IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BITCOIN THE NEW ECO-SYSTEM

[1]Sterin Saji, [2]Abhayraj Jaiswal, [3]R Raveena, [4]Rittik Mittal, [5]Lovenish,

[1]Engineering Student, [2]Engineering Student, [3]Engineering Student, [4]Engineering Student, [5]Engineering Student,

Department of Computer Science and Engineering,

Lovely Professional University, Jalandhar, Punjab, India.

Abstract: : **Bitcoin has emerged in the public imagination over the last two or three years as a key piece of technology that might, really change the way finance works for consumers, for people in developing countries and for the way that financial institutions actually conduct their business. One of the things that is challenging about this technology is that, there's so many details about how it works. And this can really be separated from what the technology is and what it does. And So, what this paper consists is really what this technology is and what kind of things it can empower. And the fact that we're not going to be able to fully forecast the best uses of this new technology.**

I. INTRODUCTION

A decentralized computation and information sharing platform that enables multiple authoritative domains, who do not trust each other, to corporate, coordinate, and collaborate in a rational decision-making process is called Blockchain. Blockchain is a decentralized database that helps in the cooperation between multiple authoritative domains.

Blockchain is a chain of blocks that contain information. It is originally intended to timestamp digital documents so that it is not possible to backdate them or tamper with them. A block chain is a distributed ledger that is completely open to anyone. If some data has been recorded inside a block chain it becomes very difficult to change.

A centralized system cannot simultaneously edit the documents. It works as a single point of failure. As centralized platforms are not scalable and as they are not robust to failure it is better to move from a centralized platform to a distributive platform. A blockchain verifiably moves 'data' on a decentralized network. Data can be value as bitcoin is a money system or the data can be computer code. In every block of a blockchain there contains some data, that hash of the block and the hash of the previous block. The data that is stored inside a block depends on the type of blockchain.

Blockchain helps to exercise individuality among documents. In a blockchain platform, simultaneous rewriting is possible as there is a network in between two nodes. The network has the task to ensure the information consistency. The consistency is maintained between documents that hold individually. All the documents are synchronized and an updated copy will only be displayed. The main advantage is that it doesn't have to rely on the internet. So, they don't depend on server crashes. Blockchain is a decentralized database platform with strong consistency support.

In many ways block chain adds costs to the verification through this consensus protocol, but it lowers some other costs of verification as it doesn't rely on centralized authority. It is a trade-off of cost to verification through decentralized networks. The data can represent value or computer code. This directly goes to the plumbing of finance, because finance is about moving money and risk through a network.

The bitcoin blockchain for example stores the details about a transaction, such as the sender, the receiver and amount of coin. A block also has a hash, it can be a fingerprint which identifies a block and all of its contents is always unique. Once a block is created its hash is being calculated. Changing something inside the block will cause the hash to change. Hashes are helpful to detect changes. If the fingerprint of a block changes, then the block is no more the same. The third element of the block is the hash of the previous block. This effectively creates a chain of blocks and that's the technique of a blockchain. By this manner the blockchain becomes more secure. Changing a single block will make all other blocks invalid. Using hashing alone can't prevent a block from tampering.

There is a mechanism called proof of work and that slows down the creation of new blocks. In case of bitcoin, it takes about ten minutes to calculate the required proof of work and add a new block to the chain. This mechanism makes it very hard to tamper with the blocks. The security of hashing comes from the creative use of hashing and the proof of work mechanism. It is also secured by being distributive as they use peer to peer network. People are allowed to join and those who joined the network they get the full copy of blockchain. The node can use this to verify that everything is still in order.

If a new block is created, then the block is sent to every one of the networks. Each node then verifies the block to make sure that it hasn't tampered. If everything checks out, each node is adding to their own blockchain. All the node in this network creates consensus. They agree about what blocks are valid and which aren't. Blocks that are tampered with will be rejected by other nodes in the network. To successfully tamper with a blockchain it is important to tamper with all other blocks.

In a typical blockchain architecture, every individual node maintains a local copy of the blockchain. The system's task is to ensure that all these individual copies are consistent with each other. Consistency means, that local copies that every node has are identical and these copies are always updated based on the global information. If an information is entered to any node of blockchain, then the information will get updated to all the copies of the blockchain that every node possesses.

