西南交通大学学报

第 54 卷 第 5 期
2019 年 10 月

JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY

Vol. 54 No. 5
Oct. 2019

ISSN -0258-2724 DOI : https://doi.org/10.35741/issn.0258-2724.54.5.7

ENHANCING PRIVACY AND IMPROVING SECURITY IN SCALABLE BLOCKCHAIN

增强可扩展区块链的私密性和安全性

Ammar Mhana [1]*, Ghassan N. Mohammed [2], Fadhel K. Jabor [3]

[1] College of the Science, University of Baghdad,
Baghdad, Iraq, ammar.mhana@uobaghdad.edu.iq
[2] Department of Planning & Studies, Ministry of Higher Education,
Iraq, ghanm1971@yahoo.com
[3] Vice President Office for Scientific Affairs, University of Baghdad,
Baghdad, Iraq, fadhel.k.jabor@uobaghdad.edu.iq

Abstract
Bitcoin is a decentralized blockchain-based cryptocurrency that has taken the world by storm. Since its introduction in 2009, it has grown tremendously in terms of popularity and market cap. The idea of having a decentralized public ledger while maintaining anonymity and security attracted the attention of developers and customers alike. Special nodes in the bitcoin network, called miners, are responsible for making the network secure by using a concept called proof-of-work. A certain degree of anonymity is also maintained as no personally identifiable information of a person, like name, address, etc., is linked to the bitcoin wallet. In terms of bitcoin, a user is anonymous if different interactions of the user cannot be linked to each other or the user. Recent research shows that bitcoin is not as anonymous as it appears to be. The inherently public nature of blockchain technology makes it difficult to achieve privacy. The purpose of this paper is to review how varying degrees of user privacy is maintained in bitcoin cryptocurrency. This paper is divided into two main segments. The first segment explores privacy-enhancing techniques adopted in bitcoin. The second segment critically analyzes these techniques.
Keywords: Anonymity, ToR, Bloom Filters, Bitcoin, Zero-Knowledge Proofs, Mixing Service, Zero-Cash, Coinjoin, Mining, Blockchain.

摘要 比特币是一种分散的，基于区块链的加密货币，风靡全球。自 2009 年推出以来，它在知名度和市值方面都取得了巨大的增长。在保持匿名性和安全性的同时拥有分散的公共账本的想法吸引了开发人员和客户的关注。比特币网络中称为矿工的特殊节点负责通过使用一种称为工作量证明的概念来使网络安全。还保持一定程度的匿名性，因为没有人的个人身份信息（例如姓名，地址等）链接到比特币钱包。就比特币而言，如果该用户的不同交互无法彼此链接或与该用户链接，则该用户是匿名的。最近的研究表明，比特币并不像看起来那样匿名。区块链技术固有的公共性质使其难以获得隐私。本文的目的是回顾如何在比特币加密货币中维护不同程度的用户隐私。本文分为两个主要部分。第一部分探讨了比特币中采用的增强隐私的技术。第二部分主要分析这些技术。

关键词: 匿名，托尔，盛开过滤器，比特币，零知识证明，混合服务，零现金，Coinjoin，采矿，区块链。

I. INTRODUCTION

Bitcoin was introduced by Satoshi Nakamoto in 2009 as a decentralized cryptocurrency [1]. It is decentralized as no single organization owns bitcoin. All peers on the bitcoin network are equal and have the same rights. A bitcoin user needs to install a bitcoin wallet, which acts as an interface

between the bitcoin network and the user. The wallet generates a paired private and public key for the user. Public keys are used to send bitcoin to any other node and private keys are used to redeem bitcoins. The bitcoin peer-to-peer network uses a public ledger called blockchain to store all its transactions [2]. All nodes in the network listen for valid transactions. A given set of valid transactions is collected into a block by the node and added into the blockchain through a process called mining [3]. Such nodes are called bitcoin miners. Miners are incentivized for adding a valid block in the blockchain. No transaction can be reversed once it is entered into the blockchain. Mining serves two purposes. First, it provides a technique to add new blocks to the blockchain. Second, it adds new coins into the network. Every miner is awarded some bitcoins for successfully adding a block. Currently, the reward is 12.5 BTC per block. This ensures that the bitcoin network is secure and stable. Mining requires solving a hard computational problem by giving proof-of-work. Proof-of-work means producing data with a high level of difficulty that matches certain conditions. It is possible that more than 1 block is mined at a time or an attacker proposes a malicious block. Other nodes of the network will validate all the transactions of the block.

