



Securing Financial Systems with Block chain: A Comprehensive Review of Block chain and Cybersecurity Practices

Noman abid

American National University USA

nomanabid12345@gmail.com



Corresponding Author

Noman abid

nomanabid12345@gmail.com

Article History:

Submitted: 13-12-2024

Accepted: 13-12-2024

Published: 13-12-2024

Key words: Block chain antifraud systems, finance solutions, quantum strike, smart contracts, phishing, privacy problematic, quantum techniques, decentralized finances (DeFi), cryptographic algorithms, multi-signature acknowledgments, audits, identity management, compliance, KYC, AML, access rights, scalability, constant monitoring.

ABSTRACT

New and innovative block chain technology is becoming the key in enhancing the security, transparency and efficiency in the financial sector. However, as financial applications based on the block chain expand and improve, so do the block chain threats and safety concerns. This paper aims to discuss the aspects of the block chain security with reference to the financial system and its advantages and drawbacks. It embraces major risks like 51% attacks, smart contract exploits, phishing, and data privacy and security issues; new risks from quantum computing and Decentralized finance (DeFi) platforms. Best practices also outlined in the paper include the use of an industry-grade cryptographic algorithm, a robust multi-signature authentication technique, auditing of the block chain application at regular intervals, the adoption of secure, decentralized identity verification and management, as well as compliance with industry standards such as KYC and AML. It also underlines the need to establish effective access controls and to develop capability in scaling solutions and sustained monitoring. Lastly, it can be noted that the acquisition of block chain-based financial applications entails the use of a combination of measures to address existing and future risks. As these best practices are implemented and the threats advance, the financial institutions will be better placed to realize the full value of block chain technology while at the same time protecting the privacy and security of people's financial transactions.

Brilliance: Research of

Artificial Intelligence is licensed

under a Creative Commons

Attribution-Noncommercial 4.0

International (CC BY-NC 4.0).

INTRODUCTION

Block chain technology is one of the innovations that is rapidly growing and has found its way into the financial sector due to promoting high securities in the trading activities. Block chain, best known as a distributed database, provides opportunities of safe and unchangeable, but non-conventional, transactions. It has become versatile and is used in mostly every financial use case such as payments/remittances and smart contract and the decentralized finance (DeFi). However, with the advancements in block chain technology in the financial sector, the society has also been awoken to the real need for effective cybersecurity measures in the financial market to avoid compromise of fiduciary information. In simple terms block chain is a distributed database used to maintain a growing list of records, called blocks that are linked using cryptography across a network of computers that makes the records reasonably resistant to modification [1]. The blocks of a block chain consist of a list of transactions that are securely encoded and once a block is attached to the chain it cannot be changed without changing all the other blocks in the chain. The immutability feature makes the block chain to have received much attention in financial networks because, in such systems, trust is hugely valued.

In finance, block chain technology has been adopted to clear payment instructions, enhance accountability and minimize expenses. It enables financial institutions and commercial enterprises to make peer-to-peer transactions removing the problem of intermediaries and lengthy processes associated with banking systems. Furthermore, block chain attributes like openness and inalterability ensure that it should be employed for application like cross border payments and trade, as well as securities trade where transactions validation is sacrosanct. That is why, the financial sector is one of the most attractive objects for cybercriminals due to the large amount of information and important infrastructure [2]. Business and financial transaction risks, for example through hacking, data violation, phishing scams and fraud can be very disastrous to various banking firms, other customers and the general economy. These attacks do not only pose a problem to the consumer trust but also cause loss of cash and regulatory fines. Consequently, the protection of financial systems is





necessary for keeping their all-important stability, the privacy of users' information, and system integrity in general. Despite the fact that block chain has some inbuilt security features like cryptographic ciphering and decentralization, it cannot be shielded from cyber evils. Smart contracts at the core of the block chain-based financial systems, including the crypto currency exchange, decentralized applications (DApps), and DeFi can be still at risks of the following vulnerabilities: bugs into smart contracts; 51% attacks; and phishing attacks on the users and the developers. Therefore there is need to respond to cybersecurity threats and proactively look for ways of protecting block chain based financial systems. The purposes of this review article are to offer an analysis of block chain approaches to security in the financial industry, and to explore block chain's relationship to existing cybersecurity frameworks [3]. The primary objectives of this review are as follows: To discuss the basic concepts of security in block chain and how they Holds True for financial applications. To assess the various threats and risks as experienced on block chain based financial systems. In this case a cross-sectional study is done to explore the different security measures and precautions being used to secure financial systems enabled by block chain. To provide case evidence to address the question of how regulation and compliance issues get manifested in block chain security of financial products. As newer and more advanced forms of block chain security are continuously being developed and new forms of cybersecurity threats continue to be identified, it is also important to identify possible future directions that may need to be taken in covering block chain security. Thus, in solving these objectives, this article intends to give comprehensive and informative perspectives with concerns to current security in block chain technologies in the field of finance as well as the protective safeguards paramount for the ongoing progressive growth of the concept [4].

Learning about Block chain Security in Financial Applications

People have come to know block chain technology because of its potential to revolution the block chain industry in provision off secure, transparent and efficient systems for conducting financial transactions. When it comes to use in financial applications, the intricately built security model of block chain including decentralization, cryptographic hashing and immutability is far better than centralized structure. However, to comprehend how block chain reduces risk in the financial system, it is necessary to look at the fundamental of block chain, the security facets of block chain and the way the guaranteed facets are implemented on the financial systems. Block chain runs as a Distributed ledger technology also known as DLT in which a number of computers otherwise known as nodes contain copies of the ledger. This includes every transaction or other data entry within a series of blocks which form a linked list in the same chronological order. Every block actually has the hash code of the previous block and this makes the connection between them very secured and practically unalterable [5]. This process makes it unlikely for one entity to hijack the system making information highly transparent and extremely hard to fake.

