Privacy and Anonymity Preserving Challenges in Bit Coin Transactions

Debasish Jana

1TEOCO Software Pvt Ltd, Kolkata -700091, West Bengal

E-mail: debashjh@gmail.com

Abstract

Bitcoin emerged as decentralized peer-to-peer (P2P) cryptocurrency, not under the hood of any ascendant obligation and is completely digital not backed by any physical commodity. The ownership of the money in Bitcoin form is completely anonymous and private. To prevent double-spending, Bitcoin uses asymmetric cryptography to create ownership of funds as well as proof-of-work (PoW) for making a transaction backed by P2P storage of transaction log in the form of distributed append-only public ledger called blockchain. Every transaction is digitally signed using public key cryptography and is irreversible and secure. Bitcoin transactions have to rely on global peer-to-peer network of participants who help to validate and certify each transaction in a decentralized system. The participating peers acting as miners certify validity of transaction by proving the ownership of the fund from the blockchain. If endorsed, it now completes new data block to add to the blockchain. This new data block includes information about addressees of sender and receiver, amount of transfer and transaction timestamp. The drive of Bitcoin cryptocurrency is to provide anonymity of the user and having no financial authority controlling the transactions. While the transactional flow of Bitcoin is globally visible, there lie critical challenges to preserve privacy of the owner in anonymous transaction. In this paper, we explore the issues and challenges of preserving anonymity and privacy of the owner involved in Bitcoin cryptocurrency transactions. We attempt to analyze the motivation of Bitcoin in digital economy and risks and challenges in such transactions in a global scale.

Key Words: Bitcoin, Cryptocurrency, Anonymity, Privacy, P2P.

1 Introduction

In ancient days, there was no concept of cash or currency. Bartering used to be the system of symbiotic relationship based on direct exchange of services or resources for mutual advantages. Things in possession as surplus used to be offered or demanded as exchange to one having some other things lacking (Davies and Glyn, 2010). This could be for services as well, i.e. offering of services in lieu of things or vice versa. For example, grain, vegetable,
cattle, sheep, spices, weapons and what not used to be early form of barter. However, the inherent drawback of bartering was confined within the legitimate trustworthiness and quality of the thing or service being exchanged in a presumably fair deal. Later, precious metals like gold, silver and metal money in terms of minted coins and paper currency evolved in different geography leading to the need to establishing exchange rates of currencies or allied as set forth by relevant authorities. Concept of credit card and later digital way of paying through online banking and mobile banking got evolved. In lieu of physical currency, digital payment emerged as methods of purchase of goods or services using electronic payment with computers, smartphones or digital wallets. But this involves transaction using money from the bank account either as debit or credit basis. In addition to card payment network like Visa, Mastercard etc., several online payment systems like Paypal, WebMoney, Amazon Pay, Google Checkout support online payment for services or goods standing as an electronic substitute to conventional paper payment methods e.g. cheques and money orders. Transactions made in these electronic payment mechanisms are connected to some physical currency denominations (e.g. Indian Rupee, Euro, US Dollars etc) with explicit identity of the owner and recipient of the transaction and also somewhat under control of some financial regularities. Digital form of currency involves storage in only digital form and no physical form. This includes cyber cash, crypto currencies. Unlike physical currencies which get regulated usually by centralized reserve bank of the country or some other financial regulatory authority, digital currency may get controlled by some Central Bank Digital Currency (CBDC) or could be unregulated as well. Cryptographic technique is the backbone of handling cryptocurrency, be its creation or its transaction. Bitcoin(Grinberg and Reuben,2012) [3] is such form of unregulated decentralized peer-to-peer (P2P) cryptocurrency, completely digital, not owned or backed by any government or other legal authority and non-redeemable against gold or any other form. One can purchase Bitcoins at online exchanges dealing cryptocurrency or one may receive them through mining process as a reward of service rendered. Bitcoin transactions for electronic payment are cryptographically secure and use virtual currency as digital tokens called Bitcoin coins or bitcoins or BTC. In Bitcoin based transaction, the owner has complete control over the bitcoins for anytime anywhere spending not involving any centralized authority in control. The impetus of Bitcoin cryptocurrency is to conceal the real identity of the user thereby protecting privacy and to provide anonymity of the owner without any back tracing. The transactions using bitcoins are also not controlled by any financial authority controlling the transactions. While the transactional flow of Bitcoin is globally visible and available as transactional log, critical challenges may exist to preserve privacy of the owner in anonymous transaction. In this paper, we explore the issues and challenges of owner privacy and anonymity preservation while analyzing the motivation of Bitcoin in digital economy and risks and challenges in such transactions in a global scale. This paper is organized into four sections. In following part, we present the working principle of Bitcoin as a decentralized distributed digital cryptocurrency. In section three, we enumerate few identified privacy and anonymity issues and challenges. Finally, the conclusion and way forward are narrated.
2 The Working Principle Of Bitcoin

