DIGITAL TIMESTAMPING METHOD FOR SECURE END TO END COMMUNICATION ON A BLOCKCHAIN

*Y.Muralimohanbabu[1], Monesh Kanth[2], K. Radhika[3]
[1, 2]ECE Dept, SITAMS, Chittoor, Andhra Pradesh, India.
[3]ECE Dept., GIST, Nellore, AP, India.

ABSTRACT

This paper comprises a computer – implemented system for controlling an exchange process, such as a loan, conducted between at least two parties via a blockchain such as the secure channel of blockchain. A method according to the invention may comprise the step of generating a first blockchain transaction which includes a redeem script. The redeem script comprises a cryptographic public key associated with an initiating party and metadata which includes a hash of an exchange - related document a redeem address and an amount of digital currency.

A blockchain transaction is generated and published to the blockchain so as to spend the digital currency to the redeem address. This provides the advantage that the further transaction will be publically available and thus detectable by other parties once it has been published. The further transaction can provide the information necessary to trigger a response e.g. an offer from another (responding) party who publishes their response on the blockchain. Thus, the exchange process can be implemented via a multi - transaction mechanism on the blockchain rather than an alternative medium. The exchange related document may be an invitation (offer/ request) which is stored off - block in a repository such as a Hash algorithm. The invitation may be an invitation to engage in a contract. A smart contract (and associated blockchain transaction) may be formed upon condition that a plurality of participants (e.g. lenders/borrowers) are matched with each other via one or more responses effected via transactions on the blockchain.

Keywords: Blockchain, digital ledger, crypto, computer

1. Introduction

In this paper we utilize the term blockchain to incorporate all types of electronic, PC based, appropriated records. These incorporate agreement convention based blockchain and exchange chain advancements, permissioned and un-permissioned records, shared records and varieties thereof. The most generally known utilization of crypto hyper-record, with different usage have been proposed and created. While cryptographic forms of money might be stored in blocks as a record in this with the end goal of collective segmentation and stacked data which cannot be modified, it can be noticed that the creation isn't constrained to use with the blockchain and optional blockchain usage.

A blockchain is a shared, electronic record which is executed as a computer based decentralized, appropriated framework made up of blocks which are comprised of exchanges. Every exchange is an information structure that encodes the exchange of control of an advanced resource between members in the blockchain framework, and incorporates somewhere around one information and no less than one yield. Each square contains a hash of the past square to that squares become binded together to make a changeless, unalterable record of all exchanges which have been composed to the blockchain since its beginning. Exchanges contain little projects known as contents installed into their data sources and yields, which determine how and by whom the yields of the exchanges can be made to. On the e-banking/cryptoledgers stage, these contents are composed utilizing a stack-based scripting language based on python. All together for an exchange to be composed to the blockchain, it must be approved. System hubs (excavators) perform work to guarantee that every exchange is legitimate, with invalid exchanges rejected from the system. Programming customers introduced on the hubs play out this approval chip away at an unspent exchange by executing its locking and opening contents. On the off chance that execution of the locking and opening contents assess to TRUE, the exchange is substantial and the exchange is composed to the blockchain. In this way, all together for an exchange to be composed to the blockchain, it must be approved by the primary hub that gets the exchange - if the exchange is approved, the hub transfers it to alternate hubs in the system.

2. Related Work

One zone of flow investigate is the utilization of the blockchain for the usage of "keen contracts". These are computer programs intended to computerize the execution of the terms of a machine-clear smart-contract or understanding. Not at all like a customary contract which would be written in regular language, a smart contract is a machine executable program which includes decides that can procedure contributions to request to deliver results, which would then be able to make activities be performed subordinate upon those outcomes. Another territory of blockchain-related intrigue is the utilization of 'tokens' to speak to and exchange genuine substances by means of the blockchain. A conceivably delicate or mystery thing can be spoken to by the token which has no discernable importance or esteem. The token in this manner fills in as an identifier that enables this present reality thing to be referenced from the blockchain.

The present creation fuses these ideas to give a blockchain-based component which empowers secure electronic correspondence and exchange between various gatherings. One preferred standpoint of the innovation is that it empowers the development and utilization of a safe correspondence channel between the gatherings, and consolidation of a safely distributed contract without the requirement for control, the board, intercession or investment by extra gatherings or elements to supervise the channel.