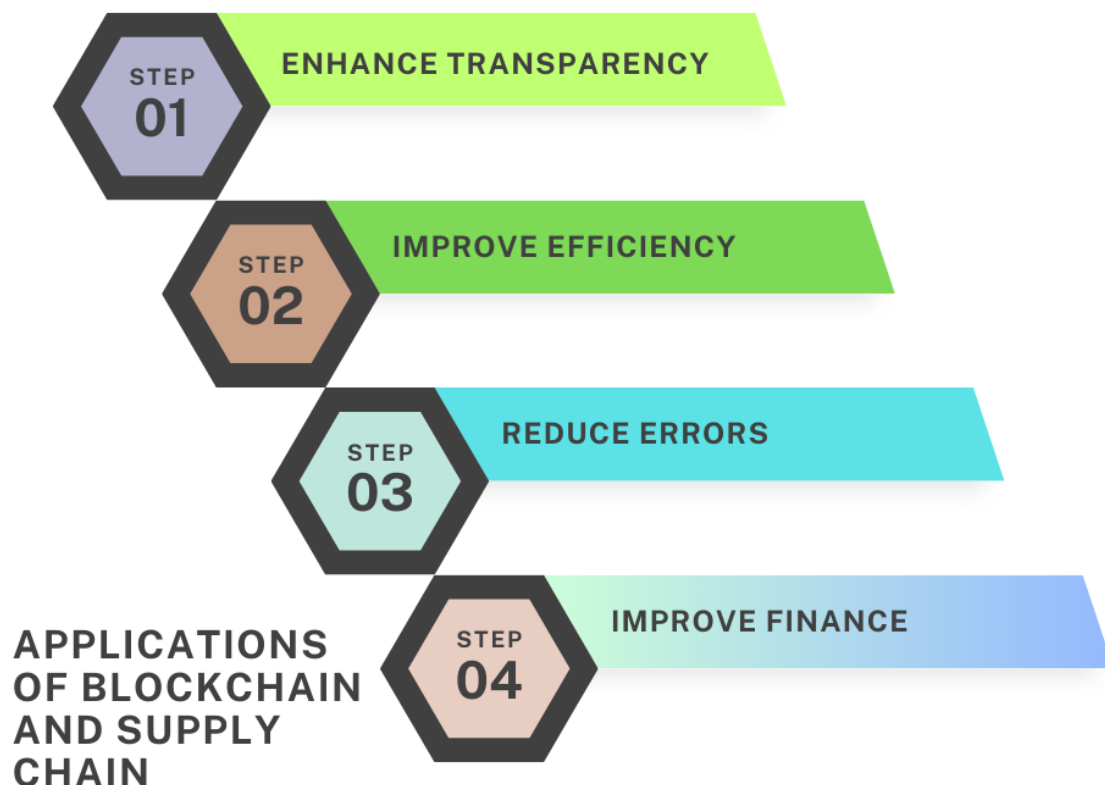


Figure: 1 showing applications of block chain and supply chain



An important characteristic of block chain is that it does not involve the use of third parties and especially no center that confirms transactions. However, the main concept in the process of creating and recording new transactions is the use of multiple nodes in the network that verifies the operations through consensus mechanism. The biggest concern measures include PoW and PoS, but DPoS and PBFT are gaining popularity as well. These mechanisms guarantee that before a transaction is included into the block chain all the players concerned with the transaction will attest to the truthfulness of the entries by responding in the appropriate hash value. The other important principle of block chain is that once a block has been added to the block chain it is irreversible. This feature holds extra security because to alter a previous transaction, would mean to change all subsequent blocks which becomes nearly impossible as more blocks are added to the chain. This means that once a financial transaction has been recorded into the block chain ledger, it cannot be manipulated or altered in anyway, which is compulsory for monetary systems which need reliable records [6].

Several key security features enable block chain technology to secure financial applications.

Cryptographic Hashing: In fact, according to the block chain definition, every block in the block chain contains a cryptographic hash that is developed based on the data part of the block and the hash value of the previous block. This hash give the opportunity to check whether the insertion or delete of additional data has occurred or not. The normal change of the figures, changes the hash completely; one could easily determine whether or not the data had been tampered with. It can, in a way, provide protection for data integrity and data authenticity simultaneously [7].

Public Key Infrastructure (PKI): The block chain systems use the public and private keys and these are extent remarkably similar to two keys. Each individual belonging to this network possesses what are known as the public key which is visible, and the private key which is hidden. When a participant acts, a transaction is signed with the participant's private key; other participants can verify the signature using the participant's public key [8]. It also ensure transaction's authenticity and no one can alter the content of the transactions.

Decentralization: Unlike having centred pulsating systems of working, this block chain system can never bring about a single point failure. In the given system each node is in fact, useless on its own, if one is corrupt or non-functional rest of the nodes are perfectly capable of delivering availability and reliability to the system. It also offers a strong solution to the issue of extending total control over the whole system to the domain of some or an antagonist who will seek to compromise the system.

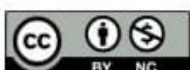
Consensus Mechanisms: Thus, consensus algorithms are inherent in the block chain securities. They ensure that all the members of the network exercise transactional legitimacy without receiving any approval from an authoritative body. For instance, Proof of Work (PoW), miners is supposed to solve some hard problems only to agree to the inclusion of a block in a chain; making the activities of fraudsters often non profitable. In proof of stake such participants use coins staking to put their support in validation of transactions and it is costly to attempt a malicious intention. Several papers elate the fact that the block chain technology is replacing traditional financial services since it offers them more security, transparency, and effectiveness than the previous techniques. In payments and money transfers, block chain causes real time, low cost, safe and cross border without banking and clearinghouse intermediaries [9]. For instance, while Bit coin and Ethereum uses block chain to facilitate peer to peer transactions that do not require any intermediation of a financial institution.

Other than use in payments, block chain has also adopted other application in other area of finance such as smart contract and decentralized finance (DeFi). Smart contracts are digital for which it enables particular business transaction to be implemented by applications whenever their terms are triggered every time pre-determined conditions are met. Smart contracts are most useful in their monetary applications when various trades and contracts like new, Insurance policies, and lending agreements are characterized by high computational and efficient values, and low probabilities of deception and human errors. Concerning decentralized markets, these rely on the block chain tech to offer services such as lending, borrowing and investing without proper involvement of banks [10]. The decentralization of these platforms utilizes block chain characteristic of security to make one of this certain transaction sacred and hence less vulnerable to counterparty risk thus the more trust in decentralized finance systems. However, even though block chain is highly secure when compared to conventional systems, block chain is not without issue when used. This problem happens in smart contracts, wallet and consensus mechanism to some extent. As block chain is used in more of the financial service, its issues in security will also be important to address to enable this technology to have more useful application.

The security of block chain is inherent to the fact that it is decentralized, cryptographed and irreversible. These characteristics make block chain a safe and sound environment for financial applications that is capable to produce faster, transparent and inseparable financial transactions. However, as with any kind of practice with the technologies, constant evaluation of security risks and development of new risks is essential to keep the block chain an active and ongoing part of the financial change process [11].

THREAT AND RISK OF BLOCK CHAIN FINANCIAL SYSTEMS TO CYBERSECURITY

Thanks to block chain technology, this promises financial applications, field-specific emphasis on security, transparency, and efficiency the field is fully exposed to cyber threats. High demand and growth of using block chain technology in financial segment turn this area into interest for attackers. To safeguard the structures of block chain based monetary systems it becomes crucial to identify what sort of threats are capable of occurring and how they can pose threat to the integrity of the monetary data, assets and transactions. The financial platforms and systems have always been most at risk





when it comes to cyber threats by virtue of the functions which include valuable content, information and support frameworks [12]. Traditional systems which employ a block chain financial system are more secure as compared to the normal systems but there are different types of risks. Some of the most common cybersecurity threats in block chain-based financial systems include:

51% Attacks: This means that an empowering node or a number of nodes gains over 50% of the computational resources in the block chain network in the systems of Proof of Work or gains the majority of the assets staked in the Proof of Stake systems is called a 51% attack. This control allow attacker to spend or fake coins, drop or authors ate a transaction, reverse a transaction and this mostly depicts the network insecurity [13]. With some more probabilistic consideration an attack of 51% is feasible even on 'weaker' block chains although more practically dangerous risks for block chain based monetary applications.

