Improving Password System using Blockchain

Dr.S.Brindha[1], Mr.S.Vishnudarshan[2], Mr.S.Arsaad[3], Mr. A.Dinesh[4]

[1]Head of Department, Department of Computer Networking, PSG Polytechnic College, Coimbatore, India
[2,3,4]Student, Department of Computer Networking, PSG Polytechnic college, Tamil Nadu, India

---***---

Abstract – *Most of the cyber information systems require users to provide identity information as a way of authentication and usually the identity information is a pair of username and password. With so many information systems to access, people need to memorize hundreds of usernames and passwords. As a result, they often forget their usernames or passwords and have to go through a time-consuming and troublesome procedure to find them back. In this article, we propose a solution storing people's usernames and passwords using block-chain in an encrypted format. When the username or password for a particular website is lost, they can be accessible through the blockchain. As a result, people do not need to memorize their usernames and passwords for different websites anymore. The password stored in the block-chain would not be compromised to any cyber-attacks because block-chain is immutable.*

Keywords *- Cyber security; block-chain; encryption; data storage; password management.*

1. INTRODUCTION

Nowadays, users increasingly employ longer passwords to provide effective cyber security. As a result, it is becoming increasingly difficult to track the multitude of system usernames and passwords needed to access information systems for a typical business or personal transaction. The credit reporting service Experian found that the average user has 26 online accounts but uses only five different passwords. For users between the age of 25 and 34, the average number of accounts jumps to 1600 . There seems to always be a dilemma – On the one hand, if we use an identical password to get access to all our information system accounts, we may save much effort. However, the concern is that it is extremely unsafe. On the other hand, we could have different passwords to get access to different systems but another question appears – can we really remember so many passwords? Some IT companies provide users with passwords keeping service. A typical example is a mobile app where you can save your account name and the corresponding password. The data would be stored at a database of the application developer, which results in two concerns: One is that the password is kept by a third party, which cannot be completely trusted. Another concern is that even if the company itself is trustworthy, there is still a chance for external threat agent to hack into the database and find your accounts and passwords stored inside.

1.1 The background and impact of Block-chain Technology

The block-chain technology and the concept of bitcoin was firstly introduced by Satoshi Nakamoto. As a bran-new cryptocurrency, bitcoin makes it possible to eliminate the third-party trust organization using P2P transaction [5]. Block-chain is the technology supporting this efficient and transparent method of payment [6]. As a decentralized distributed system that combines asymmetric encryption techniques, the block-chain technology provides safe and reliable architecture guaranteed for the bitcoin transaction. The block-chain technology and the concept of bitcoin was firstly introduced by Satoshi Nakamoto [4]. As a bran-new cryptocurrency, bitcoin makes it possible to eliminate the third-party trust organization using P2P transaction [5]. Block-chain is the technology supporting this efficient and transparent method of payment [6]. As a decentralized distributed system that combines asymmetric encryption techniques, the block-chain technology provides safe and reliable architecture guaranteed for the bitcoin transaction

1.2 The Theory of Block-chain Technology

The block-chain is a method that achieves collaboration among all participants in the system by cryptography to maintain a reliable data log with common records in an environment that eliminates the third-party trust organization [4]. This worldwide bookkeeping technology which is guaranteed by encryption shows its advantages of reliability, efficiency, transparency and immutability.

2. RESEARCH METHOD

A blockchain is a digital concept to store **data.** This data comes in blocks, so imagine blocks of digital data. These blocks are chained together, and this makes their data immutable. When a block of data is chained to the other blocks, its data can never be changed again. It will be publicly available to anyone who wants to see it ever again, in exactly the way it was once added to the blockchain.

2.1 Data model

It defines the struct of each of our blocks that will make up the blockchain. Each Block contains data that will be written to the blockchain, and represents each case when you took your pulse rate

- **Index** is the position of the data record in the blockchain

- **Timestamp** is automatically determined and is the time the data is written
- **BPM** or beats per minute, is your pulse rate
- **Hash** is a SHA256 identifier representing this data record
- **PrevHash** is the SHA256 identifier of the previous record in the chain

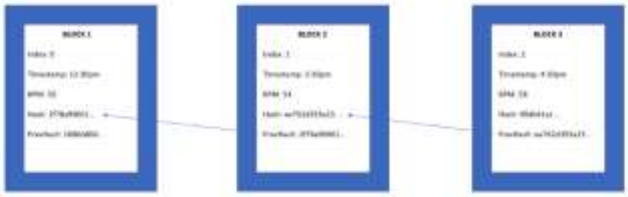


Fig -1: Block-chain structure of the system

2.2 Hashing and Generating New Blocks

We hash data for 2 main reasons:

