Blockchain - Cipher Block Chaining - A New Big Evolution to Change

Pritam Padhye[1] Niraj Palkar[2] Rehan Sayed[3] Shivsagar Gondil[4]
[4]Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Bharti Vidyapeeth College of Engineering, Navi Mumbai, India

Abstract— Cipher block chain is made of operation for a block cipher with a cipher key. Cipher block chaining uses a technique what is called as an initialization vector of certain length generally of six, it's a chain formation so to decrypt a block we will need the hash code of the previous block and this goes on to the very first block of the chain.

Keywords: Blockchain, Operations, Advantages, Working, Application, Encryption and Decryption

I. Introduction

Cipher block chain is a mode of operation for a block cipher with a cipher key. Cipher block chaining uses what is called as an initialization vector of a certain length generally of six. It's a chain formation so to decrypt a block we will need the hash code of the previous block and this goes on to the very first block of the chain. This technology can replace the current technology of the file management. This was first used in the bitcoins to maintain the transaction as the crypto currencies are open and don't have a central controlling system. The use of this technology is useful in the industries like banking and government sector to reduce data lose and corruption.

Our proposed paper will discuss about the evolution of block chain, working of the same and its applications and its impact factor on the current technologies with the additional factor of implementation of the cipher block chain. The paper focuses on the next generation technology for the management of critical data and its implementation

II. History

The work on blockchain was first started for a cryptographically secured chain of blocks in 1991 by Stuart Haber and W. Scott Stornetta which improved its efficiency by allowing several documents to be collected into one block. the documents were put into the blocks and a chain of such block were made with each block having the hash code of the previous chain. This resulted into a secure chain such that if any of the block has undergone changes then the entire hash value changes making it hard to manipulate explicitly.

The first use of the blockchain was made by the person Satoshi Nakamoto in 2009 as the main component of the cryptocurrency bitcoin, where it serves as the public passbook for all the transaction as the cryptocurrency has no central control over the transactions.

III. What are Blocks

Blocks hold the batches of valid transactions, distributed and public ledgers that is used to record the transaction across many computers so that the record cannot be manipulated explicitly. The blocks are batches of valid transactions that are hashed and encoded into a Merkle tree. Each block has the hash value of the previous block. The chain goes on increasing and such a chain of encoded blocks is called a blockchain.

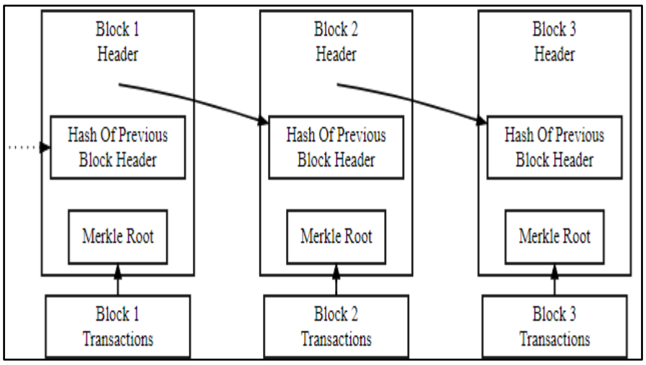

Fig. 1: Structure of block

The figure shows that the structure of block has the two main elements that are a hash value of previous block and the Merkle root this root keeps the track of the transactions and the hash value will protect the transactions from any form of tampering or manipulation.

IV. Working

The working of blockchain involves few technologies which are not at all new and are way used by the world. These technologies are combined to create a more secure and better platform for the purpose of maintaining the transactions.

The technologies used are private key encryption, public encryption and a public distributed network and a service for record keeping and security. If the people want to transact over the internet then for security each person will have a public key and a private key. The both of the keys are combined to form a digital signature which is a better form for the control of ownership. This digital signature solves the problem of authentication, but we need to authorize for the purpose of transaction. Else the transaction won't be able to track its exact destination or maybe taken to a different person.