Double-Spending: Transaction forgery is a challenge in block chain networks because of the corrosion where one person tries to spend the same electronic currency more than any other time. Yet, double spending is relatively prevalent in low-security or underdeveloped block chain consensus mechanisms, and block chain consensus mechanisms have worked to prevent it. The implication here is that attackers can force the network to approve some transaction and the money of individuals involved will be lost [14].

Smart Contract Vulnerabilities: Smart contracts are contracts under which the terms of the contract are written in such a way that they enter into operation to perform the contract's conditions as soon as they are met. Thus, although smart contract are the optimal tools to fulfill financial transactions, there are still vulnerable aspects in coding [15]. Due to poor written code the hackers, exploits or other unwanted behaviors are there which are unpublished in the program example are hacks done on ethereum on looting around million ethers.

Phishing Attacks: Phishing involves tricking the users into passing their secrets such as keys and passwords to a phisher. In the block chain based financial systems, phishing attacks are successful more often because attackers may try to steal the users' private keys or access the user's wallet to perform unauthorized transactions. Given that block chain transactions cannot be rolled back common phishing attacks result to massive losses [16].

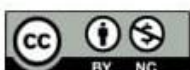
Malware and Ransom ware: New types of threats, including malware and ransom ware are known to present threats to block chain users and financial institutions. For instance, ransom ware can be used to lock a victim out of a few important block chain based systems or data until they pay the demanded ransom. The second approach is associated with a penetration of block chain networks with the use of malware; for instance, a thief steals the digital currency or increases the proportion of the smart contracts' shares fake. In addition to the above cybersecurity threats, block chain-based financial systems face several specific vulnerabilities, some of which stem from the inherent nature of the technology itself:

Weaknesses in Wallet Security: Private keys that grant access to block chain assets are being stored in pocket devices. Fundamental and simplest types of wallet security presupposes that if a wallet has been compromised, an attacker may steal all the contents of the wallet. Currently wallets are behaving insecurely for example a weak password, insufficient encryption or susceptibility to malware attacks pose a major threat to the block chain based financial systems through wallet grabbing [17]. In addition, the private keys so used by the users are also lost, and the users lose their funds and there is no way that the funds can be recovered.

Sybil Attacks: The type that is carried out when an individual deploys many fake identity accounts or nodes in a block chain network consensus. This leads to ill-intent such as the power to halt transactions, to override the conventional block chain narrative, or to manipulate voting procedures in DApps or the operations of DAOs. Such a possibility exists in the less developed as well as the less secure block chain system; nevertheless, Sybil attacks are fairly evident in fully realized block chains and are rare [18].

Consensus Mechanism Limitations: Due to the existence of various block chain networks, there is always various consensus mechanism used because of efficiency. However, PoW, and especially the further evolution of PoS, are also in some ways sensitive to certain types of attacks. For example, PoW networks require immense computational influence which is not safe from coordinated attacks by a set of entities with a lot of influence in computation. For instance, the energy efficiency of POoS can be perceived while the design might sometimes make it prone to Controlled Staking Token owners attacks [19].

Bugs in Block chain Software: Like any other program, block chain protocols and the applications coming after them are not shielded from bugs and real programming errors. These are called defects which impacting on the application's flow and to which they can bring, for example, a transaction failure, security loophole or an opportunity for an attacker. The imperfection in each block chain network requires a frequent update program, security audit, and test exercise.



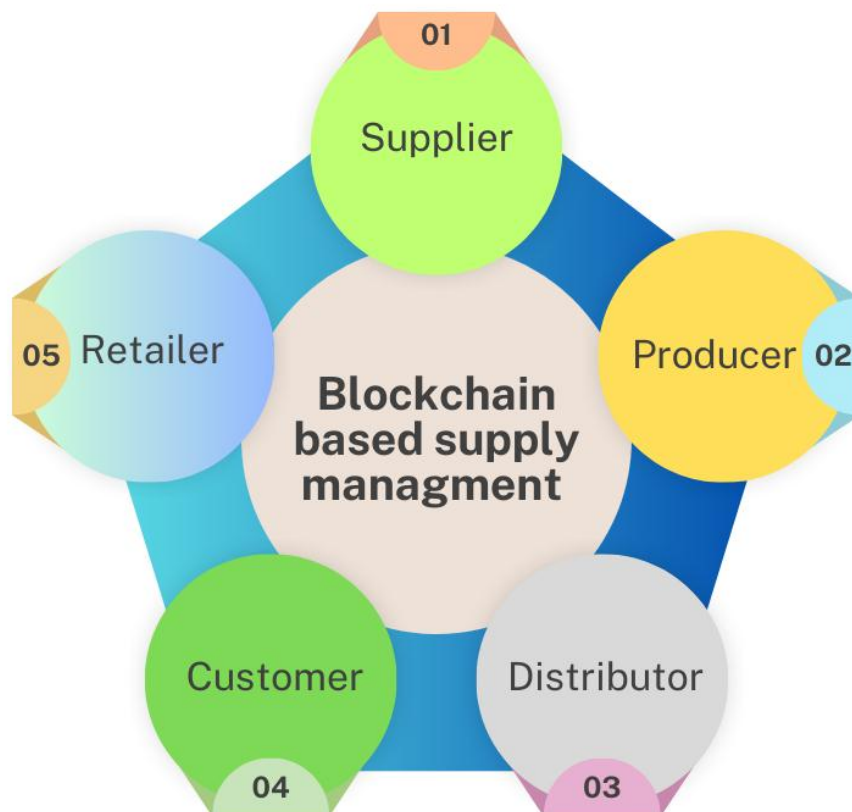


Figure: 2 showing block chain based supply management

Some of the specific examples are given below which show that many dangerous risks are associated with block chain based financial systems. Many high profile cases have unveiled these risks in the modern world. The most famous example is the attack on the «DAO» in the year 2016 when the hackers found it possible to penetrate the smart contract which was in charge of transferring close to \$60 million worth of Ether, only for them to cart the money away. This attack forced the Ethereum block chain to implement a hard fork to rescue the affected crypto currency, and questions were raised involving manipulation of block chain data and forecast of the roles of governances to protect block chain's integrity [20]. For instance the act of cyber theft that occurred at Mt Gox digital exchange in the year 2014 whereby hackers disappeared about 850000 Bit coins from the digital exchange and thereafter making a very strong case on the dangers that are associated with the use of centralised exchange and wallets. Despite the fact that the Mt. Gox hack was not strictly speaking an attack on block chain engineering per se, it paints a picture of the need to guard the frame works of block chain networks. With financial systems changing to block chain based systems they are more secure than centralised systems but not immune to cyber criminals. The attacks are; 51%, attacks, double spending, smart contract hacking, phishing among other attacks can affect the integrity of Block chain networks. Additionally, specific risks such as insecure wallets, Sybils, and interface compatibility issues need to be managed to protect block chain based financial products. Further investigation coupled with constant interest from the investors will be necessary to achieve a better shielded block chain technology that shall become standard in the finance market and its related business [21].