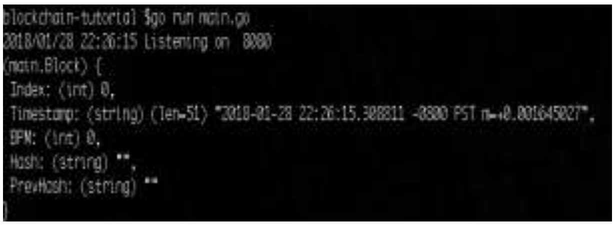
- To save space. Hashes are derived from all the data that is on the block. In our case, we only have a few data points but imagine we have data from hundreds, thousands or millions of previous blocks. It's much more efficient to hash that data into a single SHA256 string or *hash the hashes* than to copy all the data in preceding blocks over and over again.
- Preserve integrity of the blockchain. By storing previous hashes like we do in the diagram above, we're able to ensure the blocks in the blockchain are in the right order. If a malicious party were to come in and try to manipulate the data (for example, to change our heart rate to fix life insurance prices), the hashes would change quickly and the chain would "break", and everyone would know to not trust that malicious chain.

2.3 Block Validation

As, blocks are validated by every node on the network. The goal for this validation is that every block can independently be validated on any node, and is not depending on any external characteristics.

3. RESULT

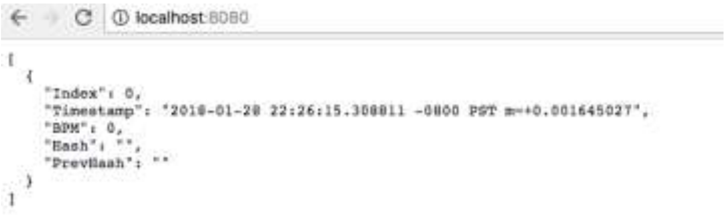
Run up your application from terminal using go run main.go In terminal, we see that the web server is up and running and we get a printout of our genesis block.



```
blockchain-tutorial $go run main.go
2018/01/28 22:26:15 Listening on  8080
(main.Block) {
 Index: (int) 0,
 Timestamp: (string) (len=51) "2018-01-28 22:26:15.308811 -0800 PST m=+0.001645027",
 BPM: (int) 0,
 Hash: (string) "",
 PrevHash: (string) ""
}
```

Fig -2: Running the blockchain Network

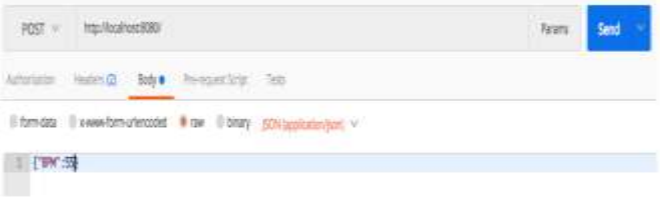
Now, visit localhost with your port number, which for us is 8080. As expected, we see the same genesis block.



```
[
  {
    "Index": 0,
    "Timestamp": "2018-01-28 22:26:15.308811 -0800 PST m=+0.001645027",
    "BPM": 0,
    "Hash": "",
    "PrevHash": ""
  }
]
```

Fig -3: Creation of Block

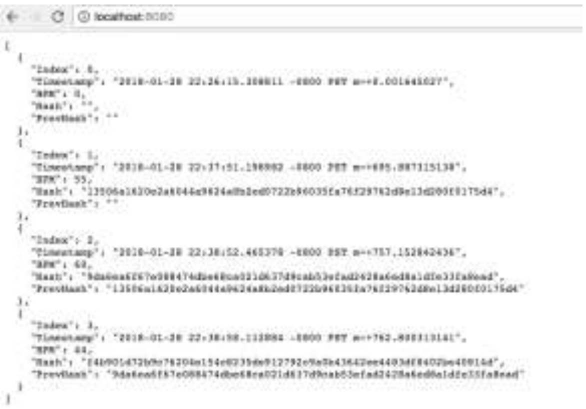
Now, let's send some POST requests to add blocks. Using Postman, we're going to add a some new blocks with various BPMs.



```
{"BPM":55}
```