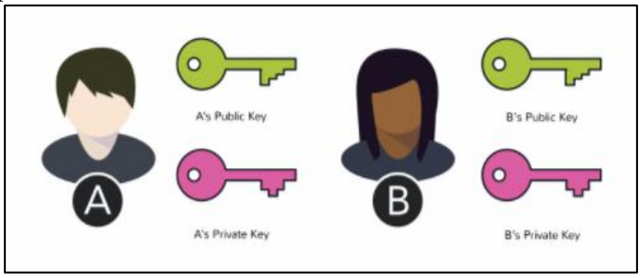

Fig. 2: Requirement of Blockchain

The main purpose of blockchain technology is to create a secure digital identity. This identity is based on possession of a combination of private key and public key. The transaction requires network for the transaction to be completed. The size of the network is important.

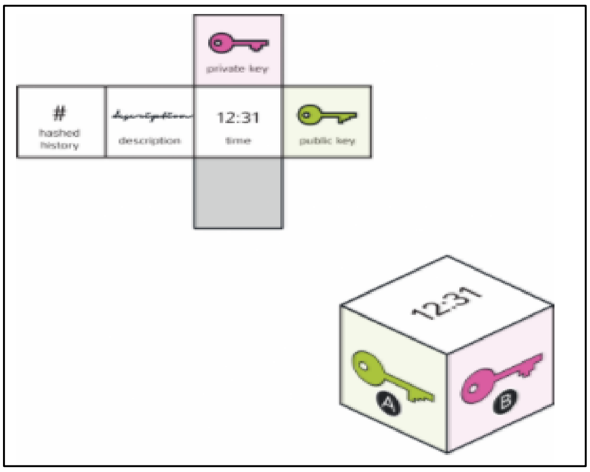

Fig. 3: Block Creation

When the encryption keys are combined with network a better form of digital signature is evolved. The process is simple and combinational in nature. The private key of the person who wants to send the transaction is combined with the public key of receiver. A block is made which has the timestamp and information required for the transaction. This block is given to the network.

When a group of blocks come together there comes a chain of blocks that are encrypted and maintained without any central control over the records. This blockchain is good at maintaining the data and the data becomes tamper proof up to some extent.

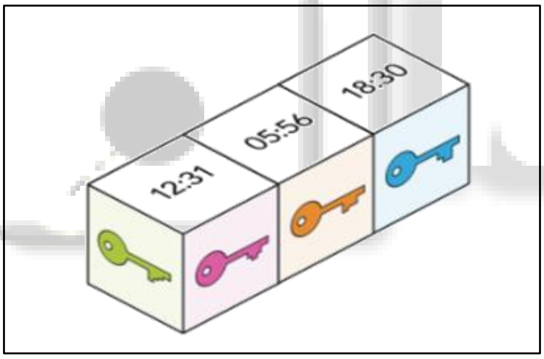

Fig. 4: Block Chain

V. Applications

A. General Potentials

Blockchain technology has a large potential to transform business operating models in the long term. blockchain distributed ledger technology is more a foundational technology with the potential to create new foundations for global economic and social system than a disruptive technology, which typically "attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly". even so, there are a few operational products maturing from proof of concept by late 2016. the use of blockchains promises to bring significant efficiencies to global supply chains, financial transactions, asset ledgers and decentralized social networking

B. Government and Currencies

the director of the office of it schedule contract operations at the us general services administration, Mr. Jose Arrieta, disclosed at the 20th September American council for technology and industry advisory council forum that its organization is using blockchain distributed ledger technology to speed up the fast lane process for it schedule 70 contracts through automation. two companies, united solutions (prime contractor) and sapient consulting (subcontractor) are developing for fast lane a prototype to automate and shorten the time required to perform the contract review process.

The commercial customs operations advisory committee, a subcommittee of the US customs and border protection is working on finding practical ways blockchain could be implemented in its duties.

