RESEARCH ARTICLE OPEN ACCESS

Open Source Software a Study on BITCOIN

Kunwar Uday Singh [1], Harshit Sinha [2], Dr. Ajay S. Singh [3], Thirunavukkarasu K [4]
2 Year B.Tech (CSE-IBM OSS) [1] & [2]
Department of Computer Science and Engineering
Professor [3], Assistant Professor [4]
School of Computing Science & Engineering, Galgotias University
Uttar Pradesh – India

ABSTRACT

Bitcoin is a peer-to-peer data transfer system facilitating monetary transactions between the participants without any interference from a third party of any kind. An example of such a party would be banks which act as moderators in transactions and transfers between customers be it their own or other banks. The bank would have all the details and specifics of the transactions. Bitcoin remove the reliance on such an entity completely. The transactions are solely the matter of the parties involved and no one else. The problem of double spending persists in the concept of bitcoin; here we shall propose possible solution to the problem. Digital signatures, timestamps, proof of work and publication of the transactions could provide a solution to double spending. With reasonable system requirements and an easily understandable concept, bitcoin could possibly provide hassle free trading for the participants.

Keywords:- BITCOIN

I. INTRODUCTION

.

The traditional method of banking dominates the electronic commerce landscape wherein the participating members have to trust the banks for resolving disputes and irregularities. Bitcoin at least in concept could provide easy conflict resolution for the parties, without the need for reliance on financial institutions. This could easily cut transaction costs and cut down fraudulent transactions. Introducing a proof based system instead of a trust based one is the next logical evolution in the financial landscape.

What is required is an electronic payment system based on a logical stored proof instead of trust, allowing any two people to do transactions directly with each other without depending on any third party vendor. Transactions which are not possible to reverse will provide sellers the protection from any kind of fraudulent. In this paper, we provide a solution to the double-spending problem with the help of time stamping server between each peer –to-peer which can generate a logical proof of the information of order of transactions. There is more security available in the system as long as honest nodes mutually control more CPU power than any cooperating group of attacker nodes.

II. BITCOIN OVERVIEW

2.1 Volatility in price

Due to presence of new economy, novel nature and illiquency in markets there is lot of variation in price which can increase or decrease in small period of time. Therefore, due to current trend it is recommended that we should right now utilize bitcoin for keeping the savings. It should be considered right now as high risk asset. Thus storing money which we cannot afford to lose should not be stored in Bitcoin. There can be easy conversion of Bitcoin into the local currency by the service providers.

2.2 Irreversibility in Payments

While performing transaction there is no concept of roll back of transaction .Refund can only be done by the person who receives the payment. Thus there should be prior knowledge of person with whom we are doing transaction and they have a reputation that we can trust. For their part, businesses need to keep control of the payment requests they are displaying to their customers. There is facility of detection of typological errors and usually won't let us transfer money to an unacceptable address by blooper. There can be more development in the Bitcoin in the

security and protection areas.

2.3 Experimentation is Active

There is still development occurring in this field of new currency. Each improvement makes Bitcoin more appealing but also reveals new challenges as Bitcoin adoption grows. There might be occurrence of several problems which might include increase in fees, slow confirmations, and many more.

There should be clear mind to face the issues and thus consultation to technical experts is advised prior to making any main expenditure. But, still the future of Bitcoin is unpredictable.

III. REQUIREMENT SPECIFICATION

Hardware requirement Disk space: 80 GB

Download: 250 MB/day (8 GB/month) **Upload**: 5 GB/day (150 GB/month)
Memory (RAM):256 MB

System Requirement
Desktop, Laptop
Some ARM chipsets >1 GHz

Operating system
Windows 7/8.x
Mac OS X
Linux

IV. PROBLEM STATEMENT

Bitcoin suffers from the problem of double spending wherein the payer x could send the same coins to two parties y and z. There is no way for either of the two payees to verify the authenticity of the coin.

A solution could be to introduce a mint or a moderator to ensure that the same come cannot be reused by issuing new coin for the used one. But this would bear close resemblance to the bank system as whoever controls the mint controls the entire bitcoin system.

A modified form of the system would make sure that the legitimate transaction of all the double spending would be the one which arrived first. A proof for the transaction could be then recorded in the history where all transactions are recorded thereby maintaining the authenticity and integrity of the coin.

There is a requirement of a solution such that the payee has knowledge that the earlier transactions are not being signed by the previous owners.

For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. For the confirmation, of no presence of transaction, we need to be aware of all transactions that took place prior to that transaction.

V. PROPOSED SOLUTION TO SECURUTY ISSUES

Time-stamping could be the solution to the problem of double spending. It will work by adding a digital timestamp to the block chain and then publishing the transactions to a publication such as a newspaper on an online news post.