Since its first deployment in 2009, popularity of Bitcoin became widespread. Satoshi Nakamato [4], either as an individual or as a group under the penname, founder of Bitcoin as well as initial creator of the original Bitcoin client [5], remained active till late 2010. After that identity of Nakamoto is still under speculative search without any success therein, and the project has been handed over. Bitcoin Core [6], written in C++, is available as open source software that supports the use of this bitcoin currency. (Tschorsch and Scheuermann, 2016) narrate an extensive technical assessment on Bitcoin and its associated technologies. The authors present the technical background with implementation details of Bitcoin and discuss the consequences of the core design decisions for Bitcoin protocol and its building blocks. Bitcoin uses public-key-cryptography that uses combination of public and private key. The user of the Bitcoin in direct possession of the private key is having no counterparty risk of losing it as long as the private key is kept secret. Being decentralized, there is no central minting process for bitcoins. While making a transaction using Bitcoin, the owner triggers the transaction after putting recipient address and then signing with the private key thus securing the address to provide ownership of fund used in transaction. The fresh transaction along with the transaction history gets broadcast over P2P network, attempting to prove that transaction owner has bitcoins. Each P2P network node or peer maintains transaction history for every transaction stored as a distributed publicly available append-only ledger called the blockchain. Through repeated broadcasting, eventually, the transaction reaches a miner. The miner then tries to find out the right nonce balance to hit target hash. The peers (or miners) thus validate validity of transaction by proving the ownership of the fund from the blockchain. If validated, it now completes new data block to add to the blockchain. This new data block includes information about addressees of sender and receiver, amount of transfer and transaction timestamp. All data stored inside each transactional block chained within blockchain remain hashed, the hash with some leading zeroes. A unique non-duplicating nonce is also kept at each block. The validation process involves finding a nonce allowing the block to have correctly formatted hash. In total, there could be 21 million of bitcoins, by design. New bitcoins are awarded by the system to appropriate cryptocurrency miners for each block on successful mining. The Bitcoin block mining reward gets halved every 210,000 blocks, and the BTC coin reward decreases from 12.5 to 6.25 coins, and is expected to halve again in 2016, and eventually drop to 0 in 2140. 1 Bitcoin equals to USD 6,388.46 or INR 4,68,625.48 as on 26 Oct, 2018 4:49 AM UTC. Let’s explore the Bitcoin mining process. Bitcoin mining task aids in appending fresher transaction records to Bitcoin's blockchain, distributed public ledger of earlier transactions. The Mining Algorithm takes the following form:
(1) The hash is reclaimed for the previous block from the P2P network.
(2) A list of potential transactions (block) is congregated as available in the P2P bitcoin network.
(3) A hash is computed for a block of potential transactions along with a randomly generated cryptographic nonce.
(4) If the hash is more than the currently set difficulty level, then mining the block is complete. Otherwise, steps are repeated from step 1. Any add-ons to transaction list from step 1 along with change in cryptographic nonce from step 2 mean that there lies a chance that the criterion will be met in the next go around.

