Survey of Blockchain Methodologies in The Healthcare Industry

Ashraf Mohey Eldin
a.mohey@fci-cu.edu.eg

Dr. Eman Hossny
e.hossny@fci-cu.edu.eg

Prof. Khaled Wassif
kwassif@fci-cu.edu.eg

Prof. Fatma A. Omara
f.omara@fci-cu.edu.eg

Department of Computer Science, Faculty of Computers and Artificial Intelligence
Cairo University, Cairo, Egypt

***Abstract*— Blockchain has been the focus of the research area in the past few years. It is considered the foundation of cryptocurrencies such as Bitcoin and Ethereum. Decentralization is the main feature of Blockchain. Blockchain provides a higher level of security and scalability. Major industries have started to consider blockchain on their platforms such as the healthcare industry which uses the blockchain to secure the patients' data, make them anti-tampering and keep track of their Electronic Health Records (EHRs). The work in this paper provides a state of art of different blockchain types and consensus mechanisms. Also, the paper recommends some guidelines to select the appropriate blockchain type, consensus mechanism and blockchain interoperability method that fulfills the healthcare industry requirements.**

Keywords*—*Blockchain, Healthcare, Consensus Mechanisms, Interoperability

I. INTRODUCTION

In 2008, Bitcoin was invented to enable two entities to perform transactions without requiring a trusted third party (TTP) such as central banks [1]. This caused a revolution in the financial industry. In addition, Bitcoin introduced the blockchain technology. The blockchain is basically a distributed database including blocks of all transactions or events that have been executed. These blocks are being shared among all entities that are participating in the blockchain network [2]. Every transaction is verified by the majority of nodes before being added to the chain. Each block contains the hash of the previous block. Thus, tampering a block on a chain will change its hash and break the whole chain which makes the blockchain immutable.

Blockchain has been adopted by many domains, such as banking, supply chain management, and healthcare [3]. The work in his paper focuses on blockchain for the healthcare domain. Recently, numerous blockchain models have been introduced for different healthcare applications.

In this paper, a comparative study has been conducted among different blockchain types, consensus mechanisms, and blockchain interoperability models to show their suitability for the healthcare industry.

The rest of the paper is organized as follows; Section II introduces a background about the healthcare industry, how it can grow, and the challenges of applying blockchain inside the healthcare industry. Also, it provides a background about blockchain types and consensus mechanisms. In section III, we show the suitability of the different blockchain types to the healthcare industry. The possibility of applying each consensus mechanism to the healthcare industry has been discussed in section IV and a comparison among them is provided. Section V discusses some blockchain interoperability models and shows a comparison among them. Finally, section VI concludes the paper.

II. BACKGROUND

Many studies and researches were conducted to improve the healthcare quality using the blockchain technology. The healthcare industry is growing in two directions, vertical and horizontal. The vertical direction is growing faster in which healthcare is providing new medications, vaccines and other medical devices. However, the horizontal direction is growing slowly, because most hospitals are still functioning using classical technology for the last two decades to record and share EHRs of their patients [4].

Adopting blockchain as a new horizontal innovation may revolutionize the healthcare industry [5]. This is because blockchain contains solutions to many problems that are facing data management for EHRs in the healthcare industry such as, EHRs tampering, data blocking among healthcare organizations, scalability issues, and others.

However, there are some challenges for applying the blockchain technology in healthcare to build new models. These challenges can be summarized as follows:

- Selecting a suitable blockchain type that fulfills the needs of the healthcare industry such as a high transaction rate with high security [6].
- Selecting an appropriate consensus mechanism that serves the model requirements and reduces the scalability issues [7].
- Selecting the appropriate model for blockchain interoperability that enables healthcare organizations to share patients' records among each other [8].

The paper discusses these challenges by providing the necessary guidelines for selecting the suitable blockchain type, consensus mechanism and interoperability method that are necessary for building a healthcare blockchain model. These guidelines were formed by inspecting some of the existing healthcare models such as [9, 10, 11].

In this part, different blockchain types are discussed. There are two types of blockchain, permissionless blockchains which are known also as public blockchains, and permissioned blockchains which are divided into private and consortium blockchains [12]. The architecture of the blockchain network can be adjusted to follow any of these types based on the requirements of the industry.

A. Permissionless Blockchains

They are also known as public blockchains. Permissionless blockchains are a form of peer-to-peer decentralized network

that allow multiple nodes to participate and perform transactions without having to rely on a trusted third party such as Bitcoin and Ethereum [13]. Any node can join the blockchain network and acquire a full copy of the blocks. Also, any node can participate in the mining process [1]. Public blockchains are best suited to provide publicly accessible, verifiable and immutable storage of data [15].