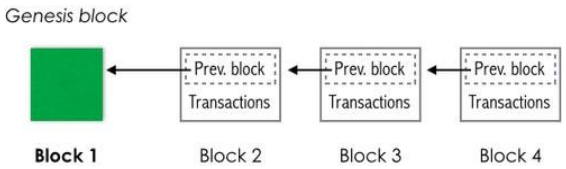

Figure 1. Blocks in blockchain containing transactions [2].

If there is something wrong, the nodes will reject the block and fail to mine any new node on top of it. Nodes give their confirmation to validate a block. A block with 6 confirmations is usually considered valid. Bitcoin follows the policy of mining from the top of the longest blockchain. The longest chain will be the one that has more confirmations and has the support of the network nodes [4]. To tamper with the blockchain, an attacker has to create a number of blocks in the blockchain and mine all of them on top of each other. Mining a single block is quite hard. It is not possible for an attacker to mine the entire blockchain by his or her self. No individual has such computing power. Thus, mining keeps the bitcoin network secure and allows the Bitcoin nodes to reach consensus. It is essential that all nodes in the network arrive at a consensus regarding the blockchain without relying on each other.

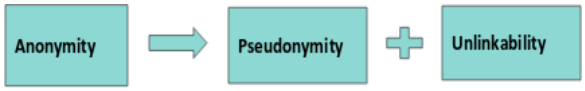

Figure 2. Anonymity in bitcoin.

Another major aspect that attracted people to bitcoin was its claim of anonymity [19], [20], [21]. Bitcoin is pseudonymous. Pseudonymous means it hides behind an alias which in this case is the public key of the user. Some level of privacy is maintained as no personally identifiable information of a person is linked to the person's bitcoin wallet. But if you know a bitcoin address, you can trace all transactions made by that address, as the ledger is public. Hence it has become common practice to use a different address for each transaction. Yet, there are still other ways through which user privacy can be compromised. It is important to add unlinkability to bitcoin to achieve full autonomy. One way to keep yourself completely anonymous is to download the entire blockchain (around 156 GB in size currently) and generate a new address for each transaction [5]. The problem with this approach is that most bitcoin users install wallets on their smartphones that do not have sufficient memory to store the chain. Bitcoin users are generally divided into two categories: full nodes and lightweight nodes. Full nodes store the entire blockchain and validate all the transactions in the block. Lightweight clients store only block headers. They are interested in only those transactions that concern them. Lightweight nodes can request full nodes to send them relevant transactions [6]. But this is a major privacy breach as lightweight nodes have to reveal their addresses to full weight nodes. A technique called bloom filter is used to obtain the required transactions without revealing the actual address [7]. This is done by sending a pattern of the required address instead of the actual address. However, this does not provide complete anonymity as a third party monitoring network traffic can still figure out public addresses. Further developments have led to the introduction of new techniques like ToR encryption and peer-to-peer encryption and authentication. Section 3 discusses threats to privacy in bitcoin. Section 4 explores privacy enhancing techniques in detail and Section IV critically analyzes them.

II. LITERATURE REVIEW

The literature review is broad enough to cover relevant work done in this field. All cited sources are pertinent to the topic of the study. All of the cited sources have been published within the last 5 years, hence it covers recent research done in this field. There is no evidence of any bias.

A. Threats to Anonymity and Privacy In Bitcoin

Bitcoin addresses are public key hashes rather than real identities [5]. No personally identifiable information of a person is linked to it. This gives a certain level of anonymity to the bitcoin user. The goal of anonymity for bitcoin is that it should not be possible to link any user with his/her addresses or transactions. Bitcoin satisfies this goal partially, hence it is pseudonymous. There exist several tools to link addresses of a person [8], [22]. By knowing the public address of a person, it is possible to track all the transactions done by that person to date. It shows how online websites like https://blockchain.info/address/ allow anyone to trace other people's transaction history [9].

B. Peer to Peer Deanonymization

A trivial solution to keep your transactions unlinkable to each other is by generating a new address for each and every transaction [1]. However, this technique fails as there are several ways in which multiple addresses of a person can link together. Suppose, Alice has 5 BTC with one public address and 4 BTC with another public address. She wants to send 8 BTC to Bob. So she needs to merge her money from both accounts to pay 8 BTC to Bob. 1 BTC will be returned as the change to her third bitcoin address. Since Bob gets payment from 2 separate addresses and he sees the change of address, he can link all the three addresses to Alice. If Bob follows her transaction history on the blockchain by tracing her public addresses, he can discover her other addresses and Alice's privacy is breached. Similarly, other linking techniques exist to deanonymize the user. Such techniques can often produce false positives and lose accuracy over time. However, they can work well if planned carefully by the adversary.

