© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Bitcoin Wallet Transaction using Peer-to-Peer Network

M. Jancy Priya, R. Sathya
Assistant Professor, Department of Computer Applications, Bon Secours College for Women, Thanjavur, Tamilnadu, India

ABSTRACT

A peer–to-peer allows online payments that sent directly from one party to another party without going through the financial institution. Digital signature is a part but the main benefit is lost, if a Trusted Third Party is still required to prevent digital signature. This digital signature uses peer–to-peer network. The network timestamps transaction by hashing them into an on-going chain of hash-based proof-of-work is done; it records that and cannot be changed without redoing the proof-of-work. The majority of CPU work is controlled by nodes. That are not cooperating to attack the network, they will generate the longest chain and outspace attackers.

Keywords : Trusted Third Party, Timestamps Transaction, Proof-of-work and Bitcoin.

I. INTRODUCTION

Bitcoin concept was released in January 2009 for transacting digital currency between two parties. Bitcoin are computer files, similar to a text file, and can be destroyed or lost just like cash. It is stored either on a personal computer or entrusted to an online service. Bitcoin is just a process of sending them from one user to another, like sending an email via the Internet.It is logged by a decentralized network that runs on thousands of computer and recorded in a public ledger. Bitcoin is an individual transaction which is encrypted. Bitcoin is of two kinds, first it is a digital currency meaning that the unit of account it employs has no physical counterpart with legal tender status. Second, Bitcoin is a "private currency"(according to Friedrich A. Hayek) It is a currency provided by private enterprise aimed at combatting government controls on the supply of money.[4] Bitcoin is a crypto currency that has recently emerged as a popular medium of exchange, with a rich and extensive ecosystem. The Bitcoin network runs at over42×10^{18} FLOPS, with a total market capitalization around 1.5 billion USDollars as of October 2013.

II. DIGITAL CURRENCY

Nowadays people switch to digital currency instead of carrying paper bills and metal coins. The growth of digital currency is now increasing by computerized and complex digital economy. Recently digital currency is said to be "bitcoin". It is a private digital currency operated on online via a peer-to-peer network. Currency serves three primary functions. First, it serves as a medium of exchange.Second, it acts as a unit of account and a measure of relative worth.Third, currency acts as a store of value of current earnings for future spending.Digital currencies like bitcoin have the potential to perform each of these roles more efficiently than traditional authorisation currencies. [4]

III. THE BITCOIN ENVIRONMENT

Bitcoin concept was released in January 2009 for transacting digital currency between two parties. First user was technophilesthey were attracted by a high-tech project that combined peer-to-peer network technology and cryptography. More importantly, they liked the idea of earning money by building specialized mining computers, known as "rigs." Along with attracting technophiles, Bitcoin has caught the imagination of assorted "gold bugs" that share Ron Paul's loathing of the Federal Reserve and are attracted by the anonymity of bitcoin transactions.

IV. BITCOIN CLIENT

Bitcoin clients are the base level of technology for conducting Bitcoin transactions, and they store the keys needed to conduct a Bitcoin transaction. They come in multiple flavors, and are customized to fit different niches.

The Bitcoin-QT Client is the original software written by Satoshi Nakamoto, the project's founder. If user is not sure which program to pick, this is a good bet. It is suited for enthusiasts, merchants, miners, developers and people who want to help support the project.

The MultiBit Client is fast and easy to use, even for people with no technical knowledge. It is also able to import Blockchain.info's wallet backups (Multibit version 5.17 and earlier), making it a versatile tool for all kinds of users.

The Electrum Client focuses at speed, with low resource usage and simplifying Bitcoin usage. Startup times are instant because it operates in conjunction with high-performance servers that handle the most complicated parts of the Bitcoin system.

Blockchain.info is also a form of Bitcoin client. We provide a web-based client with emphasis on speed, security, and ease of use.[5]

V. Comparative study of Bitcoin

An in-depth investigation of Bitcoin, we found that although Bitcoin uses nofancy cryptography, its design actually reflects a surprising amount of originality and complexity. Most importantly, it addresses the problem cause. Bitcoin has a completely distributed architecture, without any single trusted entity. Bitcoin assumes that the majority of nodes in its network are honest, and resorts to a majority vote mechanism for double spending avoidance, and dispute resolution. Bitcoin transactions quickly become irreversible. This attracts a niche market where vendors are concerned about credit-card fraud and chargebacks. Through personal communication with a vendor selling specialty magazines, hementioned that before, he could not conduct business with customers in certain countrieswhere credit-card fraud prevails. With Bitcoin, he is able to extend his business to these countries due to the protection he obtains from the irreversibility of transactions.