B. Permissioned Blockchains

They have the same features as permissionless blockchains, in addition to a higher confidentiality, privacy and scalability [14,15]. They are divided into private and consortium chains [16]. The difference between private and consortium blockchain is the number of nodes with write permissions (miners) as shown in Fig. 1.

1) Private Blockchain; In this type, one node is responsible for write permissions while read permissions may be public or restricted to specific nodes. Therefore, private blockchains suffer from centralization issues such as single point of failure [16]. The most common examples of private blockchains are IBM Blockchain and Multichain.

2) Consortium Blockchain; It is known as Hybrid Blockchain. In this type, transaction validation and approval is controlled by a preselected set of trusted nodes [17]. A block is added to the chain once approved by these preselected nodes. Consortium Blockchains are considered partially decentralized unlike private blockchains because write permissions are controlled by multiple entities [2]. Some examples of consortium blockchains are Hyperledger and R3.

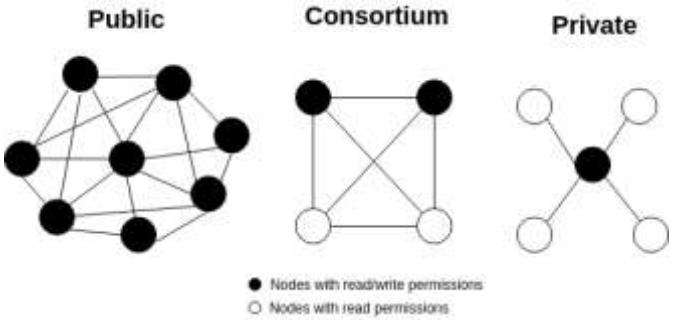


Fig. 1. A representation of public, consortium and private blockchains

The most popular consensus mechanisms are discussed in the following part. The consensus mechanism refers to the method used to verify a transaction. It shows how the group of nodes inside the distributed network agree on a specific transaction [18]. The consensus mechanism defines specific rules that identify the truth in the blockchain which makes it difficult for an attacker to add malicious blocks to the chain as it will be detected by other nodes in the network and the transaction will be rejected. There are several consensus mechanisms available until now and other mechanisms can be made up to fit the purpose of the blockchain.

A. Proof of Work (PoW)

Proof of work is a mechanism used in many cryptocurrency blockchains such as Bitcoin and Ethereum [1]. This mechanism allows cryptocurrencies to operate without central authority such as banks. It secures the whole network and prevents the double spending problem [5]. It was invented by Satoshi Nakamoto to be used in Bitcoin currency [1]. PoW is an algorithm used to add a new block to the chain. The miners select a block from the mining pool then they try to solve some mathematical puzzles to get the correct hash value. The first node to solve the puzzle sends the block to the other nodes to be added to the chain and receives reward for solving that puzzle (see Fig. 2) [19].