C. Network Layer Deanonymization

Lightweight nodes request transactions of their interest from full nodes. They do so by sending a list of their addresses, transactions, etc. This is a major breach of privacy as lightweight nodes reveal their public addresses to full nodes. A solution for this is to use bloom filters, which sends the pattern of the address instead of the actual address [10]. Bloom filters give false positives and do not provide complete anonymity. Another issue is that while transmitting transactions, their IP addresses are also attached to it. Hence, network level anonymization is needed. If not maintained, it poses a threat to user anonymity and privacy.

Table 1.
Deanonymization rate of addresses

Estimated security	Deanonymization rate with 3-tuples	
	Actual	Predicted
0.64	41%	43%
0.86	59.9%	65.6%

III. METHODOLOGY

This section describes the standard techniques used in bitcoin to enhance user privacy. In this manner, mining keeps the bitcoin system secure and enables the Bitcoin hubs to achieve consensus. It is fundamental that all hubs in the system agree to the blockchain without confiding in one another. This increases the security and transaction.

A. Bloom Filter

The bloom filter is a probabilistic search filter which provides a pattern without specifying it directly [7]. This is done by using hash functions. The required patterns are passed through a hash function whose output is used in a bit array. These filters allow a simple payment verification (SPV) node to specify a pattern corresponding to its addresses and transactions which are hashed in the filter. This filter is sent to any full node which stores the entire blockchain. The full node filters out transactions of interest according to the specified patterns and returns it to the SPV. This hides the identity of the SPV as no address or transaction detail is sent directly and provides a certain level of anonymity. However, the more specific the pattern, the lesser the privacy. There is a tradeoff between privacy and precision. The bloom filter provides an extraordinary and satisfactory result in the results section.

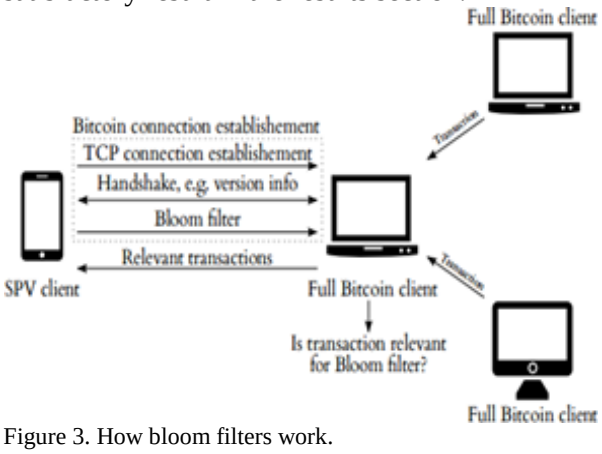

Figure 3. How bloom filters work.

B. Peer-to-Peer Mixing

A proposal to increase anonymity in bitcoin is peer-to-peer mixing [1]. A typical bitcoin transaction contains some input values which are debited from signature providers and some output values which are credited to the corresponding

recipient addresses. The idea of peer to peer mixing is to group a set of bitcoin users who want to make transactions and mix them so that it is unknown which transaction output corresponds to which input. Anonymity can be increased by the numbers of participants in the mixing set. Once all peers are found, the transaction is constructed and sent to all peers to collect signatures. All peers verify whether the output they want is present in the transaction or not. If yes, the peer signs the transaction and forwards it to other peers [11]. If no, then the peer can refuse to sign the transaction, and a new peer-to-peer will need to be created. This protects peers from theft. Once the transaction is signed by all the peers, it is broadcasted on the network where it is mined. One valuable property to note is that all individual transactions of all the peers in a mix should have the same bitcoin transfer value. This technique can help to increase privacy significantly [12].

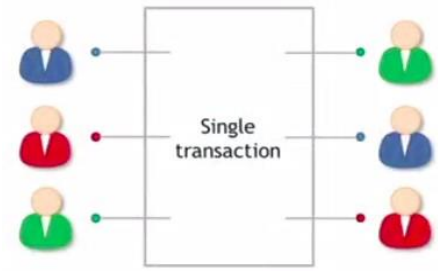

Figure 4. Peer to peer mixing.

C. Third-Party Mixing Services

To protect anonymity, an intermediary is used, which mixes all transactions of the same values for different users to unlink their identity from their address [1]. These values are decided based on standard chunk sizes predefined by the mixing service. Certain practices are followed to maximize anonymity, such as using a series of mixes and automating client-side software [13]. This technique allows anonymity from external users as well as internal users participating in the mix. To stay in business, third-party mixes need to earn the network's trust. Therefore, cryptographic warranties are provided to the user to assure them of their privacy and security [14].

