Sustainable Cities and Society 55 (2020) 102018

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development

Fakhri Alam Khan[a], Muhammad Asif[b,*], Awais Ahmad[b], Mafawez Alharbi[c], Hanan Aljuaid[d]

[a] Institute of Management Sciences, Peshawar, Pakistan
[b] Department of Computer Science, National Textile University, Faisalabad, Pakistan
[c] Department of Computer Science and Information College of Science, Majmaah University Saudi Arabia, Saudi Arabia
[d] Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Saudi Arabia

ARTICLE INFO

Keywords:
Blockchain
Bitcoin
Ethereum
Proof-of-Work
Proof-of-Stake

ABSTRACT

Blockchain technology has gained considerable attention for different types of stakeholders due to its stable implementation in the field of digital currency like Bitcoin. Some users use Bitcoin for payment exchanges against any business while others use the Bitcoin network for earning Bitcoins itself, and there is also another type of user who called hackers those flood different types of attacks to illegally earn some Bitcoins or collapsing overall network. There are also numerous uses of blockchain technology, e.g. health, automation industry, energy sector, security and authentication in smart grids. In this study, we have elaborated on different critical aspects of Blockchain technology like its style of working mechanism, possible improvement suggestions by using Proof-of-Stake, and other custom variations, attempting seven types of challenges by different novel techniques. Moreover, we have also explained the current state-of-the-artwork in blockchain's non-financial applications like Healthcare in which contribution of four-layered custom blockchain models related to precision medicine and the clinical trial was notable. Moreover, a mobile app model called HDG for the automation of medical records without compromising privacy was also a prominent contribution.

1. Blockchain technology

Blockchain technology was introduced by Nakamoto (2018), who published an article in 2008 for Bitcoin. Blockchain network is an underlying architecture on which bitcoin currency works. To understand blockchain technology, firstly, we have to know about bitcoin. Bitcoin is an online payment system that works without involving the third party. It needs the huge computing power of connected network nodes. Those are also called miners, and against their services, some incentives are paid. Transactions being executed on the bitcoin network are put into blocks that are cryptographically signed and validated automatically by a network of miners. Each block that is being solved by miners is linked to previous blocks using a hash value. It means that transactions once placed are become immutable. Transactions in the bitcoin network are managed by public/shared ledger (Linn & Koo, 2016), which allows network nodes to add verified blocks. It means that any single third party does not own a public/shared ledger. Rather any network node, aka miner, may offer its services as computing power to make legitimate transactions and maybe the part of the bitcoin network.

Now we come to blockchain technology. As discussed above, blockchain is the underlying mechanism on which bitcoin network works, so we may say that using blockchain architecture, we may develop more non-financial and financial applications like bitcoin. There are also other unique features of blockchain like a distributed database, decentralized network, better security, and having a trust system in verifiable peer to peer transactions (Angraal, Krumholz, & Schulz, 2017; Dagher, Mohler, Milojkovic, & Marella, 2018; Daniel, Sargolzaei, Abdelghani, Sargolzaei, & Amaba, 2017; Habibzadeh, Nussbaum, Anjomshoa, Kantarci, & Soyata, 2019; Watanabe et al., 2016).

By the introduction of smart contracts in 1994 by Nick Szabo, blockchain technology gains its significant benefit because, in smart contracts, a script was used to automatically execute transactions according to predefined rules like sender & receiver hashes, operation type, and date of transaction, etc. (Christidis & Devetsikiotis, 2016; Cong & He, 2019). Ethereum network firstly provides a mechanism to write smart contracts by the introduction of a programming language called Solidity. Moreover, for the execution of the smart contracts,

* Corresponding author.
E-mail addresses: fakhri.alam@imsciences.edu.pk (F. Alam Khan), asif@ntu.edu.pk (M. Asif), awais.ahmad@lcwu.edu.pk (A. Ahmad), m.alharbi@mu.edu.sa (M. Alharbi).

https://doi.org/10.1016/j.scs.2020.102018
Received 4 November 2019; Received in revised form 14 December 2019; Accepted 22 December 2019
Available online 14 January 2020

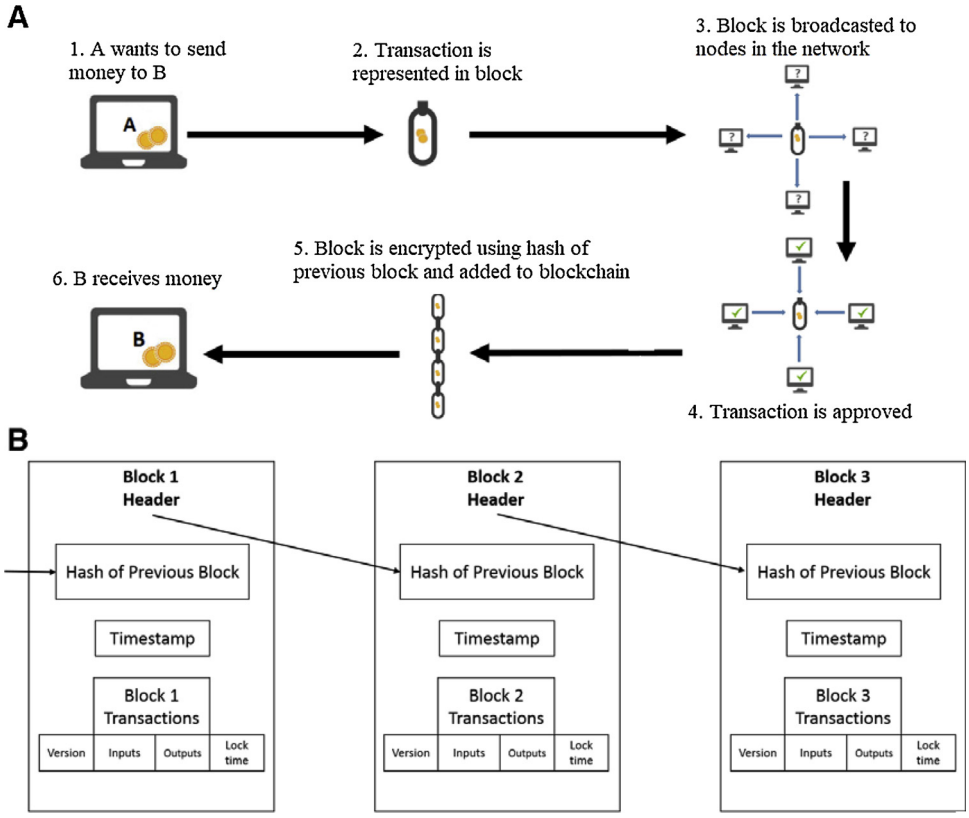

Fig. 1. Process of transaction execution on blockchain (Angraal et al., 2017).

ethereum provides a decentralized virtual machine named Ethereum Virtual Machine (EVM) (Wohrer & Zdun, 2018). The list of applications of smart contracts is long enough, but its more notable dimensions are IoT (Ande, Adebisi, Hammoudeh, & Saleem, 2019), Solar Electricity (Lin, Pipattanasomporn, & Rahman, 2019) and healthcare (Griggs et al., 2018), buildings (Reynolds, Rezgui, & Hippolyte, 2017) etc. But there is still big room for future research aspects in smart contracts like formal verification, layer 2 model and smart contract-based parallel organizational management (Wang et al., 2019).

1.1. How does blockchain technology work?

The first and physical implementation of blockchain is the Bitcoin network, which works by using SHA-256 (Dev, 2014) hashing. It is a peer to peer payment processing technique in which payments may be transferred to anyone without involving any third party. Payment transactions, once generated, cannot be revoked.

When a seller wants to transfer the digital asset to the buyer shown in Fig. 1A, he/she generates a request that is put into the block and broadcasted to every peer which are actively connected. Those peers are called miners. They devote their processing power to solve the cryptographic algorithm for the validity of transactions whether the seller owns the digital currency. That cryptographic algorithm is very complex to solve but easily verifiable. Once a transaction validated by peers, a reward is transferred to peers who participated in solution and validation. A cryptographic hash with timestamp also added to block, while that block is stored at the end of blockchain shown in Fig. 1B.

Above discussed process in general working style of the bitcoin network. By following this process, some other financial and non-financial systems may be developed for blockchain networks by only replacing the type of data which is initiated by buyers and sellers on bitcoin network like balances of the bitcoin cryptocurrency (Angraal et al., 2017).

2. Possible improvement in blockchain network

The blockchain network is considered as a secure decentralized network on which Bitcoin digital currency is working. The backbone of the stable and flawless working of Bitcoin is its security, which is ensured by miners who provide their computing power and electricity to add a particular block on the Bitcoin network by solving a compute-intensive puzzle. There is no particular strategy to solve that puzzle (finding nonce) (Ma, Gans, & Tourky, 2018) instead, it works by brute force (Ellis, 1992; Morton & Mareels, 2000) like guessing method while more guesses (needs massive computation power) increases the chances of winning (providing solution). Providing more massive processing by miners does not assure the winning of the game, although it increases the chances of a win.