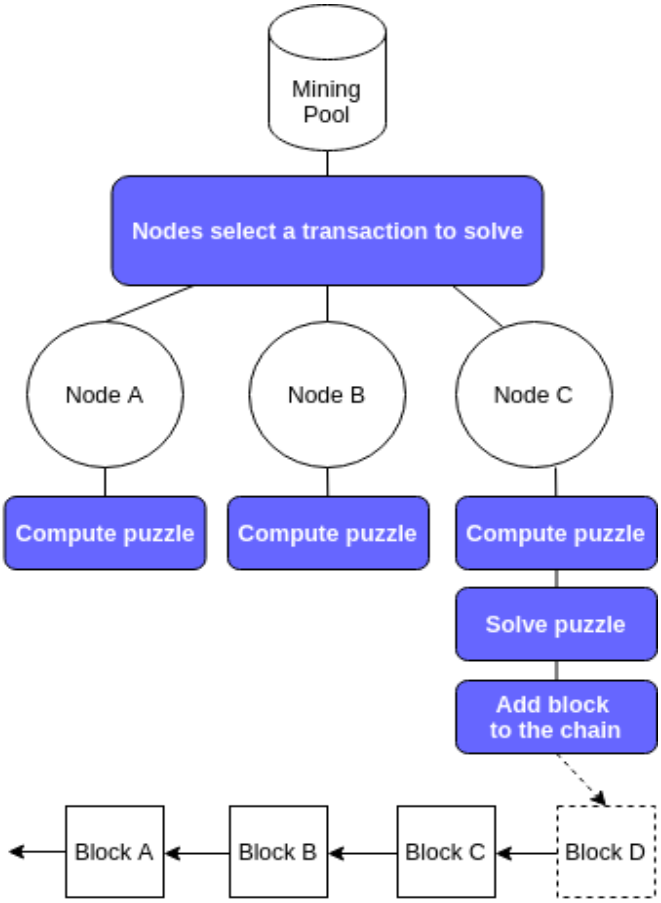


Fig. 2. A simplified steps of proof of work consensus mechanism

Actually, the process of solving the puzzle is not as easy as it looks. It requires huge computational power to brute force possible values until it reaches a nonce value that makes the hash value of the block correct. The complexity of the puzzle is decided by the difficulty level of the blockchain network [1]. When the difficulty is higher, it requires more work to find the value that makes the hash below a certain value defined by the blockchain network. Attackers would fail to tamper a block in the network as changing a single block will invalidate its hash and the other nodes would simply reject it as the new hash will break the whole chain. Since proof of work tries to make it difficult to add a new block to the blockchain, it suffers from some problems such as transaction high latency. In Bitcoin, the transaction rate is almost one transaction every 10 minutes [20]. Also, it consumes huge energy to solve the puzzle. Another problem is the scalability issues that face blockchain networks that are using PoW as a consensus mechanism. Finally, the 51% attack that may happen if an attacker can own more than 50 percent of the computing power on the network. He will be able to manipulate the chain [19]. 51% attack is nearly impossible to happen on well established networks such as Bitcoin. However, it can strike newly established or small blockchains.

B. Proof of Stake (PoS)

In this mechanism, miners get the chance to validate a block based on the amount of coins they hold. It uses a randomized selection algorithm to pick a miner. This algorithm relies on

the amount of coins that each miner holds. The more coins a miner holds, the higher the chance to be picked to mine the block [22]. PoS was invented to overcome the issues of proof of work such as high energy consumption. Instead of using energy to solve puzzles in PoW, the PoS limits the miner to the percentage of coins he owns. For example, if a miner owns 5% of the network coins, he can mine up to 5% of the new blocks.

PoS addresses the problem of 51% attack that could happen in PoW. To perform 51% attack on a blockchain network that uses PoS, one miner or more must own more than 50% of the network coins. It will be highly expensive to own this huge number of coins, however, this is not the only reason to avoid the attack. Actually, PoS highly discourages miners with high stakes to make an attack as they would be at risk of losing their stake or making the value of the currency fall down making the attacker the biggest loser [23].

Additionally, PoS provides higher scalability and throughput than PoW as the latency for producing a new block is improved in this technique. PoS is used in many cryptocurrencies such as Peercoin, Nxt, Blackcoin, and ShadowCoin. Also, Ethereum has started working on migrating to PoS since 2020 as a replacement for their PoW mechanism in an upgrade called Ethereum 2.0 to solve scalability issues [24].

C. Delegated Proof of Stake (DPoS)

The DPoS consensus mechanism was invented by Daniel Larimer to secure blockchain networks. It is an evolution of the PoS consensus mechanism. It is based on voting and election. Users on the network vote for delegates (also known as witnesses) by staking their coins to the delegate. The ownership of the tokens remains with the original user. Delegates with a high number of stakes get the chance to validate and produce the block [25]. If the elected delegate goes offline, then automatically the next delegate with high stake gets selected to complete the process. DPoS algorithm aims to eliminate centralization from the network. Also, some DPoS networks give rewards for the delegates who successfully produce the block. The reward gets shared between the users who voted for that delegate according to their percentage of coins that they have pooled for this block validation. For example, if a node stake represents 8% of the delegate stake, then it will receive 8% of the reward when the delegate mines the block successfully..

DPoS has a limited number of delegates. Most networks usually choose the number of delegates to be 20 to 100 delegates. Because the number of delegates is limited, the DPoS consensus mechanism is faster than PoS.

Similar to PoS, The DPoS mechanism increases the blockchain network scalability and throughput.

Some examples of blockchain networks that use DPoS are Lisk, Steem, Waykichain, EOS and BitShares.

D. Proof of Capacity (PoC)

PoC (also known as Proof of Space) is similar to PoW, but instead of using computational power to generate the block, it uses available empty storage. The more empty storage you have, the higher the chance to be the winner for mining the block for each round. PoC is divided into a plotting step and a mining step. The plotting step occurs beforehand to generate all possible nonce values and store them on the empty storage. The generated nonce values can be used in each round of the mining without the need to recalculate them [18]. This is why PoC reduces the electricity consumption compared to PoW, however, the plotting step may take days or even weeks depending on the size of the storage to be filled but this happens for one time. In the mining step, the miners try to match their plotted solutions to the current block. The fastest node to do this will be selected to mine the block and receive the reward. PoC is used in blockchain networks such as Burstcoin.

