Blockchain: Future of Financial and Cyber Security

Sachchidanand Singh
IBM Software Lab
Pune, India - 411 057
Email: sach.success@gmail.com

Nirmala Singh
Tech Mahindra
Pune, India - 411 057
Email: nirmala.online@gmail.com

Abstract—**Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction.**

Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it's a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks.

Satoshi Nakamoto described design of Bitcoin digital currency in his research paper posted to cryptography listserv in 2008. Nakamoto's suggestion has solved long pending problem of cryptographers and laid the foundation stone for digital currency.

This paper explains the concept, characteristics, need of Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking, financial institutions and adoption of Internet of Things(IoT).

Keywords—Blockchain; Bitcoin; Genesis Block; Rehash; LevelDB; SHA-256; IBM Bluemix; IoT; Bitfinex; BitTorrent; Ethereium

I. INTRODUCTION

The cost of cyber-crime costs quadrupled from 2013 to 2015 however a large portion of cybercrime goes undetected. Gartner report says cost of cyber-crime is expected to reach $2 trillion by 2019 [1]. IBM's CEO, Ginni Rometty said that cyber-crime is the greatest threat to every company in the world at IBM Security Summit [2].

Around two years ago Standard Chartered lost around $200 million in a fraud at China's Qingdao port [3]. Banking and financial institutions are using Blockchain based technology to reduce risk and prevent cyber fraud. For example, Nasdaq has announced its plan to launch Blockchain based digital ledger technology which will help to boost their equity management capabilities. Standard Chartered is partnering with DBS Group to develop an electronic invoice ledger using a Blockchain.

Blockchain can play crucial role in Internet of Things(IoT) and development of smart systems since we can track the history of individual devices by tracking a ledger of data exchanged. It can enable smart devices to act like an independent agent which can autonomously perform several transactions [4].

For example, smart home appliances competing with one another for priority so that laundry machine, thermostats, dishwasher and smart lighting run at an appropriate time to minimize cost of electricity against current grid prices. Another example could be smart vehicles which can diagnose any problem and schedule to pay for its maintenance.

II. WHAT IS BLOCKCHAIN

Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on network to edit the ledger in a secured way which is shared over distributed network of the computers.

For making any changes to the existing block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with Blockchain history. If majority of the nodes agree in favor of the transaction, then it is approved and a new block gets added to the existing chain.

The Blockchain metadata is stored in Google's LevelDB by Bitcoin Core client [5]. We can visualize Blockchain as vertical stack having blocks kept on top of each other and the bottommost block acting as foundation of the stack. The individual blocks are linked to each other and refers to previous block in the chain.

The individual blocks are identified by a hash which is generated using secure hash algorithm (SHA-256) cryptographic hash algorithm on the header of the block [5]. A block will have one parent but can have multiple child each referring to the same parent block hence contains same hash in the previous block hash field. Every block contains hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as Genesis block.

III. WHAT IS BITCOIN

Bitcoin is digital currency released as an open-source software in 2009. It is a decentralized cryptocurrency produced by all the participating nodes in the system at a defined rate. The chain of Bitcoins created over period and linked to each other called Blockchain. It can be used to search any past transaction happened over the network between Bitcoin

addresses. When a new block of transactions is created, it gets added to the Blockchain. The new transaction records are continuously added to Bitcoin's public ledger and this process is called Bitcoin mining.

Secure Hash Algorithm 2 (SHA-2) which is a cryptographic hash function is used by Bitcoin. We can determine integrity of a given data by comparing the execution output of SHA-2 algorithm called "hash" with an already known and expected hash value.

A hash algorithm converts a large volume amount of data into a fixed-length hash. And same data will always produce same hash but any slight modification in data will completely change the hash.

IV. WHAT IS GENESIS BLOCK

The first block #0 created in 2009 is referred as Genesis block in Blockchain. It is common ancestral parent of all the new blocks created and if traversed backward in time we will reach genesis block in the end.

Genesis block is common ancestor of all the blocks and was created in 2009. It is encoded within bitcoin client software and can't be tampered. All the node always knows the hash and structure of genesis block which is secure root. The statically encoded genesis block can be seen inside the Bitcoin Core client in chainparams.cpp [6]. We can look for exact block hash:

"000000000019d6689c085ae165831e934ff763ae46a2a6c1 72b3f1b60a8ce26f" in the block explorer websites to find details of Genesis block, latest transactions and all the newly created blocks with BlockHash, height, next block, size in bytes [7].