Proof-of-work, aka PoW (Gervais et al., 2016), is a security measure against attacks and also is the backbone of the Bitcoin network. The Bitcoin network is based on HashCash (Back, 2002) PoW. For the detection of any illegal activity, the consensus of miners related to the solution of the cryptographic puzzle is evaluated. The rule 50 % is applied on PoW, it means that not a single miner can have more than 50 % of processing power, so if any adversary node having 49 % computing power tries to add illegal transactions, will automatically rejected by other miners because that solution will be verified as illegal by miners (with only one calculation) those have more than 50 % computing power collectively.

Miner, who firstly devise a solution (solo mining (Dev, 2014; Rosenfeld, 2011)) got the reward of 12.5 BTC (Göbel & Krzesinski, 2017; Miller, 2016) along with transaction fees and reward halves every 210000 blocks (Moser, Bohme, & Breuker, 2013; Taylor, 2013), mined and will be adjusted to 6.25 BTC (Bowden, Keeler, Krzesinski, & Taylor, 2018) around the year of 2020. There are a total of 21 million BTC those will be mined approximately till 2140 (Meiklejohn et al., 2013). The difficulty of the cryptographic puzzle is adjusted dynamically after 2016 blocks (Eyal, Gencer, Sirer, & Van Renesse, 2016;

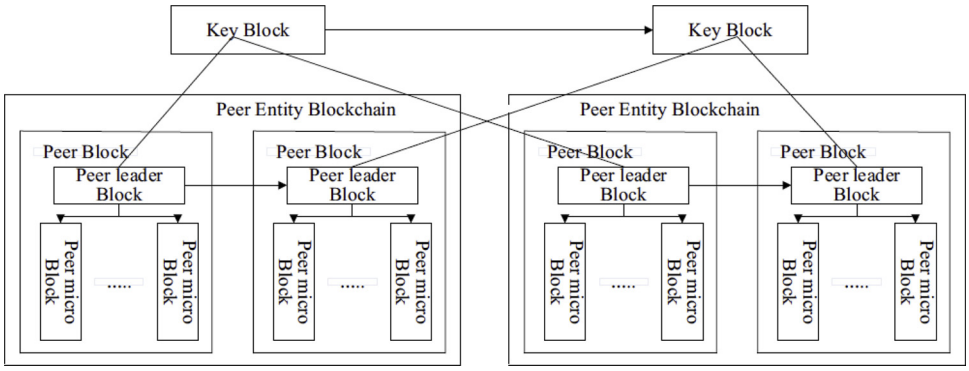

Fig. 2. Working mechanism of permission-based blockchain architecture (Min et al., 2016).

Tschorsch & Scheuermann, 2016) approximately in 2 weeks. The problem with solo mining is, a miner can take several years to solve a block that is not practically profitable. Another mining method is Pool Mining (Dev, 2014; Rosenfeld, 2011) in which several miners are working collectively, and the reward is shared among minors according to their hash power. Some researchers proposed different methods for efficient reward dissemination (Dev, 2014; Lewenberg, Bachrach, Sompolinsky, Zohar, & Rosenschein, 2015) to miners.

Some authors reveal pool mining vulnerability in the shape of selfish mining (Eyal & Sirer, 2014b) through which the system can collapse. So, after considering all facts like decreasing rewards and increasing difficulty as well as mining vulnerability, what is the future of Bitcoin mining? In 2012, some researchers proposed a new coin PPCoin (King, 2012) using Proof-of-Stake, aka PoS. The benefit of PoS is that there is no need to provide substantial computing power and more electricity consumption, like in PoW somewhat reliable validators (aka miners in PoW) are selected according to highest possession of coins and most prolonged age of possession. These validators validate the blocks, but there are also some vulnerabilities associated with PoS like 51 % attack (Houy, 2014) still possible in PoS in which a validator holding 51 % or more coins can monopolize network and ultimately the value of the coin will be reduced.

Some researchers proposed to managing credibility rather than stake (Watanabe et al., 2016) in smart contracts for a solution to the problem mentioned above in which a contractor will gain more credibility and trust after making contracts with different contractors and if he will attack then will lose credibility and turn will be moved to another contractor which will have more credibility score. However, 51 % attack is still possible because if a fictitious contractor increases his score with other adversaries using fake smart contract, then his credit score will be increased, so the solution to this problem is to make hybrid blockchain using credibility score with PoS, where a validator with the highest possession of coins along with the highest credibility will be selected as validator.

Another proposed solution in PoS (Kiayias, Russell, David, & Oliynykov, 2017) was to make timely, active transactions using parameters of persistence and liveness. Moreover, they proposed a coin-flipping protocol for ensuring randomness in leader selection for the particular period in which during a specified period, a committee is formed by stakeholders who are selected randomly who run coin-flipping protocol for selection for leader election.

3. Challenges and limitations in blockchain

Blockchain technology is error-prone and has some architectural issues. There are many technical challenges and limitations associated with blockchain technology that is elaborated by different researchers (Swan, 2015) elaborated that there are seven essential challenges associated with blockchain.

3.1. Problem of throughput

Throughput is one of seven challenges discussed by Swan (2015), which is near about seven transactions per minute, which is called a theoretical throughput. According to Xu et al. (2016), the Bitcoin network can process 3–20 transactions per second. We have analyzed blockchain.info (Wohrer & Zdun, 2018) website, which shows that maximum transactions per second never exceed 5. According to visa.com (Cong & He, 2019), after the evaluation of their network using stress tests, they have achieved 47,000 transactions per minute, which is a huge achievement. So, if general e-commerce companies deploy blockchain for transactions, then it will ultimately fail because of transaction delays and increase the cost of network communication. Permission blockchain network (Min, Li, Liu, & Cui, 2016) was proposed to enhance the performance of blockchain protocol by partitioning the main network into chunks called sub-committees as well as the division of computing power to chunks too. Each chunk operates separate peer consensuses protocol to process separate transactions by using a random partition algorithm. A special committee also formed which is responsible to write blocks of each committee into the global block. Their overall goal was to provide the same security as the original Bitcoin network but with better throughput and lower latency. Their proposed architecture is shown in Fig. 2.

The consensus algorithm from different authors was analyzed critically by Mingxiao, Xiaofeng, Zhe, Xiangwei, and Qijun (2017). They have examined six algorithms according to different factors like Byzantine fault tolerance, Crash fault tolerance, Verification speed, Throughput (transactions per second), and scalability. Algorithms were Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Practical Byzantine fault tolerance (PBFT) and RAFT. PoW and PoS have discussed above in detail while DPoS allows each node to select witnesses based on their stake and selection criteria in which at least 50 % of voters must agree on it, and it does not disturb the decentralized nature of blockchain. After that blocks are assigned to those witnesses one by one, means they all have equal right for block allocation for mining purpose and if any witness goes offline, then that particular block assigned to next witness and another election place to select another witness. BitShare (Wang et al., 2019) is a prime example of DPoS. PBFT starts with sending a request from a client to the master server, then the master server records it by order number and forwards this request to other server nodes. Those nodes take a decision whether to accept or reject, and in case of acceptance, it broadcasts prepare a message to all other server nodes while the same time it also receives prepare messages from other server nodes. After collecting a certain number of messages, they commit the message. After that server node acknowledges the client by reply. By 1999 (Castro & Liskov, 1999), the PBFT algorithm's complexity was reduced to polynomial time. The process of PBFT is shown in Fig. 3.

Paxos was that particular consistency algorithm which gained dominant position and was re-introduced in a simplified version in

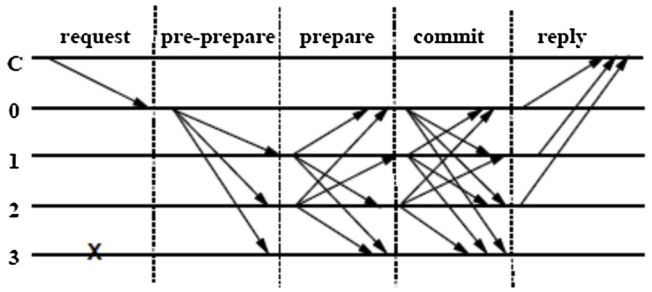

Fig. 3. Execution steps of PBFT (Mingxiao et al., 2017).

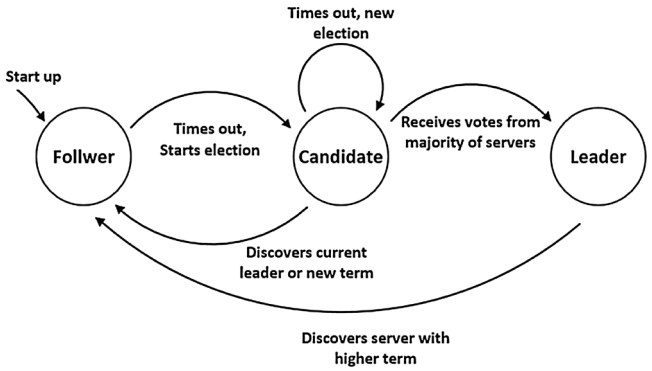

Fig. 4. Work flow of Raft process (Mingxiao et al., 2017).

