A Study on Authentication Mechanisms in Bitcoin

***Shruthi N*[1]*, Sowmyarani C N*[2]**
[1]PG Student, [2]Associate Professor
[1,2]Department of Computer Science Engineering,
RV College of Engineering, Bengaluru, Karnataka, India
***Email:** shruthibhatn@gmail.com*

DOI:

Abstract

Any number of gadgets can be associated with a Wi-Fi remotely. Anybody inside scope of the Wi-Fi can endeavour to get to the system. Due to this, Wi-Fi is progressively powerless against assaults. Consequently, client touchy data is at the danger of being misused. The clients' security and security can be ensured by unknown verification. When they use the hotspots that are very easy to access to everybody, privacy plays an important role. The existing solutions which will validate the users but do not take the responsibilities of the users or they are always dependent on intermediators. The latest development of or concept of colored coins and coin shuffle can be used to protect the users who are connected to the network without compromising or leaking any information. The bitcoin blockchain is very impressive and robust that will help to manage the user information and also very helpful to determine the possession of the users framework.

***Keywords:** Accountability, bitcoin, Wi-Fi hotspot access*

INTRODUCTION

Authentication of the users involved in the bitcoin process is very essential. The issue with the Wi-Fi is that it is very simplified to access the network compared to the wired networks. To gain access to a wired network, one must be connected through a building network (physically connecting to the network). But to gain access to a Wi-Fi, one merely needs to be within the specified range of the Wi-Fi network. So, once an attacker who has entered the network and gained the access to the Wi-Fi network may launch any type of harmful attack against any other user. The network may be tried to forge by a response before the server has a chance to acknowledge the request.

Open hotspots are easy to access and they are hosted on untrusted (not trust worthy) points through which they are accessible and are widely deployed and distributed to provide Wi-Fi connectivity. As the Wi-Fi connectivity is distributed in nature, hotspot access control, utmost care and importance is taken to enforce hotspot access control through strict user authentication so that malicious attackers and free users are controlled. Service providers that are not honest or untrusted access points might leak users' privacy and misuse the leaked data. The users' mobility pattern and sensitive information may also be leaked.

Anonymous authentication will enhance the security of the Wi-Fi network and it will also preserve the privacy of the users in the above said security situation. Theanonymous authentication scheme will cover the sensitive information (identity) of the users that are connected to the Wi-Fi network from the outer world attackers and also to the server on which the Wi-Fi is hosted. Since the users' details are not exposed, different users can perform any action and these actions are neither linked to each other nor mapped.

However, undisclosed authentication will be a issue for the network service provider because if the network is attacked by an attacker who is connected to the network then a dispute or confusion may occur to the server to find the malicious user, since all the users are authenticated anonymously. The identification of these individually misbehaving users will be a big problem to detect and also to expose the attacker.

In order to protect Wi-Fi hotspots, which are hosted publicly, from being attacked and also to supervise these malicious users,an anonymous authentication scheme will be helpful for the service providers to remove or withdraw the misbehaving user from the Wi-Fi hotspot and thus thereby securing the network and also keeping the identity of the users secret.

In [1], Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used for implementing access control, users who own the right attributes can obtain the WPA2 secret. In [2], Bitcoin 2.0, which is a derivation of Bitcoin, performed authentication, users' privacy was not considered. The illegal persons who are attackers can be removed by the administrators and user's statistics can be collected and maintained. Bitcoin addresses which improve security can be used as encryption keys by which communication is possible. The different type of Bitcoin2.0 is the Namecoin, Ethereum etc. They are some examples of the decentralized systems that use bitcoin and blockchain.

In [3], many signatures are included to form a group signature which aims at achieving anonymity and accountable users for wireless access network were used. However, the main principle was based on investing powers in different levels so that separation of powers existed. The focus was to make sure that the group manager and the network operator do not collude with each other. Communications were encrypted, so malicious usage was disabled, and high powers, functionality and convenience were also provided.

BACKGROUND ON BITCOIN

Bitcoin is known as the earliest successful implementation of the cryptocurrency in the world. Bitcoin proposed by Satoshi Nakamoto is a digital currency that has no physical existence [4]. It is used in place of hard cash. The exchanging of cash without revealing identity became common in the web [13]. Anonymity helps in keeping the bitcoin interesting and trending even after many years it was introduced.

The bitcoins are not the same as online currency over web as the linking with real world identity does not take place. Blockchain forms the main technique of bitcoin. The blockchain has a public log which is maintained globally where all the transactions are tracked and has tracking of transactions that take place in the ledger system.

The bitcoin does not have centralized framework. Cryptocurrency utilizes common cryptographic primitives. The transactions that have taken place are included in a ledger system that is distributed and publicly available. Bitcoin is most widely spread and serves as assets infrastructure.

New transactions are added to the bitcoin network. Mining process confirms transactions and new transactions get added to the blockchain. Pending transactions are added to blockchain. A cryptographic puzzle Proof of work is solved by the miner when his transaction is to be included in the transaction block.