Genesis block contains a text message "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" [5]. The message was embedded in the first block by Bitcoin's creator Satoshi Nakamoto. It offers proof of date when Genesis block was created which refers to headline of British newspaper The Times. The donation for Genesis block was made by John Wnuk and Jayden McAbee on June 9, 2016 which contains the first Bitcoin wallet.

V. PREREQUISITES OF BITCOIN

A. Authentication

BitID which is a decentralized authentication protocol allows users to connect with Bitcoin. BitID uses bitcoin wallets and QR codes to provide service or platform access points.

B. Integrity

Bitcoin's use of digital signatures ensures transactional integrity and transactions can't be modified later.

C. Non-Repudiation

The person who sent the message had to be in possession of the private key and therefore owns the Bitcoins. The sender needs to sign the previous hash and the destination public key.

VI. BENEFITS OF BITCOIN

A. Fast & Cheaper

The transactions made using Bitcoin's wallets are fast and transaction fees are minimal.

B. Decentralized Registry

Bitcoin currency is decentralized and no central authority has full control and hence central government or banks can't take it away from you and there is no chargeback.

The Central Bank during financial crisis in Cyprus wanted to take back all uninsured deposits more than $100,000 in 2013 to help recapitalize itself [8]. But this is not possible with Bitcoins since currency is decentralized.

C. Secure Payment Information

Bitcoin transactions uses a public key and a private key. When a bitcoin is sent, the transaction is signed by public and private keys together which creates a certificate.

D. Bitcoin Mining

You can create your own money by setting up a Bitcoin Miner. [9]

VII. HOW BITCOIN WORKS

Bitcoin uses Elliptic Curve Digital Signature Algorithm(ECDSA) cryptographic algorithm to make sure only rightful owners have the access to funds [10].

When Bitcoin is sent, it creates a transaction message and attaches new owner's public ECDSA key. Each Bitcoin is associated with public ECDSA key of its current owner. A new transaction is broadcasted over Bitcoin network to inform everyone that new owner of these coins is the owner of the new key.

Bitcoin kiosks are machines which are connected to the internet and allow to deposit cash in exchange of Bitcoin's given as a paper receipt or by moving money to a public key on the Blockchain [11]. Whenever a Bitcoin is sent, it attaches the new owner's public key and sign it with the sender's private key. The sender's signature on the message verifies that the message is authentic and transaction history is kept by everyone so it can be easily verified.

It uses Public Key Cryptography Asymmetric Encryption algorithm and concept of public and private keys to encrypt and decrypt data. If message is encrypted using public key(P_k), then private or secret key(S_k) is necessary to decrypt. However, when message is encrypted using private or secret key(S_k) then public key(P_k)is necessary to decrypt.

The public key can be shared with anyone but private key needs to be kept secret. One participant can create multiple public key(Pk) and secret key(Sk) pair.

Bitcoin does not require third party as it publicly distributes the ledger called Blockchain. The interested users in devoting CPU power to run a special piece of software are called Bitcoin miners and they ultimately form a network to maintain the

Blockchain. In the Bitcoin mining process, users create new Bitcoin currency and transaction is broadcasted over the network.

All the computers running the software in network compete to solve cryptographic puzzles which contains data from several transactions. The first miner who solves each puzzle get 50 new Bitcoins and the corresponding block of transactions gets added to the existing Blockchain.

The difficulty level of each puzzle is directly proportional to the number of Bitcoin miners present. As the number of miners increases, the difficulty level of puzzle is also increased to ensure production of one block of transactions for every 10 minutes.

Bitcoin works on decreasing supply algorithm which means the reward for mining Bitcoin block is reduced to half after every 210,000 blocks [12], [13]. The block creation rate is adjusted every 2016 blocks to ensure creation of roughly 6 blocks per hour. The number of Bitcoins generated per block is set to decrease geometrically and it will reduce by 50% every 210,000 blocks which is approximately 04 years' time [14]. The aim is to ensure number of Bitcoins in existence never exceeds 21 million since monetary base of Bitcoins cannot be expanded therefore Bitcoin currency would undergo severe deflation if it becomes widely used [15].