2001 (Lamport, 2001), but it was a theoretical algorithm and difficult for understandability and implementation purpose, so in 2013 (Ongaro & Ousterhout, 2014), Raft algorithm was proposed with the same efficiency as Paxos but with easy implementation. There are five server nodes in Raft (shown in Fig. 4) with three states: Leader, Follower & Candidate. Moreover, there is only one leader who is responsible for handling client requests.

Performance analysis of all the above-mentioned consensus algorithms is shown in Table 1, in which we can see that if the Bitcoin network implements the Raft algorithm for miners' consensus, then more than 10k transactions per second can be achieved, which is more than enough current and future e-commerce business.

3.2. Latency issue

Higher Latency is also a very critical problem in the Bitcoin network. Ten minutes are required to process a transaction while more time required to ensure the security against double-spending (Karame, Androulaki, & Capkun, 2012; Karame, Androulaki, Roeschlin, Gervais, & Čapkun, 2015) problem. For a successful double-spending attack, some conditions needs to be fulfilled. For example, An attacker A wants to perform double spending on the Bitcoin network with vendor V, so A will put a transaction TRv with V that will not be subsequently redeemable. At the same time, Attacker A will put another transaction TRa that will have same input as TRv like the amount of BTCs are same,

Table 1
Performance analysis of consensus algorithms (Mingxiao et al., 2017).

Characteristics	Consensus Algorithms				
	PoW	PoS	DPoS	PBFT	RAFT
Byzantine fault tolerance	50 %	50 %	50 %	33 %	N/A
Crash fault tolerance	50 %	50 %	50 %	33 %	50 %
Verification speed	> 100 s	< 100 s	< 100 s	< 10s	< 10s
Throughput (TPS)	< 100	< 1000	< 1000	< 2000	> 10k
Scalability	Strong	Strong	Strong	Strong	Weak

attacker A will replace the recipient address of TRv with the address of the recipient that will be in the control of attacker A (shown in Fig. 5). There is a great chance of confirmation of these transactions in the upcoming block if these two put on the same time. While the Bitcoin network has security implementation against this and will reject these transactions, but this will ultimately increase further latency.

During extra latency Bitcoin network verifies the inputs to check against double-spending and rejected if matched. Latency should be minimized in the Bitcoin network for transaction's consistency while Visa transactions only need some seconds to process (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016)

A new protocol Bitcoin-NG (Eyal et al., 2016) for scalability purpose was proposed in which authors tried to enhance throughput and lower latency. According to their claim, latency will only be limited to network propagation delay. They achieved this by decoupling the bitcoin network by two planes called leader election and transaction serialization along with time-division called epochs, while each epoch has its leader. One leader will be chosen, then he will serialize transactions until having a leader seat. In fact, leader election also takes time, so they conduct the election as forward-looking at which transactions will also be taken place during election time. The challenging task was to design an appropriate consensus protocol with performance evaluation. For that cause, they put several metrics on the original model of the bitcoin network for improvement perspective in terms of latency.

They experimented original Bitcoin and their Bitcoin-NG model while putting 1000 nodes. As shown in Fig. 6, the latency of Bitcoin-NG was considerably low as compared to Bitcoin.

Other authors proposed some suggestions for enhancing throughput and to lower latency (Croman et al., 2016). According to them, block size should never exceed 4MB, which will increase throughput mostly at 27 transactions per second, as well as block interval should not less than 12 s.

3.3. Limitation of size and bandwidth

The size of blockchain in the Bitcoin network is a very critical part because, according to Yli-Huumo et al. (2016) and Koteska, Karafiloski, and Mishev (2017), the size of the Bitcoin database near about 50,000 MB till February 2016, and if this network continues to grow according to Visa then the size will grow near about 214PB each year. Some authors (Kim, Kang, & Hong, 2017) proposed an attractive solution of size limitation. According to them, the size will be accumulated each year because of the addition of new blocks data into old data records, and it will continue to increase in this fashion. The addition of data is occurring because the number of nodes is also increasing, and data is broadcasting to all nodes, so ultimately, the cost will also be increased. A simple way to manage the data size is to delete the old blocks that are not needed now.

The scalability of blockchain is compulsory in order to reach the current e-commerce like Visa. According to Decker and Wattenhofer (2015), scalability in Bitcoin network is technically not possible because the average size of a transaction is near about 500 bytes and while performing one transaction per second technically needs 20 GB storage each year, while to meet against the transaction volume near about 1 % of Visa, Bitcoin network should accommodate almost 500 transactions per second (it requires considerably larger blocks to broadcast), while this ultimately need 10 TB storage each year.

The main challenge is to increase the number of transactions per block. For this purpose, different authors propose to change the size of the block, which is currently 1MB. According to Garzik (2015b), the size of the block should be adjustable by the consensus of minors, while Andresen (2015) says that block size should be 8MB and should increase every two years to 20 years (Garzik, 2015a). Proposes that size should be 2MB, while according to Wuille (2015) idea, block size should increase 4.4 % after every 97 days till 2063. However, the feasible proposal of Lombrozo, Lau, and Wuille (2015) is, do not change

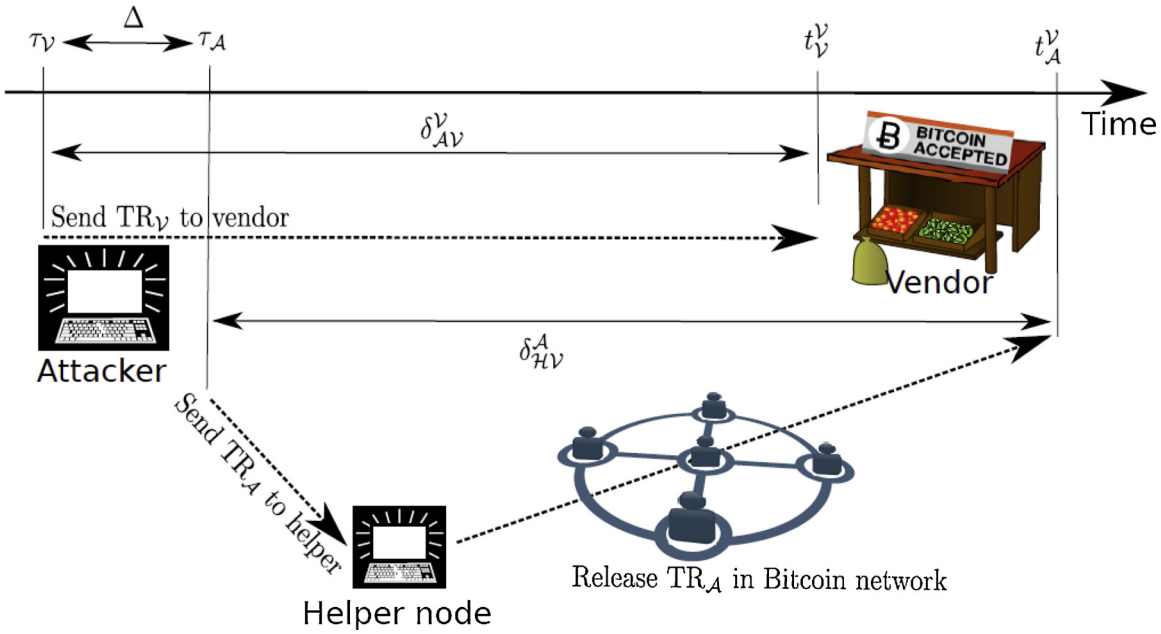

Fig. 5. Simulation of double spending attack (Karame et al., 2015).

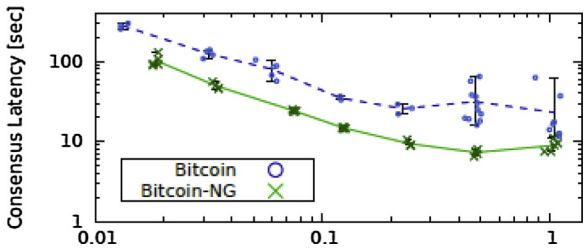

Fig. 6. Latency analysis of Bitcoin vs Bitcoin-NG (Eyal et al., 2016).

the block size rather reduce the information stored in transactions.

While considering the above-discussed challenges, some researchers proposed a scalable blockchain database called BigchainDB (McConaghy et al., 2016) considering throughput, latency, and storage problems of the original Bitcoin network shown in Table 2.

In BigchainDB, they used modern distributed DB with full-featured NoSQL which can provide more than 1 million transactions per second, more than Petabytes of capacity and latency as a fraction of a second.

An exciting feature of BigchainDB is nodes vs capacity mechanism, in which, a new node which joins networks adds 48 TB more storage option which adds to total BigchainDB capacity (shown in Fig. 7).

Table 2
Main highlights of BigchainDB (McConaghy et al., 2016).