This could help to verify transaction authenticity and keep proper records so as to not weaken the value of a bitcoin. Each timestamp will add a digital signature at the end of a bitcoin. The longest chain with the most processing power would be the only legitimate chain of transactions. Network nodes of 1.25 GB per year, there is no problem in storing with low CPU power will be disregarded. Even a complete hash block in the memory.

VI. NETWORK BLUEPRINT

Generally, the longest chain is believed as the correct one by the nodes. If more than one node broadcast altered versions of the next block concurrently, some nodes might receive one or the other first. In such scenario, other branch is being saved if it is longer and the works on first one which they received.

When a longer one branch, is found the tie can be easily broken; the nodes will switch to longer branch rather than working on other branches.

New transaction broadcasts do not necessarily need to reach all nodes. Until, they are able to reach more than one nodes, they will be able to pass through inside the block in short span of time.

Even the block broadcasts are able to handle the

messages which are being dropped.

When a node receives another block, it is able to determine whether it received a previous block or not, and thus on if it misses one then, requests for one.

VII. MEMORY ALLOCATION AND DEALLOCATION

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. There is a utilization of Merkel Tree in order to accelerate this such that there is no breaking in the block`s hash, and storage of only the root in the block`s hash. Knocking off branches of the tree can be done in order to compact old blocks. There is no requirement of storage of internal block. A transaction less block header is of size around 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With rapid increase in storage memory and primary memory of computers since 2008, and the prediction of Moore`s Law suggesting the growth of memory

VIII. SECURE PAYMENT VERIFICATION

In order to verify the payment, there is no need of execution of complete nodes of network, it can be effortlessly completed. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's time-stamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the vulnerability exists under the attacker influence. The more reliability exists in verification only if honest nodes control the network. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency.

Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

IX. PRIVACY

The conventional banks have their model which acquires the concept of privacy by barricading the access to information and also the involvement of third party vendor. Although the transactions occur in public, but then too there is a concept of privacy by keeping the public key anonymous. Anyone can see that there is a transaction taking place between two parties, but without information linking the transaction to anyone. This type of transaction resembles to amount of information which is being released by the stock exchanges, where the size and time are being available in public but there is no information about the parties which are trading.

X. ACKNOWLEDGMENT

We thank our colleagues from Galgotias University who provided assistance with their expertise and insist.

We thank Prof. Thirunavukkarasu K for assistance with particular technique and methodology of Bitcoin Currency, also for sharing their pearls of wisdom with us during the course of this research and Dr. Ajay Shanker Singh H.O.D IBM, Galgotias University for comments that greatly improved the manuscript.

XI. CONCLUSION

We have suggested an effective solution to the problems plaguing the bitcoin. The time-stamping of transaction, publishing it, using effective crypto graphical techniques and using a valid proof of work through nodes that have consumed the most CPU and have the longest chain help to weed out the fraudulent transactions.

Bitcoin can thus evolve the e-commercial landscape removing middlemen in business processes. It will cut down on fraud, pointless transaction fees and the hardware requirements for setting a node are very lenient and not very hardware heavy in this day and age. There is no requirement of identification of

nodes, only little coordination is needed for working of nodes. The messages are not needed to be routed to any place such that only required to be delivered on regular basis.

Nodes have a privilege of choice when they can join or leave the network, accepting the proof of work while they were not in the network.

They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. In order to apply any kind of rules, norms or incentives there can be enforcement of agreement.

REFERENCES

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H.Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S.Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping,"

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service countermeasure,"http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957

[9] Ron Dorit; Adi Shamir (2012). "Quantitative Analysis of the Full Bitcoin Transaction Graph" (PDF). Cryptology ePrint Archive. Retrieved 18 October 2012.

[10] Garzik, Jeff (2 May 2014). "BitPay, Bitcoin, and where to put that decimal point". Retrieved 20 November 2015.

[11] Jason Mick (12 June 2011). "Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency". Daily Tech. Retrieved 30 September 2012.

[12] Nermin Hajdarbegovic (7 October 2014). "Bitcoin Foundation to Standardise Bitcoin Symbol and Code Next Year". CoinDesk. Retrieved 28 January 2015.

[13] Romain Dillet (9 August 2013). "Bitcoin Ticker Available On Bloomberg Terminal For Employees". TechCrunch. Retrieved 2 November 2014.

[14] "Bitcoin Composite Quote (XBT)". CNN Money (CNN). Retrieved 2 November 2014.

[15] "XBT - Bitcoin". xe.com. Retrieved 2 November 2014.

[16] Shirriff, Ken (2 October 2015). "Proposal for addition of bitcoin sign" (PDF). unicode.org. Unicode. Retrieved 3 November 2015.

[17] Andreas M. Antonopoulos (April 2014). Mastering Bitcoin. Unlocking Digital Crypto-Currencies. O'Reilly Media. Retrieve

[18] SATOSHI NAKAMOTO, 2008 PAPER ON BITCOIN.