PROTECTION PRINCIPLES FOR FINANCIAL COMPANIES BASED ON BLOCK CHAIN

The block chain, however, as an intrinsic technology solution for financial systems, also employs sundry protection mechanisms to safeguard and secure transactions and prevent fraud. These mechanisms are crucial especially in the protection of block chain networks especially in environments where the financial application is in play in which issues of trust, integrity and confidentiality of data is very crucial. This section will discuss the basic security measures found in block chain financial systems including cryptographic securities, consensus securities and smart contract securities. Cryptography remains the leading security feature that supports block chain technology. It makes the transaction secure, transparent and less capable of being counterfeit because the data cannot be tampered with [21]. There are several cryptographic techniques used in block chain networks that are critical for securing financial applications:

Hashing: Every block in a block chain has the hash of the previous block and therefore forms a very secure chain. It is, for instance, the SHA-256 hash function used in Bitcoin mining: the hash function maps the block's data to a string of characters of the same length. Just changing a single word in the content of the block will change the hash value and



hence prevent anyone from tampering with the blocks [22]. Hashing warrants the block chain to remain unaltered and minimizes any alteration by an unauthorized individual.

Public Key Cryptography (Asymmetric Encryption): Today's block chain systems employ public key encryption to facilitate secure purchase transactions. Every participant has an open and secret key pair. Whereas the public key is available to the public the private key remains a secret of its owner. When a user invokes a transaction, it is executed and then signed with his or her private key, the result of which can be checked by anyone with the related public key. This make transaction authentication possible and also protect it in a way that the details cannot be changed once made confirmed [23].

Digital Signatures: In block chain, digital signatures are used to ensure that the transactions being made are genuine. For instance, a user would use their private key to sign of a transaction and the result is a unique signature. The signature can then be checked with published key of the sender and ensure that the transaction was commenced by the rightful owner of such assets [24]. This offer security and ensure that the transaction cannot be denied by the receiver once they had signed it.

Zero-Knowledge Proofs (ZKPs): A method of communication scenario that allows one person to prove to another that he/she knows a certain value but can't reveal what it is. ZKPs are becoming more incorporated in block chain applications in order to increase privacy especially in financial applications. For example, when using ZKPs, a user can show that he/she/it has enough coins to pay for a transaction without revealing either the amount of coins or information about the assets. The consensus mechanism is critical forursor block chain networks to be secure and functional [25]. Are the rules that define how transactions are verified and then integrated into a block of the block chain? Different consensus mechanisms have varying implications for security in financial systems:

Proof of Work (PoW): PoW is defined as consensus mechanism that is applied by bitcoin and many other block chain networks. It involves confirmation of transactions by the use of mathematics problems by some of its users known as miners. Doing this takes time and a lot of computation; it is expensive for an attacker to change transaction data. In general, PoW is very safe or just as safe as the platform implementing it; nonetheless, it is unbearing and hoggish when it comes to power consumption [26].

Proof of Stake (PoS): PoS is another form of consensus that chooses the validators by the tokens they own and are ready to use as security. It should be noted that in PoS, validators are incentivized with the possibility of creating new valid blocks within the chain and are penalized if they attempt to do otherwise. PoS is less energy-intensive than PoW and is adopted by a novel Ethereum 2.0 [27]. However, it may be exposed to attacks from those with almost complete control over at least a portion of the tokens which are staked.

Delegated Proof of Stake (DPoS): DPoS is similar to PoS where a few selected persons with stake holders voting them, act as the validators of the transactions. This mechanism is also relatively faster, scalable than PoW and PoS though the decentralization aspect might seem to be compromised. For the use in financial applications, DPoS might provide faster confirmation times but it's security is based on the selected list of nodes.

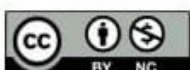
Practical Byzantine Fault Tolerance (PBFT): PBFT is consensus algorithm that has been designed to work when a number of nodes in the network are Byzantine or are simply faulty. This is especially appropriate in use cases that are on permissioned block chain that is used by participants who are well-known to each other. PBFT guarantees that the secure consensus in the network is realized if less than one-third of the nodes are ill-motivated [28]. PBFT is widely used in the enterprise block chain solutions such as the financial system involving high throughput with low latency. Smart contracts are automated block chain-based transactions created by writing the code for the contract into the program. Smart contracts automatically execute transactions in block chain based financial systems when comparing efficiency, transparency and resistance to tampering. Nonetheless, these smart contracts themselves contain their own level of security risks.

Vulnerabilities in Smart Contract Code: As is evident, when smart contract code is not well written, it is vulnerable to attack from attackers. Situations when the contract might be attacked by a reentrancy attack, integer overflow, or uncontrolled external calls may lead to large money losses. For instance, the attack on the famous DAO on the Ethereum block chian was due to vulnerability by reentrancy in the smart contract code where attackers got away with millions of dollars from Ether [29].

Auditing and Formal Verification: To reduce risks attached to smart contracts it is important to review the code as well as perform a formal review as well. The cause of the code audits is to reveal weaknesses in code for smart contracts by the time they are deployed onto the platform by specialists in the field. Smart contract verification employs the proving system to ensure that a distributed application performs as required and that its code is safe.

Upgradability and Governance: Smart contracts, once deployed, are also essentially static – this means that if there was a mistake or a weakness in the code then that cannot be patched up in the future. There are some block chain networks that have put into practice techniques for modifying or enhancing smart contracts, which includes proxy contacts where the authorized parties can enhance the contract code with the help of specified proxies which are secure, transparent and multi-signature system within a network that permits the agreed parties to change the smart contract code without any threat of intrusion [30].

Oracles and External Data Feeds: Most of the financial applications like DeFi require form external data feeds,





commonly called oracles to instigate smart contract executions. But all the same, if the oracle is corrupted or produces erroneous information it results in security risks such as fraudulent dealings or alteration of financial details. Security of oracles and their data feed is one of the essential issues affecting the smart contract-based financial applications. The security measures of implementing the block chain in financial systems involve preventing cyber threats. Hashing or digital signatures, use of public key and private key in block chain transactions are among the most important cryptographic methods used in block chain [31]. Proof of Work, Proof of Stake and Byzantine Fault Tolerance all work to guarantee that the network reaches consensus safely, without the control of a single hub. In financial applications smart contracts are automating a lot of functions but the users should remember that the smart contracts need to be well written, audited and updated due to security reasons as hackers can attack easily. With the growing use of block chain in the financial sector, it will be crucial to have enhanced security features enabling the continuances success of block chain based financial systems.

THE ROLE AND IMPACT OF BLOCK CHAIN ON FINANCIAL SECURITY

While the block chain is still changing the financial industry, its application is not only introducing unprecedented technical issues but also litany of regulatory and compliance concerns. Lenders are operating in a context defined by standards, laws and regulations of the traditional finance and those of the block chain based finance. Due to the nature of block chain and its potential to undermine financial intermediary's regulation agencies are now developing rules that will govern the block chain while aiming to protect customers and financial stability and combat money laundering. This section analyses the major concerns with regard to the regulatory and compliance issues affecting block chain based financial systems [32].

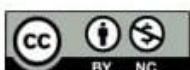
Jurisdictional Issues: A common condition regulating block chain in the financial sector is its cross-border and global character, which constitutes one of the main problems of its regulation. Due to the decentralized nature of the block chain networks it can be seen that it is bounded by no particular country or laws hence juridical problems can arise. A block chain deal can comprise of participants from different legal systems and this makes each of them applicable to that particular deal. This creates problems in issues like taxation impunity, and this affects issues to do with legal bearing, contract, and enforcement of the same [33]. There are questions as to how laws and regulations that will govern the block chain transactions can be implemented especially in cross border transactions this may call for Parliamentary and or making international policies.