The participants involved in the bitcoin are rewarded some bitcoins. The first person who succeeds in solving puzzle gets certain amount on the form of bitcoins. Blockchain is applied in industries such as industry, academia, spanning finance, education and education. Blockchain provides a platform of regional applications. Blockchain system is used as ledger system which is distributed to store various varieties of data.

Blockchain is ordered list of transactions which are clustered in blocks. Transactions consist of inputs and outputs. Output consists of specific predefined amount and cryptographic puzzle to lock funds which are involved in output. For funds to be unlocked, the person owning private key sends a transaction that is signed and funds to some other bitcoin address. Each input in the transaction consists of reference which points to valid previous output and a valid signature. The transaction also consists of previous transactions which have included transaction identifier, an index and hash value of transactions. In each transaction, puzzles are there to lock funds so that they are not misused and solutions for puzzle are represented by scripts which play an important role.

Script is composed of opcodes, several commands and data like recipient address, signature. A script is usually consists of various commands, opcodes, and some data, information about the recipient address, their valid signature etc are also present. The Bitcoin implementation usually includes one of the transactions as OP RETURN. The data embedding takes place in transactions. One of method of data embedding is provably unspendable OP RETURN outputs. Blockchain has logs of the user accessing it that are maintained and saved to it. The users have option of specifying size up to 83 bytes of data which is used in OP RETURN output. The release of the Bitcoin Core 0.12.0 had a great impact.

Once a transaction is created, transactions are sent to node that connects to blockchain that forms a network. Once transaction is valid, node propagates the valid transaction to many connected nodes which are involved in the network. The validation is done if the inputs in transaction are unspent transaction outputs. In a database called UTXO, all the unspent transactions are stored. For a transaction to be called as valid, sum of amounts inputs should always be more than or equal to sum of amount of valid outputs. Mining fee is calculated by the difference that exists between inputs and outputs for miners.

Bitcoin system is concerned only with the validity of the signature and transaction is in correct form. Miners do not have the ability to distinguish the signatures that are generated by a single entity or a group of signers. Bitcoin does not need any third party as all participants cooperate with each other. Every Bitcoin transaction includes a transaction fee that is paid to the Bitcoin miner [8].

PREVIOUS AUTHENTICATION METHODS

Since the Wi-Fi hotspots are wireless, they can be hosted at several public places. Normally, the public Wi-Fi has an easy authentication method or sometimes they do not require any mode of authentication to gain admission to the Wi-Fi network. Because of this, the public Wi-Fi hotspots are not reliable and may prone to be security problems. When malicious users are found, it is difficult to reveal the criminal. So in order to achieve the safety of the network, Wi-Fi systems have come up with different authentication methods to verify the user. The conventional authentication methods include:

- Registration of email of users.
- Mobile number registration and verification done by SMS.
- The users have to submit valid proofs

for identification such as PAN cards etc.
- Instruct the users to accept the proposed standards.

SMS authentication is easily verified by the users but risk of exposure and tampering exist. Validity of users occurs through sending emails where uniform resource locator (URL) is used to confirm the existence. URLs can only be accessed when the network connection exists and the net is on. SMS authentication is very easy for verification of users. Exposure of users may take placewhen the data is tampered. Malicious users can steal accounts.

CURRENT AUTHENTICATION METHODS

Coin Shuffle

Bitcoin mixing is done for users to exchange credentials among the network anonymously and securely [5]. Verification path ensures that existing valid credential leads to a new credential. The blacklisted credential holders are not allowed to participate in the mixing protocol. Users' accountability is achieved. Credentials are often changed by users and addresses of bitcoin are generated by them.

Colored Coins

Access credentials are held at an accountable place in a particular fashion [4]. The users access right is associated with address of bitcoin that are used as credential when accessing takes place through public hotspots that are free and do not require passwords to be entered.

Advantages of Authentication

- Communications can be encrypted where outsider finds it difficult to get original message.
- Malicious usage of data is disabled and prevented.
- High functionality and convenient for users.
- Multiple Wi-Fi systems located in different places can cooperate.
- Useful for authorization to connect access points. Access points help people to authorize, once registered users do not have to not send their information each and every time.
- Service provider has the right to remove misbehaving credentials; the credentials to users' identities cannot be linked to these.
- Users can be authenticated without sending their personal information each and every time.
- Various areas can form cooperation by using same Blockchain [7].

OVERVIEW OF AUTHENTICATION METHODS IN BITCOIN

User Registration

Only one registration transaction can be created before credential is revoked. Number of registration transactions forms the limit for size of the blacklist. The number of registrations done determines the credentials a person can be held accountable. The registration is done by the signatures.

Credential Verification

Prover uses sign based process to prove that a valid credential is held by him. Proof based on checkpoint is constructed to prove that credential is valid.