One illustrative application region for such an answer is, that of distributed loaning. Loaning is a necessary piece of the monetary administrations commercial center, enabling borrowers to get assets from banks as a byproduct of consequent installment of those propelled assets. Customary loaning by means of a money related foundation, for example, a bank has, as of late, been stretched out through distributed (P2P) loaning where people loan pooled finds to a borrower all in all for a higher individual return, however with expanded danger of loss of the propelled assets.

3. Proposed Solution

The conceptual oriented approach can be considered in this case such as One illustrative application area for such an answer is, that of shared loaning. Loaning is a basic piece of the budgetary administrations commercial center, enabling borrowers to get assets from moneylenders as a byproduct of resulting installment of those propelled assets. Conventional loaning by means of a money related organization, for example, a bank has, as of late, been reached out through distributed (P2P) loaning where people loan pooled finds to a borrower as a rule for a higher individual return, yet with expanded danger of loss of the propelled assets.

There are various P2P pools with their own bespoke exchanging trades requiring singular enlistment onto those applications so as to take an interest in the End to End loaning process. These advances are supported by the customary financial system and foundation inside the domain that they work. Subsequently, the present frameworks for P2P loaning are prohibitive and complex essentially.

It is profitable to give an elective arrangement. Advantages of this arrangement could incorporate, for instance, end of the requirement for nearby bespoke trades while empowering complex loaning procedures to be completed. Known advantages of the blockchain, (for example, its sealed, perpetual record of exchanges) could be bridled to advantage. This arrangement would give a completely new design and specialized stage. Along these lines, as per the present development there is given a strategy and framework as characterized in the added cases.

As per the process there might be given a technique and comparing framework for controlling the execution of a procedure led by means of (for example utilizing) a blockchain. The square chain could possibly be the SHA-256 blockchain. The procedure might be a correspondence, trade or exchange process. It might involve the exchange, correspondence or trade of a computerized resource, or any sort of advantage which is referenced or spoke to on the blockchain. The controlled procedure may, for instance, be a loaning procedure. It might be a distributed loaning process directed between a majority of blockchain clients. The expressions "client" or "gathering" may allude to a human or machine-based element. Each blockchain client may utilize appropriately designed equipment and programming to take an interest all the while (eg A Computer with a e-transaction customer introduced on it). The development may likewise be alluded to as a security arrangement, framework and additionally strategy as it includes the utilization of cryptographic transaction systems to guarantee the protected correspondence/exchange between gatherings. The creation may contain a strategy considerably included in this, or potentially in the utilization cases/situations as set out in this.

Also or then again, the creation may involve a PC executed technique organized. It might be organized to control a trade procedure directed between something like two gatherings by means of a blockchain. The technique may contain the means: producing a first blockchain exchange containing a recover content involving a cryptographic open key related with a starting gathering and metadata which incorporates a hash of a report a reclaim address furthermore, a measure of computerized cash producing a second blockchain exchange to spend the computerized money to the recover address.

Along these lines, the creation may incorporate the progression of utilizing a further blockchain exchange to spend the money. This gives the preferred standpoint that the further exchange will be publically accessible and hence discernible by different gatherings once it has been distributed to the blockchain. The further exchange can give the data important to trigger a reaction for example an idea from another gathering. Subsequently, the trade procedure can be executed by means of a multi-exchange component on the blockchain as opposed to an elective medium. The first and second exchange might be produced by a similar gathering. The transaction might be multi-signature blockchain exchanges. The first as well as second exchange may give access from the blockchain to a welcome (offer/demand) which is put away off-square. The welcome might be a challenge to take part in an agreement.

The trade might be a credit or identified with an advance. A savvy contract (and related blockchain exchange) might be framed upon condition that a majority of members for example moneylenders/borrowers are coordinated with one another by means of at least one reactions affected through exchanges on the blockchain. The welcome might be an organized record put away in electronic structure.

The advanced money might be e-transactions/cryptocurrencies. The storehouse might be any sort of PC based asset which can store the welcome. The vault may include a server or be housed one a server. The archive might be isolated from the blockchain. Thus, the welcome might be put away. The reference to the area may contain certain methods for distinguishing the area . The process might be publically accessible, or some security component might be utilized to limit access to the substance of the welcome to approved gatherings. The welcome might be put away in a brought together area or might be conveyed. The welcome might be publically available and put away on a Distributed Hash Table (DHT) or Secured Hash Algorithm (SHA-256).