The performance, scalability and efficiency are affected as low number of transactions can only be done in a second. It has privacy and security issues as they are public. They are interoperable as they do not work with other legacy systems. It is hard to update a software of block chain.

II. New Design for An Anonymous Cryptocurrency

III. Bitcoin and anonymity

IV. Problems with bitcoin

V. we all know bitcoin has problems with anonymity

VI. our address is public so we can know where the money goes

VII. for example, in the recent ransom ware WannaCry they published some address

VIII. where the money goes

IX. another example u can categorize transactions into classes

X. Existing technologies which can be alternative for anonymous payments

XI. -dash

XII. -Monero

XIII. -zcash

existing techniques for privacy for the technology mentioned above technologies are-:

- tumblers(dash)

- string signatures (Monero)

- zero-knowledge/snarks(zcash)

Frequently asked questions? About these technologies about their security purposes

- need for coordination?

- plausible deniability?

- provable anonymity?

- trust in 3rd party?

- size of UTXO?

3.2 Tumblers: suppose A wants to send money to B and C wants to send money to D. now they both will come together and cooperate and make 2-2 tumbler. Now A and C sends money to B and D but as an external observer you don't know the order Because It is at random. So, this can be generalized to N numbers of senders and N numbers of receivers.

Centralized tumblers And Decentralized tumblers.

Centralized tumblers are like you can send your money to some central authority and the central authority will send your money to destination but there you need to trust the central party.

Decentralized tumblers are hard you need to find people who joins together to do the decentralized protocol but there are known ways to do this using MPC.

3.3 Ring Signatures:

A ring signature is a signature where there is a set of public keys and you are signing on behalf of them but without revealing who? So, you need a distinguishability meaning that a signature for Pk-1 is 0 and signature for Pk-2 is indistinguishable and again here you can generalize to N number of public keys.

Zero-Knowledge:

Suppose that approver peter wants to send to prove the statement to verifier victor so this communication can go in multiple rounds until victor either say accept or reject.

So, it has to satisfy 3 properties-

- Completeness

P, V honest à V accepts

- Proof of knowledge

If P does not know x à V rejects

- Zero knowledge

V learns nothing about x

When the paper was published about all these techniques this was the state of these technologies-

When the paper was published about all these techniques this was the state of these technologies-

	Security		
	Anonymity	Deniability	Theft prev.
Tumblers	YES	NO	YES
Zcash	YES	NO	YES
Monero	NO	YES	YES

Table 1.1

So, we can see from the above Table 1.1, none of the technologies offer All their properties.

Quis Quis:

N to N transaction without interaction

S wants to send money to R

Add transaction from A to B for anonymity

This will create a Paradox?

- Move other people money without their approval
- While at the same time preventing theft

What if-.

- What if we have A send money to A', where A' is a random looking address OWNED by A?
  - For this, we need updatable public keys
    - public key can be "updated" with nonce to produce pk'
      - but should still verify the same signature as original public key
    - we want an unforgeable construction—given pk', you shouldn't be able to learn sk.
- Basic Quis Quis transaction:
  - Real input pk_s
  - Real output pk_r
  - Run update(pk_r) -> pk_r'

    - Pick random pk_A from UTXO set
    - Run update(pk_A) -> pk_A'
    - Then provide a zero-knowledge proof for the following statement:
        - "N - 1 public keys were updated correctly (hiding which ones)"
        - "I know the secret key corresponding to the last public key (and therefore I can spend it)"
- Towards the full construction...
    - This was of course simplistic
        - We assumed every PK held exactly 1 coin
        - Thus, no need to obscure PKs holding multiple UTXOs
        - Or having different values
    - We want to deal with variable amounts associated to keys
        - While also hiding amounts!
    - Instead, we'll have each public key have an associated balance, bl
        - The balance is stored in a homomorphic commitment
            - This allows it to be modified without knowing its value
        - Transactions are now "redistributions of value" among all balances
    - Accounts
        - Now pairs of public keys and commitments to the balance
        - acct = (pk, Com(pk, bl))
            - pk = (u, v)
            - Com(pk, bl) = (u^r, g^bl * v^r)
    - Accounts can be updated similarly
        - Update(acct = (pk, Com), v)
            - pk' = Update(pk)
            - c' = c * Com(pk, v)
            - Output acct' = (pk', c')
        - Worth noting:
            - The secret key is the same
            - Value can be increased/decreased by v
            - acct' cannot be linked to original acct!
- True QuisQuis transactions
    - Real sender: acct_s (loses v of currency)
    - Real receiver: acct_r (receives v of currency)
    - Pick random acct_A from UTXO set
    - Run update(acct_s, -v) -> acct_s'
    - Run update(acct_r, +v) -> acct_r'
    - Run update(acct_A, 0) -> acct_A'
        - This is your anonymity set!
    - Construct ZK proof that everything was done correctly:
        - All accounts were updated correctly, with amounts >= 0
        - Except one, for which I knew the secret key, whose balance was >= v
- Properties of QuisQuis
    - UTXO set does not grow
        - Only last version of accounts need be stored
    - Theft prevention
        - Can only withdraw from your own account (assuming balance is positive)
    - Anonymity
        - Updated accounts in the output are unlikable to accounts in the input set
        - Commitments hide the value
        - ZK proof hides the relationship between inputs/outputs and the value that was transferred

