International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

A Novel Block Chain Technology

T. Tejaswini , Asst.Prof.
T.Vamshi Krishna , B.Tech
S.Teja Reddy,B.Tech
A.Pranay, B.Tech
Department Of Cse , St.Martin's Engineering College , Dhulapally,Secundrabad

ABSTRACT:

In today's connected and integrated world, economic activity takes place in business networks that span national, geographic, and jurisdictional boundaries. Business networks typically come together at marketplaces where the participants, such as producers, consumers, suppliers, partners, market makers/enablers, and other stakeholders own, control, and exercise their rights, privileges, and entitlements on objects of value known as assets. Assets can be tangible and physical, such as cars,

homes, or strawberries, or intangible and virtual, such as deeds, patents, and stock certificates. Asset ownership and transfers are the transactions that create value in a business network. Transactions typically involve various participants like buyers, sellers, and intermediaries (such as banks, auditors, or notaries) whose business agreements and contracts are recorded in ledgers. A business typically uses multiple ledgers to keep track of asset ownership and asset transfers between participants in its various

lines of businesses. Ledgers are the systems of record (SORs) for a business's economic activities and interests. A distributed ledger is a type of database that is shared, replicated, and synchronized among the members of a network.

The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network. Participants in the network govern and agree by consensus on the updates to the records in the ledger. No central, third-party mediator, such as a financial institution or clearinghouse, is involved. Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable history of all transactions in the network. One implementation of distributed ledger technology is the open source hyper ledger Fabric block chain.Current business ledgers in use today are deficient in many ways. They are inefficient, costly, non- transparent, and subject to fraud and misuse. These problems stem from reliance on centralized, trust-based, third-party systems, such as financial institutions, clearinghouses, and other mediators of existing institutional arrangements. These centralized, trust-based ledger systems lead to bottlenecks and slowdowns of transaction settlements. Lack of transparency, as well as susceptibility to corruption and fraud, lead to disputes. Having

to resolve disputes and possibly reverse transactions or provide insurance for transactions is costly. These risks and uncertainties contribute to missed business opportunities. Furthermore, out-of- sync copies of business ledgers on each network participant's own systems lead to faulty business decisions made on temporary, incorrect data. At best, the ability to make a fully informed decision is delayed while differing copies of the ledgers are resolved.

I. INTRODUCTION:

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easy to steal a cookie from a cookie jar, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions. However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain distributed consensus modelas the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond. Current digital economy is based on the reliance on a certain trusted authority. Our all online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains

that these third party sources can be hacked, manipulated or compromised. This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensuswhere each and every online transaction, past and present, involving digital assets can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymityare two important characteristics of blockchain technology.

Existing System:

The only way to tamper with the data while preserving the hash would be to find a collision in the data, and that's computationally impossible. It would require so much computing power that it's

practically uneconomical. A hash can be thought of as an encrypted version of the original string from which it is impossible to derive the original string. In fact, one way to compute the hash of a string is by encrypting it and performing some scrambling and xoring of the output bits. Mathematically, a hash is produced by a hash function, f, which must have two important properties: the size of the input space and the output space must be large; it must be practically impossible to find collisions, that is, two inputs x1 and x2 that produce the same output f(x1) 5 f(x2). A typical application of hash functions is in password storage—when you register on a website, you don't want the site to store your password p in its database, otherwise anyone with access to the database could read it. The website should store the hash of the password, f(p) 5 y. When you login, the input password p is hashed again and compared with the stored value, f(p) 5 y. The probability of an incorrect password producing the same hash value y as the actual password is zero for practical purposes.

Disadvantages:

The Work is more on the basic understanding of block chain but when the scenario is considered for cryptocurrencies like bitcoin there's a lot more than this to the bitcoin network. The core understanding of block chain adding chain of blocks and validating integrity is more important to be considered in building the Blocks.