Another salient and very innovative feature is allowing users to embed scripts in their Bitcoin transactions. Although today's reference implementations have not fully utilized the power of this feature, in theory, one can realize rich transactional semantics and contracts through scripts. The Bitcoin verifiers' market currently bears very low transaction fees (which are optional and chosen by the payer); this can be attractive in micropayments where fees can dominate. Bitcoin is also appealing for its lack of additional costs traditionally tacked upon international money transfers, due to disintermediation. And also, in comparison with other e-cash schemes, Bitcoin has provided readily available implementations, not only for the desktop computer, but also for mobile phones**.**

VI. Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm or ECDSA is a cryptographic algorithm used by Bitcoin to ensure that funds can only be spent by their rightful owners.

A few concepts related to ECDSA:

- Private key: In Bitcoin, someone with the private key that corresponds to funds on the public ledger can spend the funds. In Bitcoin, a private key is a single unsigned 256 bit integer (32 bytes).
- Public key: A number that corresponds to a private key, but does not need to be kept secret. A public key can be calculated from a private key, but not vice versa. A public key can be used to determine if a signature is genuine (in other words, produced with the proper key) without requiring the private key to be divulged. In Bitcoin, public key are either compressed or uncompressed. Compressed public keys are 33 bytes, consisting of a prefix either 0x02 or 0x03, and a 256-bit integer called x. The older uncompressed keys are 65 bytes, consisting of constant prefix (0x04), followed by two 256-bit integers called x and y (2 * 32 bytes). The prefix of a compressed key allows for the y value to be derived from the x value.
- Signature: A number that proves that a signing operation took place. A signature is mathematically generated from a hash of something to be signed, plus a private key. The signature itself is two numbers known as r and s. With the public key, a mathematical algorithm can be used on the signature to determine that it was originally produced from the hash and the private key, without needing to know the private key. Signatures are either 73, 72, or 71

bytes long, with probabilities approximately 25%, 50% and 25% respectively, although sizes even smaller than that are possible with exponentially decreasing probability.[6]

Conversion from ECDSA public key to Bitcoin Address

A Bitcoin address is a 160-bit hash of the public portion of a public/private ECDSA key pair. Using public-key cryptography, user can "sign" data with their private key and anyone who knows their public key can verify that the signature is valid.

A new key pair is generated for each receiving address (with newer HD wallets, this is done deterministically). The public key and their associated private keys (or the seed needed to generate them) are stored in the wallet data file. This is the only file users should need to backup. A "send" transaction to a specific Bitcoin address requires that the corresponding wallet knows the private key implementing it. This has the implication that if user create an address and receive coins to that address, then restore the wallet from an earlier backup, before the address was generated, then the coins received with that address are lost; this is not an issue for HD wallets where all addresses are generated from a single seed. Addresses are added to an address key pool prior to being used for receiving coins. If you lose your wallet entirely, all of your coins are lost and can never be recovered.

Bitcoin allows you to create as many addresses as you want, and use a new one for every transaction. There is no "master address": the "Your Bitcoin address" area in some wallet UIs has no special importance. It's only there for your convenience, and it should change automatically when used.

Bitcoin addresses contain a built-in check code, so it's generally not possible to send Bitcoins to a mistyped address. However, if the address is well-formed but no one owns it (or the owner lost their wallet.dat), any coins sent to that address will be lost forever.