PROCESSES AND TECHNIQUES

Blockchain is a new technology, often referred as the Internet of Value. As with all new technologies, there is no consensus on its potential value, with some people claiming that it will bring more disruptive changes than the Internet and others contesting the extent of its importance.

Despite predictions that the future is perilous, there is evidence that blockchain is a remarkable, new technology that will change the way transactions are made, based on its ability to guarantee trust among unknown actors, assure the immutability of records, while also making intermediaries obsolete.

Importance of blockchain can confirmed by the interest in digital currencies, the great number of published blockchain papers, as well as MDPI's journal Future Internet which exclusively publishes blockchain articles, including this special issue covering present and future blockchain challenges.

Blockchain is an open, distributed ledger that records transactions between parties efficiently and in a verifiable and permanent manner. The present state of blockchain is often compared to that of the Internet in the mid-1990s, still in its infancy, when its value and potentials were not understood.

For instance, in a Newsweek article published in February 1995, Clifford Stoll, a computer expert, wrote "Baloney. Do our computer pundits lack all common sense? The truth is no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works"

The Unique Value of Blockchain

Blockchain provides a fundamental shift from the traditional Internet of information and communications to the Internet of Value, assuring the establishment of trust, achieved through the application of blockchain technology between strangers.

. Trust

. Immutability and Transparency

. Disintermediation

. Substantial Improvements

Longest Chain Rule: -

Have you however dealing get approved in a very Bitcoin block chain? Why you would like to attend for three to six confirmations for the transactions to seem in your notecase.

Let's assume Gobish transferred Bitcoin price 100$ from one crypto exchange to a different. Once he will the transfer, the dealing message is shipped to the network and passed around all the network participants that are referred to as nodes. this can be accessorial to the dealing pool. Currently, the dealing is in associate 'unconfirmed' state. All the dealings within the transaction pool are going to be in associate unofficial standing.

Now we are going to perceive World Health Organization may be a manual laborer. In straightforward words, those that validate new transactions and record them on the worldwide ledger of Blockchain square measure referred to as miners and this activity is termed mining.

To make it straight forward, let's assume their square measure presently three miners World Health Organization are attempting to substantiate the dealings from dealing pool as well as Gobish's transaction of $100.Ordinarily miners can choose those dealings which can generate a better transaction fee for them.

Currently, the numbers of confirmed blocks within the Blockchain public ledger are 998.

Once the miners determine that the 998th block May be a valid block they're going to attempt to produce a candidate block by adding unofficial dealings from the transaction pool. Currently these miners are attempting to feature the 999th block to feature the blocks they need to unravel a posh mathematical drawback. this can be referred to as Proof of labor (POW).

Let's assume all the three miners were ready to solve this drawback and have Proof of labor.
Now we've got three completely different candidate blocks, let's decision them 999 A, 999B and 999C
Now that of those blocks can kind a part of the valid block can rely upon the longest chain rule.
Let's perceive what's longest chain rule is.
Now their square measure alternative miners World Health Organization are attempting to make alternative valid blocks and based mostly upon the speed by that a block is made others miners can stick with it adding their blocks on prime of the sooner blocks.