The cash might be any sort of computerized money. It might be crypto's or e-currencies or digital wallets. It might be tokenised money. The exchange might be an exchange of a merchandise or administration. Ideally, the exchange is directed through the blockchain utilizing an exchange (Tx). The initating person might be a potential borrower or loan specialist. The welcome might be a report or document which includes data identifying with a solicitation or offer for an advance. It might be a computerized document. The strategy may incorporate the progression of distributing the main exchange to a blockchain.

This process may include data identifying within the blocks a reimbursement plan related with the exchange as well as a second gathering related with the starting party. The technique may incorporate the progression of producing a reaction, the reaction being related with a reacting party and involving a reference to the welcome putting away the reaction in a computer based vault producing a further (multi-signature) hashed blockchain exchange containing: a reclaim content containing a cryptographic open key related with the reacting gathering and metadata which incorporates a hash of the reaction and a reference to its area in the archive also, a measure of advanced cash.

The reaction might be put away in a similar vault as the welcome, or an alternate archive. The reaction might be an electronic record. The vault which stores the welcome or potentially reaction might be a Distributed hash table (DHT). The process may incorporate the progression of creating a trade plan related with the welcome or reaction, the calendar containing information identifying with no less than one trade sum and additionally trade date producing a P2SH address for each trade in the timetable. The trade might be a reimbursement plan. The trade sum as well as dates may identify with reimbursements of a credit sum related with the welcome or reaction.

The strategy may incorporate the progression of distributing an exchange to the blockchain to make a trade as per the trade plan. The strategy may additionally include the progression of observing the blockchain to distinguish no less than one exchange involving metadata related with the welcome and additionally reaction. Somewhere around one observing advance might be performed exactly. The strategy may additionally involve the progression of checking the blockchain to recognize somewhere around one exchange containing metadata related with the welcome and something like one exchange including metadata related with the reaction

The technique may additionally include the progression of distributing the savvy contract to a storehouse and additionally distributing an exchange to the blockchain, the exchange including a recover content involving no less than one open key and a reference to the shrewd contract. The creation may likewise contain a computer executed framework orchestrated to play out the strategy for any previous case and including: a blockchain a majority of registering gadgets organized correspondence with the blockchain. Also or on the other hand, the creation may give a PC executed framework orchestrated and designed to play out any or the majority of the strategy steps portrayed previously. Also or on the other hand, it might involve a PC executed framework orchestrated to control a loaning procedure led between somewhere around two gatherings by means of a blockchain, the framework containing a PC based vault putting away a welcome for an exchange between at least two gatherings wherein the agreement is related with a starting gathering a blockchain including a first multi-signature exchange containing a recover content containing a cryptographic open key

related with the starting party and metadata which incorporates a hash of the welcome and a reference to its area in the storehouse also, a measure of advanced cash.