E. Proof of Elapsed Time (PoET)

PoET was invented by Intel and it is used mostly in permissioned blockchains. It runs trusted code that randomly picks the mining node. It is like a lottery mechanism for choosing the winner node to mine the next block. The network assigns a waiting time for each mining node in the network. This waiting time is randomly generated and guaranteed to be more than a certain time defined by the network. Every node must go to sleep during its waiting time, then the first node to finish its waiting time, comes to work and mines the block then sends it to the other nodes to add it to the chain [26]. The waiting time generation algorithm tries to make the system fair for choosing the winning participant. If the chosen node to mine a block goes down, then the next node with the shortest time is chosen as the winner.

This mechanism reduces energy consumption as it makes the nodes go to sleep instead of performing intensive calculations. Additionally, the nodes can perform other tasks during their waiting time which increases the efficiency of this mechanism.

PoET was adopted in Hyperledger Sawtooth platform and has been used in many applications including healthcare applications such as Sawtooth Healthcare which allows clinics to keep track of patient history using blockchain [27].

F. Proof of Authority (PoA)

The PoA was invented by Ethereum co-founder Gavin Wood. In PoA, validator nodes must be pre-approved before joining the system and guaranteed the right to validate blocks. These validator nodes earn high reputation when they are approved by the system making them trustworthy nodes to secure the network transactions [28].

The validator nodes are encouraged to retain their reputation so they have to produce valid blocks or they will lose the reputation attached to them. This is similar to PoS in which nodes may lose their stake if they produce false data.

This consensus mechanism is more suitable for permissioned blockchains as the nodes need to go into a preliminary process before joining the blockchain. Also, the PoA is known for its high scalability since the validator nodes are limited within the network. Unlike PoW, there is no energy waste. The transaction rate of PoA is also very high and no special hardware is required for this consensus mechanism.

PoA might be prone to Denial-of-Service attacks as a malicious node may send a huge number of blocks to a validator node. However, this issue could be solved by only approving validator nodes that have a mechanism to defend the denial of service attack. Additionally, if a node does not respond or goes down for any reason, the block can be relayed to another validator node to verify it [29]. Using permissioned blockchain with PoA consensus mechanism makes 51% attack very difficult to perform as the attacker needs to bypass the preliminary process of joining the network as a validator node and even if he succeeds, this node will lose its reputation when it produces false data.

Some examples of blockchain networks that use PoA are VeChain and Microsoft Azure on Ethereum implementation.

III. Blockchain Types for Healthcare

This section provides guidelines for selecting a suitable blockchain type that fits the needs of the healthcare industry. The first type to consider is public blockchains which are used to make data available for everyone in the network and this is not desired by the healthcare industry because the EHRs are sensitive data that should not be exposed for everyone. The healthcare providers seek to secure these records to ensure patients confidentiality.

In public blockchains, any node can join and participate in the network by sending and mining transactions. Healthcare records are critical, if anyone could join and add false EHRs to the network, that could threaten patients' lives. Additionally, this leaves an open door for attackers to attack the network. Finally, public blockchains suffer from low transaction rate issues and as the network grows and the number of nodes increases, the scalability issues strike the network. Therefore, public blockchains are not a good choice for healthcare applications.

The second type of blockchains is permissioned blockchains. This type of network provides an extra layer of security that allows only authorized nodes to join the network. This is desired by the healthcare industry as it increases confidentiality for patients' data. It also reduces the risk of external attackers as they will not be authorized to join the network.

Private blockchain suffers from centralization issues because it has a single node with write permissions, however, consortium blockchain overcomes these issues by keeping the network permissioned and partially decentralized through distributing the write permissions over multiple preselected nodes inside the network. If one node with write permissions goes down, another node will take place and process the transaction which increases availability of the network. Additionally, if one node starts adding false transactions, the remaining nodes will reject these transactions and the node can be removed from the network.

Private and consortium blockchains provide good scalability and faster transaction verification rate because the set of mining nodes are limited. Therefore, they are suitable for healthcare applications.

IV. Consensus Mechanisms for Healthcare

The choice of a suitable consensus mechanism for a healthcare model is a vital problem as there are multiple parameters in the blockchain that will be affected by the selection. In this section, we will discuss the most popular consensus mechanisms and see how they can affect blockchains that are designed for the healthcare industry.