Hash values and the checksum data are converted to an alpha-numeric representation using a custom scheme: the Base58Check encoding scheme. Under Base58Check, addresses can contain all alphanumeric characters except 0, O, I, and l. Normal addresses currently always start with 1 (addresses from script hashes use 3), though this might change in a future version. Test net addresses usually start with m or n. Mainline addresses can be 25-34 characters in length, and test net addresses can be 26-34 characters in length. Most addresses are 33 or 34 characters long. [8]

VII. PROCESS OF BITCOIN WALLET

Bitcoins are transferred from one user to another once the transaction has been cleared by another Bitcoin user on the peer-to-peer Bitcoin network.[4] Bitcoin relies on peer-to-peer networking. That is, instead of being linked through a central server,each Bitcoin program located on an individual's PC is linked to other Bitcoin programs, which in turn are linked to still other Bitcoin programs. And each PC contains a copy of the account ledger that registers transactions in the system.[8] Transactions occur without the presence of a government, bank, payment network, regulator, or other third party entity.[4]

Bitcoin is a distributed currency which has attracted a number of users. There are several issues and attacks of bitcoin, and proposed suitable technique to address them. Instead of trusted thirty party bitcoin wallet software fetches the entire bitcoin block chain at installation, and all new transactions and blocks are broadcast to all nodes. This scalability issue in terms protect network bandwidth and computational overhead with cryptographic transaction verification. Bitcoin nodes are divided into two classes. They are verifiers and clients. Verifiers create new blocks and hence mint new coins. Clients to spend coins and that they receive transaction payable to their public keywords.

VIII. DIGITAL CURRENCY WITH REAL-WORLD VALUE

Unlike some digital currencies, Bitcoin use is not tied to a particular product or service. Bitcoins can be used to pay for various online services like Web hosting, mobile app development, and cloud file storage. These can also buy products like games, music, gift cards, and books. Unlike most digital currencies, too, Bitcoins have real world value, as some brick-and-mortar establishments

accept them as payment for various goods. These can also be traded for traditional currency. In fact, several sites offer most international currencies in exchange for Bitcoins, each of which is currently worth around US$5.

The growing awareness and recognition of Bitcoin as a legitimate currency, not to mention having real-world value, are seemingly spurring cybercriminal interest.

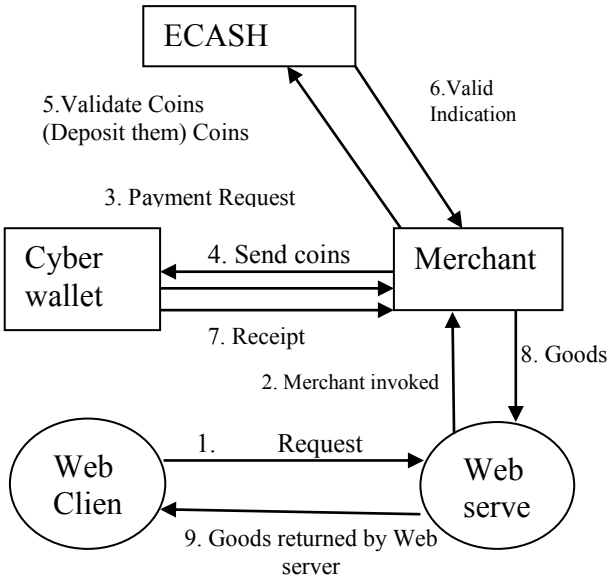
Like any other activity, Bitcoin mining, however rewarding, can take its toll on one's computing hardware. Cybercriminals, crafty as they usually are, have thus decided to remedy this setback by delegating the hard work—the mining process—to unsuspecting users. They have taken to creating Bitcoin miners in order to mine blocks without their victims' knowledge. Once processed, they then take the Bitcoins generated from their unwitting miners' systems. All that's left for cybercriminals to do is to harvest what the users have sown.

IX. BITCOIN WALLET TRANSACTION

If user wish to use bitcoin wallet software for transaction the wallet should have the public and private address. Anyone can send the bitcoin to wallet, the owner of the wallet will have the public address, where private must be entered by the wallet owner to send bitcoins. Wallet security secure and protect the private address. Wallet allows, user to complete transaction between address by requesting an update to the blockchain. This can be in variety of forms that is, mobile device, computer, hardware device and paper token.