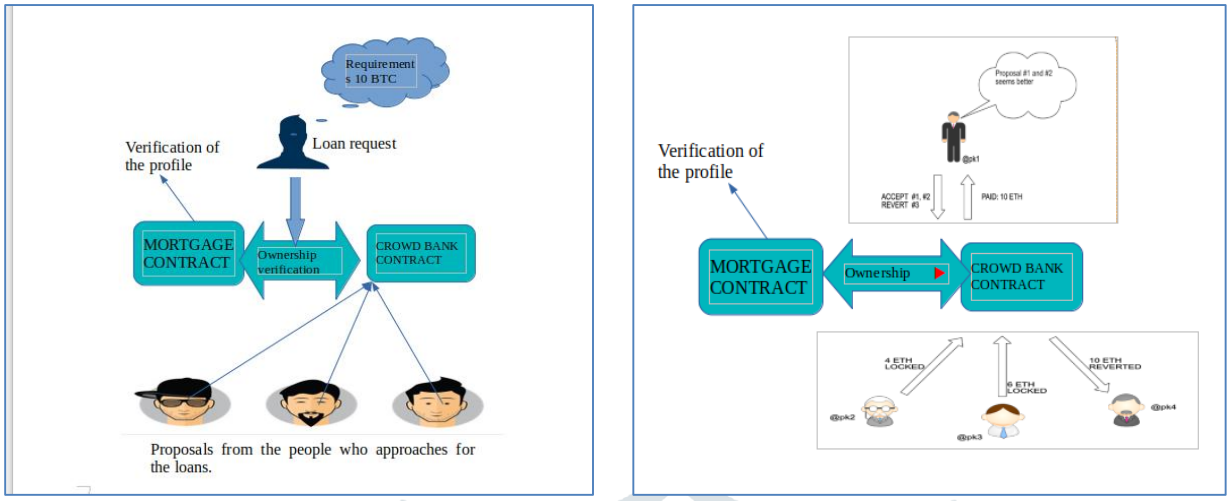

Figure 1: Request process in the blockchain

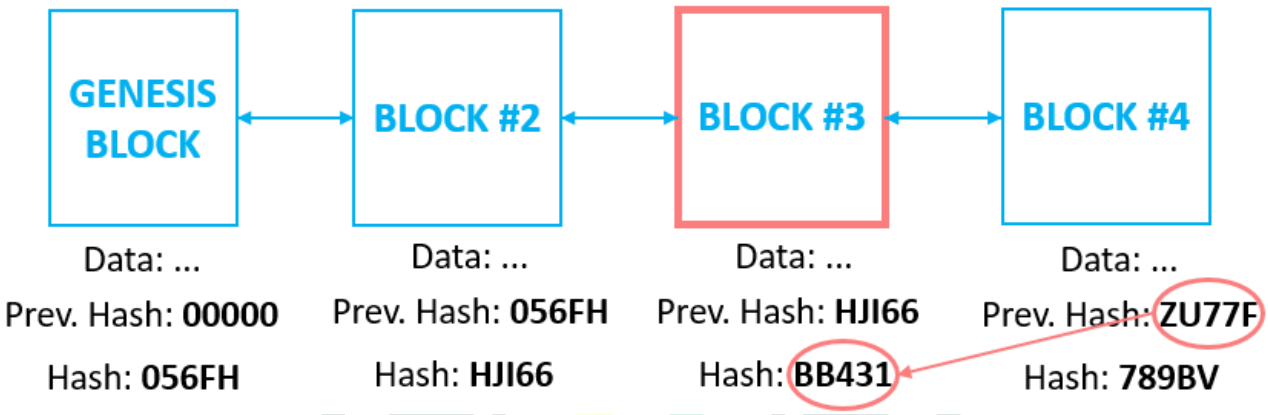

Figure 2: Immutable ledger representation with the sha-256

4. Expected Outcome

By this technique to control a protected trade with and additionally correspondence process led between something like two gatherings by means of a blockchain, the method which involves the content including a cryptographic open key related with a starting gathering and metadata which incorporates a hash of a trade related report a recover address what's more, a measure of computerized transactions creating a second blockchain exchange to spend the money with an distributed architecture. Based on the immutable ledger the data in the blocks is protected by the hash.

REFERENCES

[1] Zheng Z, Xie S, Dai H, et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE International Congress on Big Data. IEEE, 2017.

[2] Bello, Oladayo, and Sherali Zeadally. “Intelligent device-to-device communication in the internet of things", IEEE Systems Journal 10.3 (2016): 1172-1182.

[3] Leslie L, Robert S, Marshall P. “The Byzantine Generals Problem”, ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3):382-401.

[4] Castro M, Liskov B. “Practical byzantine fault tolerance and proactive recovery”, Acm Transactions on Computer Systems, 2002, 20(4):398-461.

[5] Croman K, Decker C, Eyal I, et al. “On scaling decentralized blockchains”, International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016: 106-125.

[6] Sel M, Diedrich H, Demeester S, et al. “How Smart Contracts Can Implement report Once”, Social Science Electronic Publishing,2017, 25(4): 993-101

[7] Murali Mohan Babu Y, Subramanyam MV, Giriprasad MN. A New Approach For SAR Image De-noising. International Journal of Electrical and Computer Engineering, Volume 5, Issue 5, 984-991, October 2015

[8] Murali Mohan Babu Y, Radhika K. A new approach for microwave imagery de-noising. International Journal of Image, Graphics and Signal Processing, Volume 5, issue 1, 52-60, May 2016.