Here during this case Minor C had a more robust processor that was ready to produce a block quicker than the manual laborer A and B and therefore new blocks were created on prime of the block 999C. Currently the longest chain is that the one created by 999C and it'll be stick with it adding alternative blocks like one thousand, 1001 so on as manual laborer C solved the proof of labor before manual laborer A and B.
So, what happens to the blocks 999A and 999B? they need to make the Proof of labor once more with new set of dealings from the transaction base.
Each confirmation represents adding every block. Every confirmation can defy a median of around ten minutes or additional per block.

Applying the longest chain rule and proof of labor, unofficial dealing can become a confirmed dealing and accessorial to the Blockchain ledger
Once the blocks square measure accessorial manual laborer can receive a transactions fees associated block fees which can be the new Bitcoin created as an incentive for approving the transactions.
Block rewards are going to be reducing per annum and within the finish solely dealing fees are going to be there as new Bitcoins won't be created.

XIV. FUTURE WORK: -

XV. The Future Cities Driven by Blockchain: -

XVI. Blockchain City is true story of blockchain and the reality how it impacts us all as people our cities our workspaces our families and our future. In 2008 when an entity or a group of people under the pseudonym of Satoshi Nakamoto came out with the famous white paper that highlighted a new electronic form of currencies. That would independently change everything about money.
XVII. He made the foundation of this new revolutionary currency and this revolution now culminated into global phenomena where Governments, private and public sector firms are embarking on creating more value more change and solving some of the world's biggest problems.
XVIII. When we are understanding this global movement to create more trust, secure our transactions and create more value Started in the City of DUBAI. This city where vision of tomorrow is driving and aggressive strategy if how technology can argument our Capabilities.
XIX. The Government of Dubai with its vision of tomorrow powered by technology has embarked on an aggressive plan to enable a Blockchain based government by 2022.
XX. The UAE also has a national plan to enable blockchain across all seven emirates by the Year 2030.
XXI. From Manufacturing to logistics, transportation, health care and real state every sector every industry is set to undergo a radical shift in the next few years potentially because of Blockchain.
XXII. Blockchain promises democratization of technology we need to break down the barriers to understand the blockchain itself. We must find out what blockchain really is and more than that how it can define what value it brings.
XXIII. It's a tool for decentralizing relationships contracts and decision making so that they aren't mediated by gatekeepers of various kinds. It is a very powerful idea.
XXIV. Estonia over the last two decades or so Estonia had led the foundation of a digitally powered nation and now reaping its rewards. Estonia is also considered to be the leader of Blockchain which in some ways is often a less represented fact.
XXV. Netherland with its Dutch blockchain coalition is spearheading efforts to create global awareness and impact for supporting collaboration between different companies between different governments, in supply chain it is helping them to work together and to give user a better user experience.
XXVI. Blockchain is social goods for example look into what United Nations are doing or the World Wildlife fund using the blockchain technologies to prevent overfishing in the South pacific or to prevent children trafficking by using blockchain technology then you can see that they are really kind of societal problems which can be addressed in prototypes by block trade agreements.
XXVII. From efficiency to identity management, financial transactions and more there seems to be a vast range of applications.
XXVIII. Forbes seen that what's their future because the print media is losing its share in the market so what they did they given all the power to the voters those who creates the media and realize very quickly that there are so many inequalities in the world so without giving the ownership to those who really create the value in the economy there would be no possibility to bring back the trust and create something that will be strong this monopoly that are controlling the entire media space.

HOW BLOCKCHAIN CAN TRANSFORM INDIA

Government spending our tax revenues should be done in Blockchain. We will know exactly where our taxes are being spent. It will help to reduce the corruption in the system and it should be implemented in all the governments institutions.

Agriculture is 16% of our GDP and around 120 million farmers.

Daily 23 farmers kill themselves, they don’t have farm equipment's to make yields happen if they own land their land is very small you can’t do scientific agriculture you can't get output based on the input. Even if you own that land most of the times it is recorded as theirs so they can’t get financing for all the inputs they want. Farmers go and take loans from Chit Financers who have higher interest rates and they end up killing themselves.

Blockchain is ideally suited to be the new UBER for tractors and Mahindra group also working on this concept. Where the cost will become much lesser and smart contracts make it much easier.

Blockchain is ideal technology to create fractional ownership so 11 farmers can own one tractor which is easier to do and all the financing and complications that arise from there can actually be taken care.

