Amplifying Security & Privacy through Block Chain Technology

1Prof. Vikas P. Raut
1Head - Department of Computer Science
1Vikas College of Arts, Science & Commerce

Abstract - **To sort any kind of information, performing functions, executing transactions and to gain trust in an liberal environment the best innovative offerings are from the Blockchain. The world considers block chain technology to be a big innovation in cryptography and cyber security, with cases referring from globally deployed systems like Bitcoin and smart grids over the Internet of Things to name a few. Though in the recent block chain has been well received in both corporate industry and academia the privacy and its security continue to be the matter of debate when it comes deploying it in different applications. This research paper highlights amplifying security and privacy on block chain technology, to discuss further lets first understand the notion and block chain utility in the reference like Bitcoin online transactions. Further over viewing the security properties as well as privacy properties yearning in blockchain applications reviewing the algorithms, mixing protocols, unidentified signatures, hash chained storage etc. In anticipation that this research paper will focus with regard to the techniques, attributes, concepts and systems of the security and privacy of blockchain technology.**

keywords - **Blockchain, Security, Privacy, Cyber Security, Technology.**

I. Introduction

A distributed database system which logs and evolves list of transaction records organizing them in hierarchical chain of blocks securing computing without centralized authority in an open networked system has been the recent achievement of Blockchain Technology. With reference to the security point of view it is created using peer to peer overlay network, securing via intelligent as well as decentralized usage of cryptography along with crowd computing. Artificial Intelligence and Big Data along with Blockchain is predicted to be the three core computing technologies for business and financial sectors in next gen. In U.S.A ‘ Delware Block Chain Initiative ’ has been launched by its governor, whereas Europe, U.K, China and also Indian government have released white papers along with detail technical reports on block chain to project its positive attitude towards development and enhancement of blockchain technology.

The world experts have been predicting Dollar 20.09 billion annual revenue by 2025 of block chain based applications worldwide, already technological research and capital layout experiments have been speed up by giant corporate like HSBC, Morgan Stanley, Microsoft, IBM to name a few, where in other end Apache Foundation and IBM has been sponsoring blockchain research programs on Hyper Ledger Project of Bitcoin.com and File Coin providing them open source space and platforms.

In this research paper we will discuss the two segments of security and privacy research study on blockchain which are mainly (a) Exposing few significant assaults suffered by block chain system till date (b) Proposing countermeasures against a subset of such attacks. Nevertheless, not much has been done to bestow comprehensive analysis of security and privacy properties and different implementation techniques of block chain.

II. Blockchain

Year 2008 witnessed the first documented design of Blockchain and later in 2009 the first open source blockchain was positioned as a significant and vital element of Bitcoin. Bitcoin system very clearly utilizes blockchain as its distributed public ledger which eventually verifies and records all bitcoin transactions on the related bitcoin open networked system. Experts and tech professionals even defines blockchain as a secure ledger which organizes growing list of transactions records by expanding chain of blocks and efficiently guarding it by cryptography techniques to implement well built integrity of its transaction records.

Blockchain Working Mechanism

It basically as a distributed and secure database of transaction logs, explaining it further if a person ‘ X ’ wants to send some bitcoins to another person ‘ Y ’ it has to create a bitcoin transaction by ‘ X ’, the transaction has to be authorized and approved before it initiates on bitcoin network. Further to process, the transaction is broadcasted to each and every segment in the network, by this segments the miners of the process will gather transactions into a block, verifying and broadcasting the block using consensus protocol to get approval from the network and once the segments are verified the block is added to the blockchain.

