


Security Protection Mechanisms Must Be Embedded in Blockchain Applications

Yoshiyasu Takefuji*

 Cite This: <https://dx.doi.org/10.1021/acs.jchemed.0c00040>

 Read Online

ACCESS |

 Metrics & More

 Article Recommendations

ABSTRACT: There are unknown and known attacks against the consensus algorithms used in blockchain. Detection and protection mechanisms must be embedded in blockchain applications for protecting vulnerabilities of known consensus algorithms.

KEYWORDS: *Problem Solving/Decision Making, Continuing Education*

Harry E. Pence's commentary, "Blockchain: Will Better Data Security Change Chemical Education?",¹ introduces the blockchain technology to chemical researchers and students. A blockchain is composed of a growing list of records, which are called blocks, and they are linked or chained using cryptography. Every block includes an encrypted hash of the previous block with a timestamp and transaction data. Blockchain is supposed to be robust against modification of the data. It is called an open distributed ledger. In order to record or modify a block, consensus of the network majority is needed. Once recorded, the data in any block cannot be altered without the decentralized consensus.

However, blockchain developers and users must understand the vulnerabilities of consensus algorithms in blockchain. Blockchain uses one of the decentralized consensus algorithms including POW (proof of work), POS (proof of stake), DPOS (delegated proof of stake), RPCA (ripple protocol consensus algorithm), and SCP (stellar consensus protocol). In order to avoid the vulnerabilities of the decentralized consensus algorithms, the conventional centralized consensus algorithms using public key infrastructure like X.509 protocol authentication can be used. However, X.509 protocol authentication is very popular in public, so many vulnerabilities have been reported. In order to safely use the centralized blockchain applications, security protection mechanisms must also be embedded in X.509 applications.

As far as we know, the decentralized consensus algorithms are all vulnerable against known attacks including a 51% attack, long range attack, DDoS attack, P+Epsilon attack, Sybil attack, balance attack, and BGP hijacking, respectively.^{2,3} A 51% attack refers to an attack on a blockchain (most commonly bitcoins, for which such an attack is still hypothetical) by a group of miners controlling more than 50% of the network's mining hash rate or computing power.⁴ In other words, the attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users.⁴ They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.⁴ If you can control consensus of

the network majority, you can control the entire blockchain transaction.

A long range attack is a scenario where an adversary creates a branch on the blockchain starting from the genesis block and overtakes the main chain. This branch may contain different transactions and blocks and is also referred to as an alternative history or history revision attack.⁵

A P+Epsilon attack is explained by Vitalik Buterin.⁶ Hunter Gebron wrote an article entitled "Do P+Epsilon Attacks Pose a Threat to Token-Curated Registries?".⁷

According to Wikipedia,⁸ in a Sybil attack, the attacker subverts the reputation system of a network service by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence. It is named after the subject of the book *Sybil*, a case study of a woman diagnosed with dissociative identity disorder.

A balance attack against proof-of-work blockchain systems is caused by delaying network communications between multiple subgroups of nodes with balanced mining power.⁹

According to Wikipedia, BGP hijacking is the illegitimate takeover of groups of IP addresses by corrupting internet routing tables maintained using the Border Gateway Protocol (BGP).¹⁰

CONCLUSION

Students and researchers must understand that protection mechanisms must be embedded in decentralized and centralized blockchain applications.

Received: January 15, 2020

Revised: February 18, 2020

AUTHOR INFORMATION

Corresponding Author

Yoshiyasu Takefuji – Keio University, Fujisawa 252-8520, Japan; orcid.org/0000-0002-1826-742X; Email: takefuji@keio.jp

Complete contact information is available at:

<https://pubs.acs.org/10.1021/acs.jchemed.0c00040>

Notes

The author declares no competing financial interest.

REFERENCES

- (1) Pence, H. E. Blockchain: Will Better Data Security Change Chemical Education? *J. Chem. Educ.* **2019**, DOI: [10.1021/acs.jchemed.9b00560](https://doi.org/10.1021/acs.jchemed.9b00560).
- (2) Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Appl. Sci.* **2019**, *9*, 1788.
- (3) Yang, F.; Zhou, W.; Wu, Q.; Long, R.; Xiong, N. N.; Zhou, M. Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. *IEEE Access* **2019**, *7*, 118541–118555.
- (4) Frankenfield, J. 51% Attack, May 6, 2019. <https://www.investopedia.com/terms/1/51-attack.asp> (accessed March 16, 2020).
- (5) Deirmentzoglou, E. Rewriting History: A Brief Introduction to Long Range Attacks, May 31, 2018. <https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9> (accessed March 16, 2020).
- (6) Buterin, V. The P + epsilon Attack, January 28, 2015. <https://blog.ethereum.org/2015/01/28/p-epsilon-attack/> (accessed March 16, 2020).
- (7) Gebron, H. Do P+epsilon Attacks Pose a Threat to Token-Curated Registries?, Jul 4, 2018. <https://medium.com/@huntergebron/do-p-epsilon-attacks-pose-a-threat-to-token-curated-registries-49b06511bfbf> (accessed March 16, 2020).
- (8) Sybil Attack. https://en.wikipedia.org/wiki/Sybil_attack (accessed March 16, 2020).
- (9) Natoli, C.; Gramoli, V. The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example. <https://arxiv.org/abs/1612.09426v1>.
- (10) BGP Hijacking. https://en.wikipedia.org/wiki/BGP_hijacking (accessed March 16, 2020).