Proposed System:

The goal of this project is to explain and to make clearer how is a block chain structured at the very core. There are three divisions In implementation: The Message() class, the Block() class and the Chain(). A message is the basic data container. It is sealed when added to a block and has 2 hashes that identify it: the payload hash and the block hash. Each message

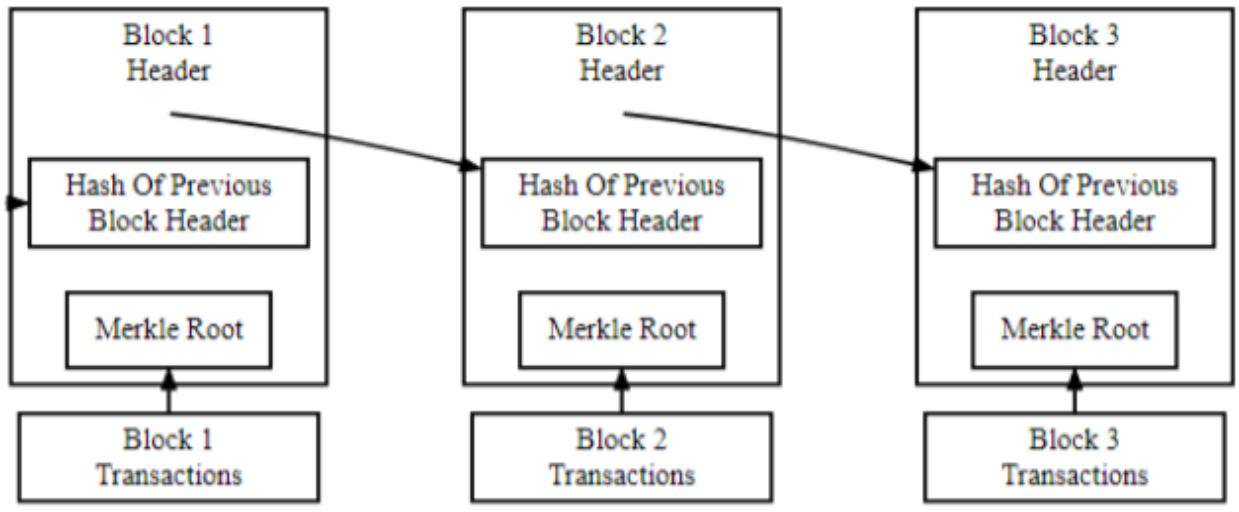
is linked to the previous message via hash pointers (the prev_hash attribute). The validate message method will ensure the integrity of each message, but will not check if the hash pointers are correct. This is left to the validate method in the Block() class. A block can contain 1,...,n messages that are linked sequentially one after the other. When a block is added to the chain, it's sealed and validated to ensure that the messages are correctly ordered and the hash pointers match. Once the block is sealed and hashed, it is validated by checking the expected vs the actual.

Advantages:

The core concept of block chain is presented starting from Add Message to Block:
Add Block to Chain, Displaying the Added Block and Validating the Integrity.

II. BLOCKCHAIN TECHNOLOGY:

We explain the concept of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the blockchain technology is applicable to any digital asset transaction exchanged online.



HOW A BLOCK CJAIN NETWORKS:

However, there is question of maintaining the order of these transactions that are broadcast to every other node in the Bitcoin peer-to-peer network. The transactions do not come in order in which they are generated and hence there is need for a system to make sure that double-spending of the cryptocurrency does not occur. Considering that the transactions are passed node by node through the Bitcoin network, there is no guarantee that orders in which they are

received at a node are the same order in which these transactions were generated.