How it works

In many ways, a Bitcoin account is like an online bank account. In both, deposits are stored in the form of electronic ledger entries, and payments consist of orders to credit one account at the expense of another. But there are crucial differences. Bitcoin relies on peer-to-peer networking. That is, insteadof being linked through a central server, each Bitcoin program located on an individual's PC is linked to other Bitcoin programs, which in turn are linked to still other Bitcoin programs. And each PC contains a copy of the account ledger that registers transactions in the system. Cleared transactions are quickly and automatically communicated to other Bitcoin programs. This decentralization helps the system evade effective attacks by hackers, because penetrating even a large number of Bitcoin programs would have little effect on the network as a whole. Note, moreover, that it also allows individuals to send money directlyto one another without the help of a bank. A peer-to-peer financial network is still potentially vulnerable to thieves and vandals who transmit bogus transactions and bogus copies of the accounts. Nakamoto'sbreakthroughwas to figure out a way to mimic many of the controls of a traditional financialsystem without enlisting banks or government regulators. It's built around "mining" –the process that creates and distributes new bitcoins. Each successfulsolution contains a copy of the most recent transactions made though Bitcoin and becomes part of the freshly balanced ledger account that is distributed across the network.



Left with Nothing but Loss

What's the worst that can happen to Bitcoin-mining victims? Users of Bitcoin-miner-infected systems suffer most from computing resource abuse. Their systems sustain increased wear and tear. Since Bitcoin mining uses up a lot of processing power, an infected system can become abnormally sluggish, particularly if the victim uses graphics-intensive applications.

While the cybercriminals do not currently target specific individuals, gamers may especially feel the brunt of involuntary Bitcoin mining, as they are the most common users of computers with highly capable GPUs.

What Can Users Do?

All is not lost, however, as adhering to sound safe computing habits like the following can keep Bitcoin miners at haven:

Never download and install applications from unknown sites. Think twice about clicking shortened links on *Twitter* or any other site for that matter, regardless of source. Remember that URL shortening makes it hard to determine a link's legitimacy. If your system suddenly slows down, check it for clues of Bitcoin mining such as an unexplained increase in processing power usage.

X. FUTURE TREND OF BITCOIN

Today, there are about 7.5 million bitcoins in existence and 50 bitcoins are awarded every 10 minutes or so. By 2030, the number of bitcoins will approach the absolute maximum, 21 million. No individual or managementcommittee has the power to change this.[8]

XI. Conclusion

This paper focuses on the financial institution that serves via third trusted party to process electronic payments. The transaction still suffers from the weakness of the trust based model. . The cost and payments can be avoided in person by using physical currency, but no mechanism is made for payment over communication channel without a trusted party.Here, the concept is to solve the double-spending problem using peer to peer distributed time stamp server. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attracter nodes. We have provided a preliminary about the study of bitcoin wallet transaction phenomenon. So this payment system will allow the web to be used as electronic market place without compromising the privacy of the users. The number of bitcoins awarded for each puzzle solution is halved every four years. Today, there are about 7.5 million bitcoins in existence and 50 bitcoins are awarded every 10 minutes or so. By 2030, the numberofbitcoins will approach the absolute maximum, 21 million. No individual or management committee has the power to change this.

XII. REFERENCES

[1]. Barber, Simon; Boyen, Xavier; Shi, Elaine and Uzun, Esrin (2012). "Bitter to Better — how to make Bitcoin a better currency".Financial Cryptography and Data Security. Lecture Notes in Computer Science (Springer) 7397: 399. doi:10.1007/978-3-642-32946-3_29. ISBN 978-3-642-32945-6.

[2]. Satoshi Nakamoto(2009)"Bitcoin: A Peer-to-Peer Electronic Cash System".

[3]. Dorit Ron and AdiShamir(2012) "Quantitative Analysis of the Full Bitcoin Transaction Graph".

[4]. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: Financial Cryptography. (2013)

[5]. Andresen, G.: March 2013 chain fork post-mortem. BIP 50, https://en.bitcoin.it/wiki/BIP_50, retrieved Sep. 2013

[6]. Namecoin Project: Namecoindns, dotbit project. https://dot-bit.org, retrieved Sep. 2013

[7]. King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake(2012)

[8]. Charts, B.: Bitcoin network. http://bitcoincharts.com/bitcoin/, retrieved Nov. 2013

[9]. https://bitcointalk.org/index.php?topic=31038.0;wap2

[10]. https://bitcointalk.org/index.php?topic=645.0

[11]. Bitcoin wiki: Contracts. en.bitcoin.it/ wiki/Contracts