A. Proof of Work (PoW)

The PoW consensus mechanism requires huge computational power to process a single block [18]. Additionally, networks that are using PoW are well known to suffer from transaction latency and scalability specially when the network grows and the number of nodes increases.

The mentioned problems make PoW an unsuitable choice for the healthcare industry because the healthcare organizations such as hospitals that use IoT medical devices connected to the patients usually require that the collected data from patients to be real time and always ready for processing. Also, the amount of EHRs that are generated from the healthcare industry is huge which will eventually make the blockchain network suffer from scalability issues [20].

B. Proof of Stake (PoS)

The PoS consensus mechanism features high scalability and high transaction rate. These two factors are very critical for the healthcare industry. Additionally, PoS does not require huge energy to reach consensus [22]. Thus, the PoS can be suitable for the healthcare industry. It depends on the model architecture but for instance, if we have a blockchain network that has some nodes which are the hospitals or other healthcare organizations. These organizations can be assigned a percentage of the network's coins so they can approve transactions and add new patients' EHRs as blocks to the blockchain network. These organizations will benefit from the PoS reputation system and will always work on adding valid blocks to the blockchain to keep their stake.

C. Delegated Proof of Stake (DPoS)

DPoS has the same features of PoS. It features high transaction rate and high scalability. DPoS requires the number of delegates to be limited because increasing these delegates will affect the network performance and latency [25]. Thus, DPoS is suitable for small healthcare industry networks since healthcare organizations will be represented by the delegates and they will be predefined and known.

D. Proof of Capacity (PoC)

In PoC, the mining process depends on the storage [18]. The more free space is available, the higher the chance to mine a block. Unfortunately, the healthcare industry generates a huge amount of EHRs that are collected from patients. These EHRs require huge storage to carry them. PoC makes it worse because it requires extra space to perform the mining process which makes the cost of the storage expenses very high. Additionally, PoC is prone to malware attacks that may change the plotted data which will require regenerating these data again and spending more days or weeks for the plotting process.

E. Proof of Elapsed Time (PoET)

PoET is a fair mechanism that gives a chance for every mining node in the network to generate a block. It assigns wait time for every node and the first node to finish its waiting time, mines the block [26]. It is usually used inside permissioned blockchains. That makes it suitable for healthcare models which do not perform real time processing because the algorithm is built on the idea of making the nodes wait. So, there will always be a delay limited to the minimum wait time defined by the network before a block gets added to the blockchain.

F. Proof of Authority (PoA)

PoA is best suited for permissioned blockchains because every node needs to go into a preliminary authentication process before joining the network. Once it is authenticated, it receives the necessary permissions to write new blocks to the chain [28]. These nodes have special configurations to overcome Denial-of-Service attacks and other malicious activities.

The nature of PoA makes it suitable for many healthcare applications because PoA provides higher transaction rate and higher scalability compared to many other consensus mechanisms. For example a permissioned healthcare blockchain that uses a PoA consensus mechanism may contain hospitals as validator nodes. These nodes are responsible for recording patient EHRs collected from IoT medical devices

that are attached to patients. Since hospitals have been given the permissions to validate transactions, they store the records into the blockchain at a high rate so the data can be always available for processing.

Table 1 represents a comparison among the mentioned consensus mechanisms in terms of energy consumption, transaction rate, security and scalability. The comparison results are supported by the analysis provided in [30].

TABLE I A COMPARISON AMONG CONSENS MECHANISMS

	PoW	**PoS**	**DPoS**	**PoC**	**PoET**	**PoA**
Energy Consumption	↑	↔	↔	↔	↓	↓
Transaction Speed	↓	↔	↔	↔	↔	↑
Security	↑	↔	↔	↔	↑	↑
Scalability	↓	↔	↔	↔	↑	↑

↑ denotes high, ↓ denotes low, and ↔denotes normal

V. BLOCKCHAIN INTEROPERABILITY MODELS

In this section, we will review some models and platforms that enable interoperability between different blockchain networks. Some of them have already launched after years of research and development. These models can be applied to any industry including healthcare.

A. InterChain [31]

This model provides a communication protocol between different blockchain networks. The protocol is built on the design of local network suite. It supports many-to-many communication. It proposes providing the ability to transfer assets from one network to another. For example, user ***X*** on bitcoin network can transfer or exchange assets to user ***Y*** on ethereum network. The architecture of the model consists of subchains which represent the blockchain networks that need to communicate with each other. It also contains interchain network which is a special kind of blockchain that links all subchains together enabling them to communicate as shown in Fig. 3. The interchain contains validator nodes which are responsible of validating cross-chain transaction and maintaining consensus in the interchain network. The subchains and interchain have common nodes called gateway nodes. These nodes are responsible of relaying transaction from the subchain to the interchain to be validated by the interchain validator nodes.

