MedCrave
Step into the World of Research

MOJ Applied Bionics and Biomechanics

Min Review

Open Access

Blockchain is vulnerable against classic database approach

Abstract

Blockchain has been used in many applications: financial services including virtual currency like Bitcoin, asset management, insurance services, government, and health care. We believe that a blockchain is resistant to modification of the data where each block uses a cryptographic hash. SHA256 is a hashing function used in the blockchain. We also believe that SHA256 cannot be reversed because it's a one-way function. However, as long as two keywords used in the blockchain-based system, it is reversible by using classic database approach from a hash string to two keywords without cracking SHA256 algorithm. This paper demonstrates how to reverse a hash string to keyword(s). The proposed database approach simply defeats its design goal of the blockchain without cracking the algorithm as long as the database can be created. This paper recommends that three or more keywords of the hash function SHA256 should be used for user account access in the blockchain-based systems.

Keywords: blockchain, SHA256, database approach, reversible

Volume 3 Issue 5 - 2019

Yoshiyasu Takefuji,[1] Harold Szu[2]
[1]Keio University, Japan
[2]The Catholic University of America, USA

Correspondence: Yoshiyasu Takefuji, Professor of Keio University, Japan, Email takefuji@z6.keio.jp

Received: September 05, 2019 | **Published:** September 09, 2019

Introduction

Blockchain has been used in many applications: financial services including virtual currency like Bitcoin, asset management, insurance services, government, and health care. At least more than $1.3 billion has been globally invested to blockchain-based systems in 2018.[1] Blockchain has an interesting history such that we don't know who actually invented blockchain. According to Wikipedia, blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The original paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" was archieved.[2] Bitcoin is based on peer-to-peer encrypted open ledger.

Bettina Warburg is the first strategist to introduce Blockchain and its applications to broad audiences in public. Her transcript of TED talk entitled "How the Blockchain will Radically Transform the Economy" is detailed.[3] She stated that the first person to really explore the idea of "Blockhchain" as a tool in economics to lower our uncertainties about one another and be able to do trade is the Nobel economist Douglass North. Harold Szu et al.,[4] proposed the national strategy of digital cryptographic currency-digital bitcoin decentralized over the internet.[4] As long as the main trustworthiness is overcome, "Blockchain and Cryptocurrency" might work this decade.[4]

We believe that a blockchain is resistant to modification of the data where each block uses a cryptographic hash. SHA256 is a hashing function used in the blockchain. We believe that SHA256 cannot be reversed because it's a one-way function. US military states that SHA256 is appropriate for protecting classified information.[5] Researchers are building blockchain-based systems to encourage patients to securely share information.[6] Many scientists and engineers are excited in building blockchain-based systems for healthcare and financial services.[7–9]

This paper demonstrates that a blockchain is vulnerable against the database approach. Blockchain uses a hash function, SHA256, for storing user access information as hash string instead of plain text keywords. As long as two keywords used in the blockchain-based system, it is reversible from a hash string to two keywords without cracking SHA256 algorithm. As long as the user access to the blockchain-based system is vulnerable, the robustness of blockchain will be lost. This paper shows the database approach for reversing the hash string to keyword(s). The limitation of the database approach is also addressed in this paper.

Why blockchain is vulnerable?

George Iosifidis et al.,[10] wrote an article entitled "Cyclic motifs in the Sardex monetary network".[10] Many blockchain-based systems including Sardex use two keywords (username and password) used for user account access in the blockchain-based systems. Two keywords are converted to a single hash string by the hash function SHA256. If the hash string can be reversed, the blockchain-based system will be vulnerable. The blockchain vulnerability was demonstrated at Cibok forum (Cybercrime Investigation Body of Knowledge) on July 5, 2018 at Tokyo.[11] As long as a blockchain uses two keywords in hash function SHA256, without cracking the SHA256 algorithm, it is reversible.[12] This short paper gives a strong warning to the developers and users of the all blockchain-based systems.

How to generate a hash string from keyword(S)

Consider a single keyword 'ieee'. Instead of storing a plain text keyword used for user account access, the hash string is stored in the blockchain-based system. The hash string of 'ieee' can be generated by the following simple three-line Python program sha256.py:

```
import hashlib
ho=hashlib.sha256(b'ieee')
print(ho.hexdigest())
```

The generated hash string is as follows:

dda47a668088d1e 402d0a8ce2b489 870631ea5a1 d0746c4729 1c3b0a5 b672ede

Remember that the hash string converted from keyword(s) is stored in the blockchain-based systems.

How to reverse hash string to keyword(S)

Copy the generated hash string and paste it to the following site:

http://md5decrypt.net/en/Sha256/#answer

Then, click the Decrypt button on your browser. Within 0.041s, the keyword 'ieee' will be displayed on the browser. This demonstration shows that reversing the hash string to a keyword 'ieee' is successful. Without cracking SHA256, the hash string can be converted to a keyword using the database approach while k database must be prepared for reversing where k is the number of possible keywords. If you have two keywords for demonstrating the reversibility, we must use the k x k database where k is the number of possible keywords for reversing a hash string to two keywords. Even if k is million keywords with two keywords in a blockchain, building a tera (10^12) database is still feasible for reversing in the blockchain-based system. Therefore, we must use at least three keywords or more for securing the blockchain-based system. However, the current blockchain systems usually use two keywords (username and password) which should be avoided.

Conclusion

This paper recommends that three or more keywords of the hash function SHA256 should be used for user account access in the blockchain-based systems. The database approach simply defeats its design goal of the blockchain-based system without cracking the SHA256 algorithm as long as the database can be created.

Acknowledgments

None.

Conflicts of interest

The authors declare there is no conflict of interest.

Funding details

None.

References

1. Jason Rowley. With at least $1.3 billion invested globally in 2018, VC funding for blockchain blows past 2017 totals. 2018.
2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.
3. Pangambam S. Bettina Warburg: How the Blockchain will Radically Transform the Economy. 2018.
4. Harold S, Irene Hsu, Benachenhou D, et al. National strategy of digital cryptographic currency-digital bitcoin decentralized through the internet. *MOJ App Bio Biomech*. 2018;2(6):324–332.
5. https://www.acq.osd.mil/dsb/reports/2000s/ADA498577.pdf
6. AI diagnostics need attention. Nature. 2018;555:285–286.
7. William Gordon, Adam Wright, Adam Landman. Blockchain in Health Care: Decoding the Hype. 2017.
8. Anne Q Hoy. Emerging scientific technologies help defend human rights. *Science*. 2018;361(6405):859–860.
9. Jennifer Abbasi. Personal Genomics and Cryptocurrency Team Up. *JAMA*. 2018;319(14):1427.
10. George Iosifidis, Yanick Charette, Edoardo M Airoldi, et al. Cyclic motifs in the Sardex monetary network. *Nature Human Behaviour*. 2018;2:822–829.
11. https://www.cibok.org/ja/261/
12. Takefuji Y. A blockchain is fragile against the database approach. *Science*. 2018;361(6405):859–860.