	Traditional Blockchain	Traditional Distributed DB	BigchainDB
High Throughput; increases with nodes	–	✓	✓
Low Latency	–	✓	✓
High Capacity; increases with nodes	–	✓	✓
Rich querying	–	✓	✓
Rich permissioning	–	✓	✓
Decentralized control	✓	–	✓
Immutability	✓	–	✓
Creation & movement of digital assets	✓	–	✓
Event chain structure	Merkle Tree	–	Hash Chain

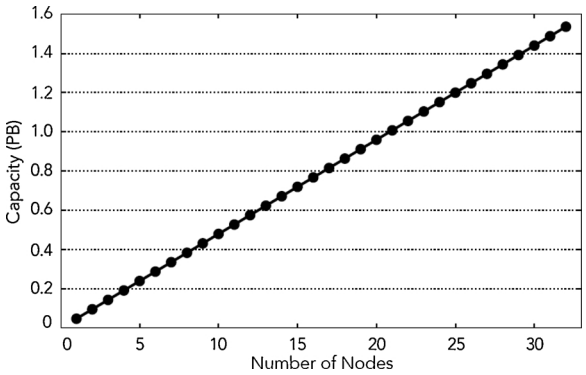

Fig. 7. Nodes vs Capacity analysis in BigchainDB (McConaghy et al., 2016).

3.4. Security threats

Blockchain technology is famous because of its security features with distributed nature ultimately make it more secure. Blockchain's notable implementation is of Bitcoin, which is a digital currency and currently has more value than real Gold. Their attractions are enough for attackers who are trying to manipulate the Bitcoin network after the rise of currency worth. A straightforward risk is Identity theft (Xu, 2016), which is not curable. Identity on the Bitcoin network is the combination of public and private keys. The overall security of currency lies behind the private key, and wallets are required to store private keys. There are many types of wallets available in the market (Bitcoin Wallets, 2018; How to Store Your Bitcoin, 2018; Types of Bitcoin Wallets, 2018) like Hardware, Desktop, Web, Mobile, and Paper wallets. Hardware and Paper wallets are considered to be more secure. However, even paper and hardware wallets can do nothing in case of private key theft. Ethereum (Wood, 2014), is another cryptographic currency. For the security of private keys of Ethereum, a wallet provider company (Sohaib, Naderpour, Hussain, & Martinez, 2019) provides a solution of password protection of private keys, so if the private key is stolen, then the adversary will not be able to steal funds. Another solution against misplacement for theft of private keys is the Two-factor security (Goldfeder, Bonneau, Kroll, & Felten, 2014) in which private keys can be shared among two devices like mobile and computer. If

Table 3
Key management evaluation in blockchain network (Eskandari et al., 2018).

Category	Example	Malware Resistant	Key(s) Kept Offline	No Trusted Third Party	Resistant to Physical theft	Resistant to Physical Observation	Resilient to Password Loss	Resilient to Key Churn	Immediate Access to Funds	No New User Software	Cross-device Portability
Keys in Local Storage	Bitcoin Core			●		●	●	●	●		
Password-protected Wallets	MultiBit			●	○	●		●	●		
Offline Storage	Bitaddress	○	●	●			●				●
Air-gapped Storatge	Armory	○	●	●		●	●	●			
Password-derived keys	Brainwallet		●	●	○			●	●	●	●
Hosted Wallet (Hot)	Coinbase.com						●	●	●	●	●
Hosted Wallet (Cold)		○	●				●	●		●	●
Hosted Wallet (Hybrid)	Blockchain.info		○	○			●	●	●	●	●
Cash		●	●	●		●	●	●	●	●	●
Online Banking						●					

someone executes a transaction from a computer or different mobile, then a confirmation will be forwarded to the owner's mobile. After the original's confirmation from the mobile transaction will be signed successfully for execution.

Other types of attacks are proposed by Heilman, Kendler, Zohar, and Goldberg (2015) called Eclipse attacks. According to them, an adversary can exploit several IP addresses to monopolize all connections through a victim node. In this way, they can attack the consensus systems, double-spending or selfish mining. Some countermeasures can be performed to escape, like disabling incoming connections and choosing specific outgoing connections like miners to fall in the whitelist.

The most notable threats are 51 % and Double spending attacks, which are already discussed above (Bastiaan, 2015; Karame et al., 2012; Lin & Liao, 2017). A 51 % attack is the base of other attacks. If a single node or group of nodes will acquire 51 % of computing power, then there will be extreme aftereffects like transaction data can easily be modified so that a Double spending attack will be straightforward. Even they can manipulate the mining of miners and in the more severe case, can be: to stop the blockchain network for transaction verification (Lin & Liao, 2017).

According to the authors of Karame et al. (2012), the Bitcoin network is not able to perform fast payments. They simulated a double-spending attack on a fast payment system on Bitcoin. According to their results, attacks like double-spending are more successful in fast payments as well as the detection of double spending is not that effective. So according to their analysis, scalability in terms of faster transactions is not practically possible, and it invites a double-spending attack.

As the difficulty of mining increases in the Bitcoin network, solo mining is no more profitable. So, the solution is to join mining pools, which are the collection of miners, who jointly work, and incentives are paid equally. However, as the pool size increases, attacks like 51 % are inevitable. In 2014, a mining pool GHASH.IO was vulnerable to 51 % attack, so many miners left that pool. A solution named Two Phase Proof of Work, aka 2P-PoW against 51 %, was proposed by Eyal and Sirer (2014a) in which pool operators must share private keys to participants. In this way, all participants can usurp all newly generated coins and can move coins to any other address.

3.5. Resources wastage

Whether PoW is very important in the Bitcoin network and provides security against adversaries but at the same time, a bundle of computing resources is wasted in terms of heavy hardware costs and electricity bills. According to Yli-Huumo et al. (2016), Koteska et al. (2017) and Reynolds et al. (2017), 15 million dollars per day are wasted in terms of energy. There are many practical solutions against wastage of resources are proposed from different researchers while using combination PoW and PoS are discussed in detail in the previous section.

3.6. Usability problem

Most of the research on the blockchain is based on the technical side of security, privacy, data integrity, performance, and scalability, but the usability aspect is ignored (Habibzadeh et al., 2019; Pillai, Muthukkumarasamy, & Biswas, 2020). The reason may be the first and stable implementation of blockchain in financial markets like Bitcoin and Ethereum, and people are attracted because of digital money having worth more than any metal like gold and physical currency like the dollar. So, they ignore an important aspect of usability.

In the blockchain, usability covers many aspects of the usability of identity management (Eskandari, Clark, Barrera, & Stobert, 2018) like the management of public and private keys and usability of blockchain application development language (Coblenz, 2017).

Contributions of Eskandari et al. (2018) were a survey of 6 key management techniques and proposed usability measures according to results, and lastly, performing cognitive walkthrough on Bitcoin clients.

According to authors, six key management techniques are, storing keys on local storage like internal storage of computers, or storing keys with additional security like password protection, or storing keys on external drives like USBs, or storing keys on devices those are not directly connected to internet, or storing keys as Hierarchal Deterministic aka HD format in which keys can create new keys, and last technique is to store keys on third party web service providers.

They have used ten parameters to characterize usability measures according to 6 keys management techniques (shown in Table 3), and for cognitive evaluation, their focus was learnability for novice users step by step. In the first step, the question was, "Will the user see what to do?"; secondly, "Will the user see, how to do," and lastly, "Will the user know if they have performed the correct the correct action." Their results show that each client on Bitcoin network has different preferences like clients having a small amount of digital currency prefer ready to spend key management method like local storage or web-enabled wallets whether clients those have the largest amount on currency prefer secure wallets like air-gapped or offline storage.

Authors of Coblenz (2017) have put the focus on a blockchain programming language called Solidity. According to them, there are cases of smart contract vulnerability which were designed using the same language, and 40 million dollars loss (Sirer, 2018) was noted. They have proposed a new and less bug-prone language called "Obsidian," focusing on usability features.

3.7. Fork problems

Forking in blockchain occurs when a change is needed to be implemented. There are two types of forks, Soft and Hard forks. Peers or nodes or miners are the main drivers of blockchain. When any type of change occurs, that change should be adopted by nodes. Moreover, when nodes are upgraded, then they continue to validate blocks. Although when non-upgraded nodes may continue to validate blocks then it is called soft fork and when non-upgraded could not continue to validate blocks and then its hardware fork. In a hard fork, a critical situation occurs because blockchain is permanently split into two separate chains and non-upgraded nodes remain on exiting blockchain and upgraded nodes shifted to a new blockchain. On the other side, a soft fork is temporary till software upgrade completed, after that, all nodes continue to work on the same chain, and no split occurs. Most of the time, a hard fork occurred after the system up-gradation when a severe attack occurs like an attack on Decentralized Autonomous Organization, aka DAO (Atzei, Bartoletti, & Cimoli, 2017; Fahmy, 2018) in June 2016, which was on Ethereum blockchain and written by smart contracts. DAO's objective was to have decentralized business with non-profit organizations but unfortunately ended due to disaster. DAO raised its business to 150 million dollars in May 2016, but a clever hacker took the benefit of a bug in the smart contract and usurped near about 50 million dollars. So as a solution, some members of Ethereum agreed upon to initiate a Hard Fork on blockchain in which they modified blockchain and reversed the funds into the right owner's account. However, the after-effects of this action were not normal because the Ethereum community was against this action, and most of the miners refused to fork.