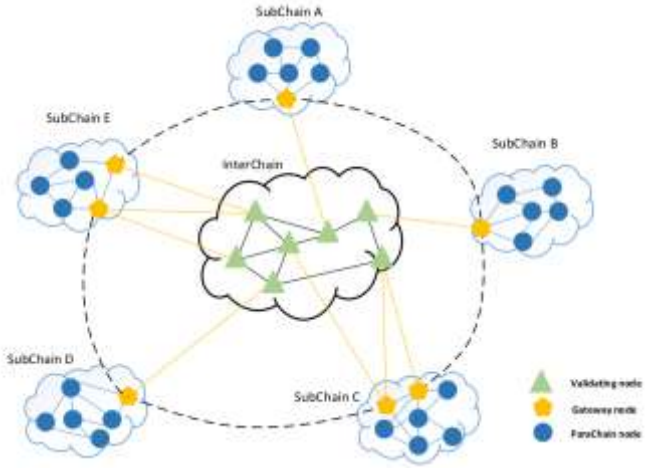


Fig. 3. The architecture of InterChain [31]

The model requires special configuration for the subchains before participating in the network. For instance, the gateway nodes must install special client software and the subchain must host two special smart contacts to perform the communication. The smart contracts are Sending Contract and Exchange Contract. The Sending Contract is used to allow a user to transfer the assets from a blockchain to another while the Exchange Contract is used to facilitate exchanging assets.

Unfortunately, the model does not describe much about the interchain internal strategy such as consensus mechanism. This model is still a novel model. It has no actual implementation yet and cannot be evaluated.

B. Cosmos (The Internet of Blockchains)

Cosmos is a cross-chain communication platform [32]. It was designed to make the Internet of Blockhains (IoB) a real concept. It uses the Inter-Blockchain Communication protocol (IBC). The cosmos platform is created in a modular architecture to enable interoperability between blockchain networks. These blockchains are independent of each other and have their own rules and maintain control of their own governance. The Cosmos platform consists of two main layers. Tendermint layer which contains the consensus mechanism of cosmos and the Application layer which contains Software Development Kit (SDK) to help developers focus on the application development and deployment instead of worrying about the protocol which makes the system run. This platform tries to solve both scalability and usability issues. Cosmos tends to increase scalability by using the PoS consensus mechanism for its cryptocurrency called ATOM. ATOM staking is responsible for securing the network transactions. Additionally, Cosmos increases usability by enabling blockchains to maintain their own governance. For example, if an application is deployed with a bug to the network or a new feature is added to the application, developers can resolve such issues without waiting for approval from higher level authority unlike Ethereum network which forces developers to wait until they approve the changes. Also, Cosmos provides a higher level of sovereignty as each blockchain is responsible for maintaining its own security besides the security provided by the platform itself. Cosmos uses hubs and zones to move assets from one blockchain to another. Hubs are specialized blockchain networks which are used to connect blockhains together. Zones are the blockchains that are willing to transfer or exchange assets. Zones are connected to hubs via IBC protocol which relays the transactions from one zone to another as shown in Fig. 4.

Not only does the platform allow interoperability between the blockchains that are deployed to the Cosmos ecosystem, but also it allows interaction with other existing blockchain networks such as Bitcoin and Ethereum. This is done via an intermediate special blockchain called the Peg-Zone which acts as a bridge. The external blockchain network gets connected to the Peg-Zone via IBC protocol and the Peg-Zone is connected to the hub via IBC protocol as well which enables communication between the external blockchain and any blockchain on Cosmos platform to share data (see Fig. 4).

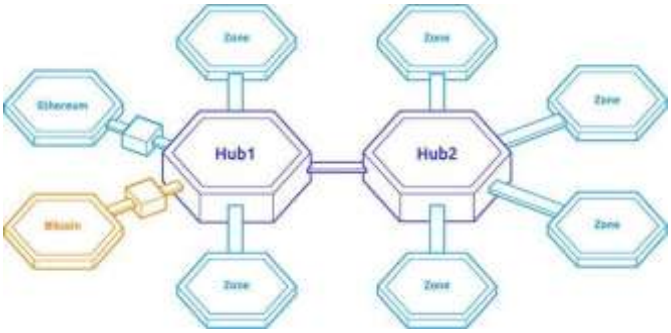


Fig. 4. External blockchains such as Bitcoin and Ethereum are connected to Peg-Zones which are connected to the hub via IBC protocol [32]

The main role of the Peg-Zone is to track the state of the external blockchain until the transaction is processed.