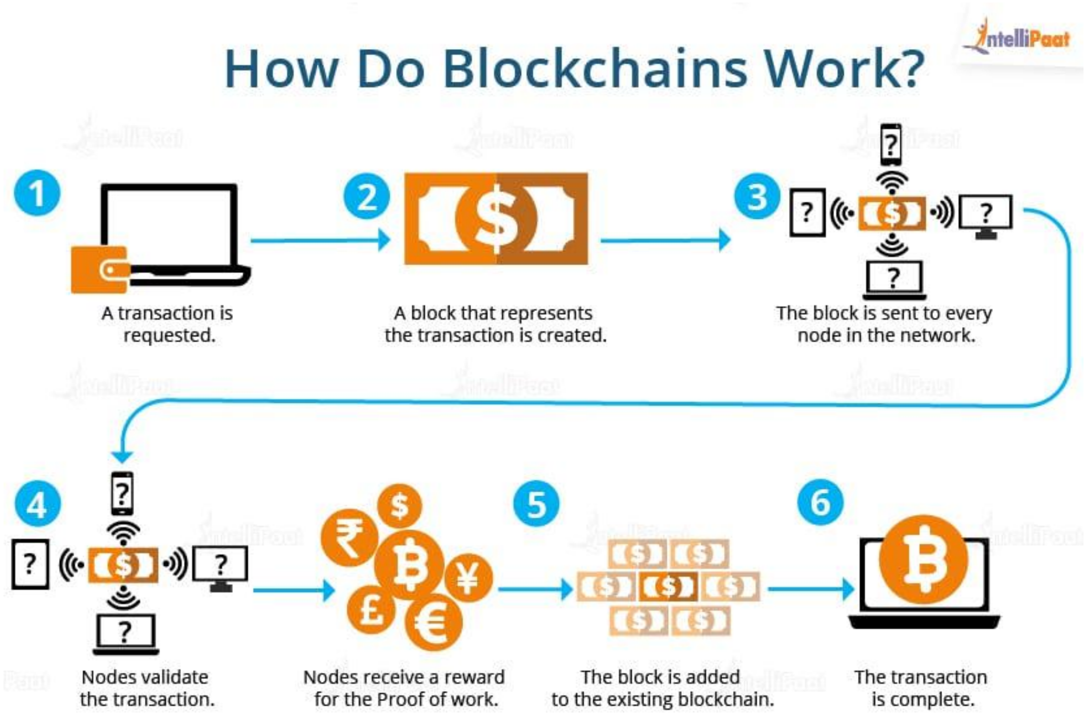
IntelliPaat
How Do Blockchains Work?
1
A transaction is requested.
2
A block that represents the transaction is created.
3
The block is sent to every node in the network.
4
Nodes validate the transaction.
Nodes receive a reward for the Proof of work.
5
The block is added to the existing blockchain.
6
The transaction is complete.

Image Source : Intellipat

- Hash Chained Storage
- Digital Signature
- Consensus for adding a new block to the chained storage

The above three key efficiencies are supported by the blockchain implementation in Bitcoin, through this bitcoin can even prevent double spending problem and can halt demonstrating modifications of any transaction data once block has been committed into a blockchain.

Security & Privacy in Blockchain

Lets sort out the online transaction's security and privacy requirements –

- Uniformity of the ledger among all the participating organisations / institutions
- System & Data availability
- Certitude of privacy of the transactions
- Unlink ability of Transactions
- Secrecy of users identity
- Avoidance of double spending
- Veracity of the transactions

The basic security and privacy properties pops from the cryptography advances and bitcoin's design and execution, improving efficiency of the cryptographic chain of block was proposed in 1993 by adding Merkle Trees and various other documents in one block and this blockchains were constructed keeping in mind the inbuilt security features like tamper resistant, consistency and resistance to a (DDos) distributed denial of service assault, but to use the secure distributed storage of blockchain additional properties of security and privacy is required.