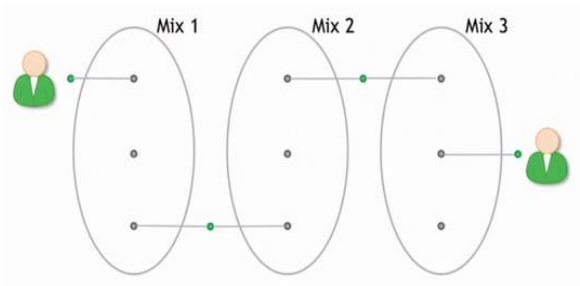

Figure 5. Third party mixing services.

D. Bitcoin with Built-In Privacy

Instead of a third party mixing transactions, it can be directly incorporated into the protocol [1]. This eliminates the need to trust any third party and provides a crypto-graphic guarantee of mixing. Bitcoin, like zerocoin, uses zero-knowledge proofs to make a statement, without revealing any other information. Every user generates a public serial number and a private secret number. The hash of this pair is posted on the blockchain as a cryptographic commitment. An arbitrary zerocoin in the blockchain of the required value can be chosen as input to the new transaction [15]. This provides full anonymity. No one knows which serial number belongs to which zerocoin user. Similarly, zero-cash was developed as a more efficient implementation of zerocoin with better cryptographic proofs to make it more secure [16].

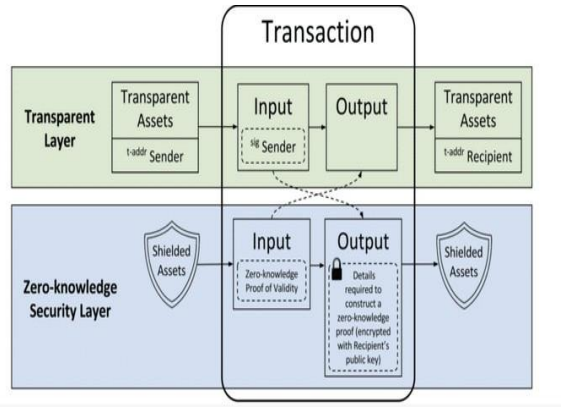

Figure 6. How zero-knowledge proofs work.

E. ToR Processing

In the original implementation of bitcoin, all nodes communicate openly throughout the network. All information is broadcasted in the form of plaintext. This vulnerability can be exploited to perform network deanonymization. A simple solution to this problem is to transmit encrypted data over the network. This is where The Onion Router (ToR) comes in [17]. It is an open-source software used to communicate anonymously over the network. Bitcoin users are encouraged to use Tor along with bitcoin core software to increase user anonymity. Original bitcoin core software was later modified to offer support for ToR. This is mainly done so that the privacy of the SPVs is not compromised. There is one entry node, one exit node, and at least one relay node in between [10]. Any data that needs to be communicated is encrypted at the sender side and is sent to the receiver through random paths. ToR provides an anonymity service that bitcoin currently lacks.

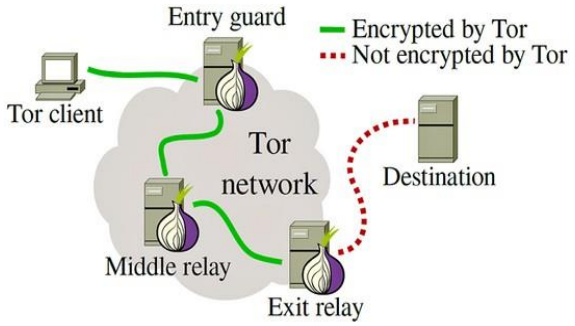

Figure 7. How ToR works.

IV. RESULTS

This section describes the results obtained in enhancing the privacy and improving the security of scalable blockchains and further its pros and cons of the above-discussed privacy techniques.

A. Bloom Filter Prediction

Bloom filters are easy to use for an SPV client for whom anonymity is not of utmost importance. They give a probabilistic answer as they are based on patterns which can also be inaccurate. According to [7], using bloom filters leads to leakage of users' private information. A user who uses many addresses (20) faces the risk of revealing some or all the addresses. A malicious attacker who is observing the network for some time can leak users' addresses. Moreover, the precision of bloom filters decreases when several patterns are added to it. It is also known to give false positives.

Additional verification has to be performed by the SPV to eliminate false positives. Figure 8 shows the number of false positives that increase as the number of wallet addresses increases. Figure 9 shows that the number of true positives that decrease as the number of wallet addresses increases. Bloom filters work as a temporary solution but they will fail in the long run to provide full anonymity to the user.

