

Charity with Minimum Fraud using Blockchain Technology

Shadab Shaikh¹ Disha Devalia² Jainam Zaveri³ Tousif Ansari⁴ Khushboo Tiwari⁵

⁵Lecturer

^{1,2,3,4,5}Department of Computer Engineering

^{1,2,3,4,5}Thakur Polytechnic, India

Abstract— In the current scenario of various charity trusts we donate money online for a good cause. After we donate the money online we don't know where that money goes, is it even being used for the said cause. There are a lot of trust issues. To overcome this issue, we can implement blockchain technology into the charities. After the implementation of blockchain we can see history of all the transactions made by the NGO in the past. By this we can determine whether the NGO is trustworthy or not. After the donation of money, we can also track where our money is being used. Also if the NGO is unable to collect the required amount in the given time then the money can easily be wired back to the donator. Or the people who have donated the money can cast their vote to extend the time limit for fund collection depending upon the milestone reached.

Keywords: Blockchain, charity

I. INTRODUCTION

Today charities has an accountability problem. Why? You don't know how your money is being used. So what happens if you give money to the wrong campaign and someone misuses the money? You may never want to support a charity program again.

With blockchain technology, you know more information. Like who you're going to send money to and how they spend the money. On the other hand, NGOs will receive more support for their projects with lower fees and overall cost, without hefty fees from lawyers.

Blockchains are supported an innovative use of cryptography and have attracted tons of attention thanks to their characteristics which reduce the necessity for trusted third parties and intermediaries. These characteristics include the: - Creation of knowledge records that are permanent, i.e. cannot be changed or deleted - Ability to spot the time and origin of each entry within the Blockchain - Access by all participants to all or any data within the Blockchain - Guaranteed implementation of smart contracts (programmes) that automatically execute once a set of agreed conditions are met like, Only when the estate developer builds the house for you, a portion of funds is released. Likewise, charity money will not be released with the help of a smart contract until the NGO is making progress on the project. So, you have trust.

II. WHAT IS BLOCKCHAIN?

Commerce on internet depends on third parties to process the payments done between people. While this system works well enough for most transactions, it still suffers from the innate weakness of the trust based model. Completely non reversible transactions are not possible. Since financial institutions cannot avoid mediating disputes between transferor and transferee. The cost of mediation increases

the cost of transactions, limiting the minimal transaction size. With the possibility of reversal, trust is needed.

What is needed is an electronic payment system supported by cryptographic proof rather than counting on trust, allowing two parties willing to transact directly with one another instead of relying on trusted third party. Transactions will be computationally not possible to reverse which will protect the sellers and routine mechanisms can be implemented to protect the buyers. This would solve the problem of double spending by making transactions peer to peer and creating a computational proof on the timestamp server.

III. TRANSACTIONS ON BLOCKCHAIN

We define an electronic coin as a sequence of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and therefore the public key of subsequent owner and adding these to the top of the coin. A payee can verify the signatures to verify the chain of Ownership.

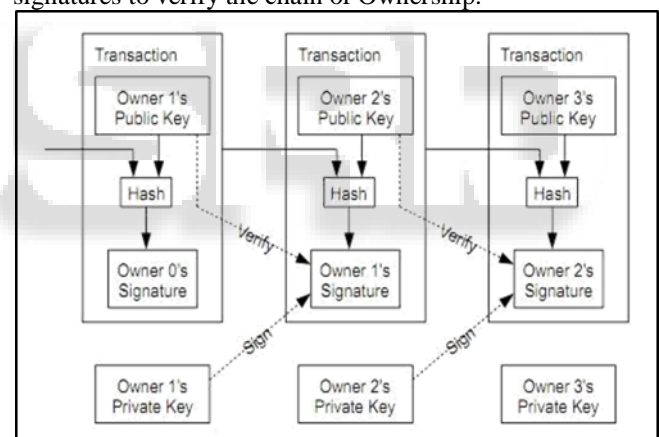


Fig. 1: Transactions structure [3]

The problem in fact is that the payee can't verify that one among the owners didn't double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a replacement coin, and only coins issued directly from the mint are trusted to not be double-spent. The problem with this solution is that the fate of the whole money system depends on the company running the mint, with every transaction having to travel through them, a bit like a bank. We need how for the payee to understand that the previous owners didn't sign any earlier transactions. For our purposes, the earliest transaction is that the one that counts, so we do not care about later attempts to double-spend. The only thanks to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was conscious of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1],

and that we need a system for participants to agree on one history of the order in which they were received. The payee needs proof that at the time of every transaction, the majority of nodes agreed it had been the primary received.

IV. TIMESTAMP SERVER

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of things to be time stamped and widely publishing the hash. The timestamp proves that the info must have existed at the time, obviously, so as to urge into the hash. Each timestamp includes the previous timestamp in its hash, forming a sequence, with each additional timestamp reinforcing those before it.