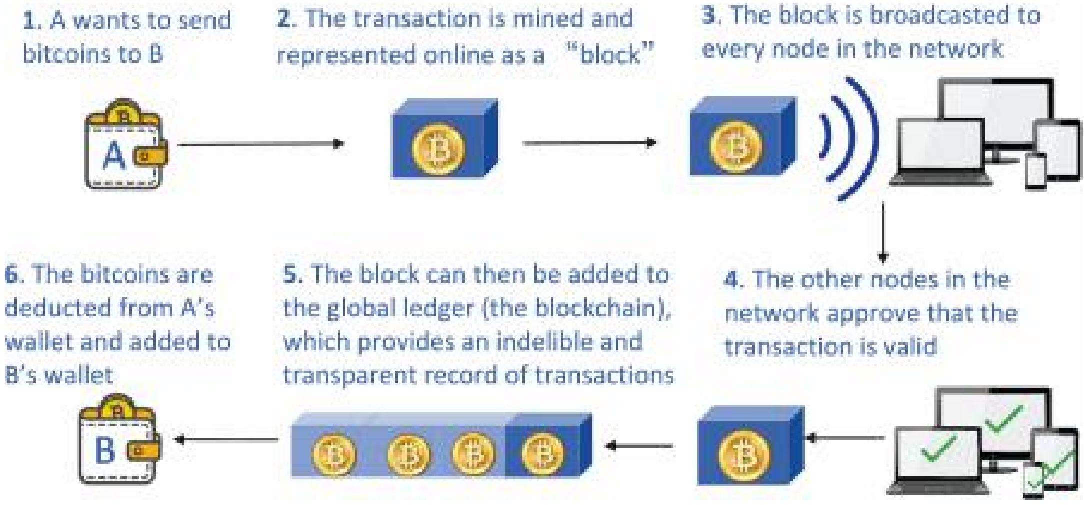
1. A wants to send bitcoins to B
2. The transaction is mined and represented online as a "block"
3. The block is broadcasted to every node in the network
4. The other nodes in the network approve that the transaction is valid
5. The block can then be added to the global ledger (the blockchain), which provides an indelible and transparent record of transactions
6. The bitcoins are deducted from A's wallet and added to B's wallet
A
B

Image Source : dl.acm.org

Extra Security and Privacy Properties of Blockchain

As mentioned in Bitcoin blockchain converse three basic security properties but the system might desire benefit from extra security and privacy properties that are crucial to digital currency and distributed global ledger services. Though blockchain in Bitcoin offers false identity through its pseudo-identity which is basically for users anonymity but it fails to give the protection of breakup of the transaction, so naturally the user who always uses pseudo-identity on the system can protected only by false identity and transaction breakup properties, because this breakup property makes it impossible to launch de-anonymization inference assault. Hence the blockchain system in bitcon can achieve only false identity feature but not the transaction breakup feature so the blockchain system must be upgraded by other cryptographic techniques.

Consensus Algorithms

A group based protocol for reaching dynamically in a particular group is known as Consensus, and the key problem of dynamically getting a consensus in a group depends on its group based coordination but such consensus can be tampered by fraudsters and faulty processes, it is also known as Byzantine Fault. The popularly used consensus algorithms in blockchain provides a probabilistic solution to counter byzantine faults. With reference to different constraints in practical applications there are two types of consensus algorithms : Eventual Consistency Consensus and Strong Consistency Consensus. In eventual consistency consensus algorithms comprises PoW, PoS and DpoS whereas in strong consistency consensus include BFT and PBFT.

Blockchain : Privacy & Security Techniques

- Mixing
- Anonymous Signatures
- Homomorphic Encryption (HE)
- A_ribute-Based Encryption (ABE)
- Secure Multi-Party Computation
- Non-Interactive Zero-Knowledge (NIZK) Proof
- The Trusted Execution Environment (TEE) Based Smart Contracts
- Game-Based Smart Contracts

III. Conclusion

In order to achieve privacy and security in blockchain system it needs multiple security and privacy requirement along with desired properties. In the said paper we distinguished the privacy and security attributes of blockchain into two segments. Firstly, Inbuilt qualities and additional qualities with reference of online transactions and secondly the privacy and security techniques were explained of blockchain systems and applications, which comprised consensus algorithms, mixing, , encryption, secure multiparty computation, non-interactive zero-knowledge proof, anonymous signatures and secure verification of smart contracts. We discussed privacy and security properties of blockchain which plays crucial role in amplifying the trust blockchain provides in developing technological innovation. We can very well assume that developing a light weight cryptographic algorithms and other properties of privacy and security methods will prove to be a significant breakthrough in enabling technology if blockchain and its application.

References

[1] Kristov Atlas. 2014. Weak Privacy Guarantees for Shared Coin Mixing Service. (2014).
[2] YouTube Videos
[3] IBM Blockchain based on Hyperledger Fabric from the Linux Foundation.
[4] Bitcoin - Open source P2P money. https://bitcoin.org/en
[5] What is BitShares. http://docs.bitshares.org/bitshares/whatis.html