A fork which was occurred in DAO was a hard fork in which blockchain splits into two branches, and nodes also split into old and new branches. Whether these two branches will not be compatible with each other, so old nodes will not agree upon the mining of new nodes. Then it was requested to old nodes to upgrade their system, so nodes that will not upgrade will not be able to perform usual work. Whether the new nodes will accept old and new system rules will continue their work on a new chain, and it is called compatible hard fork, which is shown in Fig. 8.

The same case was occurred in Bitcoin (Fahmy, 2018) when the hard fork occurred, and a new blockchain named Bitcoin Cash comes into existence. Here the problem was the block size on which

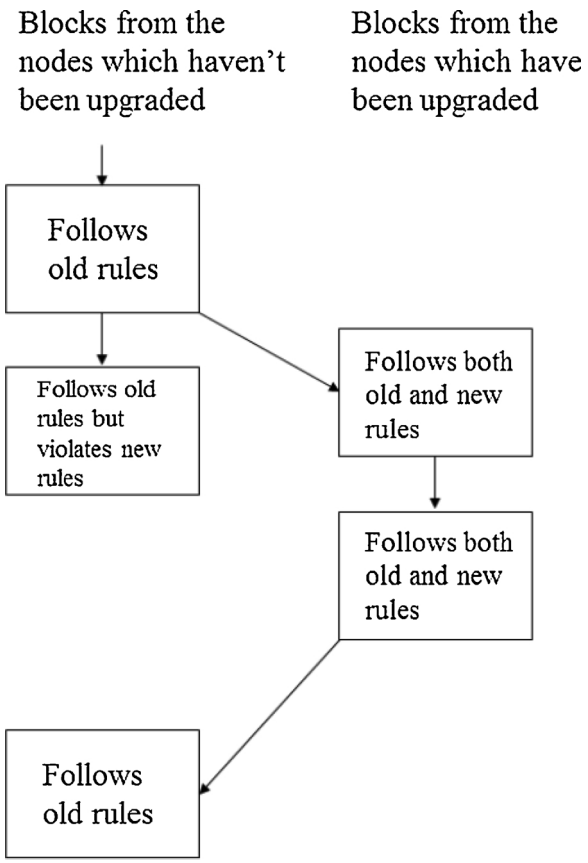

Fig. 8. Process flow of compatible hard fork (Lin & Liao, 2017).

developers did not agree, and on the original Bitcoin network, it was set to 1MB, so those who were in favor of change adopted the Bitcoin Cash network, which has 8MB block size.

Another type of Fork also exists named Soft Fork in which blockchain also split into two chains, but these two chains will be compatible with each other (Back et al., 2014). This process occurred with the consent of a supermajority of nodes who have major computing power. The soft fork has been deployed many times in the Bitcoin network for minor upgrades (some restrictions, like what is valid now) (Arora, 2018).

4. Blockchain in healthcare

There are enormous applications of blockchain in healthcare. The main challenge in the healthcare industry is the privacy and security of existing records (Ekblaw, Azaria, Halamka, & Lippman, 2016). Patient Master Identifier (MPI) is an example of blockchain in healthcare in which a single unique identifier is used for all healthcare providers seamlessly. Many researchers have worked for the identification (Mettler, 2016) of patients and permission-based systems (Sohaib, Solanki, Dhaliwa, Hussain, & Asif, 2019) using patient authorization to share data with others using blockchain. Another possible application for settlement of claims (Witchey, 2015) to only eligible patients and fraud detection (Nath, 2016; Sohaib, Kang, & Miliszewska, 2019) without involving third parties with the use of smart contracts which is another feature of the blockchain. Fraud detection can also be another application of blockchain because, in the blockchain, every transaction made is verified for its legitimacy. Supply chain management (Daniel et al., 2017; Sohaib, Kang et al., 2019) in healthcare can also get benefit from the deployment of blockchain with the use of smart contracts, those are written about raw material to finished product, delivery and payment details (Dagher et al., 2018). Another sensitive and most

important issue is drug counterfeiting (Mettler, 2016) in developing countries in which ingredients are not up to the mark or non-active ingredients. Drug counterfeiting can be eliminated if verification is performed by the blockchain network.

A research was conducted for anti-counterfeits products related to post supply chain (Toyoda, Mathiopoulos, Sasase, & Ohtsuki, 2017). Currently, RFID tags are implemented all over the world for checking the ownership of any product from the manufacturer to the end-user. However, RFID tags can be manipulated and cannot be guaranteed in the second-hand market. So, a new method of validating RFID tags by blockchain technology was proposed in which a customer can reject to buy a product if the seller is unable to provide ownership and this will be verified by blockchain network with proof of possession of product idea. Their results showed that the cost of managing the products using this idea is less than 1$, while the number of ownership transfers is not more than six.

Poor care and unnecessary hospitalization of patients also ultimately increase costs. Now the patient care system is evolving in which remote care and multi-staged treatment with health monitoring systems are there (Khan, Khan, Asif, Khalid, & Haq, 2019; Khan, Jamjoom, Ahmad, & Asif, 2020).

The interoperability of healthcare-related data is another challenge for medical practitioners in which different information technology systems can communicate, share, and use information. The feasibility of implementing interoperability is proposed by Zhang, White, Schmidt, and Lenz (2017). There are three types of interoperability (Zhang, Walker, White, Schmidt, & Lenz, 2017), like foundational, structural, and semantic interoperability. Foundational interoperability refers to data exchange among systems without requiring the ability of the receiving party to interpret data. Structural interoperability ensures whether received data is preserved and interoperable while semantics interoperability deals not only with the structure of data but also the meaning of data. According to researchers, first twos are prerequisites for the third one, and the third one is the hardest to implement on the blockchain.

Some researchers (Zhang, Xue, & Huang, 2016) had proposed techniques to manage computing power challenges of blockchain for pervasive social networks (PSN), which work with low power devices like sensors. It is infeasible to store healthcare on PSN devices, so they have divided their network into two security protocols, one for secure links for sensors and mobile devices and second for blockchain technique to share healthcare data among nodes.

4.1. Noteworthy contributions of blockchain in healthcare

In 2019 (Agbo, Mahmoud, & Eklund, 2019), published a review paper that is considered to be best because they conducted a systematic review about the research trend on blockchain specifically on healthcare areas for the years of 2016, 2017 and 2018. They used a systematic mapping process through which they have classified all articles published in these years. They explored four databases named PubMed, IEEE Xplore, Web of Science and Scopus. From these databases, they selected 42, 72, 37, and 53 as a total of 204 papers for analysis, respectively. After the analysis, the final selection was 65 articles. Among these selected 65 articles, 5, 28 and 32 were from the year 2016, 2017 and 2018 respectively. Moreover, 42, 14, 2, 4, 3 articles were from Journals, Conferences, workshops, symposiums and book chapters, respectively. They further analyze (shown in Fig. 9) the paper and reported that among these 65 articles 48 % of were related to EMR aka electronic medical records, 15 % were RPM aka remote patient monitoring, 11 % were biomedical research, 5 % from drug supply chain, 5 % data analytics, 2 % insurance claim, 11 % reviews and 3 % from others.

Precision medicine (Khan, Shaheen et al., 2019; Linn & Koo, 2016; Rabah, 2017; Tahir, Hassan, Asif, & Ahmad, 2019) is a new treatment option in which different treatment is performed on the same type of disease according to individual characterizes of patients, while clinical trial (Irving & Holden, 2016; Nugent, Upton, & Cimpoesu, 2016) is another research topic in which new drugs are evaluated after performing tests on a sample of patients. Research is proposed in Shae and Tsai (2017) in which a custom and advanced version of traditional blockchain were proposed. They have also embedded big data analytics and IoT for data analytics purposes and device management, respectively. Their prime focus was to decrease costs, which can be done after exploring and integrating many datasets of different diseases.

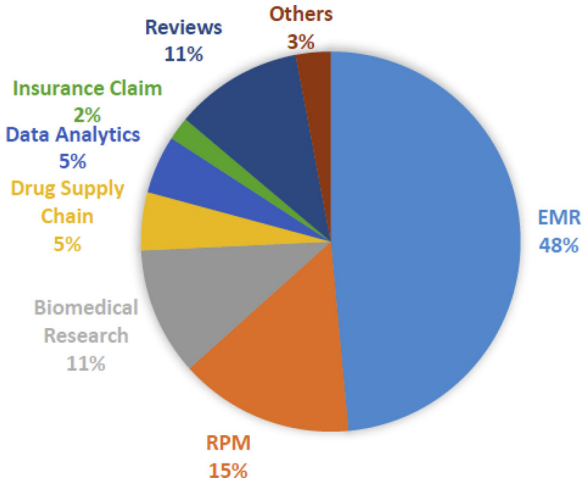

Fig. 9. Paper distributions according to the category of research (Agbo et al., 2019).

According to their model shown in Fig. 10, they will deploy a new distributed and parallel system with high bandwidth for big data analytics. Moreover, with the use of smart contracts and distributed ledger features of the blockchain, they will provide data integrity features plus the handling and integration of medical disparity data. The patient's identity issue will be addressed as well as the security of patient data, and data access will be in the control of that specific patient. Trust for sharing data will be accomplished by a secure data sharing features with the use of smart contracts.