Anti-Money Laundering (AML) and Know Your Customer (KYC) Compliance: However, because block chain is pseudonymous, regulators have more reservations: money laundering and terrorist financing. Any financial institution which uses block chain technology must adhere to high standards of AML / KYC checks in order to ascertain the identity of participants and check transactions for any related illicit activities. Authorities expect financial institutions to make all block chain transactions legal, which usually entails identifying and verifying users and scrutinizing their transactions for crimes such as money laundering and fraud [34]. Nevertheless, the use of anonymous digital wallets contained within block chain networks as well as the use of crypto currencies pose a challenge to KYC/AML.

Data Privacy and Protection: The onshore FA regulations multiply the data protection rules that govern the handling of the personal information, for instance; the EU's General Data Protection Regulation for financial institutions. Where block chain has a problem regarding these privacy laws is in the impossibility, once data is recorded on the block chain, of changing the data in any way [35]. The lack of detail erasure option poses issues about data rights as well as privacy from those who need to apply and the right to be forgotten such as GDPR. Since block chain solutions will be implemented in the financial sector, these solutions have to be developed with these challenges in mind, taking into consideration privacy regulations.

Securities Regulation: Crypto currencies and tokenized assets that essentially represent financial products based on a block chain classification are quite in a legal no man's land in as far as their nature under securities law is concerned. Legal authorities such as the U.S Securities and Exchange Commission (SEC) have offered guidelines under which some crypto currencies are classified as securities, given how they will be governed. ICO or STO is a common practice by tokens and is usually in question with regard to whether it is a security and if it is, does it have to adhere to relevant securities laws [36]. The question arises on which block chain assets are regarded as securities and how this subjecting can be done. This is due to the fact that clarity in the regulation of this area will help the financial institution to understand areas that block chain based financial services providers violated the law.

Smart Contract Legality and Enforceability: Terms traditionally found in smart contracts such as; 'code is the investment contract', 'Terms are self-executing', and 'Performance is automatic' cast some legal doubt on the concept. Smart contracts thus have been developed to be autonomous in executing the agreed terms, but most legal systems in different countries use traditional law to enforce compliance to the agreed terms. Target auditors decide whether and how the regulation of smart contracts fits into contract law, and if adjustments require codification to enforce smart contracts. Furthermore, the novelty and innovation of smart contracts coupled with the direct dealings with the customer lead to questions in relation to how courts and intermediaries would handle disputes resulting from smart contract based financial transactions [37].



THE APPROACH OF THE REGULATORS TOWARDS BLOCK CHAIN AND FINANCIAL SERVICES

Different countries and jurisdictions have taken varying approaches to regulate block chain technology in financial services, ranging from cautious to proactive frameworks:

The European Union (EU): The EU has been quite busy in working towards coming up with a regulatory framework for block chain and crypto currencies. Next year, European Commission introduced the Digital Finance Package that consists of the so-called Markets in Crypto-Assets Regulation (MiCA), aiming to create legal certainty for crypto currencies, stable coins, and other tokens based on the block chain. The MiCA seeks to establish a consistent legal framework with which a block chain based financial services without a violation of the laws of the European Union as well as safeguard the interest of the investor and consumer. In this regard, GDPR of the EU also applies strict regulation for data privacy to block chain solutions, in particular to consideration of individual data.

United States: As with most innovative technologies, the legal frameworks governing block chain-based financial services in the United States are shared between federal and state agencies. For determination on whether a particular crypto currency or token is a security that is legally traded the Securities and Exchange Commission (SEC) has some guidance [38]. CFTC regulates block chain based derivatives markets while FinCEN enforces AML and KYC norms for crypto currency exchange and other block chain based financial platforms. As a result, the regulatory framework in the USA is rather unsynchronized – each state, for example New York introduced its own rules, known as the Bit License, which controls the crypto currency businesses operating in this state.

China: In specifically China has gone very tough on block chain and crypto currency where the government has unleashed a series of crackdowns on crypto currency mining as well as trading. However, China has also advanced in establishing the central bank's digital assets, also referred to as the Digital Yuan, to accelerate the integration of block chain technology into the country's established financial structure while preserving strict government supervision. The two countries' approaches to block chain regulation are quite different from each other with China seeking to regulate the movement of digital assets while seeking government endorsed centralized solutions [39].

Other Jurisdictions: Switzerland and Singapore are among the nations that have embraced much more conducive conditions regarding block chain technologies. For instance, the Swiss countryside of Zug has transformed into Crypto Valley owing to the government's clear legal requirements and tax benefits for block chain business startups. Singapore has set a pace in block chain regulation with the MAS providing legal guidance to the required crypto currencies and block chain-based financial services [40]. While regulatory frameworks for block chain are evolving, several challenges remain in the practical implementation of compliance measures:

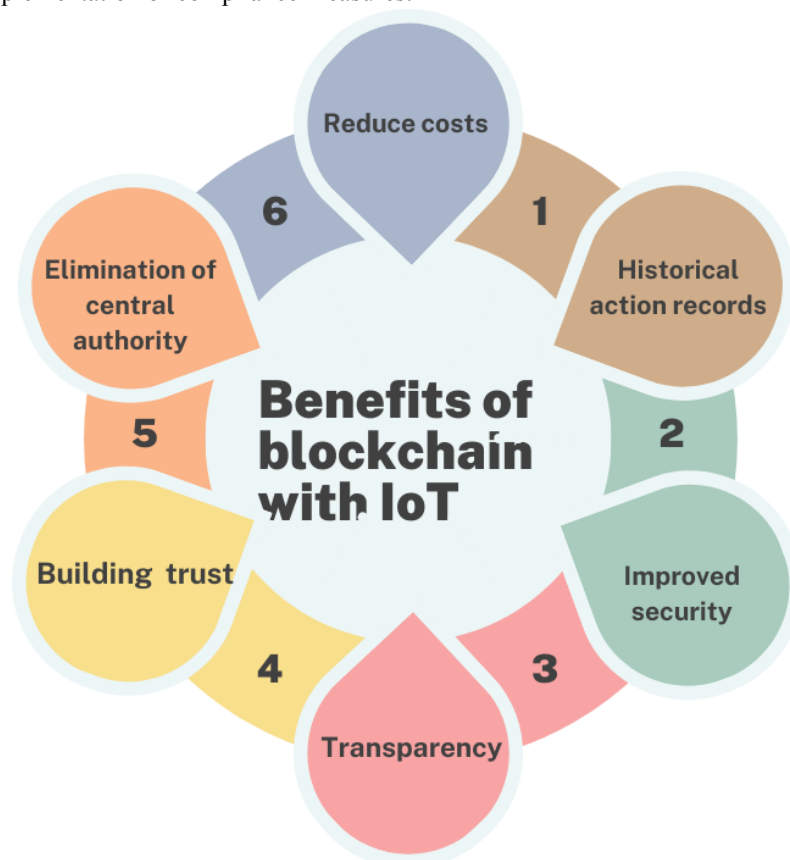


Figure: 3 showing benefits of block chain



Global Coordination: Due to the global interconnectedness of block chain networks, the task of achieving global consensus on the right regs is complicated. Lack of cooperation also results in confusion or conflict once block chain based financial services achieve cross border operations due to varying laws and regulations in countries. Although the regulation of banking services necessarily involves the cooperation of the regulators of various nations, this project is challenging due to the differences in legal systems that are put in place as a basis for regulating the institutions in various countries [41].