Fig -4: Sending data using postman

Let's refresh our browser, we now see all our new blocks in our chain with the PrevHash of our new ones matching the Hash of the old ones.



```
[
  {
    "Index": 0,
    "Timestamp": "2018-01-28 22:26:15.308811 -0800 PST m=+0.001645027",
    "BPM": 0,
    "Hash": "",
    "PrevHash": ""
  },
  {
    "Index": 1,
    "Timestamp": "2018-01-28 22:37:51.198982 -0800 PST m=+695.887115138",
    "BPM": 55,
    "Hash": "13506a1620e2a8044e9624a8b2ed0722b96035fa76f29762d9e13d200f0175d4",
    "PrevHash": ""
  },
  {
    "Index": 2,
    "Timestamp": "2018-01-28 22:38:52.465378 -0800 PST m=+757.152842436",
    "BPM": 68,
    "Hash": "9da6ea6f67e088474dbe68ca021d637d9cab53efad2428a6ed8a1dfe33fa8ead",
    "PrevHash": "13506a1620e2a6044a9624a8b2ed0722b96035fa76f29762d8e13d200f0175d4"
  },
  {
    "Index": 3,
    "Timestamp": "2018-01-28 22:38:58.112884 -0800 PST m=+762.800313141",
    "BPM": 44,
    "Hash": "f4b9014f72b9e76204e154e0235de912792e9a0b43642ee4403df8402be40014d",
    "PrevHash": "9da6ea6f67e088474dbe68ca021d637d9cab53efad2428a6ed8a1dfe33fa8ead"
  }
]
```

4. CONCLUSION

Due to the difficulty of keeping numerous Internet accounts and passwords, we propose a password keeping system based on the block-chain technology. This system not only has the high efficiency and convenience as the third-party-solution, but also tackles the trust issue due to the randomness and high security of Sha-256 and the transparency and immutability of the block-chain.

REFERENCES

[1] Portland, OR. 2012. “Online Americans Fatigued by Password Overload Janrain Study Finds”. http://www.janrain.com/about/newsroom/pressreleases/online-americans-fatigued-by-password-overloadjanrain-studyfinds/?_ga=2.151728953.1095589413.151089571015456420.1510895710

[2] Whitman Michael. 2014. “Principles of Information Security”, 5th edition, Course Technology, ISBN: 9781285448367

[3] Manuel Stagars. 2017. “THE BLOCKCHAIN AND US”. www.blockchain-documentary.com.

[4] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander. 2016. “Where Is Current Research on Blockchain Technology—A Systematic Review”, PLOS ONE. https://doi.org/10.1371/journal.pone.0163477.

[5] Sarah Underwood. 2016. “Blockchain Beyond Bitcoin”. Communications of the ACM, Vol. 59 No. 11, Pages 15-17.

[6] Wang Xu. 2017. “The Optimize Research on Block Chain Finance to Cross-border E-commerce Payment Mode”, Reformation

[7] Richard, Levina, Aaron, O'Brienb, Madiha M. Zuberic. 2015. “Real Regulation of Virtual Currencies”, Handbook of Digital Currency, Chapter 17, P327-360.

[8] K. Coperich, E. Cudney, H. Nembhard, eds. 2017. “Blockchain Technology Innovations”, Proceedings of the 2017 Industrial and Systems Engineering Conference, Abstract ID: 2054: P51

[9] Wang jiye, Gao lingchao, Dong aiqiang, Guo shaoyong, Chen hui, Wei xin. 2017. “Block Chain Based Data Security Sharing Network Architecture Research”, Journal of Computer Research and Development, Vol.54(04), 2017, P742-749

[10] Rooger Woodworth. 2017. “Blockchain is coming! A future of distributed ledgers”, Public Utilities Fortnightly, Apr 2017, Vol.155(4), P60-61

[11] Ding wei. 2015. “Block Chain Based Instrument Data Management System”, China Instrumentation, 2015, Issue 10, P15-17

[12] Will Matthews. 2017. “WHAT IS BLOCKCHAIN”, TechTalk. 18 February 2017: P38

[13] Alison Salka. “The Blockchain Opportunity”, Risk Adviser, BEST’S REV, P19

[14] Kate Smith. 2016. “Blockchain Reaction”, Bests Review, November 2016: p64

[15] Berger, Brian. 2017. “WannaCry exposes defense supply chain vulnerabilities”, National Defense, 2017, Vol.101(764), P20(2)

[16] Kazuo Sakiyama, Yu Sasaki, Yang L. 2016. “Security of Block Ciphers: From Algorithm Design to Hardware Implementation”, Security of Block Ciphers: P12

[17] J. Bethencourt, A. Sahai, and B. Waters. 2007. "Ciphertext-policy attribute based encryption," in S&P'07. IEEE Computer Society, 2007, pp. 321-334

[18] B. Waters. 2011. "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization", in PKC'11. Springer, 2011, pp. 53-70

[19] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang. 2013. “DACMACS: Effective data access control for multi-authority cloud storage systems”, in INFOCOM, 2013 Proceedings IEEE