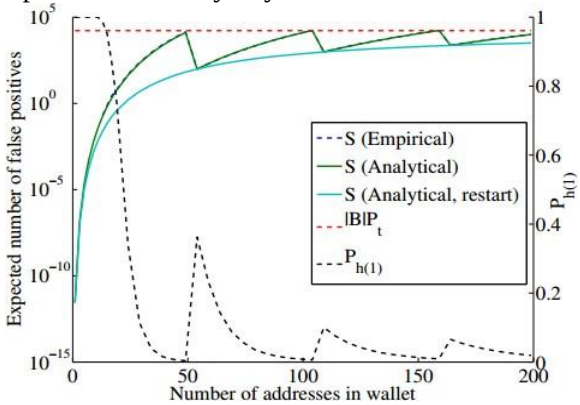

Figure 8. False positives result using bloom filters.

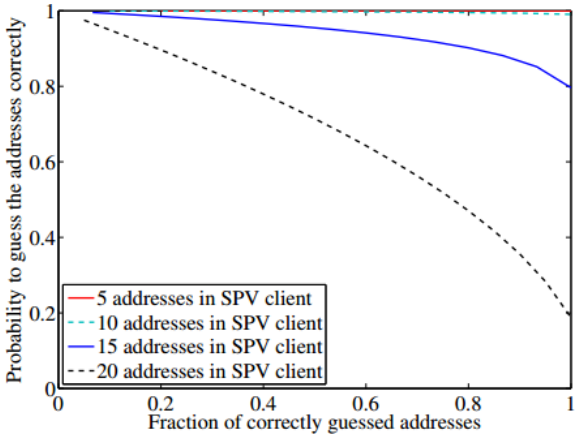

Figure 9. True positives result using bloom filters.

Table 2.
Resultant table of bloom filter for enhaced privacy for block-chained currencies

Factors	Guesses addresses	SPV client
5 addresses	0.4	1
10 addresses	0.6	0.85
15 addresses	0.8	0.45
20 addresses	1	0.2

B. Peer to Peer Mixing Prediction

Peer to peer mixing allows peers the right to refuse to sign the transaction to reduce money laundering. This also makes it vulnerable to Denial Of Service attacks [1]. Another issue is that all peers in the mixing set can see individual inputs and outputs within the transaction. Hence, such mixing only provides external anonymity. There is no anonymity within the set. This defeats the purpose of mixing, if a peer within the mix is malicious, he can leak users private information for whatever reasons. The additional restriction imposed is that the transfer value of bitcoin has to be the same in the mix. A valid node may have to wait for a while to get a suitable mix.

C. Bitcoin with Built-In Privacy Prediction

This technique is the only one which provides full anonymity without any risk as it incorporates privacy enhancing techniques within the cryptocurrency [16]. The disadvantage is that altcoins which provide full anonymity are not as popular as bitcoin [18]. They may catch up in the future [1]. Altcoins use zero-knowledge proofs for achieving built- in-privacy [15]. Table 3 shows the comparison of Zcash and Bitcoin.

Table 3.
Comparison between Bitcoin and Zcash.

Measures	Zcash	Bitcoin
Privacy	zk-SNARKs	N/A
Block time	2.5 mins	10 mins
Block size	2MB	1MB
Mining algorithm	Equishash	SHA-256
Difficulty	Every block	Every 2016

adjustment		blocks

Figure 10 represents the comparison between various existing bitcoins on the basis of the following five categories: Internal Unlinkability, Theft Resistance, DoS Resistance, Bitcoin-compatibility and number of transactions [1]. A fully shaded circle means the property is fully present, whereas a half shaded circle implies that the particular property is partially present. The absence of circle represents the absence of the property. An interesting observation is that blindcoin is bitcoin compatible and satisfies most of the properties. Bitcoin developer community can use properties of blindcoin to improve its existing code, shown in Figure 10.

Proposal	*Class*	*Security*			*Deploy.*	
		Internal Unlinkability	Theft Resistance	DoS Resistance	Bitcoin-compatible	# Transactions
CoinJoin	P2P	●			●	1
Shuffle Net	P2P	●			●	1
Fair Exchange	P2P	●			●	4
CoinShuffle	P2P	●	●	◐	●	1
Mixcoin	distr.	◐	◐	●	●	2
Blindcoin	distr.	●	◐	●	●	4
CryptoNote	altcoin	●	●	●		0
Zerocoin	altcoin	●	●	●		2
Zerocash	altcoin	●	●	●		0

Figure 10. Comparative evaluation of Bitcoin.

E. ToR Prediction

ToR is a general anonymous network service. It is easy to integrate ToR with Bitcoin as the Bitcoin core was modified to provide in-built support for ToR. ToR aims to hide who is talking to whom on the network. Yet, there exist several ways through which ToR users can be de-anonymized. By linking Bitcoin to ToR, we link Bitcoin with all the attacks and vulnerabilities associated with ToR. Additionally, using ToR with Bitcoin makes Bitcoin vulnerable to man in the middle attacks [10]. It also makes the Bitcoin software slow. Figure 11 shows the clients state after the man in the middle attack. By performing man in the middle attack, not only is the identity of the person is revealed, but the person can also be robbed of Bitcoins. Some researchers argue that ToR increases existing problems rather than solving them.