VIII. Bitcoin Advanced

Bitcoin transactions are made using script which is stack-based and processed from left to right. The script contains list of instructions recorded with each transaction having description on how receiver can gain access to it.

The transactions are valid if script returns true.

if verify_signature(transaction.signature, transaction.input.public_key): return True

else

return False

The standard transactions on Bitcoin network are called single-signature transactions because it requires just one signature from the owner. But Bitcoin also supports complex transactions which require signature of more than one people. It supports Multisignature (Multisig) transaction which sends funds from a multi-signature address and referred as M-of-N transactions which is associated with N private keys and requires signatures from at least M keys [16].

Lock times is a bitcoin feature which makes a transaction not allowed to the network until a certain time. The locked transaction will spend the coins it uses as inputs at a certain time in the future, unless those coins are first spent by a prior transaction.

Micropayment channels use both multi-sig technology and a lock time. Bitcoin multisig wallets have potential for increasing the security of funds and giving technology tools to enforce better corporate governance.

Each transaction is added to the blockchain after consensus among nodes and verification to protect against double spending. The transactions are validated when a mathematical problem is solved. The Bitcoin transactions require a time window before they are confirmed which is an issue since speedy transaction is expected from digital currency in the modern world.

But using marker address also called as green address approach we can reduce the time taken for confirmation of Bitcoin transaction. The marker addresses use Bitcoin's own communication channel and parties can establish trust sine a receiver is already waiting for an address to send money.

Pay to script hash (P2SH) transactions is supported by Bitcoin which allow transactions to be sent to a script hash instead of a public key hash [17]. The recipient must provide a script matching to the script hash to spend bitcoins sent via P2SH and the data which makes script evaluation true.

We can send bitcoins using P2SH to an address that is secured. The bitcoins can be sent to ~34-character P2SH address and recipient needs signatures of several people to spend bitcoins or a password or there could be entirely unique requirements.

Byzantine consensus problem is used in a large peer-to-peer network [18], [19], [20]. All the processes in the network should come to a common agreement. The networks without admission controls are vulnerable to the Sybil attack in which malicious processes can claim multiple fraud identities.

Satoshi Nakamoto inventor of the Bitcoin protocol published his research paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008. This paper talked about peer-to-peer electronic cash transfer directly from one party to another without going through the channel of financial institutions [21].

Ethereum is a public Blockchain based distributed computing platform which runs smart applications without any downtime or third party interference. These applications run on a custom built Blockchain which enables to store registries of debts or promises and move funds without requiring a middle man or counterparty risk. Ethereum provides a decentralized virtual machine called Ethereum Virtual Machine (EVM) which can execute peer-to-peer contracts using a cryptocurrency called Ether [22]. Ethereum project was bootstrapped by an Ether pre-sale during 2014 and developed by a Swiss nonprofit group called Ethereum Foundation.

Blockchain based DNS and Blockchain based internet could be future. The DNSChain offers a free and secure decentralized alternative while remaining backwards compatible with traditional DNS.

IX. Blockchain Adoption Trends

PricewaterhouseCoopers(PwC) reports shows Blockchain is being explored and adopted at an unprecedented speed [23]. Blockchain is still five to ten years from mainstream adoption but it's already reached peak of inflated expectations reported by Gartner in Hype Cycle for Emerging Technologies 2016 [24].

Blockchain stores multiple transactions in one centralized ledger which is accessible to all parties and activities are regulated by a decentralized network. There are around dozens of offerings on distributed-ledger products in the market but Bitcoin is most popular and proven among all [24].

