International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

BLOCKCHAIN -THE DRIVING FORCE BEHIND BITCOIN

Sumit Gupta[1], Shashwat Rastogi[2], Tanmey Srivastava[3]

[1,2,3] *Department of Computer Science and Engineering, Inderprastha Engineering College, Ghaziabad, (India)*

ABSTRACT

BITCOIN is the first de-unified advanced digital currency, created and held electronically. There is no central authority in the Bitcoin network. Blockchain is a large network of PCs which works regularly to check the authenticity of transactions and process them progressively so that no bank or government should be a central authority. Blockchain is the technology for new era of transactional-based applications that sets up trust, responsibility and straightforwardness while streamlining business processes. This paper examines the blockchain and why the blockchain (alongside bitcoin) holds the possibilities of being a market disrupter in near future.

Keywords:Block trade, Blockchain, Blockchain mining, Fraud Detection, Double Spend, ECDSA

I. INTRODUCTION

The blockchain is viewed as the technological advancement of Bitcoin, since it remains as verification of all the transactions on the network. A block is the "underlying" part of a blockchain which records a few or the majority of all the transactions, and on completion goes into the blockchain as permanent database. Every time a block gets completed, another block is created. are connected to each other (like a chain) in legitimate straight, sequential request with each block containing a hash of the previous block. Every block is ensured to come after the previous block chronologically because the past block's hash would somehow not be known. A chain is valid if all the blocks and transactions within it are valid, and only if it starts with the genesis block thus being immutable.

II. TYPES OF BLOCKCHAIN

two categories:

A. Public Blockchain

All information on public blockchains are open as a matter of course, despite the fact that it is basic to shroud the actual character of all associated participants on them like Bitcoin Does They determine their security by their extremely "open ness," where each member can see all account balances and the transactions performed.

Advantages:

A public blockchain is a transparency engine. Public blockchains "shield the clients of an application from the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

developers, building up that there are such things that even the designers of an application have no power to do that might be harmful to others.

B. Private Blockchain

A private blockchains are secured by the archaic model of client rights and secret facts that we've become so comfortable with ever since the first lock was invented. The fewer individuals who think about your database, the more secure it is in this model. The more private a blockchain is run, the more probable the tenets administering the blockchain can be modified which deceives the entire motivation behind blockchain.

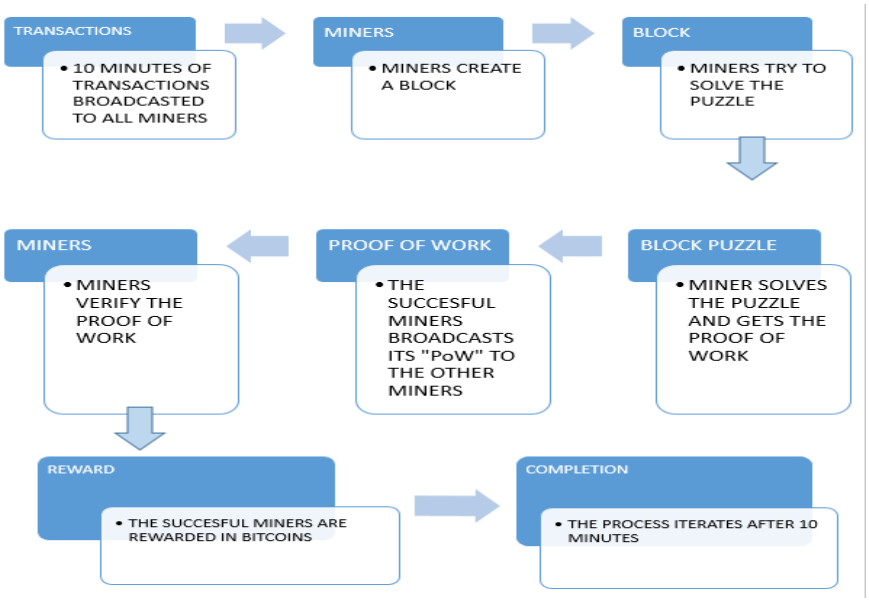
Advantages:

There are couple of nodes all with high trust levels. No requirement for each node to confirm all the transactions and speed of a privately run blockchain can be quicker than some other blockchain solution, drawing nearer even the rates of a typical database that isn't a blockchains.