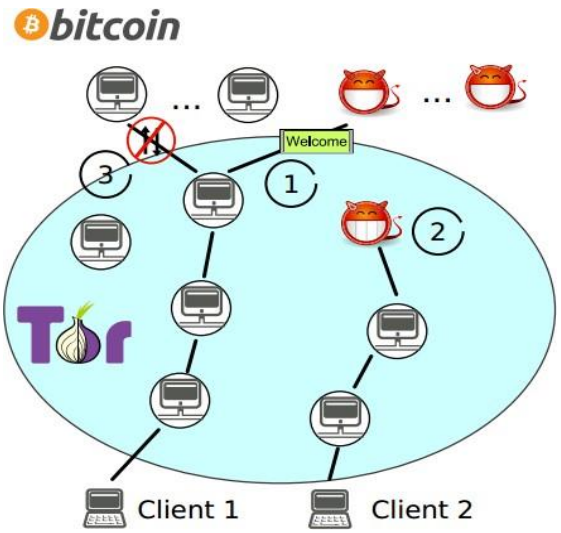

Figure 11. Man in the middle attack using ToR.

V. Discussion

Cryptocurrencies are the future of banking. Removing any vulnerability in them is of utmost importance. Bitcoin is the most popular cryptocurrency. There is a huge debate over bitcoin privacy within the bitcoin developer community. Researchers have created several techniques to fully anonymize the bitcoin, but none have proven to work perfectly. After reviewing many research papers on this topic, I conclude that there is no single existing technique in use currently that can be considered the most effective for increasing privacy in the bitcoin. A major change needs to be brought into the bitcoin core software to achieve privacy without creating further risks for bitcoin owners. Experiments conducted on altcoins show that privacy within the protocol can be efficiently achieved. Altcoins like zerocoin and zero-cash have successfully achieved complete privacy, though they are not as popular as the bitcoin. Analyzing how inbuilt privacy can influence the way the bitcoin operates would be interesting. It is an open area for research.

Table 4.
Comparison and privacy techniques assessment

Privacy technique	Issues
Bloom filters	False positives, low precision, leaks information
P2P mixing	No internal anonymity, DoS attack
Third-party mixing	Trust third part, risk of theft
Altcoins	Not as popular as the bitcoin
ToR	Man-in-the-middle attacks

VI. Conclusion

This paper highlights the need for implementing new techniques that would improve user anonymity in cryptocurrencies like Bitcoin. Many users believe Bitcoin is anonymous. Researchers have proved that that is far from

reality. Without privacy, Bitcoin is worse than centralized banking. There exist several techniques which aim to enhance the pseudonymity provided by Bitcoin. These techniques succeed partially in doing so. None of them provide total anonymity that can be adopted by Bitcoin. Techniques like using bloom filters, ToR, peer to peer mixing, and decentralized mixing services are flawed. Table 1 shows all the mentioned techniques with their issues in brief. They would not work in the long run. Using ToR with Bitcoin makes Bitcoin vulnerable to further attacks. The best approach to achieve full anonymity without involving any third party is to change the Bitcoin protocol to have an inbuilt privacy feature like Zerocash. This would truly make Bitcoin anonymous. Many ongoing experiments on achieving complete privacy are occurring on various altcoins. These groundbreaking changes should be incorporated into Bitcoin. However, a major challenge lies in convincing the Bitcoin developer community and Bitcoin users to support this move. The paper provides a great window into research and enhancing the privacy and improving the security in block-chain based currencies.

ACKNOWLEDGMENT

This work was done with the collaboration of our supervisors and advisors. This research work was carried out without any internal or external funding.

REFERENCES

[1] BONNEAU, J., MILLER, A., CLARK, J., NARAYANAN, A., KROLL, J.A., and FELTEN, E.W. (2015) SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, pp. 104–121.

[2] BARRERA, A. (2014) *A guide to bitcoin (part I): A look under the hood.* [Online] Available from: http://tech.eu/features/808/bitcoin-part-one/ [Accessed 12/03/19].

[3] EYAL, I. (2015) The miner's dilemma. *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, pp. 89–103.

[4] GERVAIS, A., KARAME, G.O., WU¨ST, K., GLYKANTZIS, V., RITZDORF, H., and CAPKUN, S. (2016) On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16.

