Blockchain and Cryptocurrency- The Journey So Far

1st Mr. Bhaskar Mondal
School of Computer Science
MIT-World Peace University
Pune, India

2nd Dr. C.H.Patil
School of Computer Science
MIT-World Peace University
Pune, India

3rd Mr.Balvant Ghanekar
School of Computer Science
MIT-World Peace University
Pune, India

4th Mr. Chirag Kapadia
School of Computer Science
MIT-World Peace University
Pune, India

5th Ms. Riya Jain
School of Computer Science
MIT-World Peace University
Pune, India

***Abstract*-This paper describes how blockchain technology came into existence and how it is associated with cryptocurrency. It explains how cryptocurrency emerged on blockchain, how it is mined, how cryptocurrencies are traded, how they are introduced to the market, hashing algorithms, mining algorithms and circulation of cryptocurrency in the market.**

I. INTRODUCTION

Blockchain, is a technology which first emerged with a vision of work on a sequence of blocks. These chain of blocks are cryptographically secured no one can tamper or backtrack the timestamps of these documents. Block chain was introduced globally by two research scientists Stuert Haber and W.Scott Stornetta. A typical block header in a blockchain consists of version, last block, Merkle root, and target. The first block of any blockchain is known as **Genesis Block**. It contains information such as number of transactions, transaction fee, block height, timestamp, nonce, block and difficulty.[1]

The first ever implementation of blockchain technology was done by **Satoshi Nakamoto**. This may be a single person or a group of persons Satoshi Nakamoto used blockchain as a base and created Bitcoin.

II. EVOLUTION OF BLOCKCHAIN

Phase 1- Transactions: In the year 2008-2013 with first version of Blockchain 1.0 Bitcoin emerged.

Phase 2- Smart Contracts: In the year 2013-2015 to utilize full capabilities of Blockchain 2.0, developer Vitalik Buterin developed Ethereum which became one of the first contributors of Bitcoin Codebase.

Phase 3- Applications: In the year 2013with Blockchain 3.0 number of projects emerged. One of them is NEO which is the first opensource, decentralized blockchain platform launched in China. In the year 2015, Hyperledger- Umbrella project of open source blockchain was introduced by Linux Foundation. It is focused to support global business transactions.

III. DIGITAL TRANSFORMATION OF BLOCKCHAIN

1. Finance:

Finance: Higher efficiency and security in banking system and money transactions.

Financial Protection: Insurance Agreement Preservation, validating the agreement and transaction process.

Banking Interface: More accuracy, better interface, security in transactions.

2. Contracts:

Inheritances: Validity of wills and smart contract system to ensure inheritance.

Property or Land: Property information, transparency in payment, ownership changes.

Legal Contracts: Preserving legal documentation and contracts. Smart contracts defines the rules of contracts.

3.Entertainment:

Music Industry: No illegal downloads, proper channel for artist compensation.

*Entertainment Industry:*_Ownership Rights, Preserving copyright.

4.Technology:

Cyber Security: Protection against DDoS attack. Ledger system prevents hacking.

IoT: Implementing IoT System within industries, IoT applications for transactions.

AI: Automating and securing AI Tech.
Cloud Storage: Extra security with decentralized network, low transaction costs, unused space.
Power Management: Low cost energy, peer to peer energy transfer, utility metering.

5.Media:
Advertising: No intermediates, low cost advertising.
Gaming: Decentralized gaming platforms, enable players to trade in-game items.

6.Law and Crime:
Police/Law: Preservation of evidence, no falsification data, time stamps, chain of facts.
Gun Safety: Tracking criminal ID's and preserving ownership of gun possession.

***7. Transportation**:*
Business Transportation: access to trip data and access the path.
Automotive: Tracking vehicles, supply chain management, production and sales history.
Public Transportation: Accurate payments, ride sharing, streamlining rides.

8. Governmental Services:
Government: Transparent voting system, minimization of fraud, citizen rights.
Travelling: Travel information, passport boarding information, passenger identification.
Healthcare: Patient database management, drug supply chain management, medical fee transactions, privacy.
Education: Proper educational channel, digitization, academic information.

9. Human Rights and Contributions:
Right to Information: Identity verification, history of employees, payment process.
Contributions: Maintaining donation integrity, ensuring safe fund raising channels.
Voluntary Organizations: Tracking all donations ensuring the integrity, reduces the complexity of process.[2]

IV.WHAT IS CRYPTOCURRENCY?