The 3 trends appearing in Gartner Hype Cycle for emerging technologies 2016 are Blockchain, Smart machines giving transparent immersive experiences like 4D printing and Internet of Things (IoT) leading to perceptual smart machine age [24].
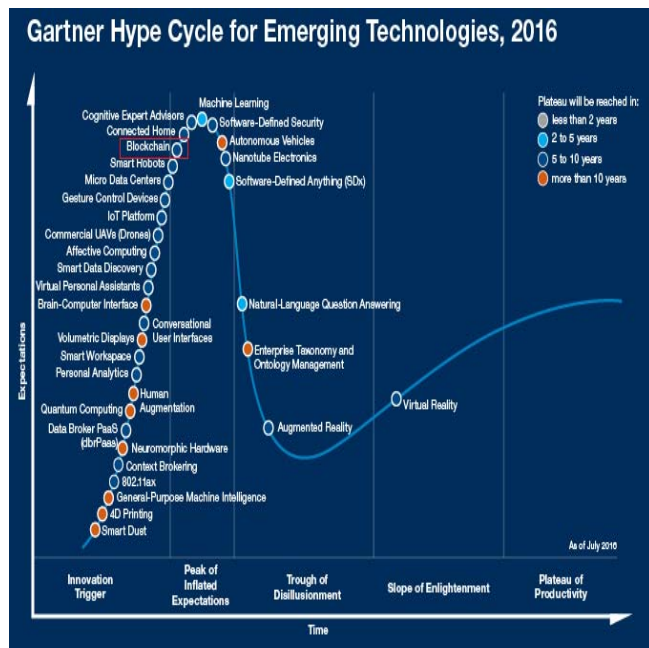

Fig. 1. Gartner Hype Cycle 2016[24]

Nasdaq has announced plan to launch Blockchain-enabled digital ledger technology which will help to expand and enhance its equity management capabilities. They will initially leverage Open Assets Protocol which is a Bitcoin based colored coins' implementation [25].

Bitfinex is Hong Kong based world's leading Bitcoin exchange which one of the most advanced cryptocurrencies exchange offering margin trading, advanced order types & margin funding for low-risk returns [26], [27].

IBM Blockchain service on Bluemix provides four-node development and test blockchain network to write applications and deploy chain code immediately instead of creating Blockchain network from the scratch. It is basically a peer-to-peer permissioned network which is built on top of Hyperledger Fabric from Hyperledger Project of Linux Foundation [28].

The land registry system is broken in Honduras, a Central American country due to corruption. Government of Honduras announced a deal with Factom Inc, a Texas-based Blockchain company to implement Factom's Land Registry Tool to create

transparency in land registry. They are using Blockchain technologies to update and maintain land registry records to prevent corruption since once land records are verified it can't be tampered [29].

IBM and Samsung are working on a proof of concept (PoC) to build next generation Internet of Things(IoT) which will be based on Autonomous Decentralized Peer-to-Peer Telemetry(ADEPT) which uses BitTorrent peer-to-peer file sharing protocol, Rehash peer-to-peer communication protocol, Bitcoin cryptocurrency & Ethereium [30].

Everledger is using Blockchain to tackle conflict diamonds and insurance fraud since tracking of diamonds from mine to retail stores is a lengthy and complex process. They are combining data from insurance companies and police departments to provide an accurate database which can be made available to everyone on Blockchain [31].

Distributed Autonomous Organization(DAO) is an organization meant to support Ethereum-related projects. DAO has received over $50m worth of digital token called ethers (ETH) from investors. People supporting DAO receive voting rights in form of digital token to determine future direction of the organization and support startups and projects by dispensing ethers (ETH). The participants in the voting and decision making process receive dividends for supporting the project [32].

X. SUMMARY AND CONCLUSION

Venture capital(VC) firms are betting big on Bitcoin and the Blockchain. CoinDesk's Bitcoin Venture Capital data shows that VC firms are investing heavily in bitcoin startup projects. Blockchain can act as ledgers or record-keeper for billions of transactions generated by Internet of Things(IoT) since sharing, storing data and information is always a risk.

Mckinsey report says that Blockchain have potential to reshape the capital markets industry with impact on business models, reductions in risks, cost and capital savings [33]. The adoption of Blockchain technology will have significant benefits and reduce number of ledgers required to be maintained by financial institutions and ensure more precise audit trails [33].

A recent study from IBM Institute for Business Value (IBV) shows that 70 percent of early adopters surveyed are prioritizing Blockchain efforts to reduce barriers in creating new business models to reach new markets. The seven out of 10 early adopters surveyed in financial market institutions have Blockchain efforts focused mainly on four areas: clearing and settlement, equity and debt issuance, wholesale payments and reference data [34].

The device cost is decreasing and computing power is increasing every day therefore Blockchain presents an immense possibility in Internet of Things(IoT) and providing security. Blockchain can offer a trustless system having peer-to-peer messaging protocols and secured distributed data sharing.