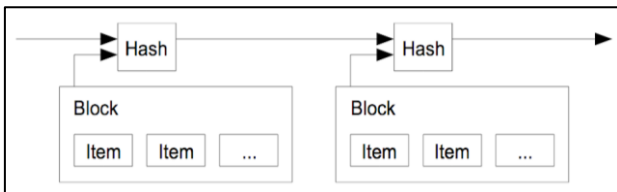


Fig. 2: Timestamping [3]

V. PROOF OF WORK

To implement a distributed timestamp server on a peer-to-peer basis, we'll need to use a symbol of-work system almost like Adam Back's Hashcash [2], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a worth that when hashed, like with SHA-256, the hash begins with variety of zero bits. the typical work required is exponential within the number of zero bits required and may be verified by executing one hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce within the block until a worth is found that provides the block's hash the specified zero bits. Once the CPU effort has been expended to form it satisfy the proof-of-work, the block can't be changed without redoing the work. As later blocks are chained after it, the work to vary the block would include redoing all the blocks after it.

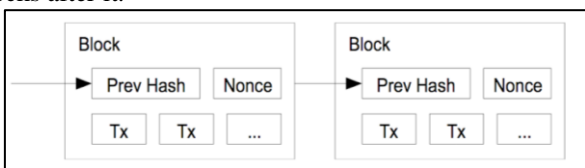


Fig. 3: Chaining of Blocks [3]

The proof-of-work also solves the matter of determining representation in majority decision making. If the bulk were supported one-IP-address-one-vote, it might be subverted by anyone able to allocate many IPs. Proof-of-work is actually one-CPU-one-vote. the bulk decision is represented by the longest chain, which has the best proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. to switch a past block, an attacker would need to redo the proof-of-work of the block and every one blocks after it then catch up with and surpass the work of the honest nodes. we'll show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To catch abreast of increasing hardware speed and ranging interest in running nodes over time, the proof-of-work difficulty is set by a moving average targeting a mean number of blocks per hour. If they're generated too fast, the problem increases.

VI. INCENTIVE

By convention, the primary transaction during a block may be a special transaction that starts a replacement coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides how to initially distribute coins into circulation, since there is no central authority to issue them.

The steady addition of a continuing of amount of latest coins is analogous to gold miners expending resources to feature gold to circulation. In our case, it's CPU time and electricity that's expended. The incentive also can be funded with transaction fees. If the output value of a transaction is less than its input value, the difference may be a transaction fee that's added to the motivation value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the motivation can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to remain honest. If a greedy attacker is in a position to assemble more CPU power than all the honest nodes, he would need to choose from using it to defraud people by stealing back his payments, or using it to get new coins. He need to find it more profitable to play by the principles, such rules that favour him with more new coins than everyone else combined, than to undermine the system and thus the validity of his own wealth.

VII. WHY WORKING ON BLOCKCHAIN?

Blockchain is kind of a set of transactions data that is owned and maintained and managed by all users of the system. Any donors in any country or any part of the world act as 'nodes' to verify and confirm that transactions added to the blockchain are real, safe and secured.

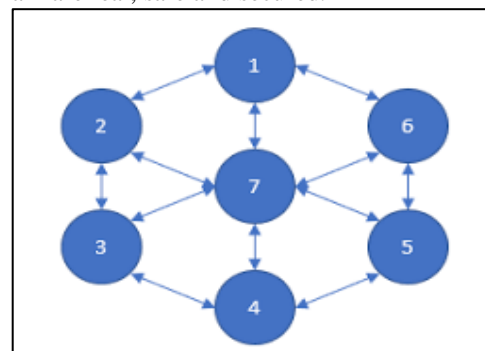


Fig. 4: Nodes on Blockchain [6]

These transactions are then encrypted and added onto the public view, these makes donor encourage to donate and feel comfortable to work with this also this type of transactions discourages fraud and theft because they mean complete transparency of all transactions carried out, and is completely tracked and verified. Nothing can be removed or deleted once it's in the set of transactions and it ensures security against all kind of data manipulation and

fraud. we can also make non-profit sector more transparent, efficient and cost-effective. Blockchain technology could help resurrect the pictures of charities willing to adopt its services .By minimizing administrative costs through automation, providing more accountability through traceable giving milestones, and allowing donors to ascertain more clearly where their funds are going, blockchain may help restore a number of the lost credibility to charities that prove deserve the public's trust

VIII. HOW WOULD THIS PROJECT ENSURE THAT DONATIONS ARE BEING USED PROPERLY?

Many problems, thefts and scandals have affected the confidence in the charity sector. Many charity-based websites have been experiencing these types of troubles, but these blockchain based web app has improved the transactions and transparency of money in this charity sector. Smart contracts will help in freezing the amount in charity account until they are used for their proposed purpose, timestamp servers will make sure that each and every transaction is recorded which can later be checked if needed. The proof of work chain will ensure that attackers can't easily change a past block ensuring no transactions can be changed. The incentive provided makes sure that the nodes in the chain stay honest so that attackers can't change the past block easily.

IX. CONCLUSION

This blockchain technology implementation in the world of charity will not only help in cutting down the frauds but also provide a better tracking of funds donated by the donors without having any risk of getting theft. It will also solve the problem of double spending by using the concept of cryptographic proof.

REFERENCES

- [1] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
- [2] A. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
- [3] S. Nakamoto, "Bitcoin: A peer-to-peer Electronic cash system," <http://www.bitcoin.org/bitcoin.pdf>, *year
- [4] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.
- [5] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.
- [6] <https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f>