A case study of cerebrovascular disease was taken, and a model was proposed for precision medicine treatment shown in Fig. 11. They have two goals, firstly to integrate disparity of medical data and secondly to devise distributed and parallel computing paradigm for data analytics.

They have integrated multiple datasets from different sources of patient data like two datasets from the hospital and insurance database and two datasets from medical questions and analytics databases. Data from biomedical research with the use of question/analytics method will be extracted with the use of national structure language, which will provide accuracy of answers to questions and analytics. The biomedical research database has near about 24 million research articles that will be analyzed.

They have also proposed a model for clinical trial shown in Fig. 12, in which they have set two goals here too. Peer verifiable data integrity with data access security and data sharing management like trust and collaboration. They will collect biomedical information data and will use the smart contract of blockchain to link and store data on the blockchain network. The new researcher can verify the correctness of data integrity. When trust is developed, then sharing will be occurred.

There is no HIPAA (Annas, 2003) equivalent Electronic Healthcare Record (EHR) in third world countries (Malik & Paton, 2008; Qureshi, Shah, Khan, Miankhel, & Nawaz, 2012), which ensures patient-centric privacy according to the willingness of patients. EHR plays a vital role in patient care quality, better and accurate healthcare intelligence, and minimizing operating costs.

However, the biggest challenge is how to gain, store, and analyze health data without disturbing the privacy feature. According to recent

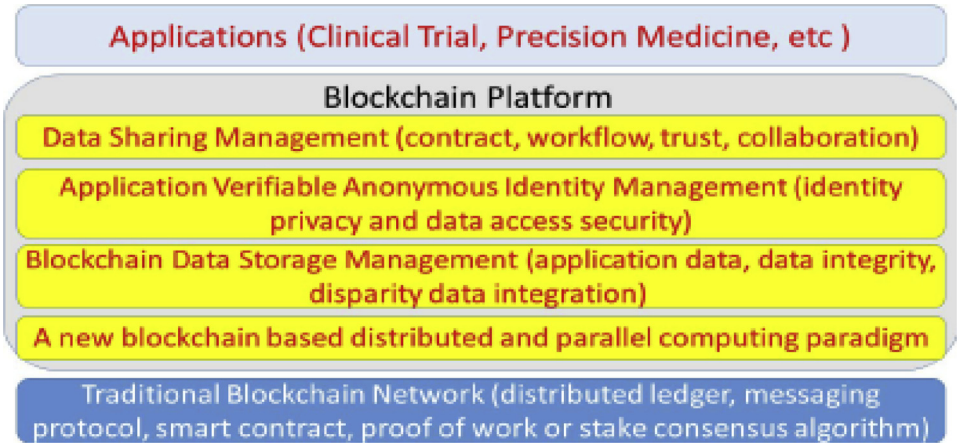

Fig. 10. Proposed layers applicable to traditional blockchain (Shae & Tsai, 2017).

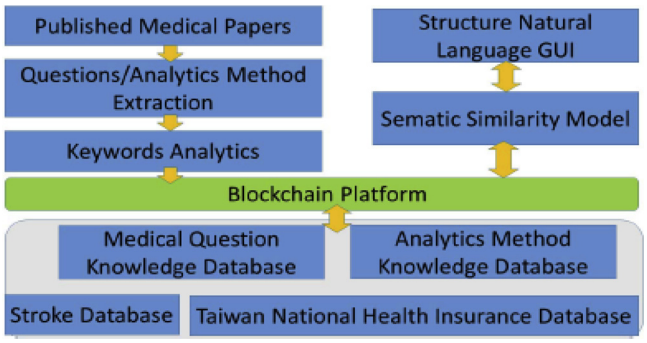

Fig. 11. Precision medicine workflow proposal for traditional blockchain (Shae & Tsai, 2017).

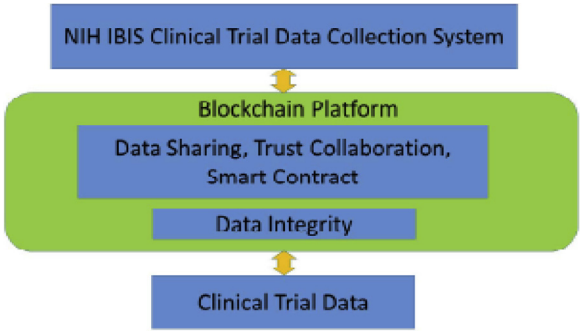

Fig. 12. Clinical trial workflow proposal for traditional blockchain (Shae & Tsai, 2017).

researches, there is a bundle of security breaches in patients' data that indulge them in psychological conditions. However, in developed countries, despite privacy concerns, patients give more importance for online access to their medical data.

The best option to safeguard patients' data against attacks and misuse is to put it to blockchain because third parties are no more reliable. Some authors (Yue, Wang, Jin, Li, & Jiang, 2016) have proposed a mobile app to control the sharing of EHR designed specifically for patients named Healthcare Data Gateway, aka HDG, which is a combination of a database and gateway. It provides storage of medical records, personalized access to patients, and allows multiparty processing on patients' healthcare data without compromising privacy.

They preferred to use a smartphone for their app because of the match of portability and computing power in the pocket as well as easy adoption because the app will be available on the web-store and will be installed instantly. And, more specifically, speedy cloud-based 5 G network facilities.

HDC is composed of three layers, shown in Fig. 13. The data storage layer is a secure and scalable service and has protection against integrity and confidentiality attacks. This is a private blockchain rather than public. Private blockchains are best elaborated in Pilkington (2015), Teutsch, Jain, and Saxena (2016) and Sharples and Domingue (2016). All features of the original blockchain are embedded here like cryptography, hashing, and signatures.

The data management layer has individual HDGs that are independent and interlinked with each other. It has a data access gateway which evaluates all incoming and outgoing data accesses. At the same time, the gateway performs another feature of database engine which manages all heterogeneous data about patients.

The data usage layer consists of entities that will be directly involved in HDG, like Physicians, researchers, Government, and others.

They have presented a case study that shows the working of their proposed system. John, a patient visits a physician named Bob. Now according to the willingness of Patient John, blood test-related data was authorized from John to physician Bob for a prescription. For this purpose, John will decrypt his blood data and encrypt it with a new key and forward it to Bob. Now Bob can see medical data replica, which is stored in Bob's HDG for one day on which Bob can perform operations according to the authorization granted by John. Actions performed by Bob will be forwarded back to John with blood test prescription.

Here the main challenge is to manage heterogeneous data like text, images. They used one simple table having all data of one patient, and attributes were "Time, Indicator, Type, Value, and Description." Time used for a certain value generation. The indicator shows that "what is the meaning of value." What was the type of value like text or image? Value shows the actual data value. Moreover, what was the category of an indicator like a blood test? Each patient has such type of table, and the patient identity was used for the table name.

According to their proposal, there will be two types of users, R-users, those who need to access raw and data, and P-users who will use raw to generate results. However, the problem is that, who will add data into the blockchain database initially.

Some authors (Griggs et al., 2018) proposed a new idea about the patient monitoring system, which works remotely and maybe executed automatically.

The architecture of their proposed system may be seen in Fig. 14 in which it is to be noted that on patients' body some sensors are installed that send raw sensor data in encrypted format to master device which is oracle based. Afterward master device forwards data to nodes those are participating in blockchain. On that particular blockchain smart contracts are deployed those are executed automatically.

They have also introduced a data analysis module as well as an acknowledgment system shown in Fig. 15. Analysis module obtains

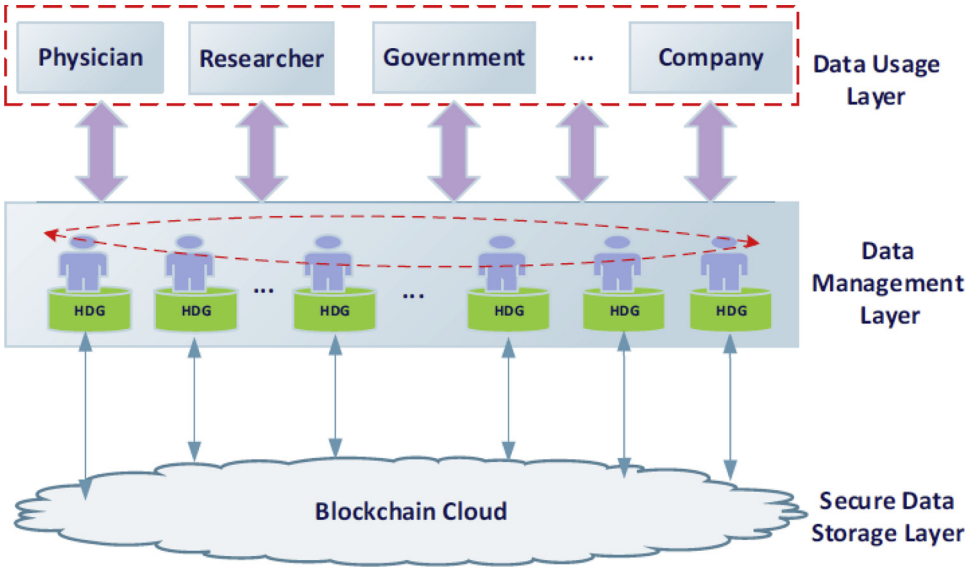

Fig. 13. Architecture of HDC layered system (Yue et al., 2016).

formatted data and forward relevant information to three entities. It firstly forward processed information to blockchain for the record. Secondly an alert is sent to the master device, and thirdly, an alert also forwarded to relevant hospital. A final alert is also forwarded to the relevant patients too.