CONCLUSION

Blockchain is growing list of records called blocks that are linked using cryptography. Cryptocurrencies are a form of a Digital or virtual currency that run on a technology known as blockchain.

Cryptocurrencies are immune to counterfeiting don’t require a central authority and protected by string and complex encryption algorithms and in a market of more than thousands of cryptocurrencies like Bitcoin, Litecoin, Aetheriom Libra etc. but in all the names bitcoin is Supreme Leader

A simple analogy for understanding blockchain technology is Google Doc When we create a document and share it with a group of people the document is distributed instead of copied or transferred.

Example:

Ever wondered if there is an easier way of complete transaction without having complete transaction without having to deal with online wallets, banks and third-party applications well it’s possible because of blockchain.

Imagine four friends Jack ted Sam and phil meet up for lunch after they are done jack pays the bill and all of them decide to spill the expense amongst each other now on the next day when phil sends his share to jack via online money transfer the transaction goes through without a hitch and then ted and Sam send their respective share to jack but their transactions don’t go through the failed transaction site have some issues at the bank that’s when jack comes to know about the many ways a bank transaction could fail it could be due to technical issues at the bank on of their accounts were hacked daily transfer limits being exceeded in sometimes additional charges like transfer charges associated with transferring money to solve these problems the concept of cryptocurrency came into existence.

Now Assume the phil ted and Sam have three bitcoins in reserve while jack have five. First phil sends two bitcoins to jack a record is created in the form of Block the transaction details between permanently inscribed in this block. This Record also holds the number of bitcoins each of the friends own, so after phal's transaction jack have seven bitcoins while phil have one, following this Sam and ted sends two bitcoins to Jack a new block is created for each of these transactions these blocks hold the transaction details as well as how many bitcoins Sam ted and Jack have in reserve. These blocks are Linked to Each other as each of them takes reference from the previous one for the number of bitcoins each friend owns. This chain of records and blocks is called a ledger and this ledger shared is shared among all the friends which acts as a public distributed ledger this forms the basis of blockchain so what happens when phil has only one bitcoin left and he tries to send two more bitcoins to jack the transaction will not go through this is because all his friends have copies of the ledger and it’s clear that phil has only one bitcoin left so his friends will flag this transaction as invalid. A hacker will not able to alter the data in the blockchain because each user has a copy of the ledger the data within the blocks are encrypted by complex algorithms.

REFERENCES

[1] Manish Nagaraj and Somali Chatterji, “Panel 3 Position Paper: Blockchain can be the Backbone of India’s Economy”, IEEE, 7-11 Jan. 2019.

[2] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. kroll, Edward W. Felten, “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”, IEEE, 17-21 May 2015

[3] Meg Murray, Kennesaw State University, “A Descriptive Introduction to the Blockchain”, AIS Journals, 10.17705/1CAIS.04525

[4] Aabhas Sood and Rajbala Simon, “Implementation of Blockchain in Cross Border Money Transfer”, IEEE, 21-22 Nov, 2019.

[5] Mohammad Rabiul Islam, Rizal Mohd Nor, Imad Fakhri Al-Shaikhli, Kabir Sardar Mohammad,” Cryptocurrency vs. Fiat Currency: Architecture, Algorithm, Cashflow & Ledger Technology on Emerging Economy: The Influential Facts of Cryptocurrency and Fiat Currency “, IEEE, 23 July 2018

[6] Sachchidanand Singh, Nirmala Singh, “Blockchain: Future of financial and cyber security”, IEEE, 14-17 Dec. 2016.

[7] Gang Wang, Mark Nixon, “Blockchain: Practical Scalable Decentralized Randomness Attested by Blockchain”, IEEE, 11 December 2020.

[8] Leila Bahri, Sarunas Girdzijauskas, “Blockchain Technology: Practical P2P Computing (Tutorial), 2019 IEEE 4th International Workshops on Foundations and Applications of Self* Systems (FAS*W).

[9] Xiufeng Xu, “Towards Automated Migration for Blockchain-based Decentralized Application”, IEEE, 1 December 2020.

[10] Ghareeb Falazi, Michael Hahn, Uwe Breitenbücher, Frank Leymann, Vladimir Yussupov, “Process-Based Composition of Permission and Permissionless Blockchain Smart Contracts”, IEEE, 30 December 2019.