Cryptocurrency is termed as a digital or virtual currency which came into existence as a medium of exchange. It uses various cryptographical functions to secure and verify transactions as well as to control the creation of new units of a particular cryptocurrency. At core they are built on blockchain technology which supports decentralization, transparency and immutability. Basically, they are limited entries in a database that remain unchangeable unless specific conditions are fulfilled. [3]

V.ORIGIN OF CRYPTOCURRENCY

In the 1990's many researchers tried to create digital currencies. They existed for a while but due to several scams and frauds government had to shut it down. Some of the digital currencies were
DigiCash – Invented by an American cryptographer David Chaum which went bankrupt in 1998.
Web Based Money – In 90's many organization tried to advance DigiCash, one of them was PayPal. Paypal revolutioned person to person payment online . This company ran into various scams and shut down by federal government in 2005.
B-Money – Developed by WeiDai in 1998 was a distributed e-cash which came to an end.
e-gold was introduced in 1996 which grew users in millions and shut down by US government in 2008.
Satoshi Nakamoto's intension was not to create a currency. He wished to create a decentralized digital cash system/ledger.
Satoshi proposed that a consensus with a decentralized digital cash system could be achieved . This gave birth to digital decentralized currency in the form of Bitcoin.
Satoshi invention of Bitcoin became the first and most important cryptocurrency.
As Bitcoin was mined but never traded, it was nearly impossible to assign a monitory value to the units of cryptocurrency.[4]

VI. BEGINNING OF CRYPTOCURRENCY TRADING.

The first ever transaction according to records was made to buy two pizzas for exchange of 10,000BTC on 2nd May 2010. It was done by Laszlo Hanyecz. That day was commemorated as Bitcoin Pizza Day. [5] In the year 2011 bitcoin was used to buy drugs online on darknet, which attracted almost 1 million customers. Bitcoin and other currencies were also used for funding terrorism and illegal transactions.

VII HOW IS CRYPTOCURRENCY MINED?

Mining is a process in which each and every transaction between any number of users are verified and added in the blockchain public ledger. Cryptocurrency mining process also allows to introduce new cryptocurrencies to the existing circulatory supply.
Candidate Block: A temporary block created by the miner. It consist of unconfirmed transactions from the memory pool. In order to validate the new block created by the miner they complete with other miners for adding their block in the blockchain. Whenever the transactions are made they are received by all the nodes in the network to verify their validity.
The first ever step of mining a block is to hash each transaction individually which is taken from the memory pool. But before the process starts the miner adds a transaction in which he sends himself a mining reward. It is known as a Coinbase transaction. A Coinbase transaction is something where coin is created out of thin air. It becomes the first transaction in the new block.
After each and every transaction is hashed, they are organized in something known as **Merkle Tree.** In a Merkle tree, the root hash contains hash of previous block and a random number known as nonce. The nonce is added to the block header.
Hashing: Hashing is a technique of generating a fixed size output from a variable input with the use of cryptography and mathematical functions. The property that maintains data integrity and secure is that it cannot be easily reverted

without large amount of computing time and resources. It is easy to create the output but difficult to backtrack the input from the generated output. Several hashing algorithms are currently relevant which are used in various cryptocurrencies.

Block Difficulty: It is a measurement to find a hash below a given target. A block which is valid must have a hash below this target. Formula for difficulty is

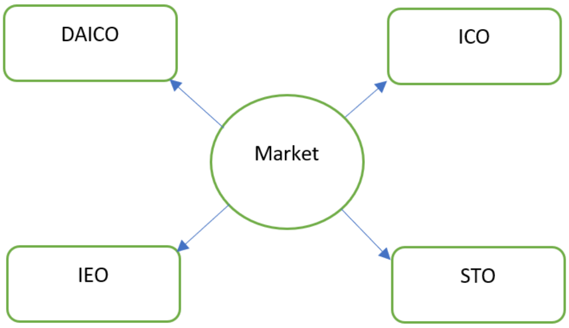
difficulty = difficulty of 1st target / current target.

People/Organization have developed large hardware setups to mine cryptocurrencies.[6][7]

VIII HASHING ALGORITHMS USED IN VARIOUS CRYPTOCURRENCIES

1. SHA-256: Used in Bitcoin, Devcoin, etc.
2. ETHash: Used in Etherium,etc.
3. Scrypt: Used in Dogecoin, Litecoin, etc.
4. EquiHash: Zcash, Zcoin,BitcoinGold etc.
5. Cryptonight: Monero, Dashcoin etc.