Rapid Technological Change: It is common to find that growth is outracing the formulation of more effective regulations in the area as manifested by the current block chain technology. Since the development of various new block chain based financial products like decentralized finance (DeFi) platforms and tokenized assets, regulators require consistent transformation.

Regulatory Overreach vs. Innovation: Regulating and encouraging innovativeness at the same time is always a problem. Huge and small regulations could end up hampering development of new sector and block chain based financial services and credit, but inadequate regulations would mean that customers expose their selves to high risks of fraud and financial insecurity. Companies also need to abide by the provisions of the law but at the same time be able to come up with pro grammes and services that will meet the competition factor. Blockchain technology is one of the most promising technologies that can enable radical changes to the processes taking place in the financial sectors of various countries; at the same time, this technology brings countless questions related to regulation and compliance [42]. Banking and other services involving block chain as well face legal issues covering regulatory requirements for AML/KYC, data protection, securities laws, and standby enforcement of smart contracts. However, m collaboration and especially clear regulations regarding block chain remain a work in progress in many jurisdictions. Increasing block chain deployment would require that regulators, finance industries, and block chain firms continue working together and in harmony to enhance block chain-based financial services implementation spaces that are secure, compliant, and evolutionary [43].

Contemporary Risks and Opportunities in the Protection of Block chain for Financial Frameworks

Despite good visibility and the opportunities that block chain technology presents in the fields of security, transparency, and decentralization, it is not impervious to a number of novel threats and challenges. That is why, the closer financial systems are associated with block chain, the more they need to adapt security measures to the changes taking place in this sphere. This section focus on the new security threats facing block chain in financial systems and the challenges organizations face to sustain block chain based business financial applications reliability and credibility. A 51% attack is a situation where one or many parties attain control for over 50% of the hashing power in a PoW network or the voting power in a PoS network. In such attack, the attacker can influence the block chain, regarding transaction history by spending the same digital coins more than once or prevent fresh transactions from being verified [44].

Global blockchain market BFSI market USD-BILLION

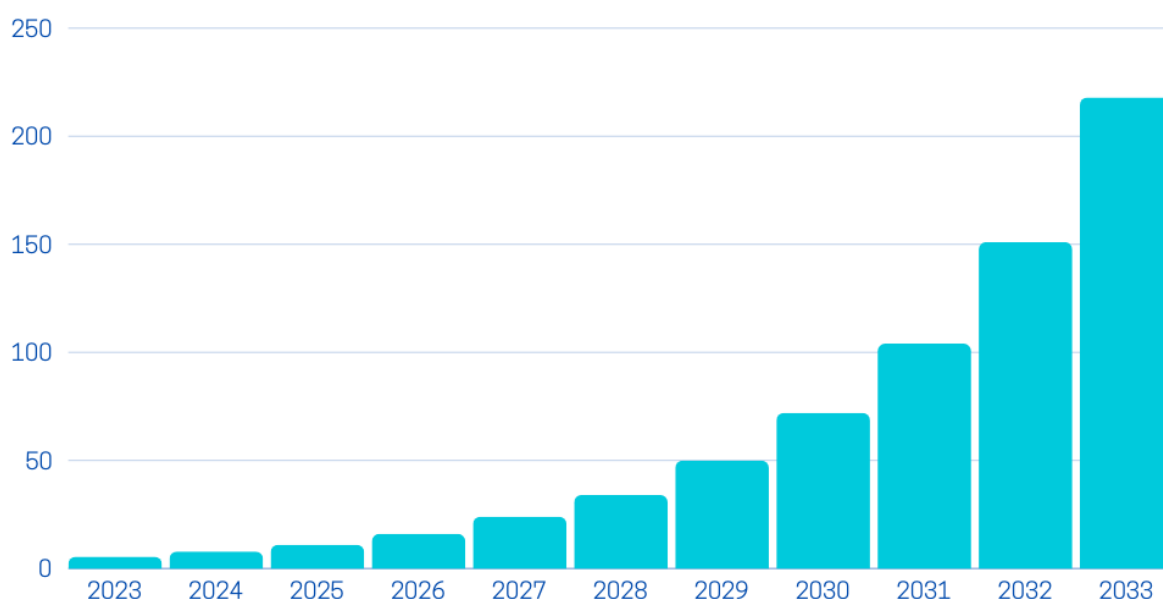
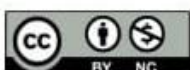


Figure: 4 showing block chain market BFSI market





While 51% attacks are mostly related to smaller block chain networks, they are still an issue, especially where financial applications are concerned, with percentages similar to some of the largest networks and 12 percent more attacks on financial application block chains with an average of 74 percent. In this sense, its successful realization can lead to huge financial losses, disruption of trading platforms, and consequently, to the damage of block chain-based financial systems' credibility. The financial institutions are required to confirm that the block chain networks with which they deal possess adequate decentralization and security to counter such attacks. Smart contracts are digital contracts where the operations of the contract are coded in lines of computer code [45]. As they are efficient and can be automated, they also present the risks that are related to this kind of approaches. Some common vulnerabilities in smart contracts include:

Reentrancy Attacks: Smart contracts may be hacked by calling extrinsic functions at the moment before the first function being called is finished, which results in unpredictable actions.

Integer Overflow/Underflow: Some smart contracts do not assert the numerical input and thus result in overflows or underflows, which have adverse financial impacts.

Access Control Issues: Weak controls over access lead to unauthorized users performing certain banned features or even embezzling money.

These are the weaknesses that can be utilized to assume control over decentralized financial potential customers or to organize embezzle from DeFi. Such possibilities require constant auditing and formal verification to be revealed and addressed in order to provide smart contract protection and reliability. Phishing and social engineering are the most practices used by hackers in order to get away the private keys or login details through which attackers can get access to the individual and company block chain wallets or any financial account [46]. According to the definition of block chain, phishing can involve fake websites or fake messages with the appearance of a genuine crypto currency exchange, wallet service provider, and block chain service. Wrongdoers can also infiltrate financial institutions indirectly through exploiting the targets or the employees through a pretexting attack with the use of cloned phone numbers and knowledgeable voice modulation. Most of these are not knocks on the technological structure and tend to mostly cause financial losses due to other human element vulnerabilities. The banks and other parties involved in using the block chain must uphold strong security measures and enhanced multi-factor security to prevent such attacks.

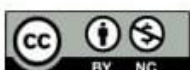
A Sybil attack is a crime where an individual forms multiple fake identities with the intention of controlling a block chain network's consensus process. In the block chain networks that have adopted the reputation system or the voting based consensus protocols, an attacker can bring many fake nodes to the network and control flow of decision making in the network. Sybil attacks are specifically dangerous to permission less block chain networks since anyone can join in. In the context of the fs, Sybil attacks can distort the prevalence and application of fs technology within DA, distort the function and effectiveness of self-governance processes, or threaten the security of consensus processes [47]. Some preventative measures about Sybil attack include the following, Identity verification systems, reward systems that encourage honest nodes participation.

