International Conference on "Recent Trends in Technology and its Impact on Economy of India"
Guru Nanak College for Girls, Sri Mukstar Sahib, Punjab (India) (ICRTTIEI-17)
24th October 2017, www.conferenceworld.in ISBN: 978-93-86171-74-0

Expeditious Transaction Using Block Chain

[1]Ashwini Abhyankar,[2]Prachi Dhanmeher, [3]Krupali Gami

[4]AnkitaChavan, [5]Prof. Amruta Pokhre

[1,2,3,4,5]Department of Information Technology,Atharvacollege of engineeringMalad, Mumbai

ABSTRACT

Blockchain is an answer to the question "How can we trust what happens online?" The Blockchain is a distributed database that maintains a list of records these records are called blocks. Each block contain the history of every block that came before it down to the second block chaining those blocks together hence Blockchain. The Blockchain is maintained by a scalable network of computers(nodes), creating a chain.Blockchain technology was first introduced as the technology behind the Bitcoin(virtual currency), but it is expected that its characteristics of accurate and guarded data transfer in distributed P2P network could make other applications possible.

I. INTRODUCTION

Blockchain is the world's leading software platform for digital assets. We are using this new technology to build a better financial system. The term "blockchain technology" typically refers to the transparent, trustless, publicly accessible ledger that allows us to securely transfer the units of value using public key encryption and proof of work methods.The technology uses decentralized approach to maintain the network, which means it is not centrally controlled by any bank, corporation, or government. In fact, the larger the network grows and becomes increasingly decentralized, the more secure it becomes.

The financial Sectors have gained popularity and have become part of our daily lives interaction. The attraction of blockchain is its method of verifying and tracking the transactions. Instead of a trusted third-party or a central bank, it relies on a peer-to-peer network of computers. Rather than being stored in a single database, blocks of time-stamped transactions are stored on all systems across the chain. This elimination of middlemen and decentralization of trust has introduced possibilities to use the process for cross-border payments, trading and settlement faster, more reliable and less costly.

The figure 1.1 is a step-by-step breakdown of how a transaction between two parties occurs via distributed ledger technology.

The Procedure of transaction will be:

First of all Software receives Validate user in the system and allow only those nodes to participate in the process and it is further Message transfer request to all validated nodes and acknowledgement is returned back and the final balance is updated and acknowledgment and broadcasted so that all the validate nodes have the detail of transaction and cannot be altered by attacker as it is a blockchain so it will notified and identified easily and at last response is generated

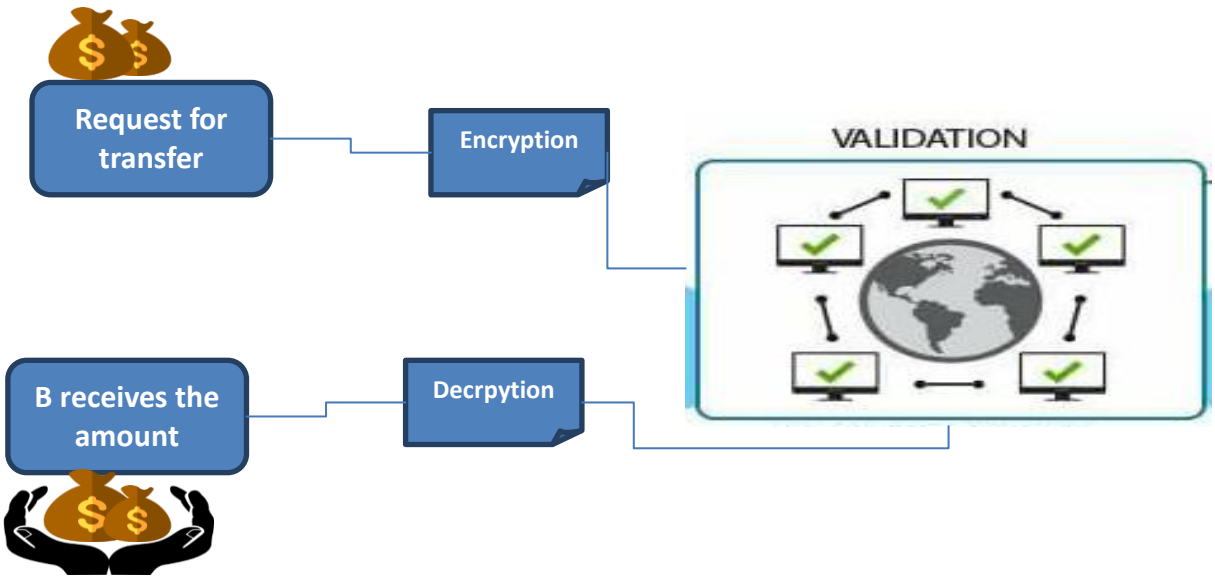

Fig 1.1Transaction in distributed environment

After the request for transferring money to B is passed it is converted through hash function. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. One use is a data structure called a hash table, widely used in computer software for rapid data lookup.

The aim of using the blockchain is to develop a system of improved facilities and provide great level of security. Using this concept we can overcome all the limitations of the existing system. The system provides proper security and reduces the manual work and transaction time.

