BLOCKCHAIN

SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR

THE TECHNICAL & SEMINAR WRITING

By

Rahul Kumar 1906049

Brij Mohan Diwakar 1906044

Kumawat Lakhan Makhanlal 1906055

UNDER THE SUPERVISION OF

Asst. Professor CSE Dept, NIT PATNA

Dr. Kakali Chatterjee

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY PATNA

(An Institute of National Importance)

MAHENDRU, PATNA, BIHAR - 80000

CERTIFICATE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY PATNA

This is to certify that **Brij Mohan Diwakar** (1906044), **Kumawat Lakhan** (1906055), **Rahul Kumar** (1906049) have carried out the technical & seminar writing entitled "**Blockchain**" under the supervision of **Dr. Kakali Chatterjee**, Department of Computer Science and Engineering, NIT Patna. This project is bonafide work done by them for the fulfillment of the requirements for the minor project.

Dr. Kakali Chatterjee
Supervisor

Dr. Maheshwari Prasad Singh
Head of Department CSE

DECLARATION

We students of 7th semester hereby declare this project entitled "**Blockchain**" has been carried out by us in the department of Computer Science and Engineering of National Institute of Technology Patna under the guidance of **Dr Kakali Chatterjee**, Department of Computer Science and Engineering, NIT Patna. No part of this work has been submitted to any other institute nor copied from any journals or articles or project reports.

| --- | --- | --- |
| **Brij Mohan Diwakar** | **Kumawat Lakhan Makhanlal** | **Rahul Kumar** |
| **1906044** | **1906055** | **1906049** |

Place : ----------

Date : ----------

ACKNOWLEDGEMENT

We hereby take the privilege to express our gratitude to all the people who were directly or indirectly involved in the execution of this work, without whom this project would not have been a success. We extend our deep gratitude, respect and obligation to our project mentor, **Dr. Kakali Chatterjee,** Department of Computer Science and Engineering, NIT Patna. for being a constant source of inspiration. Our heartiest thanks to our classmates who have supported us in all ways. Words are inadequate to express our gratitude to our parents and friends who have been supportive all the time. We would also like to thank our institution and the faculty members without whom this project would have been a distant reality. Above all we bow before the Almighty for his immense blessings throughout life.

1. Rahul Kumar 1906049
2. Brij Mohan Diwakar 1906044
3. Kumawat Lakhan Makhanlal 1906055

TABLE OF CONTENTS

ABSTRACT

Blockchain has promise as an approach to developing systems for a number of applications within cybersecurity. In Blockchain-based systems, data and authority can be distributed, and transparent and reliable transaction ledgers created. Some of the key advantages of Blockchain for cybersecurity applications are in conflict with privacy properties, yet many of the potential applications have complex requirements for privacy. Privacy-enabling approaches for Blockchain have been introduced,

such as private Blockchains, and methods for enabling parties to act pseudonymously, but it is as yet unclear which approaches are suitable in which applications. We explore a set of proposed uses of Blockchain within cybersecurity and consider their requirements for privacy. We compare these requirements with the privacy provision of Blockchain and explore the trade-off between security and privacy, reflecting on the effect of using privacy-enabling approaches on the security advantages that Blockchain can offer.

1. INTRODUCTION

Blockchain has revolutionized the exchange of information and media after the Internet. Blockchain technology is pertained to as a path-breaking innovation and the forerunner of a fresh economic period. Blockchain call forth a new type of recent system called the Blockchain Economic System. The blockchain economic system conventions will be determined by the smart contracts, whenever stimulatory transactions are enforced autonomously. Evidently, the blockchain economy has taken the shape of a novel organizational structure called the decentralized autonomous organizations (DAO). Blockchain is the basis for the Decentralized Autonomous Organizations (DAOs) which provides novel stages of crowd coordination by eradicating the trust and fault problems.

Types of Blockchain

Blockchain technologies can be roughly divided into three types.

1.Public blockchain

Everyone can check the transaction and verify it, and can also participate the process of getting consensus. Like Bitcoin and Ethereum are both public blockchains. Fig. 7.2 shows public blockchain.

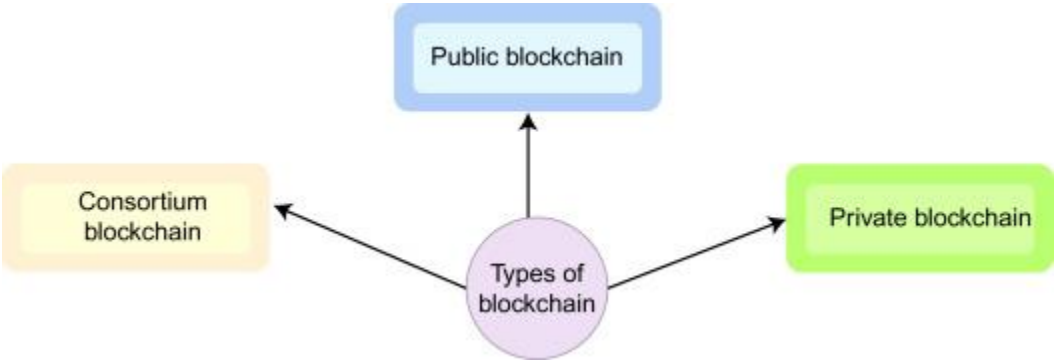
2.Consortium blockchains

It means the node that had authority can be choose in advance, usually has partnerships like business-to-business, the data in blockchain can be open or private, can be seen as Partly Decentralized. Like Hyperledger and R3CEV are both consortium blockchains.

3.Private blockchain

Nodes will be restricted, not every node can participate this blockchain, has strict authority management on data access.

2. OVERVIEW



The comparison among different blockchain system is listed below:

Consensus determination: Each node in public blockchain participates in the agreement process. Whereas, for validation of the block in consortium blockchain, only a few nodes are involved. Private blockchain system is under control by a single organization which also responsible for the validation.

Visibility: In a public blockchain, transactions are transparent and available to the nodes, whereas the control is under one organization in the case of a private blockchain or a consortium blockchain.

Flexibility: In public blockchains, the transactions are validated and checked by all the nodes in the public and it is not possible to tamper transactions. On the contrary, agreements in private or consortium blockchain can be meddled easily as it involves only a set of people.

Efficiency: With limited number of nodes in consortium and private blockchain, the transactions are efficient as it is not propagated throughout the network. In public chain network, a large amount of time is required to deliver the transactions and blocks among the nodes. This results in limited transaction throughput and high latency.

Centralized: Consortium blockchain involves partial centralization, public blockchain is decentralized, and private blockchain is completely centralized as the control is under a single unit.

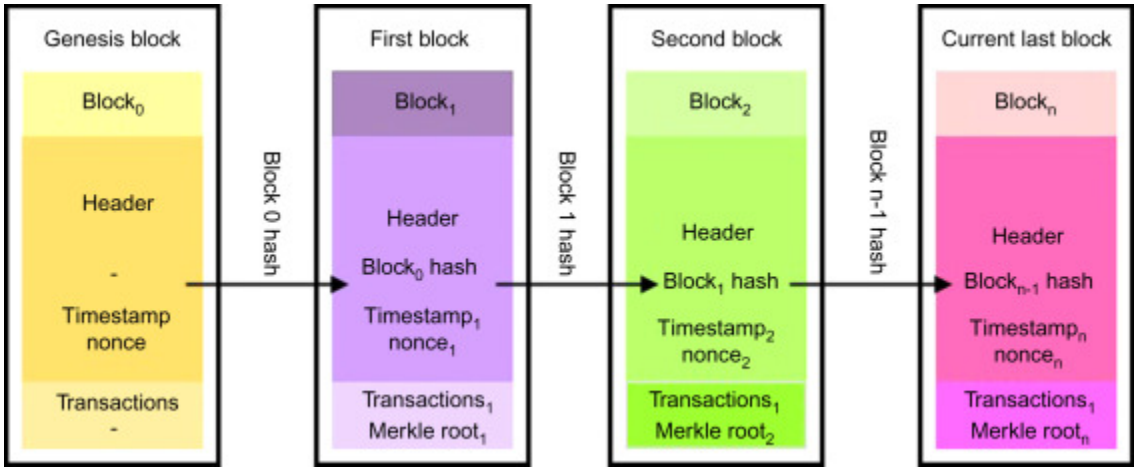
Consensus Process: Anyone can actively participate in the consensus process associated with public blockchain. Private and consortium blockchain nodes both being decentralized require permission from the regulatory organization.

3. BLOCKCHAIN PROPERTIES

A block is the basic unit of blockchain. It can also be termed as a committed transaction and has many functionalities. Block body and block header are the two major components of the block. Block header comprises of the below components:

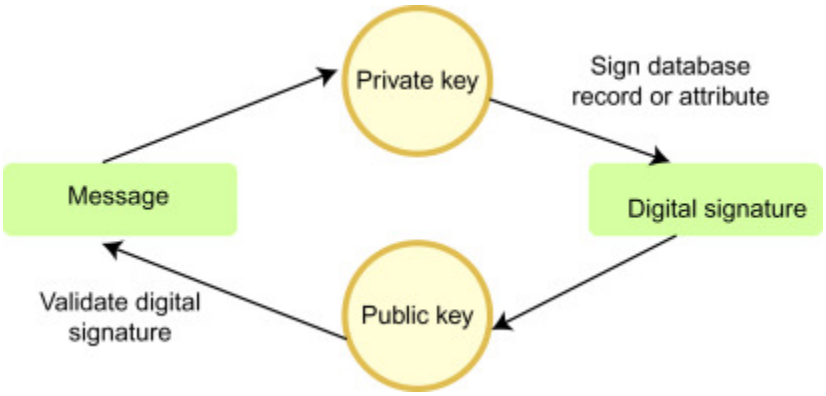
1.*Parent block hash:* This signifies the previous block's hash value, which is 256-bit.
2.*Version of block:* Signifies the block verification guidelines to be followed.
3.*Merkle tree root hash:* All agreements in the block are associated with a hash value described by merkle tree root hash.
4.*Timestamp:* Refers to the present timestamp in terms of seconds since 1970-01-01T00:00 UTC.
5.*Nonce:* For every hash calculation, nonce is a 4-byte field, starting with a zero and raises with every computation of hash value.
6.*nBits:* A compact format of the current hash target.

Another major component of a block consisting of transactions and its counter is the block body. The magnitude and the block size of every transaction are responsible for the large amount of transactions the blocks contain.



4. DIGITAL SIGNATURE

In a deceitful environment, an asymmetric cryptographic mechanism is used to verify the credibility of the transaction. Digital signature works on the principle of asymmetric cryptography. Each transaction member has a private and public key. A private key is stored confidentially because it is used for signing negotiations. The transactions that are signed are transmitted across the distributed network and the public keys are used for their accessibility. There are two levels involved with digital signature: verification phase and signing. During the phase of signing, the encryption of the data is carried out using the private key by the sender. Encrypted result and native data are delivered, which are sent to the receiver of the transaction. In the verification stage, for the validation of the received value by the receiver, the public key is used and the data are checked if it has been meddled. Elliptic Curve Digital Signature Algorithm (ECDSA) is used for blockchains in the digital signature mechanism.

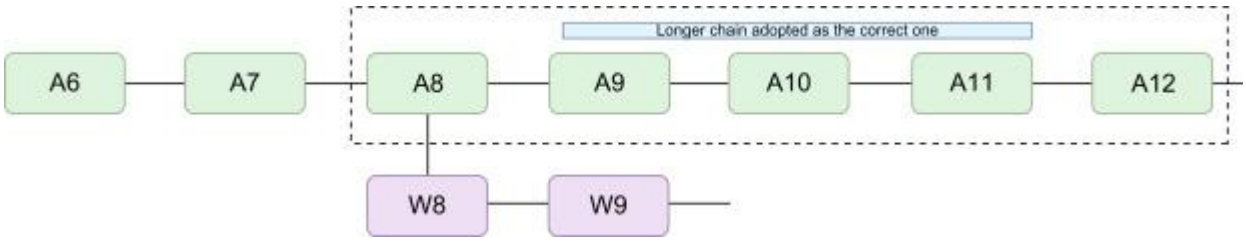


5. TAXONOMY OF BLOCKCHAIN

Proof-of-work model

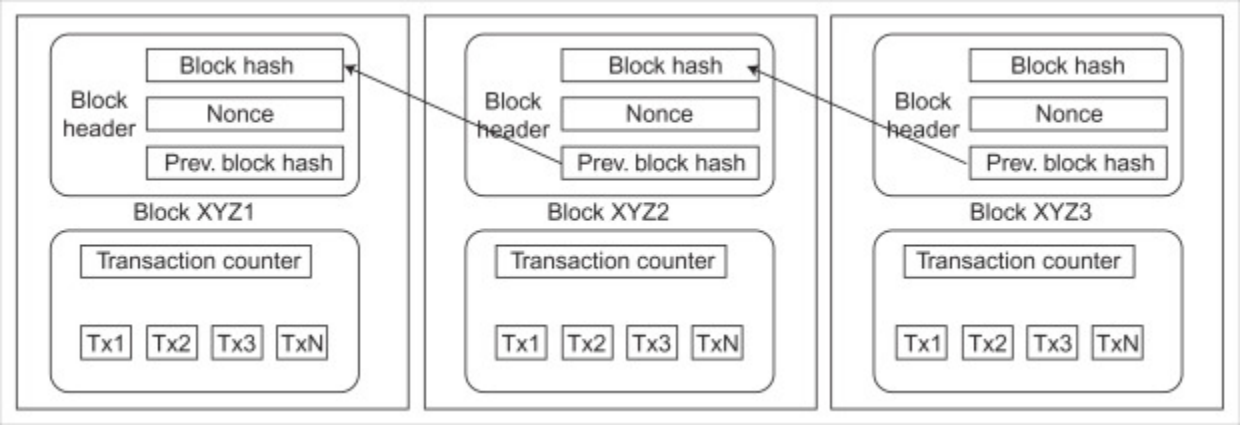
PoW is a consensus strategy applied to Ethereum (called Homestead, in its current version) and bitcoin. PoW has its own variation for different cryptocurrencies—EthHash, Hashcash PoW, Merkle Tree-based, and others. In PoW, by requiring a set of work from the service requester, denial of service (DoS) and other abuses/attacks are deterred. In blockchains, this model is used to verify transactions and, thus, generate new blocks for the chain .

Fig. represents the chain selection in blockchains. A6, A7, …, A12 represent nodes of one chain, while W8 and W9 represent nodes of another chain. The process of chain selection is as described below—on the basis of the longest chain rule.



In bitcoins, hashcash is used as a part of the mining algorithm. To add nodes in bitcoins, each participant must obtain a hash value lower than a particular numeral by solving computational puzzles

set by the blockchain network. The dynamically tuned difficulty level presently ensures that each block is added every 10 minutes. The first node to obtain the winning hash takes the mining prize and is added to the proposed blockchain. When more than multiple nodes find the winning hash simultaneously, each winning node attaches the proposed block to the network and transmits this over the blockchain generating a temporary fork. However the mechanism that establishes the longest branch (greatest PoW) gets included and the others get discarded, as more blocks are attached to these forks.



6. COMPARISON

Comparison of Some Blockchain Consensus Models

Empty Cell	**PoW**	**PoET**	**PoS**	**Federated BFT**	**BFT and Variants**
Trust model	Untrusty	Untrusty	Untrusty	Semi-trusted	Semi-trusted
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Instantaneous	Instantaneous
Transaction rate	Slow	Medium	Rapid	Rapid	Rapid
Cost of participation	Present	Absent	Present	Absent	Absent
Scalability	Large	Large	Large	Large	Low
Token requirement	Yes	No	Yes	No	No
Type of blockchain	Permissionless	Both	Both	Permissionless	Permissioned

7. CONCLUSION

The blockchain technology provided a revolution in the way transactions were handled and is now being used in various fields. The transparent nature and decentralized infrastructure of the mechanism is appraised by many. The various cryptocurrencies present at the moment are working toward providing the users with faster and secure transactions. Even though, currently, blockchain is being used mostly with cryptocurrency, it's potential for transforming any industry is now being recognized. It is evident that even through the technical challenges, rapid change, and lack of acceptance in various countries, the technology is here to stay. There have been a development of various other distributed ledger such as IOTA Tangle and Hedera hashgraph, going beyond blockchain and alleviating all its limitations. These are more energy-efficient and transparent form of technologies. The cryptocurrencies based on the above distributed network are supported with features of management, fair ordering, secure services, and *ad hoc* transactions.

8. REFERENCES

[1]J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander Where is current research on blockchain technology?—a systematic review PLoS One, 11 (10) (2016), p. E0163477 CrossRefView Record in ScopusGoogle Scholar

[2]D.K.C. Lee, L. Guo, Y. Wang Cryptocurrency: a new investment opportunity? J. Alternat. Invest., 20 (3) (2018), pp. 16-40 https://doi.org/10.3905/jai.2018.20.3.016 CrossRefView Record in ScopusGoogle Scholar

[3]M.H. Miraz, M. Ali Applications of blockchain technology beyond cryptocurrency Ann. Emerg. Technol. Comput. (AETiC), 2 (1) (2018), pp. 1-6 CrossRefView Record in ScopusGoogle Scholar

[4]E. Kazan, C.-W. Tan, E.T.K. Lim Value creation in cryptocurrency networks: towards a taxonomy of digital business models for bitcoin companies PACIS 2015 Proceedings (2015), p. 34 Google Scholar

[5]A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, ACM SIGSAC Conference on Computer and Communications Security (2016), pp. 3–16. Google Scholar

[6]M. Vukolić The quest for scalable blockchain fabric: proof-of-work vs. BFT replication IBM Research, Zurich (2015) Google Scholar

[7]D.D. Wood, Ethereum: A Secure Decentralized Generalized Transaction Ledger, 2014, http://gavwood.com/paper.pdf. Google Scholar