Although providing high levels of transparency and traceability, the block chain may also raise privacy issues when it comes to such a sensitive financial data. Information on a public block chain is easily accessible for all the members of the network and due to this finances transaction may include or including the wallet balances [48]. Although these addresses can be somewhat anonymous, they can be linked back to specific real life individuals using data mining methods. In the select financial applications specifically in crypto currency exchanges or in decentralized finance platforms, leakage of such information poses high risk in terms of users' privacy and may contravene data protection laws. The remedies to such issues as privacy are in Dev such as zero knowledge prove (ZKP), where parties share proofs concerning some facts without disclosing the truth about the content. However, the general usage can be intricate, and the value of disclosure still poses a question.

One of the largest issues of block chain networks is their scalability, especially when used as the foundation of financial systems that demand high TPS and low output latency. Many conventional block chain networks such as the Bit coin and Ethereum encounter a bottleneck through use, and the entire block chain network becomes congested through heavy usage, thus paving a way for the slow processing of many transactions and increased fees charged. Such delays can be an issue in financial systems because real-time operation of financial transactions is expected [49].

To this end, different solutions are being implemented to solve scaling issues that include layer two scaling solutions, lightening network for the Bit coin and rollups for the Ethereum. Such solutions seek to optimize TPS while ensuring that no cores of sacrosanct principles of the blockchain such as security and decentralization are violated. However, maintaining scalability continues to be a work in progress, and the best of both worlds approach – optimal performance and security – is one that continues to present a challenge. The factors likely to threaten block chain security in the future is quantum computing. Although quantum computers possess relativistic capability to break current encryption algorithms like block chain networks that engage in the use of RSA or Elliptic Curve Digital Signature Algorithm (ECDSA). Even though fully fledged quantum computers capable providing break of block chain encryption is not available, research in specific domain has been progressing at a very brisk pace, which gives certain degrees of worry or prospect of quantum attacks over block chain networks in the near future [50].

If quantum computers develop the capability to harm current cryptographic methods, then the block chain based financial





systems would be at a high risk of being exposed to attacks that endanger the data information, transaction and personal keys. Scientists are vigorously looking for a quantum-resistant solution that will protect block chain networks against future quantum attacks. On the other hand, conversion to quantum-resistant algorithms is another major shift that has to be made to existing block chain systems and which would be hard to popularize [51]. Decentralized Finance is an ecosystem of platforms which attempts to replicate the traditional financial sector in a decentralized way, and has been rapidly growing in recent years. Nonetheless, such a high growth rate also means that new threats to security have appeared. DeFi protocols depend on smart contract mechanisms and multi-dApps interactions characterized by high chances of bugs, hacks, or exploitation.

They discovered that DeFi platforms do not have control centers where they can tell their clients to make some changes to their wallets or accounts in case of attacks or loss of funds. The vulnerabilities of DeFi protocols have already been exploited, and since it grasps the decentralized financial systems within block chain, it is still a problem [52]. More effective security solutions, regular checks, as well as insurance solutions are required to create secure DeFi mobile applications. Recently, applications of block chain have been gradually introduced into the financial sectors, new threats and challenges with regard to those technologies need to be taken into consideration in order to provide secure, stable and, reliable block chain based financial platforms. Nonetheless, block chain has robust security features, there are challenges such as, weak smart contracts, possibility of 51% attacks, privacy consideration, and others which pose threats to financial institutions and its users. However, with the adaption of new technologies in the market, there is the acutely effect of new threats that will act as challenges to the DeFi security such as quantum computing and DeFi exclusive risks, among them are. Financial institutions need to be cautious and continue studying potential risks and putting up with appropriate security measures for possible cyber risks within the block chain financial systems.

CONCLUSION

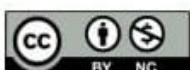
There are many opportunities in applying block chain technology in the financial sector: much is possible in terms of security, transparency, and efficiency. However, like any other new technology, it has its own merits as well as demerits or shortcoming associated with it. This review has looked at the facets of block chain security embracing the strengths, weaknesses, emergent threats and precaution measures with regard to block chain associated financial applications. This is the reason why block chain provides a highly secured and decentralized environment where it becomes very hard for the wrong people to alter the transaction records. It is due to the attributes that make block chain almost immutable and transparent regarding its transaction, especially within the payment, remittances and the decentralized finance (DeFi) sectors. However, there are many incidents that cannot be accommodated by block chain networks, which include 51% attacks, vulnerabilities in smart contracts, phishing attacks, and the risks that are likely to arise from quantum computing. All the above threats also require constant working hard on the side of the financial institutions to improve security and embrace innovation.

The above threats are relatively new in block chain; the following best practices need to be observed: Block chain audits, Cryptographic algorithms security, and Identity verification systems. Advanced measures like multi-sig authorization, permissioned block chain and second layer scaling can greatly improve the security of block chain applications. Further, adoption of decentralized identity management, strong access controls and multi-factor authentication prevent just about anybody from accessing financial data. Also, financial institutions offer services that underpin compliance with critical regulations since user's privacy is vital; this includes KYC, AML policies and data protection laws. This is in regard to updating regularly security features, time checking on audit trails and preparations made for future threats such as quantum computing. He or she adds that constant supervision and having the incident response plan can help to reduce effects of new security threats.

In conclusion, the use of block chain financial applications can only be secured by balancing the best of block chain technology that provides for decentralised and transparent systems, yet need to fully address the emergent threats inherent from the vulnerabilities identified above. Financial institutions that have proper security measures they adhere to, maintain their innovation and keep up with risks which are ever changing, will be able to realize the full potential of block chain technology and provide secure and efficient services to individuals or other entities using the financial system. The development of block chain technology will progress in time and penetration in the financial industries means that for the major key players, the developers, the regulators, the financial institutions, it is crucial to cooperate, to exchange the experiences and knowledge, and strive for one major common goal, which is to develop safe and robust financial structures.

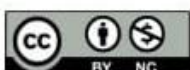
REFERENCES

1. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. 2nd Int. Conf. Open Big Data (OBD), Vienna, Austria, Aug. 2016, pp. 25–30.
2. J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," IEEE Access, vol. 4, pp. 9239–9250, 2016.