II. REVIEW OF LITERATURE

2.1 TheBlockchain as a Software Connector

Cryptocurrencies are low-cost and inherently independent of any centralized authority to transfer virtual money or issue new units of money. New units of money are issued by the users of the cryptocurrency through mining. The virtual money can be transferred among peer-to-peer users without going through a trusted authority to purchase goods and services in real world. Bitcoin is the first and most widely used cryptocurrency.[10]

2.2 Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS

In the Big Data era, personal metadata may willbecome a new type of corporate asset, however there have already been a growing public concern about user's privacy mined from metadata. In this paper we address the problem of implementing the self-sovereignty of personal metadata on the existing OpenPDS/SafeAnswers framework according to the Windhover Principle.[2]

2.3 Proposed Classification of Blockchains Based on Authority and Incentive Dimensions.

The potential of blockchain technology has received attention in the area of FinTech- combination of finance and technology. Blockchain technology was first introduced as the technology behind the Bitcoin decentralized virtual currency, but there is the expectation that its characteristics of accurate and irreversible data transfer in a decentralized P2P network could make other applications possible[4]

III. OBJECTIVES

Reducing the settlement time to mere seconds by removing intermediaries. Replacement of trusted third parties with access by all participants in the value chain to cloud-based assets that verify eachparty's identity. Significant security enhancement in areas such as payments and credit card fraudthrough a decentralized public transaction record that stores details of every transaction and undergoes continuous verification by miners. Material cost reduction through the elimination of expensive proprietary infrastructure.

IV. METHODOLOGY

4.1Decentralized Authority

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

Two important properties result from this:

1. Transparency data is embedded within the network as a whole, by definition it is public.
2. It cannot be corrupted altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

4.2Cryptographic Hash Function

A generic hash function maps arbitrary size inputs ormessages to fixed size hash values or tags. In order tojustify the authenticity of a message through its tag, a cryptographic hash function tries to ensure pseudo one-wayness, that is, the practical infeasibility of generating the input message given the tag, and pseudo collision resistance, that is, the practical infeasibility of generating two input messages that produce the same hash value or tag. Due to these two properties of cryptographic hash functions, it is probabilistically ensured that if a message isinadvertently exposed to errors, or has been intentionally tampered with, its hash value will not match with the original tag, and thus, the tampering will be evident. In fact, for minor differences in the input message, the tag generated by a cryptographic hash function is supposed to exhibit major (random) difference. This allows us to utilize hash functions for creating tamper evident structures.

4.3Tamper-evident Linked-List

Each block in the blockchain acts as a node in the list (or chain), holding some amount of data, and a hash

pointer pointing to the previous block on the chain. The first block in the chain is called the genesis block, and this is the only one that does not have to contain a hash pointer.

V. CONCLUSION

A number of traditional financial services firms have nowinitiated strategic partnerships and investments in the space. The involvement of several keycompanies has resulted in an acceleration of activity; start-ups, banks, and financial services firms are dedicating ever-more resources to exploring ways to harness the technology. A variety of blockchain systems have emerged, though it is still too early in the innovation and development cycle to determine which of these systems, if any, will become sustainable, scalable and successful in the future. In all probability, an enormous amount of cooperation between key players, including banks, technology firms, stock exchanges, regulators, developers, programmers, and entrepreneurs, will be required for a blockchain-driven financial ecosystem to emerge. We can, however, assume continued experimentation by technology companies, financial services firms, and other key players in the space going forward as they work to make an effective, secure, and viable real-world blockchain ecosystem a reality. Thus our proposed system is to develop a system of improved facilities and provide great level of security by using the blockchain technology. Using the proposed system we will overcome the limitations of the existing system. We ensure that this system will provide proper security and will reduce the manual work and transaction time.

REFERENCES

[1] Bitcoinwiki. Contract. https://en.bitcoin.it/wiki/Contract#Example Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS: https://www.researchgate.net/publication/319184164_BC PDS_Protecting_Privacy_and_Self-Sovereignty_through_BlockChains_for_OpenPDS

[3] Crypto-currency market capitalizations. http://coinmarketcap.com/
https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world

[4] Proposed Classification of Blockchains Based on Authority and Incentive Dimensions.: https://www.researchgate.net/publication/315869370_Proposed_classification_of_blockchains_based_on_authority_and_incentive_dimensions

[5] J. Walent (2016, July)"Blockchain: A Case for theGeneralLedger." PaymentsJournal [online] Available:http://www.paymentsjournal.com/Content/Featured_Stories/31920/ [Mar.01.2017].

[6] "Know More AboutBlockchain: Overview, Technology, Application Areas and Use Cases," Let's Talk APayments, http://letstalkpayments.com/an-overview-ofblockchain-technology/

[7]"Financial Institutions: Blockchain Activity Analysis," Let's Talk Payments, Sept. 7, 2015, http://letstalkpayments.com/financial-institutionsblockchain-activity-analysis/

[8] "What is Blockchain Technology? A Step-by-Step Guide For Beginners," Block Geeks, http://blockgeeks.com/guides/what-is-blockchaintechnology/

[9] S.Iyer (2016 .July)," The Benefits of Blockchain Across Industries." Oracle [on-line].Available: http://www.oracle.com/us/corporate/profit/bigideas/041316-siyer-2982371.html, [Mar.01.2017].

[10] TheBlockchain as a Software Connector:https://publications.csiro.au/rpr/pub?pid=nicta:9244

ISBN: 978-93-86171-74-0

[11] Ian Allison, "R3 Connects 11 Banks to Distributed Ledger using Ethereum and Microsoft Azure," International Business Times, Jan. 20, 2016, http://www.ibtimes.co.uk/r3-connects-11-banksdistributed-ledger-using-ethereum-microsoft-azure-1539044

[12]T.Virdi.(2016 , Mar)," The benefits of Blockchain for financial services.", beta news [online].Available: https://betanews.com/2015/12/28/the-benefits-ofblockchain-for-financial-services/