REFERENCES

[1] Cyber Crime Costs Projected To Reach $2 Trillion by 2019, http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#768e4f293bb0

[2] IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World', http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#16ff2faf3548

[3] Banks Look To Blockchain To Reduce Fraud In $4 Trillion Trade Finance Field, https://www.cryptocoinsnews.com/banks-blockchain-trade-finance-fraud/

[4] Blockchains and the Internet of Things, http://www.postscapes.com/blockchains-and-the-internet-of-things/

[5] Chapter 7. The Blockchain, http://chimera.labs.oreilly.com/books/1234000001802/ch07.html/

[6] bitcoin/src/chainparams.cpp, https://github.com/bitcoin/bitcoin/blob/3955c3940eff83518c186facfec6f50545b5aab5/src/chainparams.cpp#L123

[7] Bitcoin Block Explorer, https://blockexplorer.com

[8] Why Use Bitcoin? http://www.coindesk.com/information/why-use-bitcoin/

[9] How to Set Up a Bitcoin Miner, http://www.coindesk.com/information/how-to-set-up-a-miner

[10] Elliptic-curve digital signatures, http://davidederosa.com/basic-blockchain-programming/elliptic-curve-digital-signatures/

[11] How to sell bitcoins using Bitcoin ATM, https://coinatmradar.com/blog/how-to-sell-bitcoins-using-bitcoin-atm/

[12] The Rise and Fall of Bitcoin, https://www.wired.com/2011/11/mf_bitcoin

[13] State Of Bitcoin 2016 – A Summary For Bitcoin Investors, http://cryptorials.io/state-of-bitcoin-2016-investors-summary

[14] Currency with Finite Supply, https://en.bitcoin.it/wiki/Controlled_supply

[15] Bitcoin Monetary Inflation, https://plot.ly/~BashCo/5.embed?share_key=ljQVkaTiHXjX2W41Uiqz Cn

[16] What is Multi-Sig, and What Can It Do? https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do

[17] Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide#block-chain-overview

[18] How Consensus Algorithms Solve Issues with Bitcoin's Proof of Work, http://www.coindesk.com/stellar-ripple-hyperledger-rivals-bitcoin-proof-work/

[19] Tendermint: Consensus without Mining, http://tendermint.com/docs/tendermint.pdf

[20] Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, https://socrates1024.s3.amazonaws.com/consensus.pdf

[21] Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[22] What is Ethereum, https://cryptocrawl.in/what-is-ethereum/

[23] What's next for blockchain in 2016? - PwC, https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-qa-whats-next-for-blockchain.pdf

[24] 3 Trends Appear in the Gartner Hype Cycle for Emerging Technologies, 2016, http://www.gartner.com/smarterwithgartner/3-trends-appear-in-the-gartner-hype-cycle-for-emerging-technologies-2016

[25] Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative, http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196

[26] Bitfinex Examined: Inside the Troubled Bitcoin Exchange's History, http://www.coindesk.com/bitfinex-examined-bitcoin-exchange/

[27] How To: Earn Passive Income with Bitfinex Margin Funding,http://cryptocrooks.com/how-to-setup-bitfinex-margin-funding-for-passive-income/

[28] Getting started with IBM Blockchain, https://console.ng.bluemix.net/docs/services/blockchain/index.html

[29] Factom Partners With Honduras Government on Blockchain Tech Trial,http://www.coindesk.com/factom-land-registry-deal-honduran-government/

[30] Is blockchain the key to the Internet of Things? IBM and Samsung think it might just be http://www.zdnet.com/article/is-blockchain-the-key-to-the-internet-of-things-ibm-and-samsung-think-it-might-just-be

[31] Can Blockchain Help Curb The Flow of Blood Diamonds? http://www.nasdaq.com/article/can-blockchain-help-curb-the-flow-of-blood-diamonds-cm673953

[32] The DAO: Or How A Leaderless Ethereum Project Raised $50 Million, http://www.coindesk.com/the-dao-just-raised-50-million-but-what-is-it

[33] Beyond the hype: Blockchains in capital markets, http://www.mckinsey.com/industries/financial-services/our-insights/beyond-the-hype-blockchains-in-capital-markets

[34] Blockchain Adoption Moving Rapidly in Banking and Financial Markets: Some 65 Percent of Surveyed Banks Expect to be in Production in Three Years, https://www-03.ibm.com/press/us/en/pressrelease/50617.wss