[5] ANDROULAKI, E., KARAME, G.O., ROESCHLIN, M., SCHERER, T., and CAPKUN, S. (2013) Evaluating user privacy in bitcoin. *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 34–51.

[6] KOSBA, A., MILLER, A., SHI, E., WEN, Z., and PAPAMANTHOU, C. (2016) Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *Proceedings of the 2016 IEEE Symposium on, Security and Privacy*, pp. 839–858.

[7] GERVAIS, A., CAPKUN, S., KARAME, G.O., and GRUBER, D. (2014) On the privacy provisions of bloom filters in lightweight bitcoin clients. *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 326–335.

[8] BIRYUKOV, A., KHOVRATOVICH, D., and PUSTOGAROV, I. (2014) Deanonymisation of clients in bitcoin p2p network. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 15–29.

[9] BLOCKCHAIN (2018) *Bitcoin address.* [Online] Available from: https://blockchain.info/address/1JC6DLSJ8PEEsSXViVA8ZvPwWS55RYgMs3 [Accessed 12/03/19].

[10] BIRYUKOV, A. and PUSTOGAROV, I. (2015) Bitcoin over tor is not a good idea. *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, pp. 122–134.

[11] KOGIAS, E.K., JOVANOVIC, P., GAILLY, N., KHOFFI, I., GASSER, L., and FORD, B. (2016) Enhancing bitcoin security and performance with strong consistency via collective signing. *Proceedings of the 25th USENIX Security Symposium*, pp. 279–296.

[12] E-LEARNING SPOT (2017) *Bitcoin mixing to improve anonymity.* [Online] Available from: http://learningspot.altervista.org/bitcoin-

mixing-to-improve-anonymity/ [Accessed 15/04/19].
[13] E-LEARNING SPOT (2017) *Bitcoin decentralized mixing.* [Online] Available from: http://learningspot.altervista.org/bitcoin-decentralized-mixing/ [Accessed 15/04/19].
[14] ABDULSHAHEED, H.R., BINTI, S.A., and SADIQ, I.I. (2018) A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing. *International Journal of Pure and Applied Mathematics*, 119(18), pp. 461–486.
[15] MANGAL, A. (2019) *What Is Monero (XMR)? An In-Depth Guide to the Privacy Coin.* [Online] Available from: https://coincentral.com/what-is-monero/ [Accessed 20/05/19].
[16] SASSON, E.B., CHIESA, A., GARMAN, C., GREEN, M., MIERS, I., TROMER, E., and VIRZA, M. (2014) Zerocash: Decentralized anonymous payments from bitcoin. *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 459–474.
[17] TIWARI, A. (2017) *Everything about Tor: What is Tor? How Tor works?* [Online] Fossbytes. Available from: https://fossbytes.com/everything-tor-tor-tor-works/ [Accessed 25/06/19].
[18] MILLER, A., JUELS, A., SHI, E., PARNO, B., and KATZ, J. (2014) Permacoin: Repurposing bitcoin work for data preservation. *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 475–490.
[19] BARAZANCHI, I.A., ABDULSHAHEED, H.R., SHAWKAT, S.A., and BINTI, S.R. (2019) Identification key scheme to enhance network performance in wireless body area network. *Periodicals of Engineering and Natural Sciences*, 7(2), pp. 895–906.
[20] BDULSHAHEED, H.R., YASEEN, Z.T., and AL-BARAZANCHI, I.I. (2019) New Approach for Big Data Analysis Using Clustering Algorithms in Information. *Journal of Advanced Research in Dynamical & Control Systems*, 2(4), pp. 1194–1197.
[21] ANDRYCHOWICZ, M., DZIEMBOWSKI, S., MALINOWSKI, D., and MAZUREK, L. (2014) Secure multiparty computations on bitcoin. *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 443–458.
[22] ALRUBAYE, A.M.K. (2014) Intrusion Detection System Based on Carpenter / Grossberg Artificial Neural Network. Master Thesis. Department of Computer Science, Middle East University.

参考文

[1] BONNEAU，J.，MILLER，A.，CLARK，J.，NARAYANAN，A.，KROLL，J.A。和 FELTEN，E.W。（2015 年）索克：比特币和加密货币的研究前景和挑战。2015 年电气工程师学会安全与隐私专题研讨会论文集，第 104–121 页。
[2] BARRERA，A.（2014）比特币指南（第一部分）：深入了解。[在线]可从以下网站获得：http://tech.eu/features/808/bitcoin-part-one/ [访问时间 12/03/19]。
[3] EYAL，I。（2015）矿工的困境。2015 年电气工程师学会安全与隐私专题研讨会论文集，第 89–103 页。
[4] GERVAIS，A.，KARAME，G.O.，WUST，K.，GLYKANTZIS，V.，RITZDORF，H。和 CAPKUN，S。（2016 年），关于工作量证明区块链的安全性和性能。2016 年 ACM SIGSAC 计算机和通信安全会议论文集，第 3-16 页。
[5] E. ANDROULAKI，G.O。KARAME，M。ROESCHLIN，T。SCHERER 和 S. CAPKUN，S。（2013）评估比特币中的用户隐私。金融密码学和数据安全国际会议论文集，第 34–51 页。
[6] KOSBA，A.，MILLER，A.，SHI，E.，WEN，Z。和 PAPAMANTHOU，C。（2016 年）鹰：加密和隐私保护智能合约的区块链模型。2016 电气工程师