The hash of the earlier block is also hashed along with the list of transactions. The bitcoin mining uses SHA256 applied twice. As the number of probabilistic hashes per unit time (say, second) across the entire P2P network increases, the difficulty level is automatically raised so that the solving for the solution takes more time. When a transaction block is successfully mined, the miner transmits the transaction block to all other miners in the P2P network as proof that it could found it. This block contains a list of earlier transactions, the found hash, the specific nonce, and a reference to the earlier hash. As each miner gets the newly mined block, it removes all mine-in-progress transactions and propagates the block to other miners to do the same. The original miner receives a reward. Sender and receiver addresses could be one or more each, as funds may be splitted during transaction, to choose as multiple sender addresses and multiple receiver addresses. Once added to the blockchain, this cannot be further altered or tampered, and is irreversible. In summary, Bitcoin, by itself, does not have any intrinsic value, but gains value dynamically through demand in a highly secured way (Kaplanov and Nikolei, 2012). The miners also gain their value through transaction fees as newly generated bitcoins. The motivation of Bitcoin cryptocurrency is to provide anonymity of the user and having no financial authority controlling the transactions. For example, when we store our money in banking system, we are governed by the rules and regulations of the banking system of our country. Therefore, this is subject to any change brought to the system by the authorities that may not be aligned to our best interest. To prevent double-spending, Bitcoin uses asymmetric cryptography to create ownership of funds as well as proof-of-work (PoW) [9]. By double spending, we mean that even after transferring a bitcoin, the user has re-attempted to make another transfer using same bitcoin. P2P participating nodes are aware of all transactions made. Transactions are stored as blockchain as chain of blocks, each block chained with the previous block with respect to timestamp of the transaction made. This blockchain remains publicly available to every participating node within the P2P network. Transaction blocks being chained into previously validated transactional chains, reinforces validity of the entire transaction chain. This process of Bitcoin transactions are anonymous or more specifically, pseudo-anonymous as Bitcoin transactions do not keep explicit identity of the payer or the payee. Users may keep multiple virtual addresses which may not map to physical one, unless user keeps the actual physical address as virtual identity.
3 Privacy And Anonymity Issues And Challenges

The conventional banking system provides access to transaction information only to the relevant account holders and select authorities or government agencies as trusted third party thereby protecting the privacy of the banking users. In Bitcoin, the blockchain stores all the transactional data and being available in P2P network publicly could theoretically reveal all the information related to transaction virtually to any user. The privacy is preserved to certain extent by breaking the flow of information somewhere in the processing chain. Bitcoin attains it by keeping anonymous public keys, thus anyone can see that an amount is being sent by someone to someone else, but with no information linked to the transaction. (Dupont and Squicciarini ,2015) have demonstrated methods of gathering information of users transacting Bitcoin by analyzing data about cryptocurrency spending habits available in public domain. This could be a potential drawback of the system having functioning of the Bitcoin network. (Dupont and Squicciarini ,2015) chose multiple addresses used in one or more transactions having common address used as common owner and analyzed the transaction times during a day and made an educated guess about user's residence time zone, thus probabilistically predicting physical address from extracted significant information in the pseudonymous blockchain. (Meiklejohn et al.,2013) examined the gap between actual and potential anonymity in Bitcoin transaction. Bitcoin protocol ensures that no physical identity of the actors participating in a transaction, the payer and the payee, be identified. Bitcoin blockchain is however available in public domain across P2P networks as a transactional graph data structure encoding all Bitcoin activity.

(Conti et al.,2018) presented an orderly assessment of Bitcoin security and privacy aspects. Some potential risks and challenges are enumerated below.

- **Double spending problem**: In general, a double spend is characterized by two different transactions in quick sequence where same set of bitcoins are attempted to be spent simultaneously, without being detected. Notwithstanding the use of stringent transaction ordering in blockchain, proof-of-work (PoW) scheme, time-stamping in distributed manner and consensus or agreement protocol, double spending attack is possible. This could be of the following types:
  - **Finney Attack**: Finney Attack [13] is a deceitful double-spend that needs the involvement of a miner after a block has been mined. To cheat, when a block is generated, it is not broadcast. Instead, the store site is opened to make payment. The store, waiting a few seconds for suspected double-spends, and not hearing anything, transfers the goods. The lock is now broadcast and the transaction may take precedence over.
Brute-force Attack: Brute-force attack [14] in which a capable attacker takes control over some nodes in the network, and these nodes together work on a private mining scheme privately mining to perform double spending.