Other authors (Khan et al., 2020) proposed different suggestions that patient will create the first version of his/her information record during his first visit which will then be loaded to blockchain and smart contracts will be deployed to verify the initial version because patients will only be able to create the initial version of information record.

Some researchers proposed an idea of electronic prescription (Seitz & Wickramasinghe, 2020) in which medical doctors not only prescribe medicine but also supervise medication processes remotely. By the use of IoT enabled devices, which can remind patients to take medicine and report to a medical doctor about patient behavior about overdosing as well as allowing or interrupting medicine dispensation according to payment confirmation from patient or insurance company. They have suggested using smart contracts to control the overall process.

5. Conclusion

The success of the blockchain network lies under the working mechanism called Proof-of-Work, and it is a security mechanism, which is a cryptographic puzzle. However, there are still possible threats like a 51 % attack that must be cured using other working styles like Proof-of-Stake and its custom variations proposed by different authors.

Improvement in Throughput of the blockchain network can be enhanced by using RAFT which allows more than 10k transactions, while for Latency issue, authors of Bitcoin-NG technique claimed that only propagation delay of the network would be suffered and concerning Size and Bandwidth problems, BigchainDB was proposed which allows more storage option. For the security of private keys, different wallets were proposed in which Paper wallets and Hardware wallets are more secure while web and desktop wallets are easy to use. To escape from wastage of computing resources like hardware and electricity costs can be eliminated by using Proof-of-Stake techniques. Forking is also a big challenge in Blockchain, which cannot be eliminated because improvement options never end.

There is no famous non-financial application implementation of blockchain like Bitcoin which is a financial application, but there are noteworthy contributions of blockchain in healthcare, like the application of precision medicine and a clinical trial using separate layers of blockchain consisting distributed and parallel computing paradigm, storage management, anonymous identity management, and data sharing management. Another contribution was the mobile app called Healthcare data gateway. It ensures storage of medical records, personalized access for patients, and permits multiparty processing on healthcare data without compromising privacy.

Author contributions

All the authors have equally contributed to all parts of the paper e.g. literature, study design and proofread.

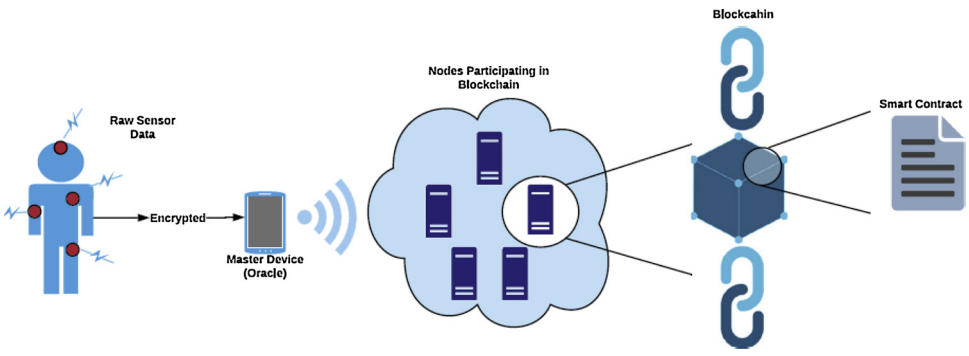

Fig. 14. Architecture of automated remote patient monitoring system (Griggs et al., 2018).

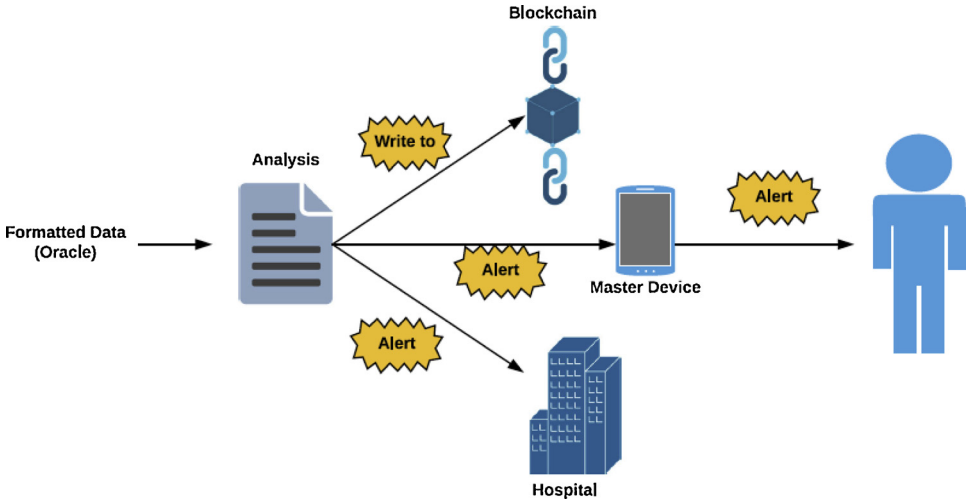

Fig. 15. Analysis mechanism of automated remote patient monitoring system (Griggs et al., 2018).

Declaration of Competing Interest

The authors declare no conflict of interest.

Acknowledgments

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

References

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). *Blockchain technology in healthcare: A systematic review. Healthcare*56.
Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2019). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society,* 101728.
Andresen, G. (2015). *BIP 101: Increase maximum block size.* Accessed June, 2016.
Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation Cardiovascular Quality and Outcomes, 10,* e003800.
Annas, G. J. (2003). HIPAA regulations-a new era of medical-record privacy? *The New England Journal of Medicine, 348*, 1486–1490.
Arora, R. U. (2018). Financial sector development and smart cities: The Indian case. *Sustainable Cities and Society, 42*, 52–58.
Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). *International conference on principles of security and trust,* 164–186.
Back, A. (2002). *Hashcash - a denial of service counter-measure.* Available:http://www.hashcash.org/papers/hashcash.pdf.
Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., et al. (2014). *Enabling blockchain innovations with pegged sidechains.* http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.
Bastiaan, M. (2015). *Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin.* Availab le athttp://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf.
Bitcoin Wallets (2018). *Bitcoin wallets for beginners: Everything you need to know.* 20 Feb, Available:https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin-wallets.
Bowden, R., Keeler, H., Krzesinski, A., & Taylor, P. (2018). *Block arrivals in the Bitcoin blockchain.* arXiv preprint arXiv:1801.07447.
Castro, M., & Liskov, B. (1999). *Practical Byzantine fault tolerance. OSDI*173–186.
Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303.
Coblenz, M. (2017). Obsidian: A safer Blockchain programming language. *2017 IEEE/ACM 39th international conference on software engineering companion (ICSE-C),* 97–99.
Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies, 32*, 1754–1797.
Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., et al. (2016). On scaling decentralized blockchains. *International conference on financial cryptography and data security,* 106–125.
Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297.
Daniel, J., Sargolzaei, A., Abdelghani, M., Sargolzaei, S., & Amaba, B. (2017). Blockchain technology, cognitive computing, and healthcare innovations. *Journal of Advances in Information Technology, 8*.
Decker, C., & Wattenhofer, R. (2015). *A fast and scalable payment network with bitcoin duplex micropayment channels. Symposium on self-stabilizing systems*3–18.
Dev, J. A. (2014). Bitcoin mining acceleration and performance quantification. *2014 IEEE 27th Canadian conference on electrical and computer engineering (CCECE),* 1–6.
Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A case study for blockchain in healthcare:"MedRec" prototype for electronic health records and medical research data. *Proceedings of IEEE Open & Big Data Conference*.
Ellis, J. (1992). Brute force: Allied strategy and tactics in the Second World War. *Naval War College Review, 45*, 126–127.
Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). *A first look at the usability of bitcoin key management.* arXiv preprint arXiv:1802.04351.
Eyal, I., & Sirer, E. G. (2014a). *How to disincentivize large bitcoin mining pools.* Blog posthttp://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools.
Eyal, I., & Sirer, E. G. (2014b). *Majority is not enough: Bitcoin mining is vulnerable. International conference on financial cryptography and data security*436–454.
Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-NG: A scalable blockchain protocol. *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation,* 45–59.
Fahmy, S. F. (2018). *Blockchain and its uses*.
Garzik, J. (2015a). Block size increase to 2MB. *Bitcoin Improvement Proposal, 102*.
Garzik, J. (2015b). *BIP 100: Making decentralized economic policy.* Accessed June, 2016.
Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security,* 3–16.
Göbel, J., & Krzesinski, A. (2017). Increased block size and Bitcoin blockchain dynamics. *Telecommunication networks and applications conference (ITNAC), 2017 27th international,* 1–6.
Goldfeder, S., Bonneau, J., Kroll, J., & Felten, E. (2014). *Securing bitcoin wallets via threshold signatures*.
Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems, 42*, 130.
Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*.
Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). *Eclipse attacks on bitcoin's peer-to-peer network. USENIX security symposium*129–144.
Houy, N. (2014). It will cost you nothing to" kill" a proof-of-stake crypto-currency. *Economics Bulletin, 34*, 1038–1044.
How to Store Your Bitcoin (2018). *How to store your bitcoin.* 20 Feb, Available:https://www.coindesk.com/information/how-to-store-your-bitcoins/.
Irving, G., & Holden, J. (2016). How blockchain-timestamped protocols could improve the trustworthiness of medical science. *F1000Research, 5*.
Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. *Proceedings of the 2012 ACM conference on computer and communications security,* 906–917.
Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). *Misbehavior in bitcoin: A study of double-spending and accountability. ACM transactions on information and system security (TISSEC), vol. 18*, 2.
Khan, F. A., Jamjoom, M., Ahmad, A., & Asif, M. (2020). *An analytic study of architecture, security, privacy, query processing, and performance evaluation of database-as-a-service. Transactions on emerging telecommunications technologies*.
Khan, F. A., Khan, M., Asif, M., Khalid, A., & Haq, I. U. (2019). Hybrid and multi-hop advanced zonal-stable election protocol for wireless sensor networks. *IEEE Access, 7*, 25334–25346.
Khan, F. A., Shaheen, S., Asif, M., Rahman, A. U., Imran, M., & Rehman, S. U. (2019). Towards reliable and trustful personal health record systems: A case of cloud-dew