3. H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in Proc. IEEE ISADS, Bangkok, Thailand, Mar. 2017, pp. 229–234.
4. M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of Internet of Things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, 2017.
5. Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
6. F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in Proc. Int. Conf. Service Syst. Service Manage., Dalian, China, Jun. 2017, pp. 1–6.
7. M. Samaniego and R. Deters, "Internet of smart things—IoT: Using blockchain and CLIPS to make things autonomous," in Proc. IEEE Int. Conf. Cogn. Comput. (ICCC), Honolulu, HI, USA, Jun. 2017, pp. 9–16.
8. N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.
9. M. S. Hossain, G. Muhammad, and S. U. Amin, "Improving consumer satisfaction in smart cities using edge computing and caching: A case study of date fruits classification," *Future Gener. Comput. Syst.*, vol. 88, pp. 333–341, Nov. 2018.
10. Weber et al., "on availability for blockchain-based systems," in Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS), Hong Kong, Sep. 2017, pp. 64–73.
11. R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in Proc. Int. Smart Cities Conf. (ISC2), Wuxi, China, Sep. 2017, pp. 1–4.
12. N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "towards using blockchain technology for eHealth data access management," in Proc. 4th Int. Conf. Adv. Biomed. Eng. (ICABME), Beirut, Lebanon, Oct. 2017, pp. 1–4.
13. K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
14. L. Liu, Z. Chang, X. Guo, S. Mao, and T. Ristaniemi, "Multiobjective optimization for computation offloading in fog computing," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 283–294, Feb. 2018.
15. P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," in Proc. IEEE Healthcom, Dalian, China, Oct. 2017, pp. 1–4.
16. W. Liu, S. S. Zhu, T. Mundie, and U. Krieger, "Advanced block-chain architecture for e-health systems," in Proc. IEEE Healthcom, Dalian, China, Oct. 2017, pp. 1–6.
17. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
18. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in Proc. IEEE PIMRC, Montreal, QC, Canada, Oct. 2017, pp. 1–5.
19. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.
20. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.
21. T. M. Fernández-Caramés and P. Fraga-Lamas, "a review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685
22. L. Ma, X. Liu, Q. Pei, and Y. Xiang, "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2018.2825986.
23. T. Zhang, "Data offloading in mobile edge computing: A coalition and pricing based approach," *IEEE Access*, vol. 6, pp. 2760–2767, 2018.
24. F. Wang, J. Xu, X. Wang, and S. Cui, "Joint offloading and computing optimization in wireless powered mobile-edge computing systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1784–1797, Mar. 2018.
25. M. Liu, Y. Mao, S. Leng, and S. Mao, "Full-duplex aided user virtualization for mobile edge computing in 5G networks," *IEEE Access*, vol. 6, pp. 2996–3007, 2018.
26. W. Fan, Y. Liu, B. Tang, F. Wu, and Z. Wang, "Computation offloading based on cooperations of mobile edge computing-enabled base stations," *IEEE Access*, vol. 6, pp. 22622–22633, 2018.
27. Z. Zhu et al., "Fair resource allocation for system throughput maximization in mobile edge computing," *IEEE Access*, vol. 6, pp. 5332–5340, 2018.
28. P. Bellavista, S. Chessa, L. Foschini, L. Gioia, and M. Girolami, "Humanenabled edge computing: Exploiting the crowd as a dynamic extension of mobile edge computing," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 145–155, Jan. 2018.





29. Kiani and N. Ansari, "Edge computing aware NOMA for 5G networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1299–1306, Apr. 2018.
30. L. Tang and S. He, "Multi-user computation offloading in mobile edge computing: A behavioral perspective," *IEEE Netw.*, vol. 32, no. 1, pp. 48–53, Jan./Feb. 2018.
31. Q. Yuan, H. Zhou, J. Li, Z. Liu, F. Yang, and X. S. Shen, "Toward efficient content delivery for automated driving services: An edge computing solution," *IEEE Netw.*, vol. 32, no. 1, pp. 80–86, Jan./Feb. 2018.
32. M. Marjanović, A. Antonić, and I. P. Žarko, "Edge computing architecture for mobile crowdsensing," *IEEE Access*, vol. 6, pp. 10662–10674, 2018.
33. Y. Hao, M. Chen, L. Hu, M. S. Hossain, and A. Ghoneim, "Energy efficient task caching and offloading for mobile edge computing," *IEEE Access*, vol. 6, pp. 11365–11373, 2018.
34. P. Verma and S. K. Sood, "Fog assisted-IoT enabled patient health monitoring in smart homes," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1789–1796, Jun. 2018.
35. G. Premsankar, M. Di Francesco, and T. Taleb, "Edge computing for the Internet of Things: A case study," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1275–1284, Apr. 2018.
36. Y. Cao et al., "Mobile edge computing for big-data-enabled electric vehicle charging," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 150–156, Mar. 2018.
37. L. Liu, Z. Chang, and X. Guo, "Socially aware dynamic computation offloading scheme for fog computing system with energy harvesting devices," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1869–1879, Jun. 2018.
38. Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Gener. Comput. Syst.*, vol. 85, pp. 76–87, Aug. 2018.
39. H. Ko, J. Lee, and S. Pack, "Spatial and temporal computation offloading decision algorithm in edge cloud-enabled heterogeneous networks," *IEEE Access*, vol. 6, pp. 18920–18932, 2018.
40. K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Mobile edge computing and networking for green and low-latency Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 39–45, May 2018.
41. Y. Bi, G. Han, C. Lin, Q. Deng, L. Guo, and F. Li, "Mobility support for fog computing: An SDN approach," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 53–59, May 2018.
42. Poon J, Dryja T. 2016. The bitcoin lightning network: Scalable off-chain instant payments. Available at <https://lightning.network/lightning-network-paper.pdf> (accessed on 1 October 2019).
43. Popov S. 2018. Seebacher S, Schüritz R. 2017. Blockchain technology as an enabler of service systems: a structured literature review. In: *Proceedings of the international conference on exploring services science*. 12–23.
44. ShipChain. 2019. The end-to-end logistics platform of the future: trustless, transparent tracking. Available at <https://shipchain.io/> (accessed on 1 October 2019).
45. Spagnuolo M, Maggi F, Zanero S. 2014. Bitiodine: extracting intelligence from the bitcoin network. In: *Proceedings of the international conference on financial cryptography and data security*. 457–468.
46. Sun Y, Zhang R, Wang X, GAO K, Liu L. 2018. A decentralizing attribute-based signature for healthcare blockchain. In: *2018 27th International conference on computer communication and networks (ICCCN)*. IEEE, 1–9.
47. Swan M. 2015. *Blockchain: blueprint for a new economy*. California, CA, USA: O'Reilly Media. Tanwar S, Parekh K, Evans R. 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications* 50:1–13 DOI 10.1016/j.jisa.2019.102407.
48. TomoChain. 2018. Tomochain: masternodes design technical white paper version 1.0. Available at <https://tomochain.com/docs/technical-whitepaper--1.0.pdf> (accessed on 1 October 2019). T°, T. 2017. Preventing fake degrees.
49. Nhân Dân. Available at <http://nhandan.com.vn/giaoduc/tin-tuc/item/33377202-ngan-chan-nan-bang-gia-va-tinh-trang-chay-bangcap.html> (accessed on 1 October 2019).
50. Turkanović M, Hölbl M, Košič K, Heričko M, Kamišalić A. 2018. EduCTX: a blockchain-based higher education credit platform. *IEEE Access* 6:5112–5127 DOI 10.1109/ACCESS.2018.2789929.
51. Wang H, Cen Y, Li X. 2017. Blockchain router: a cross-chain communication protocol. In: *Proceedings of the 6th international conference on informatics, environment, energy and applications*. 94–97.
52. Wang L, Liu Y. 2015. Exploring miner evolution in bitcoin network. In: *Proceedings of the international conference on passive and active network measurement*. 290–302.