Registration Transaction

A transaction that takes place for registration contains three types of outputs in it. A checkpoint output is the first type of transaction. The checkpoint maybe used as genesis checkpoint and in future credential exchange may take place. The checkpoint tells how many times credential exchange may take place without extra charges to user. As the misbehaviour of a user increases the deposit transaction charge also increases. Marker output contains payload field.

Multi-signature Transaction

This type of transaction can be used when same output can be used and spent with more than one signature. The signature is signed by two persons namely the service provider and user who signs it.

Credential Verification

Hash value of an "ECDSA" public key and the encodings in Bitcoin addresses are used. Credential verification takes place by using the signature used and by secret key. All transactions which are created contain OP RETURN output, which is the marker output. It distinguishes system transactions from other transactions.

Credential Revocation

The credentials of persons leaving system and persons tampering date are revoked. They are added to blacklist. The service provider plays an important role as he punishes ill behaving credential holders and also updates the details of such users. All the members in the transaction get to know the details of him. A list can have maximum 3 such users. A person who leaves system makes sure that his deposit is removed.

Checkpoint Updating

The path included in the verification increases as the credential exchanges also increases. When length reaches maximum, checkpoint is changed by request of request provider.

CONCLUSION

The bitcoin blockchain technology is growing rapidly and also the increase in percentage of public Wi-Fi hotspots paves the way for securing the user identity and also to develop a new authentication schemes with the help of bitcoin, although existing authentication methods are exists.

In order to achieve anonymous nature, security and efficiency for Wi-Fi access, the bitcoin authentication can be used. By this method, the users' identity is also not compromised and also the identification of the malicious user is made easy. Bitcoin is being considered in many applications where anonymity and security are important.

REFERENCES

1. C. Pisa, A Caponi, T Dargahi, G Bianchi, N Blefari-Melazzi (2016), "WIFAB: Attribute-based WLAN access control, without pre-shared keys and backend infrastructures", *HotPOST16*.
2. T Sanda H Inaba (2016), "Proposal of new authentication method in WiFi access using Bitcoin 2.0", *IEEE 5th Global Conference on Consumer Electronics.*
3. DHe, SChan, MGuizani (2016),"An accountable, privacy-preserving, and efficient authentication framework for wireless access networks",*IEEE Transaction on Vehicular Technology*,Volume 65, Issue 3, pp. 1605–1614.
4. MRosenfeld (2012), "Overview of colored coins", *White Paper,* Available: https://bitcoil.co.il/BitcoinX.pdf.
5. T Rffing, P Moreno-Sanchez, A Kate (2014), "CoinShuffle: Practical decentralized coin mixing for Bitcoin". *The 19th European Symposium on Research in Computer Security.*
6. Lewis Tseng (2017), "Bitcoin's Consistency Property". *IEEE 22nd Pacific Rim International Symposium on Dependable Computing,* pp. 219–220.
7. Tomoyuki Sanda, Hiroyuki Inaba (2016), "Proposal of new authentication method in Wi-Fi access using bitcoin 2.0", *IEEE 5th Global Conference on Consumer Electronics.*
8. Qi wang, Xiangxue li, and yuyu "Anonymity for Bitcoin from Secure Escrow Address". IEEE access, vol. 6,

pp. 12336-12341, 2018.

9. J.Bonneau, EW Felten, H Kalodner,R Gennaro, JAKroll, S Goldfeder, A Narayanan, (2015), "Securing bitcoin wallets via a new dsa/ecdsa threshold signature scheme".
10. M Moser, R Bohme, D Breuker (2014), "An inquiry into money laundering tools in the bitcoin ecosystem", *Ecrime Researchers Summit,* pp. 1–14.
11. G. Maxwell (2013), "Coinjoin: bitcoin privacy for the real world," *Post on Bitcoin Forum.*
12. A Biryukov, I Pustogarov (2015), "Bitcoin over Tor isn't Good Idea", IEEE Symposium on Security and Privacy", *San Jose, 37th .CA,* pp. 122–134. doi:10.1109/SP.2015.15,2015.
13. S Nakamoto (2008),"Bitcoin: A peer-to-peer electronic cash system (1st ed.) [Online], Available: https://bitcoin.org/bitcoin.pdf.
14. GO Karame, E Androulaki, S Capkun (Oct 2012), "Two Bitcoins at thePriceofOne? Double-Spending Attacks on Fast Payments in Bitcoin". *Proceedings of Conference on Computer and Communication Security, Raleigh.,* NC.
15. ES Robla, "Analysis of reward strategy and transaction selection in bitcoin block generation". *M.S. thesis, Dept. Elect. Eng., Univ. of Washington,* Seattle, WA, 2015.
16. YukunNiu, Lingbo Wei, Chi Zhang, Jianqing Liu, Yuguang Fang 2017, "An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain". IEEE/CIC *International Conference on Communications in China (ICCC).*

Cite this article as: