Performance Evaluation of Various Block Chain Platforms

P. Sriramya, Golda Dilip

Abstract: Blockchain is a decentralized data processing and sharing platform that enables multiple domains that do not trust each other to cooperate, coordinate and collaborate in a rational decision making process. As internet made us all communicate with each other in just one click, Blockchain can do same for business environment. Blockchain for business environment provides a way to execute multiple transactions with multi-users in a much secured manner. For doing this a secure blockchain platform needs to be set up for various kinds of businesses. This paper presents a comparative analysis of thirty-four various blockchain platforms suitable for different applications. The objective of the paper is to provide an in-depth comparison of the various blockchain platforms belonging to different blockchain generations to help developers select a suitable blockchain platform for their application. Finally we conclude with our findings as well as a note on future directions for expanding the research blockchain technology platforms.

Keywords: Blockchain, decentralized data processing.

I. BLOCKCHAIN TECHNOLOGY OVERVIEW

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.[1] Blockchain was introduced by a Satoshi Nakamoto in 2008 to serve as the public transaction ledger for the cryptocurrency bitcoin. A blockchain is a growing list of transactions, called as blocks, which are linked together using cryptographic techniques. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data which is generally represented as a tree like structure called merkle tree root hash.

Information stored in a blockchain works in a distributed and unremittingly updated record in the form of a Public ledger. The blockchain records are not stored in any single location, which means that it is public ledger which is verifiable by all in the network. Since there is no centralized system here the hackers cannot hack any one system and say that they have crashed the system.

II. BLOCKCHAIN CHARACTERISTICS

2.1 Stability and Strength

Blockchain technology by storing the various transactions of different applications in the form of blocks are chained together, reflects the same in the whole network. It cannot be organized by any solo object and the chance of failure is also less as the environment is decentralized.

2.2 Immutable and obvious

The blockchain network is in state of agreement, where a set of consensus algorithms like Proof of work, Proof of Stake, RAFT, PAXOS etc are used for automatically checking with in itself. A kind of self-analysing ecosystem of a digital value, the network brings together every transaction that happens in a particular interval of time. Two significant characteristics result from this:

The data embedded within the network is obvious and is defined by the public. The blockchain is immutable as it is not possible for an attacker to corrupt all the systems in the network as it requires a huge amount to computation power to override the network. The computers used in the network of blockchain technology cooperatively manage the database which records the Bitcoin transactions. This means that, Bitcoin is managed by its network, and not by any centralized authority. So the blockchain works on peer-to-peer network in a decentralized platform.

III. BLOCKCHAIN AS AN APPLICATION PLATFORM

Blockchain can be applied to any business use case that needs to be improved by using distributed ledger technology. If a business requires trusted serviced environment then blockchain can be implemented to the application platform to build the trust infrastructure of the system. Blockchain technology in Bitcoin is a cryptographic currency that secures the transactions that are executed by scripting languages like forth programming language. To avoid the human intervention Smart contracts are useful to replace intermediaries in various business applications. Smart Contract is a self-verifying and self executing agreement that can be executed autonomously.

To have a high degree of trust for various business transactions distributed ledger technology is used in blockchain to give various advantages to business solutions. This also lowers the cost involved when compared the traditional centralized models. The main advantages are transaction are faster as they dont rely on a centralized infrastructure, the system is prone to cyber attacks because of the distributed nature of blockchain and the users can query any transactions.
IV. BLOCKCHAIN PLATFORMS

Various platforms [3] focus on different aspects, some on speed, others on privacy and security, and yet others on ease of use. In the first generation blockchain platform[4] cryptocurrencies like bitcoin were used as a secure payment method fit for the tech-savvy times and to meet the demands of modern users. The list of cryptocurrencies has been increasing gradually since its inception. People chose to mine and invest in new decentralized money that imitated Bitcoin. Second Generation platforms[4] marked the rise of decentralized apps(DApps) , decentralized autonomous organizations(DAOs) and the newer platforms with blockchain smart contracts.

Vitalik Buterin who is a Russian-Canadian programmer and writer primarily known as a co-founder of Bitcoin proposed a wider use of Bitcoin called Smart Contracts. He proposed Ethereum an open source blockchain technology based platform that helps developers to build and deploy decentralized applications(DApps). Bitcoin[5] was a monetary revolution in the first generation, whereas Ethereum revolutionized and decentralized the world wide web in the second generation resulting in the rise of DApps, DAOs and the like. Bitcoin traded in cryptocurrency whereas Ethereum offers multiple methods of exchange encircling cryptocurrency, smart contracts and Ethereum Virtual Machine. Ethereum, NEO, NEM and various other blockchain platforms joined the regiment of second-generation blockchains platforms.

The third blockchain generation[4] still in its inception will be characterized by humongous blockchain platforms that automates organizational structures like cities, in which every single organizational body is block chained and connected to other bodies or units. In short third generation platforms will be blockchain of blockchains handling million transactions per second. In short Scalable, Interoperable Ecosystems earmarks third generation platforms.

Various blockchain platforms are outlined below.

- **Cardano**

Cardano[6] believed to be the incentive blockchain platform that originated out of a research driven scientific philosophy was built by a team of leading academics and engineers across the globe. Cardano uses Proof of Stake as consensus algorithm. Plutus, Haskell are the strictly typed pure functional programming language which is used in Cardano.

- **Ethereum**

Ethereum[7], is an open-source public-permission less decentralized blockchain platform developed by the Ethereum Foundation in 2013, that runs smart contracts. It uses Proof of Work as consensus algorithm which is comparatively slow. Solidity and LLL are contract oriented high level programming languages which are popularly used in Ethereum platform. Serpent a programming language motivated by Python and Solidity are being used for developing and running smart contracts in Ethereum. Ethereum is the cryptocurrency of Ethereum, which is used in Ethereum ecosystem. Ethereum has a blockchain platform called ‘Ethereum Virtual Machine’(EVM) which enables developers to launch their own customized blockchain projects and also their own cryptocurrencies. Also the platform enables users to specify how computing power is consumed for a transaction, using a measure of processing power, called ‘Gas’. Those transactions that exceed gas limit are reverted.

- **Quorum**

Quorum[8] is a permissioned open source blockchain platform founded by J.P. Morgan which can be considered as an enterprise-ready extension of Ethereum. Since it is permissioned, the network will not be open to everyone. It is capable of handling applications and private transactions which requires high throughput and speed. By enabling private and public on-chain transactions quorum tenacities the problem of the privacy of records that Ethereum and other blockchains could not handle.

- **Ripple**

RippleNet[9] is a blockchain based network aims at connecting payment providers, corporates and asset exchanges without any charges. XRP or Ripple is an emerging cryptocurrency like Bitcoin and Ether. Ripple uses the concept of probabilistic voting to reach on an agreement between nodes. XRP is considered to be more accessible and quicker than other blockchains. Ripple uses probabilistic voting to reach the consensus between nodes. The rationale behind developing Ripple was to enable quick as well as cheap global money transfer.

- **Hyperledger Sawtooth**

Hyperledger Sawtooth[10] is an enterprise solution launched by Linux Foundation for building, deploying, and running distributed ledgers or blockchains. This modular platform enable digital documents to be maintained in the absence of a crucial authority. Sawtooth uses Proof of Elapsed Time (PoET) consensus technique to integrate with trusted execution environments.

- **Hyperledger Fabric**

Hyperledger Fabric[11] uses an integrated architecture for building enterprise grade blockchain based applications and solutions. The modularity feature enables network developers and designers to plug in their required modules like membership services and consensus. Since Hyperledger Fabric framework is designed for permissioned networks it allows only known identities who are authorized and have the credibility to participate in the blockchain. This is the most preferred platform for building enterprise-grade applications for blockchain companies.

- **Hyperledger Iroha**

Hyperledger Iroha[12] is a blockchain platform launched by Linux Foundation and suitable for supply chain and IoT use cases. It is portable and supports macOS as well as Linux based operating systems and can build trusted, secure and agile decentralized applications. The consensus algorithm behind Hyperledger Iroha that protects Iroha network from rival nodes or failures is a unique chain based Byzantine Fault Tolerance Consensus Algorithm called Yet another Consensus.
It is written in a high level programming language C++.

- **R3 Corda**
  Corda[13], developed by R3 consortium, is an open source cutting-edge blockchain platform designed initially for financial sector. It uses a Pluggable Consensus technique and is implemented in Kotlin and Java. This platform does not have any cryptocurrency associated with it and operates in a permissioned mode. By eliminating costly frictions in business processes and transactions, Corda allows institutions to transact directly with smart contracts.

- **EOS**
  EOS[14] is an open-source blockchain platform initiated by a private firm, Block.one for the development of Decentralized applications(dApps). The rationale behind developing this platform is to enable decentralized applications hosting, enterprise storage solutions and smart contract capability. The main advantage of using this platform is that it is free for all users where each account will be provided with a varying permission level to protect the data in a more secure manner. EOS achieves consensus by using the concept of multi-threading as well as a delegated proof-of-stake algorithm.

- **OpenChain**
  OpenChain[15] is a open-source distributed ledger platform developed by Coinprism. OpenChain uses the concept of Partitioned Consensus where single instance will have a sole authority for validating the transactions. The transactions in this platform are free of costs and can is validated by the asset administrator and is considered to be more efficient compared to other platforms.

- **Multi Chain**
  Multi Chain[16] is a platform specifically for the creation and deployment of private blockchains. It is specifically used by organizations for financial transactions. It provides a simple API and a command-line interface to the users. Proof of work is the algorithm used in Multichain and this model transacts only with the validated account users or participants of this chain.

- **Stellar**
  Stellar[17] is a distributed blockchain based ledger platform with modest computing as well as financial requirements that facilitates cross-asset transfers of value. It deals with cryptocurrency as well as fiat based currency exchanges. Stellar network enables building of mobile wallets as well as smart devices. Unlike other platforms it uses Stellar Consensus Protocol (SCP) to accomplish consensus. In the event of misbehaving nodes it halts the progress of the network until a consensus is reached.

- **NEO**
  NEO[18] is a blockchain platform as well as a cryptocurrency designed by Da Hongfei and Erik Zhang to build a scalable network of decentralized applications. The basic building block of this platform is NEO token that generates GAS tokens that is used to pay transaction fees to run applications on the network. Neo uses Byzantine Fault Tolerance as its consensus algorithm. This platform uses Java, C# etc to develop smart contracts.

- **Hedera Hashgraph**
  Hedera Hashgraph[19] is a secure, fast and fair distributed ledger platform developed by Leemon Baird in the year 2016. It is an asynchronous Byzantine fault tolerant platform that has the strongest level of security. The platform is regulated by Hedera Hashgraph Council which ensures that no single member can have control over the entire network.

- **Zilliqa**
  Zilliqa[20] is a high throughput public blockchain platform designed to scale to thousands of transactions per second. The platform is designed in such a way that the throughput scales linearly as the number of nodes increases, a factor which will ensure that the network capacity can continue to grow to meet the rising demand. Practical byzantine fault tolerance (PBFT) is the consensus algorithm used here. The language used in Zilliqa is Scilla.

- **Waves**
  Waves[21] Platform is an emerging blockchain platform that comprehensively earmarks fiat gateways, smart contracts, mobile wallet, and a decentralized exchange. Proof of stake is the consensus algorithm used in this platform. The programming language that is used to write smart contracts is RIDE.

- **Wanchain**
  Wanchain[22] platform supports decentralized exchange, provides asset management tools, records cross-chain and intra-chain applications, transactions among mainstream public chains, private chains, and between public and private chains. Proof of stake is the consensus algorithm used. The programming language used is Solidity.

- **Tezos**
  Tezos[23] is a new platform for smart contracts and decentralized applications. It supports on-chain governance, provides security by securing smart contracts and avoiding buggy code. Tezos’ unique proof-of-stake consensus algorithm provides every stakeholder the chance to vote on amelioration to the protocol, including amelioration to the voting procedure itself, to reach consensus. Michelson is the domain-specific, strongly typed language used on Tezos blockchain.

- **Stratis**
  Stratis[24] is an enterprise grade business blockchain platform which enables creation of applications easily on private blockchains. The Application Programming Interface associated with Stratis helps business organizations to quicken their blockchain creation and development process. Stratis also offers a comprehensive solution called BaaS (Blockchain as a Service) to reduce the expenses and complexities involved in procuring as well as managing nodes. Stratis utilizes C# in the .Net framework for developing blockchain applications.
Performance Evaluation of Various Blockchain Platforms

- **Smilo**
  Smilo[25] is described as a hybrid, eco-friendly, affordable, scalable and fast blockchain platform that ensures transparency while protecting individual’s data. Smilo uses advanced Byzantine Fault Tolerant algorithm called Smilo BFT+ as consensus algorithm. Languages like lidity, Javascript, Java, Python are being used in this platform for application development.

- **Qtum**
  Qtum[26] is a decentralized and open-source blockchain platform which employs a decentralized governance protocol abbreviated as DGP. This protocol allows the various blockchain parameters like block size, block time, gas plans for agreements to be modified without requiring a divergence. Proof of Stake is the consensus algorithm used and Solidity is the programming language used in Qtum environment.

- **Nxt**
  Nxt[27] is an progressive open source, permissionless blockchain platform that contains many core-level features. To name a few it supports Decentralized Strength Exchange, trading place, and Voting system. Nxt uses Proof of Stake as consensus algorithm. This platform features Nxt digital currency. Nxt provides complete freedom to users to build custom applications.

- **Ardor**
  Ardor[28] is a blockchain-as-a-service-platform that has evolved from the Nxt blockchain. It is considered to be a scalable and secure blockchain platform which offers a lot of unique features and child chains. It has a lightweight smart contract written using Java that saves resources. It employs Proof of Stake as consensus algorithm.

- **NEM**
  NEM[29] is an open, public blockchain platform as well as a cryptocurrency launched in 2015. Its written in Java as well as in C++. It uses the revolutionary Proof of Importance technique for reaching consensus. It was designed and coded from the scratch for scalability and speed.

- **Neblio**
  Neblio[30] described as the next generation enterprise blockchain solution is basically a secure as well as distributed platform. Proof of Stake consensus technique is employed here. It uses a variety of programming languages like Java, Javascript, Ruby, Python, Go, C#, PHP, Objective-C. The cryptocurrency associated is called Neblio Cryptographic Coin(NEBL).

- **Lisk**
  Lisk(LSK) is a blockchain application platform[31] developed in 2016. The idea behind Lisk is to bring blockchain technology to the world in a simplified manner to the users. It is written in JavaScript and uses Delegated Proof of Stake (dPoS) algorithm for arriving at a consensus. The block time in a Lisk platform is 10 seconds.

- **Komodo**
  Komodo[32] is a secure, independently scalable, and fully interoperable blockchain ecosystem that provides end-to-end blockchain technology solutions. It provides cryptocurrency anonymizer to make private transactions more secure and it deploys a novel delayed Proof of Work (dPoW) algorithm to arrive at a consensus.

- **IOTA**
  IOTA[33] is described as a next generation permissionless distributed ledger that utilizes a novel invention, called a “Tangle”, at its core. Here the individual transactions are entangled together rather than grouping into blocks. Coordinator consensus is employed here. Rust, Javascript, Java, C++ are popularly used for developing applications.

- **ICON**
  ICON[34] is a decentralized blockchain network in which various independent blockchain-based communities are associated to form a greater community. At the core of ICON platform is a high-performance loopchain and it employs Loop Fault Tolerance(LFT) technique to reach a consensus. This blockchain uses ICX coins. The programming language employed here is Python.

- **Enigma**
  Enigma[35] is a decentralised permissionless peer-to-peer network platform. With Enigma, “smart contracts” are called “secret contracts”, where input data is kept hidden from nodes in the Enigma network that execute code. Proof of Stake consensus technique is used here and a contract oriented programming language called Solidity is employed here for implementing smart contracts.

- **ArcBlock**
  ArcBlock[36], built with an open standard, is a platform and an ecosystem for building and deploying decentralized blockchain applications. Arc Block is listed on Huobi, OKEX and GAtie io. ArcBlock uses a Algorand based consensus technique to arrive at a consensus.

- **Aion**
  Aion[37] is a multi-tier network touted as third-generation blockchain network that enables multiple blockchain networks to communicate among themselves. It enables fast transaction processing and increased data capacity. It also has a decentralised application platform(Dapp) with its own virtual machine and allows an organization to Federate and Scale. Aion uses a neural network inspired verification algorithm for arriving at consensus called Proof-of-Intelligence Staking. Programming language such as Aion, Solidity are used in this environment.

- **NULS**
  NULS[38] is an open-source public blockchain platform with a modular architecture. It includes a variety of features like smart contracts, the multichain system, cross-chain consensus. It is an adaptable blockchain suitable for enterprise applications.
NULS coins or token, which operates on the NULS platform is expected to have an stimulating future in the cryptocurrency sector.

**ARK**

ARK[39] is a user-friendly blockchain platform that facilitates a robust and decentralized ecosystem. This platform includes many practical services that customers can utilize. ARK’s SmartBridge Technology make the platform interoperable and allows communication between validated blockchains. ARK can act as an intermediary to blockchain systems such as Bitcoin, Ethereum by inserting a tiny code snippet into these ecosystems. It has a blocktime of 8 seconds making it one of the fastest in the industry. ARK coin is the cryptocurrency associated with this network.

V. COMPARING VARIOUS BLOCKCHAIN PLATFORMS

5.1 Consensus Algorithm

The various consensus algorithms employed by various platforms are PoW(Proof-of-Work), PoC(Proof-of-Consensus), PoS(Proof-of-Stake), dBFT(delegated-Byzantine Fault Tolerance), LPoS(Leased Proof-of-Stake), DPoS(Delegated Proof of Stake), BFT (Byzantine Fault Tolerance), Chain based BFT, Pluggable framework for consensus, Probabilistic Voting technique, PoET(Proof of Elapsed Time Consensus), Partitioned Consensus technique, Stellar consensus and Majority Voting. Although Bitcoin and majority of the platforms uses Proof- of -Work (PoW), proof-of-stake (PoS) ranks next, along with other emerging consensus protocols.

5.2 Language

One of the biggest differences among the various platforms is the language support. Java is the most popular language widely used across majority of platforms. Ethereum supports programming languages that are explicitly designed to be used for writing Ethereum smart contracts, such as Solidity and Vyper. When Ethereum is used as a runtime environment JavaScript is used. Multiple programming languages such as Java Script and Go are used with Hyperledger Fabric. In many cases the developer need not learn any new language. Sawtooth currently permits developers to use Interpreted Languages such as Python and Javascript, Compiled Languages such as Rust, C++ and Go, Virtual Machine language such as Java to develop smart contracts.

5.3 Compatibility

The same concept used for any standard operating system is extended to blockchain wherein any prevailing operating system like Windows, Apple Mac or mobile operating systems like Android, iOS executes various transactions depending on user commands that are issued and all the tasks gets done locally on the device. A blockchain is being used as a support in the background by a blockchain operating system. In other words, activities like validation, execution, documentation happens on the blockchain whereas all instructions and relations from any user’s device is hooked on a blockchain based operating system. Overledger[40], a yet to be released operating system is being considered as a blockchain operating system for future by the experts.

5.4 Block Time and Security

Block Time is defined as the time taken to mine a block. Generally the normal block time is set to a uniform value to confirm that the miners don’t impact the security aspect of the network by increasing the computational power. The logic behind block time is that if the average block time of the network is greater than the estimated block time, then the exertion level will be decreased otherwise the difficulty level is increased. The block time for various blockchain platforms is depicted in Figure1.0. From the graph it is evident that NXT, STRATS and ARDOR has more blocktime compared to other platforms. In terms of security, blockchain as well as its decentralized public ledger are widely seen as solutions in domains like big data, supply chain management as well as in financial services.

![Blockchain Platforms Vs Block Time](image)

**Fig. 1** Blockchain Platforms Versus BlockTime
VI. CONCLUSIONS AND FUTURE DIRECTIONS

Bitcoin blockchain has recently implemented an improved technique for handling bitcoin transactions called SegWit (Segregated Witness) technology. This technique has numerous impacts on the network as a whole. It improves the scalability of the network by removing the limitation on block size limit, separates signature information from the transaction data and also provides a fix for the transaction malleability bug. Blockchain technology and cryptocurrencies have gone through an huge rise both in terms of modernism as well as embracement since its inception ten years ago. It is recommended that another comparison of the various platforms be made sometime in the future, to allow these platforms time to establish. Table 1 gives a broad comparative analysis of certain key features of various blockchain platforms. It is believed that the revolutionizing blockchain technology will be omnipresent very soon.

REFERENCES

<table>
<thead>
<tr>
<th>No.</th>
<th>Cryptocurrency</th>
<th>Available Link</th>
</tr>
</thead>
</table>