Balance Attack: Balance Attack (Natoli,2015) is delaying network communications between multiple subgroups of miners with balanced hash power, thereby allowing to perform double spending.

Mining Pool Attacks: Mining pools increase the overall computing power improving the verification time of a block, thereby increases chance of success followed by reward.

Selfish Mining: Selfish Mining (Eyal,2018) dishonestly tries to hide information by discarding blocks [17] in an unfair way to claim the reward.

Fork After Withholding: Fork After Withholding (Kwon et al.,2017) attacks with two mining pools executing, the larger pool can consistently win.

Bribery Attack: Bribery Attack (Bonneau,2016) enables an attacker to bribe other miners and obtain the majority of computing resources for a short duration thus becoming computationally powerful to act fast and also mine on other miner’s behalf.

Client-side Security Threats: Each Bitcoin client owns a set of keys (to use in public-private key combination) to access wallet. However, if the key gets stolen or compromised, the client suffers.

Wallet Theft: The adversary nodes stole or destroyed private key of users

Installation of Buggy Software: This is potential dangerous where buggy software may produce or verify transactions in a faulty way.

Incorrect Usage: Incorrect usage of underlying resources could make the client side compromised.

Bitcoin Network attacks: Existing weaknesses in the design and implementation of the protocols may get the nodes compromised.

Code Vulnerability: Wrong code could inject weakness in implementation that could induce misbehavior of the system.

Distributed Denial of Service (DDOS): Malevolent miners may perform a DDoS on competing miners, effectively putting them out of the P2P network and increasing the mischievous miners effective hash rate.

Sybil Attack: attacker tries to compromise a part of the P2P network.

Eclipse Attack: Eclipse attack (Nayak, et.al,2016; Heilman,2015) is when an attacker principally taking control of the P2P network, concealing a node’s view of the public ledger i.e. blockchain.

Tampering: Adversary could bring delays in the packets being broadcast by presenting network congestion or making a victim node busy by distributing requests to all its ports.

Wanna Cry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. The malware locked the computer and demanded money payable
in Bitcoin in order to unlock. Despite the swiftness in slowing the attack, the attackers received thousands of dollars in Bitcoin. Wallet privacy could be leaked (Barcelo, 2014). This wallet leakage could be exploited by the fraudulent nodes. At the time of broadcasting the transaction, an attacker may deduce that all the inputs of the transaction and their associated addresses belong to the same user. Herrera-Joancomartí, and Pérez-Solà (Herrera-Joancomartí, and Pérez-Solà, 2016) presented a comprehensive description of the most pertinent scalability solutions proposed for the bitcoin network and the impact on users’ privacy. By analyzing traffic, the anonymity degree of users is restricted by the underlying technologies used. Bitcoin transactions get transmitted over a P2P network, so the TCP/IP information retrieved could be used to reduce the anonymity of the system, (Krombholz et al, 2016) presented a survey to investigate how users experience Bitcoin ecosystem in terms of security, privacy and anonymity. If a client in the P2P network finds a combination of valid transactions and nonce that could produce a desired result, he/she publishes this new block in the Bitcoin network and gets rewarded with newly created bitcoins. In the process, several users have already experienced security breaches and lost bitcoins (Krombholz et al., 2016)

4 Conclusion And Way Forward

Bitcoin is the first ever decentralized virtual cryptocurrency, completely digital in form to establish as medium of electronic payment system built on cryptographic proof as opposed to trust. No centralized financial institution or authority is managing the governance. Bitcoins are transmitted and received using P2P bitcoin network without any intermediaries. Bitcoin transactions are entries in the globally available transactions blocks in the ledger book or blockchain. Until proof of work is solved, new transactions are not logged in blockchain. All bitcoin transfer is protected through digital signature using secured public key cryptographic protection. No governmental authority can print or generate more bitcoins but the exchange rates may face radical fluctuations. Since the transactions are based on P2P network, the overall global transaction cost is low. There exist issues and challenges in terms of anonymity and privacy that need to be addressed through on-going research and more extensive study in this emerging and interesting area of digital currency system.

Reference


Jana: Privacy and Anonymity Preserving Challenges …