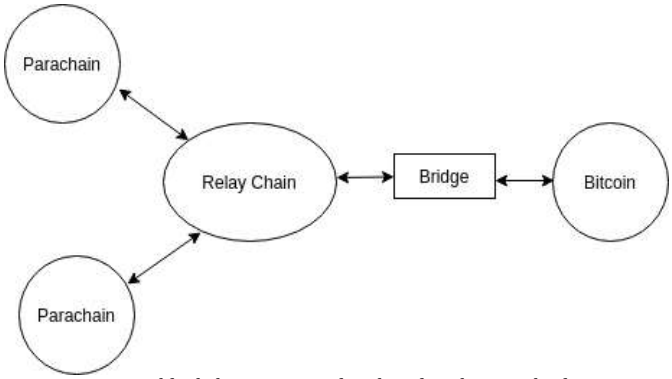
Cosmos has been in research and development cycles since 2014, but it has been successfully launched in 2019. It already hosts many blockchains and applications. This ecosystem can be used to launch different healthcare blockchains and facilitate interoperability between them to share EHRs.

C. Polkadot

The Polkadot platform was started by Gavin Wood, the co-founder of the Ethereum network [33]. It aims to build a whole network of interconnected blockchains that can share assets among each other. Technically, the platform consists of Relay Chain and Parachains. The Relay Chain is a blockchain that connects different parachains together. It uses PoS as a consensus mechanism. Additionally, the relay chain is responsible for the network security and carries out cross-chain interoperability. The Parachains are the different blockchain networks that are built on the Polkadot platform. Every blockchain can have its own rules and tokens.

Polkadat maintains the security for all connected parachains. This reduces the effort when launching a new blockchain. However, these blockchains pay for the security by purchasing and staking the DOTs which is the official cryptocurrency of Polkadot. This may make it harder later to start a small blockchain network if the price of the DOT increases. Similar to Cosmos, Polkadot provides a structure to share and exchange assets with external blockchain networks such as Bitcoin and Ethereum. It has a special blockchains called Bridges. These allow Polkadot networks to connect and communicate with external networks as shown in Fig. 5. The platform also provides SDK that helps developers create their custom blockchains.

Fig. 5. Parachains connected to the relay chain and external Bitcoin blockchain connected to the relay chain via bridge



Polkadot has launched in 2020, However, some features are still under development and are not launched yet. For example, the bridges with external blockchains networks.

This platform can also be a suitable base for making interoperable healthcare blockchains that can communicate with each other and benefit from the shared relay chain security.

Table II shows a comparison among the mentioned interoperability platforms. The external structure of the three models is similar, but the internal implementation is different.

TABLE II A COMPARISON AMONG INTERCHAIN, COSMOS AND POLKADOT.

	Interchain	**Cosmos**	**Polkadot**
Launched	No	Yes	Yes
Cryptocurrency	—	ATOM	DOT
Blockchains name	Subchains	Zones	Parachains
Intermediate blockchain name	Interchain	Hub	Relay Chain
Communication with external blockchain via	—	Peg-Zone	Bridge

VI. CONCLUSIONS

Healthcare is a critical industry that is suffering from security and interoperability issues which can endanger patients' lives or cause deaths. The paper showed the importance of applying blockchain to the healthcare industry to resolve these issues. Additionally, different blockchain types and consensus mechanisms are discussed. Also, the paper mentioned which mechanisms can be practical for the healthcare models. Finally, The descriptions of some interoperability models and a comparison among them are introduced.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] Z. Alhadhram, S. Alghfeli, M. Alghfeli, J. A. Abedlla and K. Shuaib, "Introducing Blockchains for Healthcare", International Conference on

Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 2017.

[3] J. Abou Jaoude and R. George Saade, "Blockchain Applications – Usage in Different Domains," in IEEE Access, vol. 7, pp. 45360-45381, 2019, doi: 10.1109/ACCESS.2019.2902501.

[4] Heeringa, J., Mutti, A., Furukawa, M. F., Lechner, A., Maurer, K. A., & Rich, E. (2020). Horizontal and Vertical Integration of Health Care Providers: A Framework for Understanding Various Provider Organizational Structures. International journal of integrated care, 20(1), 2. https://doi.org/10.5334/ijic.4635

[5] T. Le Nguyen, "Blockchain in Healthcare: A New Technology Benefit for Both Patients and Doctors," 2018 Portland International Conference on Management of Engineering and Technology (PICMET), 2018, pp. 1-6, doi: 10.23919/PICMET.2018.8481969.