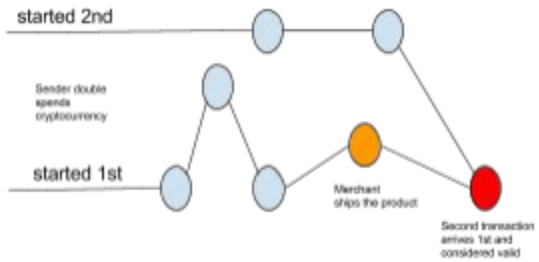


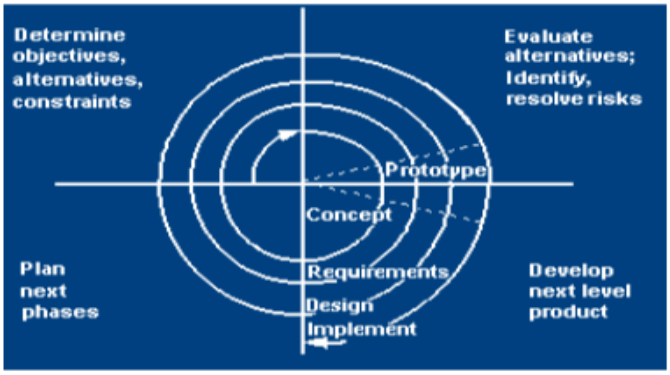
FIG.1.Double spending due to propagation delays in peer-to-peer network

III. SYSTEM ANALYSIS:

SDLC METHDOLOGIES

This document play a vital role in the development of life cycle (SDLC) as it describes the complete requirement of the system. It means for use by developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process.

SPIRAL MODEL was defined by Barry Boehm in his 1988 article, "A spiral Model of Software Development and Enhancement. This model was not the first model to discuss iterative development, but it was the first model to explain why the iteration models. As originally envisioned, the iterations were typically 6 months to 2 years long. Each phase starts with a design goal and ends with a client reviewing the progress thus far. Analysis and engineering efforts are applied at each phase of the project, with an eye toward the end goal of the project.



The steps for Spiral Model can be generalized as follows:

- The new system requirements are defined in as much details as possible.

This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

- A preliminary design is created for the new system.
- A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

IV. IMPLEMENTATION

Code is produced from the deliverables of the design phase during implementation, and this is the longest phase of the software development life cycle. For a developer, this is the main focus of the life cycle because this is where the code is produced. Implementation my overlap with both the design and testing phases. Many tools exists (CASE tools) to actually automate the production of code using
information gathered and produced during the design phase.

V. CONCLUSION:

This book has tried to demonstrate that blockchain technology's many concepts and features might be broadly extensible to a wide variety of situations. These features apply not just to the immediate context of currency and payments (Blockchain 1.0), or to contracts, property, and all financial markets transactions (Blockchain 2.0), but beyond to segments as diverse as government, health, science, literacy, publishing, economic development, art, and culture (Blockchain 3.0), and possibly even more
broadly to enable orders-of- magnitude larger-scale human progress.

Blockchain technology could be quite complementary in a possibility space for the future world that includes both centralized and decentralized models. Like any new technology, the blockchain is an idea that initially disrupts, and over time it could promote the development of a larger ecosystem that includes both the old way and the new innovation. Some historical examples are that the advent of the radio in fact led to increased record sales, and ereaders such as the Kindle have increased book sales. Now, we obtain news from the New York Times, blogs, Twitter, and personalized drone feeds alike. We consume media from both large

entertainment companies and YouTube. Thus, over time, blockchain
technology could exist in a larger ecosystem with both centralized and decentralized models.

REFERNCES:

1. Bitcoin: A Peer-to_peer Electronic Cash System
2. Smart Contracts: Nick Szabo
3. Formalizing and Securing Relationships on Public Networks: Nick Szabo
4. Introduction To Smart Contracts
5. The Ultimate List of Bitcoin and Blockchain White Papers
6. Bitcoin Tutorial
7. A Risk-Based View of Why Banks are Experimenting with Bitcoin and the Block 8. Blockchain:The Information Technology of The Future
9. Bitcoin 2.0 Applications
10. Beyond Bitcoin:How the Blockchain Can Power a New Generation of Enterprise Software