III. BLOCKCHAIN MINING

The "Distributed Trust" given by the blockchain network makes Bitcoin for all intents and purposes un-hackable and truly coming out of the age.

How Bitcoin Mining Works:



IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

At regular intervals or so mining PCs gather a couple of hundred pending bitcoin transactions (a "block") and transform them into a mathematical puzzle. The first miner to discover the solution reports it to others on the network. Other miners then check whether the sender of the assets has the privilege to spend the cash, and whether the answer for the puzzle is right. If enough of them allow their endorsement, the block is cryptographically added to the record and the miners proceed onward to the following set of transaction (subsequently the expression "blockchain"). The miner who found the solution gets 25 bitcoins as a reward, yet simply after another 99 pieces have been added to the record. This gives excavators an impetus to take an interest in the framework and approve transactions.

IV. BLOCK TRADE

A block trade, otherwise called a block order, is a request or trade submitted for the sale or purchase of a large amount of securities. Block trades are typically directed through a mediator known as a block house. These organizations spend significant time in large trades and know how to start such transaction deliberately, in order to not trigger an unstable ascent or fall in the cost of the security. In this way, when a large institution chooses to start a block trade, it will connect with the staff of a block house, believing they will collectively get the best deal. For guaranteeing the security in block trade and bitcoin exchanges very large numbers are used for its base point, prime modulo, and order therefore gigantic values are used in ECDSA (Elliptic Curve Digital Signature Algorithm).

Elliptic curve equation: $y2 = x3 + 7$

Prime modulo

$=2256 – 232 – 29 – 28 – 27 – 26 – 24 - 1$

= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

Base point

= 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Order

= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

The security of the algorithm relies on these values being large, and therefore impractical to brute force or reverse engineer hence security in block trade and bitcoin exchanges is achieved.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

V. WHY THE BLOCKCHAIN HYPE?

The blockchain idea speaks to an outlook change in how programming designers will compose programming applications later on, and it is one of the key concepts that needs to be well understood. Blockchain obviates the need of any central authority/bank by

- Decentralized consensus
- Proof of work (and proof of stake)

Decentralized consensus (on or off bitcoin's blockchain): A decentralized plan, on which the bitcoin convention is based, transfers authority and trust to a decentralized virtual network and enables its nodes to continuously and sequentially record transactions on a public "block," creating a unique "chain": the blockchain. Each progressive block contains a "hash" (a unique finger impression) of the past code; therefore, cryptography (by means of hash codes) is utilized to secure the validation of the transaction source and obviates the need of a middle man. The mix of cryptography and blockchain innovation together guarantees there is never a duplicate recording of similar transaction.

Proof of work (and proof of stake): Confirmation of work is a key building piece since it can't be "fixed," and it is secured by means of the qualities of cryptographic hashes that guarantees its authenticity. In any case, proof of work is costly to keep up (evaluated cost of $600M every year for bitcoin), and may keep running into future scalability issues as the exclusivity of miners decreases. Proof averts undesirable forking of the basic blockchain.