[6] Mark Gaynor, Janet Tuttle-Newhall, Jessica Parker, Arti Patel, Clare Tang, "Adoption of Blockchain in Health Care", September 2020.

[7] A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid and M. F. Yusof, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review," in IEEE Access, vol. 8, pp. 23663-23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

[8] G. Lodha, M. Pillai, A. Solanki, S. Sahasrabudhe and A. Jarali, "Healthcare System Using Blockchain," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 274-281, doi: 10.1109/ICICCS51141.2021.9432157.

[9] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT", Sensors, vol.19, iss.2, no.326, Jan.2019.

[10] E. Yasser, Y. Awad and S. Yuan, "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management". IEEE, vol.7, no.2169-3536, pp. 164595-164613, Nov.2019.

[11] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications", In IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 2017.

[12] M. Cash and M. Bassiouni, "Two-Tier Permission-ed and Permission-Less Blockchain for Secure Data Sharing", IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 2018.

[13] G. Vizier and V. Gramoli, "ComChain: Bridging the Gap Between Public and Consortium Blockchains", IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, Canada, 2019.

[14] Kadena, "Confidentiality in Private Blockchain", available at https://www.kadena.io/kadena-confidentialitywhitepaper

[15] On Public and Private Blockchains, available at https://blog.ethereum.org/2015/08/07/on-public-and-privateblockchains [Accessed 13-8-2017].

[16] M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2021, pp. 1-4, doi: 10.1109/ICCCEEE49695.2021.9429554.

[17] Y. Aungand and T. Tantidham, "Review of Ethereum: Smart home case study", In 2nd International Conference on Information Technology (INCIT), Nakhonpathom, Thailand, 2017.

[18] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), 2018, pp. 54-63, doi: 10.1109/ICOSST.2018.8632190.

[19] S. Ghimire and H. Selvaraj, "A Survey on Bitcoin Cryptocurrency and its Mining," 2018 26th International Conference on Systems Engineering (ICSEng), 2018, pp. 1-6, doi: 10.1109/ICSENG.2018.8638208.

[20] A. Hari, M. Kodialam and T. V. Lakshman, "ACCEL: Accelerating the Bitcoin Blockchain for High-throughput, Low-latency Applications," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 2019, pp. 2368-2376, doi: 10.1109/INFOCOM.2019.8737556.

[21] K. D. Gupta, A. Rahman, S. Poudyal, M. N. Huda and M. A. P. Mahmud, "A Hybrid POW-POS Implementation Against 51 percent Attack in Cryptocurrency System," 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2019, pp. 396-403, doi: 10.1109/CloudCom.2019.00068.

[22] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," in IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[23] E. Deirmentzoglou, G. Papakyriakopoulos and C. Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols," in IEEE Access, vol. 7, pp. 28712-28725, 2019, doi: 10.1109/ACCESS.2019.2901858.

[24] M. Cortes-Goicoechea, L. Franceschini and L. Bautista-Gomez, "Resource Analysis of Ethereum 2.0 Clients," 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2021, pp. 1-8, doi: 10.1109/BRAINS52497.2021.9569812.

[25] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[26] A. Pal and K. Kant, "DC-PoET: Proof-of-Elapsed-Time Consensus with Distributed Coordination for Blockchain Networks," 2021 IFIP Networking Conference (IFIP Networking), 2021, pp. 1-9, doi: 10.23919/IFIPNetworking52078.2021.9472787.

[27] Z. Leng, Z. Tan and K. Wang, "Application of Hyperledger in the Hospital Information Systems: A Survey," in IEEE Access, vol. 9, pp. 128965-128987, 2021, doi: 10.1109/ACCESS.2021.3112608.

[28] N. A. Asad, M. T. Elahi, A. A. Hasan and M. A. Yousuf, "Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing," 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), 2020, pp. 35-40, doi: 10.1109/ICAICT51780.2020.9333488.

[29] S. Alrubei, E. Ball and J. Rigelsford, "Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021, pp. 1-7, doi: 10.1109/CyberSA52016.2021.9478257.

[30] L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1545-1550, doi: 10.23919/MIPRO.2018.8400278.

[31] Ding, Donghui. "InterChain : A Framework to Support Blockchain Interoperability." (2018).

[32] J. Kwon, E. Buchman, "Cosmos Whitepaper" Available: https://v1.cosmos.network/resources/whitepaper

[33] G. Wood, E. Buchman, "Polkadot: Vision For A Heterogeneous Multi-Chain Framework" Available: https://polkadot.network/PolkaDotPaper.pdf