to 15.8% of all smart contracts [11].

CONCLUSION

The blockchain has been developed for a purpose, i.e., decentralizing security and data storage, and it has unique properties. If it is adopted to use for an application but the application does not support the features of the blockchain, then we need to analyze carefully whether we need it. If yes, then the blockchain needs to be reprogrammed according to the application specifications before its use.

REFERENCES

1. D. Yaga, P. Mell, N. Roby and K. Scarfone, “Blockchain Technology Overview”, *NISTIR 8202*, Oct. 2018. Available at: https://doi.org/10.6028/NIST.IR.8202
2. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain" *IEEE Consum. Electron. Mag.*, Vol. 7, no. 4, pp. 6-14, 2018.
3. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework" *IEEE Consum. Electron. Mag.*, Vol. 7, no. 2, pp. 18-21, 2018.
4. S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)" *Consum. Electron. Mag.*, Vol. 9, no. 2, pp. 8-16, 2020.
5. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTchain: Establishing trust in the internet of things ecosystem using blockchain", *IEEE Cloud Computing*, Vol. 5, no. 4, pp. 12-23, 2018.
6. D. Puthal, and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains", *IEEE Potentials*, Vol. 38, no. 1, pp. 26-29, 2018.
7. A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, "A Computing Perspective of Quantum Cryptography", *IEEE Consum. Electron. Mag.*, Vol. 7, no. 6, pp. 57-59, 2018.
8. I. Eyal, and E. G. Sirer. "Majority is not enough: Bitcoin mining is vulnerable", in *Proc. Int. Conf. Finance Crypto. and data security*, pp. 436-454, 2014.
9. S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation", *IEEE Trans. Information Forensics and Securi*ty, Vol. 12, no. 8, pp. 1967-1978, 2016.
10. V. Buterin, "A next-generation smart contract and decentralized application platform", 2014, https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf, Accessed on 02 Aug 2020.
11. J. H. Mosakheil, "Security threats classification in blockchains", *MS Thesis, St. Cloud State University*, 2018.

ABOUT THE AUTHORS

Deepak Puthal is an Assistant Professor in the School of Computing at Newcastle University, Newcastle upon Tyne, UK. Contact him at: deepak.puthal@newcastle.ac.uk.

Saraju P. Mohanty is a Professor in the Department of Computer Science and Engineering at the University of North Texas, USA. Contact him at: saraju.mohanty@unt.edu.

Elias Kougianos is a Professor in the Department of Electrical Engineering at the University of North Texas, USA. Contact him at: elias.kougianos@unt.edu.

Gautam Das is a Professor in the Department of Computer Science and Engineering at the University of Texas at Arlington, USA. Contact him at: gdas@uta.edu.