architecture based provenance framework. *Journal of Ambient Intelligence and Humanized Computing,* 1–14.
Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. *Annual international cryptology conference,* 357–388.
Kim, N. H., Kang, S. M., & Hong, C. S. (2017). Mobile charger billing system using lightweight Blockchain. *Network operations and management symposium (APNOMS), 2017 19th Asia-Pacific,* 374–377.
King, S. N. S. (2012). *PPCoin: peer-to-peer crypto-currency with proof-of-stake.* Available:http://peercoin.net/assets/paper/peercoin-paper.pdf.
Koteska, B., Karafiloski, E., & Mishev, A. (2017). *Blockchain implementation quality challenges: A literature review. Sqamia*.
Lamport, L. (2001). *Paxos made simple. ACM sigact news*, *vol. 32*, 18–25.
Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., & Rosenschein, J. S. (2015). Bitcoin mining pools: A cooperative game theoretic analysis. *Proceedings of the 2015 international conference on autonomous agents and multiagent systems,* 919–927.
Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *IJ Netw. Security, 19*, 653–659.
Lin, J., Pipattanasomporn, M., & Rahman, S. (2019). Comparative analysis of blockchain-based smart contracts for solar electricity exchanges. *2019 IEEE power & energy society innovative smart grid technologies conference*.
Linn, L., & Koo, M. (2016). *Blockchain for health data and its potential use in health it and health care related research. ONC/NIST use of blockchain for healthcare and research workshop*. Gaithersburg, Maryland, United States: ONC/NIST.
Lombrozo, E., Lau, J., & Wuille, P. (2015). *BIP141: Segregated witness (consensus layer)*.
Ma, J., Gans, J. S., & Tourky, R. (2018). *Market structure in bitcoin mining.* National Bureau of Economic Research.
Malik, M., & Paton, C. (2008). Why is there is a lack of open source initiatives for electronic health record systems in Pakistan? *Journal of Health Informatics in Developing Countries, 2*.
McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., et al. (2016). *BigchainDB: A scalable blockchain database. White paper, BigChainDB*.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., et al. (2013). A fistful of bitcoins: Characterizing payments among men with no names. *Proceedings of the 2013 conference on internet measurement conference,* 127–140.
Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom),* 1–3.
Miller, P. (2016). *The cryptocurrency enigma. Digital forensics*. Elsevier1–25.
Min, X., Li, Q., Liu, L., & Cui, L. (2016). A permissioned blockchain framework for supporting instant transaction and dynamic block size. *Trustcom/BigDataSE/I SPA, 2016 IEEE,* 90–96.
Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC),* 2567–2572.
Morton, A. B., & Mareels, I. M. (2000). An efficient brute-force solution to the network reconfiguration problem. *IEEE Transactions on Power Delivery, 15*, 996–1000.
Moser, M., Bohme, R., & Breuker, D. (2013). *An inquiry into money laundering tools in the bitcoin ecosystem. eCrime researchers summit (eCRS), 2013*, 1–14.
Nakamoto, S. (2018). *Bitcoin: A peer-to-peer electronic cash system.* 21 January, Available:https://bitcoin.org/bitcoin.pdf.
Nath, I. (2016). Data exchange platform to fight insurance fraud on blockchain. *2016 IEEE 16th international conference on data mining workshops (ICDMW),* 821–825.
Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research, 5*.
Ongaro, D., & Ousterhout, J. K. (2014). In search of an understandable consensus algorithm. *USENIX annual technical conference,* 305–319.
Pilkington, M. (2015). *Blockchain technology: Principles and applications. Browser download this paper*.
Pillai, B., Muthukkumarasamy, V., & Biswas, K. (2020). *Challenges in designing a blockchain platform*.
Qureshi, Q. A., Shah, B., Khan, N., Miankhel, K., & Nawaz, A. (2012). Determining the users' willingness to adopt electronic health records (EHR) in developing countries. *Gomal University Journal of Research, 28*, 140–146.
Rabah, K. (2017). Challenges & opportunities for blockchain powered healthcare systems: A review. *Mara Research Journal of Medicine & Health Sciences, 1*, 45–52 ISSN 2523-5680.
Reynolds, J., Rezgui, Y., & Hippolyte, J.-L. (2017). Upscaling energy control from building to districts: Current limitations and future perspectives. *Sustainable Cities and Society, 35*, 816–829.
Rosenfeld, M. (2011). *Analysis of bitcoin pooled mining reward systems.* arXiv preprint arXiv:1112.4980.
Seitz, J., & Wickramasinghe, N. (2020). *Blockchain technology in e-health: The case of electronic prescriptions in Germany*.
Shae, Z., & Tsai, J. J. (2017). On the design of a blockchain platform for clinical trial and precision medicine. *2017 IEEE 37th international conference on distributed computing systems (ICDCS),* 1972–1980.
Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. *European conference on technology enhanced learning,* 490–496.
Sirer, E. G.u. (2018). *Thoughts on the DAO hack.* 21 Feb, Available:http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/.
Sohaib, O., Kang, K., & Miliszewska, I. (2019). Uncertainty avoidance and consumer cognitive innovativeness in E-commerce. *Journal of Global Information Management, 27*(2), 59–77.
Sohaib, O., Naderpour, M., Hussain, W., & Martinez, L. (2019). Cloud computing model selection for E-commerce enterprises using a new 2-tuple fuzzy linguistic decision-making method. *Computers & Industrial Engineering, 132*, 47–58.
Sohaib, O., Solanki, H., Dhaliwa, N., Hussain, W., & Asif, M. (2019). Integrating design thinking into extreme programming. *Journal of Ambient Intelligence and Humanized Computing, 10*(6), 2485–2492.
Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
Tahir, N., Hassan, A., Asif, M., & Ahmad, S. (2019). MCD: Mutually Connected Community Detection using clustering coefficient approach in social networks. March *2019 2nd International conference on communication, computing and digital systems (C-CODE)* (pp. 160–165).
Taylor, M. B. (2013). Bitcoin and the age of bespoke silicon. *Proceedings of the 2013 international conference on compilers, architectures and synthesis for embedded systems,* 16.
Teutsch, J., Jain, S., & Saxena, P. (2016). When cryptocurrencies mine their own business. *International conference on financial cryptography and data security,* 499–514.
Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). *A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE access*.
Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials, 18*, 2084–2123.
Types of Bitcoin Wallets (2018). *7 types of bitcoin wallets.* 20 Feb, Available:http://coinoutletatm.com/7-types-of-bitcoin-wallets/.
Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). *Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE transactions on systems, man, and cybernetics: Systems*.
Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016). Blockchain contract: Securing a blockchain applied to smart contracts. *2016 IEEE international conference on consumer electronics (ICCE),* 467–468.
Witchey, N. J. (2015). *Healthcare transaction validation via blockchain proof-of-work, systems and methods.* Google Patents.
Wohrer, M., & Zdun, U. (2018). Smart contracts: Security patterns in the ethereum ecosystem and solidity. *2018 International workshop on blockchain oriented software engineering (IWBOSE),* 2–8.
Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper, 151*, 1–32.
Wuille, P. (2015). *Block size following technological growth (bip 103)*.
Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation, 2*, 25.
Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., et al. (2016). The blockchain as a software connector. *2016 13th Working IEEE/IFIP conference on software architecture (WICSA),* 182–191.
Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PloS One, 11*, e0163477.
Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40*, 218.
Zhang, J., Xue, N., & Huang, X. (2016). A secure system for pervasive social network-based healthcare. *IEEE Access, 4*, 9239–9250.
Zhang, P., Walker, M., White, J., Schmidt, D. C., & Lenz, G. (2017). Metrics for assessing blockchain-based healthcare decentralized apps. *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom),* 1–4.
Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). *Applying software patterns to address interoperability in blockchain-based healthcare apps.* arXiv preprint arXiv:1706.03700.