IX HOW ARE CRYPTOCURRENCIES INTRODUCED IN THE MARKET?



1: ICO- Initial Coin Offerings is a process by which a individual or organization can raise funds through cryptocurrencies by offering a token. This may involve issuing three types of tokens, (i) Utility tokens. (ii) Security Token (iii) Payment Tokens (iv)Equity token.

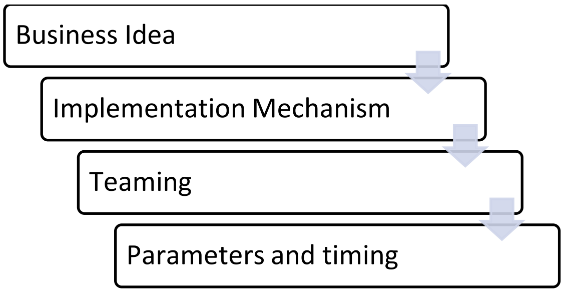
2: DAICO- Decentralized autonomous organizations and initial coin offeringsare more secure as investors funds are available in more controlled manner.

3: IEO- An IEO is a modified alternative of ICO. In IEO crowdfunding is done by issuing utility token or coin by crypto currency exchanges.

4:STO-Type of digital “securities papers” comparable with IPO.[9]

To create a new token and to determine the value of cryptocurrency there are several steps that are to be followed. Typically the first step should be selecting an existing blockchain network like etherium or any other public blockchain technology. Alternative is to create your own private blockchain technology. Second step is to issue tokens on the blockchain platform.

As a rule, Whitepaper should contain the following sections:



• *Description:* This must include the business idea or problem and proposed solution.

• *Implementation Mechanism:* It must contain implementation mechanism of how that token will interact with the product what are its economics and how will it be technically implemented.

• *Project team:* The project team members will be mentioned in the section.

• *Parameters and Timing:* It must include the parameters and timing of token at the time of release of the token. It may also contains its future plans.

To issue an ICO following are the 2 steps:

1. Launch Pre-ICO: This event is termed as the presale of units of the new currency. The prices are initially kept attractive to the investors later on with the demand supply prices may vary.
[10]

2.ICO Launch: In this event as soon as the coins are launched in the market, the first purchase are the sale investors of the ICO who plan to resell the currency after the demand of currency increases and prices hike over time.

X CIRCULATION OF CRYPTOCURRENCY IN GLOBAL MARKET

Circulating a cryptocurrency means coins or tokens are publicly available for trade. The circulation of crypto currencies is done on various platforms known as cryptocurrency exchanges. The circulating supply of a cryptocurrency can increase or decrease gradually over time. For example, maximum supply of bitcoin is 21 million. As the supply reaches the limit of 21 million the circulation of bitcoin will increase. Alternatively, coin burn event also occurs which causes a decrease in the circulating supply and the coins are removed permanently from the market.

Moreover, circulating supply of a cryptocurrency can be used for calculating its market capitalization. It is generated by multiplying current market price with total number of coins in circulation. If 100 BTCs are in circulation costing $8000 each, Market capital would be $800000.[8]

REFERENCES

[1]. "What is blockchain?", https://www.blockchain.com/
[2]. The History of Blockchain Technology: Must Know Timeline, https://101blockchains.com/history-of-blockchain-timeline/
[3]. Bitcoin and Cryptocurrency Technologies
[4]. "A Comprehensive Introduction", Princeton University Press Princeton and Oxford
[5]. How Cryptocurrency was Invented, https://medium.com/swlh/how-cryptocurrency-was-invented-71a62726fef6
[6]. A brief history on Bitcoin & Cryptocurrencies, https://www.ledger.com/academy/crypto/a-brief-history-on-bitcoin-cryptocurrencies/
[7]. "What is cryptocurrency mining?", https://www.binance.vision/blockchain/what-is-cryptocurrency-mining
[8]. "A Short History of Bitcoin and Crypto Currency Everyone Should Read", https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#1b43ff5e3f27
[9]. Circulating Supply, https://www.binance.vision/glossary/circulating-supply
[10]. Comparison analysis of ICO, DAOICO, IEO and STO. Case study.
[11]. Author: Alina Myalo, PhD Student, National Research University Higher School of Economics,
[12]. Assistant: Nikita Glukhov, National Research University Higher School of Economics.
[13]. What Makes an ICO Successful?
[14]. An Investigation of the Role of ICO Characteristics, Team Quality and Market Sentiment, Lauren Burns, Cranfield University.