VI. ADVANTAGES AND DISADVANTAGES

Advantages of blockchain technology

- **Durability, reliability, and longevity**
  Due to the decentralized networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks.
- **Disintermediation & trustless exchange**
  Two parties are able to make an exchange without the oversight or intermediation of a third party, strongly reducing or even eliminating counterparty risk.
- **Empowered users**
  Users are in control of all their information and transactions.
- **High quality data**
  Blockchain data is complete, consistent, timely, accurate, and widely available.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

- **Process integrity**
  Users can trust that transactions will be executed exactly as the protocol commands removing the need for a trusted third party.
- **Transparency and immutability**
  Changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.
- **Faster transactions**
  Interbank transactions can potentially take days for clearing and final settlement, especially outside of working hours. Blockchain transactions can reduce transaction times to minutes and are processed 24/7.
- **Lower transaction costs**
  By eliminating third party intermediaries and overhead costs for exchanging assets, blockchains have the potential to greatly reduce transaction fees.

Challenges of blockchain technology

- **Nascent technology**
  Resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making blockchain widely applicable.
- **Uncertain regulatory status**
  Because modern currencies have always been created and regulated by national governments, blockchain and Bitcoin face a hurdle in widespread adoption by pre-existing financial institutions if its government regulation status remains unsettled.
- **Double Spend**
  A double spend is an attack where the given set of coins is spent in more than one transaction. There are a couple main ways to perform a **double spend**: Send two conflicting transactions in rapid succession into the Bitcoin network. This is called a race attack
- **Cost**
  Blockchain offers tremendous savings in transaction costs and time but the high initial capital costs could be a deterrent.

VII. CONCLUSION

Investments in bitcoin and blockchain infrastructure is booming with blockchain being under the limelight of everyone – banks, security firms, hacker groups, small businesses. But as with any new technology, people are still figuring out the best applications of this nascent technology. By registering digital assets there (anything from financial data to system configurations), you can protect them against unauthorized changes. Then again, the push

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

to re-evaluate the worldwide money related framework is, at present, little more than a collection of ideas and incubators — in an industry that is almost immutable.

The mass media's inclination to depict Bitcoin as a withering away trend and the blockchain as a failed technology anyhow the overall population's lack of understanding of Bitcoin and blockchain are some of the biggest roadblocks. This strategy still feels odd to us since we're so new to this approach to security, yet in seven years of bitcoin's presence, nobody has figured out how to beat the security level of blockchain. This processing paradigm is essential since it is the impetus for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs.

REFERENCES

Journal Papers:

[1] Bitcoin's block number 0, http://blockexplorer.com/b/0

[2] Block v2, height in coin base, Bitcoin Improvement Proposal, 2012, https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki.

[3] Bitcoin's block number 180,000, http://blockexplorer.com/b/180000

[4] Block chain: Bitcoin charts, http://blockchain.info/charts

Books:

[5] Re: [Bitcoin-development] is there a way to do bitcoin-staging? 2013, Mailing list post, http://sourceforge.net/p/bitcoin/mailman/message/ 31519067/.

[6] L. Bahack, Theoretical Bitcoin attacks with less than half of the computational power (draft), arXiv preprint arXiv:1312.7013 (2013).

[7] Reid, F., Harrigan, M.: An Analysis of Anonymity in the Bitcoin System, arXiv:1107.4524v2 [physics.soc-ph] (May 7, 2012)

[8] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology Proceedings of Crypto 82 (1983), no. 3, 199–203.

Proceedings Papers:

[9] Forbes: Top 10 Bitcoin Statistics, http://www.forbes.com/sites/jonmatonis/2012/07/31/top-10-bitcoin-statistics/

[10] Silvio Gesell, The natural economic order, Peter Owen Ltd. 1958., London, 1916, https://archive.org/details/TheNaturalEconomicOrder.

[11] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)

[12] G. Maxwell, Deterministic wallets, 2011, BitcoinTalk post, https://bitcointalk. org/index.php?topic=19137.0.

[13] Hamacher, K., Katzenbeisser, S.: Bitcoin - An Analysis (December 29, 2011), http://www.youtube.com/watch?v=hlWyTqL1hFA

[14] A. Poelstra, ASICs and decentralization FAQ, 2014, https://download. wpsoftware.net/bitcoin/asic-faq.pdf.