学会安全与隐私专题研讨会论文集，第 839–858 页。

[7] GERVAIS，A.，CAPKUN，S.，KARAME，G.O 和 GRUBER，D。（2014 年），关于轻量级比特币客户中盛开过滤器的隐私条款。第 30 届年度计算机安全应用程序会议论文集，第 326-335 页。

[8] BIRYUKOV，A.，KHOVRATOVICH，D. 和 PUSTOGAROV，I.（2014）比特币 p2p 网络中客户的匿名化。 2014 年 ACM SIGSAC 计算机和通信安全会议论文集，第 15–29 页。

[9] 区块链（2018）比特币地址。 [在线]可从以下网站获得：https://blockchain.info/address/1JC6DLSJ8PEEsSXViVA8ZvPwWS55RYgMs3 [访问日期：12/03/19]。

[10] BIRYUKOV，A。和 PUSTOGAROV，I。（2015）比特币过高并不是一个好主意。 2015 年电气工程师学会安全与隐私专题研讨会论文集，第 122–134 页。

[11] KOGIAS，E.K.，JOVANOVIC，P.，GAILLY，N.，KHOFFI，I.，GASSER，L. 和 FORD，B.（2016）通过集体签名增强比特币的安全性和性能。第 25 届 USENIX 安全研讨会论文集，第 279-296 页。

[12] 电子学习点（2017）比特币混合以提高匿名性。 [在线]可从以下网站获得：http://learningspot.altervista.org/bitcoin-mixing-to-improve-anonymity/ [访问日期 19/04/15]。

[13] 电子学习点（2017）比特币去中心化混合。 [在线]可从以下网站获得：http://learningspot.altervista.org/bitcoin-decentralized-mixing/ [访问日期：19/04/15]。

[14] H.R. ABDULSHAHEED，S.A。BINTI 和 I.I. SADIQ。 （2018）基于云计算和无线传感的智能解决方案回顾。国际纯粹数学与应用数学杂志，119（18），第 461–486 页。

[15] MANGAL，A.（2019）什么是门罗币（XMR）？隐私权硬币深度指南。 [在线]可从以下网站获得：https://coincentral.com/what-is-monero/ [19.05.20 访问]。

[16] SASSON，E.B.，CHIESA，A.，GARMAN，C.GREEN，M.，MIERS，I.，TROMER，E。和 VIRZA，M。（2014 年）零现金：分散式匿名比特币付款。 2014 年电气工程师学会安全与隐私专题研讨会论文集，第 459-474 页。

[17] TIWARI，A.（2017）关于托尔的一切：托尔是什么？托尔是如何工作的？ [在线]字节。可从以下网站获得：https：//fossbytes.com/everything-tor-tor-tor-works/ [访问时间：19/06/25]。

[18] MILLER，A.，JUELS，A.，SHI，E.，PARNO，B. 和 KATZ，J.（2014）永久币：重新利用比特币工作来保存数据。 2014 年电气工程师学会安全与隐私专题研讨会论文集，第 475–490 页。

[19] I.A. 巴拉赞奇，H.R 。ABDULSHAHEED，S.A。SHAWKAT 和 S.R. BINTI。 （2019）用于增强无线人体局域网中网络性能的识别关键方案。工程和自然科学期刊，7（2），第 895–906 页。

[20] H.R. BDULSHAHEED，Z.T 。YASEEN 和 I.I. AL-BARAZANCHI。（2019）使用信息中的聚类算法进行大数据分析的新方法。动力与控制系统高级研究杂志，2（4），第 1194-1197 页。

[21] M. ANDRYCHOWICZ，S 。DZIEMBOWSKI，D。MALINOWSKI 和 L. MAZUREK（2014）比特币的安全多方计算。 2014 年电气工程师学会安全与隐私专题研讨会论文集，第 443-458 页。

[22] ALRUBAYE，A.M.K。 （2014）基于木匠/格罗斯伯格人工神经网络的入侵检测系统。硕士论文。中东大学计算机科学系。