Companies have supposedly been suggesting blockchain-based currency solutions in the following two countries:

e-dinar, Tunisia's national currency, was the first state currency using blockchain technology. ECFA is Senegal's blockchain-based national digital currency.

some countries, especially Australia, are providing keynote participation in identify the various technical issues associated with developing, governing and using blockchains

C. Other uses

notable non-cryptocurrency designs include:

- Steemit – a blogging/social networking website and a cryptocurrency
- Hyper ledger – a cross-industry collaborative effort from the Linux foundation to support blockchain-based distributed ledgers, with projects under this initiative including hyper ledger burrow (by Monax) and hyper ledger fabric (spearheaded by IBM)
- counterparty – an open source financial platform for creating peer-to-peer financial applications on the bitcoin blockchain
- quorum – a permission able private blockchain by JP Morgan with private storage, used for contract applications
- bit nation – a decentralized borderless "voluntary nation" establishing a jurisdiction of contracts and rules, based on Ethereum
- Factom, a distributed registry
- Tezos, decentralized voting.

VI. Disadvantages

1) They verify the same transactions in accordance with the same rules and perform identical operations.
2) They record the same thing into a blockchain (if they were fortunate enough to be allowed to do so).
3) They store the entire history, which is the same for all of them, for all time.
4) Every high-grade Bitcoin network client stores the entire transaction history, and this record has already become as large as 100GB. That’s the full capacity of a cheap laptop’s or the most advanced smartphone’s storage. The more transactions processed on the Bitcoin network, the faster the size grows. And the greatest bulk of it has appeared over the past couple of years.

VII. Advantages

1) Supply chain management: For supply chain management, the blockchain technology offers the benefits of traceability and cost-effectiveness. Put simply, a blockchain can be used to track the movement of goods, their origin, quantity and so forth. This brings about a new level of transparency to B2B ecosystems -- simplifying processes such as ownership transfer, production process assurance and payments.
2) Quality assurance: If an irregularity is detected somewhere along the supply chain, a blockchain system can lead you all the way to its point of origin. This makes it easier for businesses to carry out investigations and execute the necessary actions.
3) Accounting: Recording transactions through blockchain virtually eliminates human error and protects the data from possible tampering. Keep in mind that records are verified every single time they are passed on from one blockchain node to the next. In addition to the guaranteed accuracy of your records, such a process will also leave a highly traceable audit trail.
4) Smart contracts: Time-consuming contractual transactions can bottleneck the growth of a business, especially for enterprises that process a torrent of communications on a consistent basis. With smart contracts, agreements can be automatically validated, signed and enforced through a blockchain construct. This eliminates the need for mediators and therefore saves the company time and money.
5) Voting: Just like in supply chain management, the promise of blockchains in the aspect of voting all boils down to trust. Currently, opportunities that pertain to government elections are being pursued. One example is the initiative of the government of Moscow to test the effectiveness of blockchains in local elections. Doing so will significantly diminish the likelihood of electoral fraud, which is a huge issue despite the prevalence of electronic voting systems.

VIII. Conclusion

The blockchain technology will be a boon for the future industries and may even replace the traditional relational database management system because of the problem of manipulation and lack of inbuilt security. The technology using blocks is better using the basic technologies of encryption and networking. The banks would be safer and the government can keep a track of all activities going around the nation.

Acknowledgement

This paper was possible because of the able guidance of our professor HOD Dr. D.R Ingle so we extend heartfelt acknowledge to our professor and would also like to thanks others who helped us to fulfill this paper. Would also extend our heartfelt acknowledge to our parents for encouraging us.

References

[1] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.

[2] Morris, David Z. (15 May 2016). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune. Archived from the original on 21 May 2016. Retrieved 23 May 2016.

[3] Popper, Nathan (21 May 2016). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". The New York Times. Archived from the original on 22 May 2016. Retrieved 23 May 2016.

[4] Brito, Jerry; Castillo, Andrea (2013). Bitcoin: A Primer for Policymakers (PDF)(Report). Fairfax, VA: Mercatus Center, George Mason University. Archived (PDF) from the original on 21 September 2013. Retrieved 22 October 2013.

[5] Trottier, Leo (18 June 2016). "original-bitcoin" (self-published code collection). github. Archived from the original on 17 April 2016. Retrieved 18 June 2016. This is a historical repository of Satoshi Nakamoto's original bit coin sourcecode

[6] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[7] "Blockchain". Investopedia. Archived from the original on 23 March 2016. Retrieved 19 March 2016. Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system.