AK Tech Training and Placements

Transform Dreams into Reality

BLOCK CHAIN TECHNOLOGY

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

INTRODUCTION

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

PROPOSED SYSTEM

We propose aelectronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes

WORKING

First of all we need to run the project and open the admin panel. There we can see four models chains, blocks, peers and transactions. Whenever an individual needs to transfer the money from one end to another end, every individual is considered as a chain. Every individual possesses a unique id that means every chain is unique. Suppose one chain name as A123 and B123 are present who needs to transact money amongst themselves. To transfer the money A123 will open transaction model and will fill details of transaction form. Once the transaction is done for the bit coins then the number of bit coins is converted into blocks and that block is assigned to the B123. A123 will be in the senders end and B123 will at the receiver end. After that we will add blocks in the block model and fill in the details of block form. Here a block will be assigned to B123 and A123. This is main concept behind the block chain concept.

ADVANTAGES

Transaction histories are becoming more transparent through the use of blockchain technology. Because blockchain is a type of distributed ledger, all network participants share the same documentation as opposed to individual copies. That shared version can only be updated through consensus, which means everyone must agree on it. To change a single transaction record would require the alteration of all subsequent records and the collusion of the entire network. Thus, data on a blockchain is more accurate, consistent and transparent than when it is pushed through paper-heavy processes. It is also available to all participants who have permissioned access. To change a single transaction record would require the alteration of all subsequent records and the collusion of the entire network. Which can be, you know, a headache.

If your company deals with products that are traded through a complex supply chain, you're familiar with how hard it can be to trace an item back to its origin. When exchanges of goods are recorded on a blockchain, you end up with an audit trail that shows where an asset came from and every stop it made on its journey. This historical transaction data can help to verify the authenticity of assets and prevent fraud.

When you use traditional, paper-heavy processes, trading anything is a time-consuming process that is prone to human error and often requires third-party mediation. By streamlining and automating these processes with blockchain, transactions can be completed faster and more efficiently. Since record-keeping is performed using a single digital ledger that is shared among participants, you don't have to reconcile multiple ledgers and you end up with less clutter. And when everyone has access to the same information, it becomes easier to trust each other without the need for numerous intermediaries. Thus, clearing and settlement can occur much quicker.

Mail: **careers@aktechsolutions.in** **Phone:** **7777-976-476** **Web:** **http://aktechsolutions.in/**

For most businesses, reducing costs is a priority. With blockchain, you don't need as many third parties or middlemen to make guarantees because it doesn't matter if you can trust your trading partner. Instead, you just have to trust the data on the blockchain. You also won't have to review so much documentation to complete a trade because everyone will have permissioned access to a single, immutable version.

CONCLUSION

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis.

Mail: careers@aktechsolutions.in **Phone:** 7777-976-476 **Web:** http://aktechsolutions.in/