A Survey on Blockchain Technology Concepts, Applications and Security

Asma Mubark Alqahtani[1], Abdulmohsen Algarni[2]
College of Computer Science, King Khalid University
Abha, Asir, Saudi Arabia[1,2]

***Abstract*—In the past decade, blockchain technology has become increasingly prevalent in our daily lives. This technology consists of a chain of blocks that contains the history of transactions and information about its users. Distributed digital ledgers are used in blockchain. A transparent environment is created by using this technology, allowing encrypted secure transactions to be verified and approved by all users. As a powerful tool, blockchain can be utilized for a wide range of useful purposes in everyday life including cryptocurrency, Internet-of-Things (IoT), finance, reputation system, and healthcare. This paper aims to provide an overview of blockchain technology and its security issues for users and researchers. In particular, those who conduct their business using blockchain technology. This paper includes a comparison of consensus algorithms and a description of cryptography. Further, most applications used in blockchain are focused on in this paper also analyzing real attacks and then summarizing security measures in blockchain. Even though Blockchain holds a promising scope of development in several sectors, it is prone to several security and vulnerability issues that arise from different types of blockchain networks which represent a challenge to deal with blockchain. Finally, as a research community, we encourage future research challenges that can be addressed to improve security in blockchain systems.**

***Keywords*—Blockchain; cryptography; cryptocurrency; consensus algorithms; blockchain security**

I. Introduction

Blockchain is based on a decentralized, unchangeable database that makes it simpler to record assets and keep track of transactions in a corporate network. An asset may be tangible or intangible. On a blockchain network, virtually anything of value may be stored and traded, reducing risk and improving efficiency for all users. Generally, a blockchain is a digital ledger of transactions that are being recorded. It is decentralized and is not controlled by any individual, group, or company [1].

As a structured technology, blockchain can be very difficult to change without the approval of the people who use it. Blockchain stores data as a decentralized ledger. Participants in this network can read, write, and verify transactions. Transactions cannot be modified or deleted. To support and secure the blockchain system, digital signatures, hash functions, and other cryptographic functions are used. These primitives ensure that transactions recorded in the ledger are integrity-protected and authenticated. This technology is called blockchain because new blocks are linked to older ones to form a chain. The first appearance of this term was a publication written by S. Haber and W.S. Stornetta in 1991 [2]. In general, blockchain technology is credited to Satoshi Nakamoto, who developed the theory and implemented the technology in 2008 and 2009, respectively in the cryptocurrency Bitcoin, the most well-known blockchain application. Blockchain technology in recent years has attracted significant attention from academics and industries because of its advanced features. It can be applied to a variety of applications beyond cryptocurrencies. Blockchain technology has become a leading technology of internet interaction systems, including the Internet of Things (IoT) [3].

Our motivation in this paper is to inform and assist someone to become familiar with blockchain technology and its security issues, particularly for those who carry out transactions using blockchain technology and for researchers interested in developing blockchain technology and evaluating its security issues. To search publications and information on the Internet, the first step is to identify keywords such as blockchain, consensus algorithm, cryptography, cryptocurrency, and blockchain security. A second approach is to review papers that have been published in top conferences and journals that deal with blockchain. In this paper, we provide the following main contributions:

- A detailed survey was conducted on blockchain technology.
- A systematic survey of Blockchain applications is conducted in this paper. 10 application areas are considered.
- Security and privacy issues were also addressed.

Therefore, we encourage further efforts to survey and develop blockchain technology for widespread adoption.

The rest of this paper consists of the following sections: In Section II, we provide an overview of the history of blockchain technology. A typical consensus algorithm used in the blockchain is described in Section III. In Section IV, we focused on blockchain applications. In Section V, we summarize the technical risks, attacks, and challenges of security in this area, and in Section VI, we conclude this paper.

II. History of Blockchain

Chaum's Ph.D. thesis, published in 1982, was the first to suggest a blockchain as a protocol. A paper by Haber and Stornetta published in 1991 titled "How to Time-Stamp a Digital Document" detailed the concept of time stamping digital data cryptographically [3].

In 1998, Nick Szabo proposed the creation of Bit Gold, an early attempt at the creation of a decentralized virtual currency.

However, Szabo's attempt to implement Bit Gold is generally regarded as the basis for Satoshi Nakamoto's bitcoin protocol, even though the project was never implemented [4].

Modern day blockchain technology is widely believed to have been first implemented by Satoshi Nakamoto in 2008. He hypothesized a direct online payment between parties without the use of a third-party intermediary. Rather than relying on trust, that paper presented a cryptographic proof-based electronic payment system [5].

Blockchain was introduced by Ethereum in 2013 as a technology for executing smart contracts on a decentralized platform. With Ethereum, it is possible for developers to create markets, store transactions, and move funds according to written instructions, all without the involvement of middlemen. Unlike Bitcoin, Ethereum is a ledger technology that is being used by companies to develop new programs, which are being expanded beyond the realm of currencies for the first time [6]. With the launch of the Ethereum platform in 2015, blockchain could be used for storing and processing loans and contacts. Using an algorithm known as a smart contract, this technology ensures the implementation of an action between two parties. Due to Ethereum's ability to provide a faster, safer, and more efficient environment, it became extremely popular. Instead of all the different blockchain projects, Ethereum enables communication via untrusted distributed applications on its own blockchain, thus creating a new concept called Ethereum 2.0 [7].

Hyperledger is open source software for blockchains that was announced by the Linux Foundation in 2015. The Hyperledger blockchain framework aims to build enterprise blockchains, which are different from Bitcoin and Ethereum. Blockchain attracted interest with its capability to enable anonymity, but the real appeal lies in its capability to enable complete privacy. As will be discussed in the fourth section, there have been many applications for blockchain technology that have been discovered across a wide range of industries.

The following Fig. 1 summarizes the history of blockchain technology. Since everyone can participate in Bitcoin and Ethereum's blockchain networks, they are considered public blockchains. Due to their need to verify participants before joining the network, the Hyperledger blockchain networks are considered private blockchains, also known as permissioned blockchains.The following Table I summarizes the differences between Hyperledger and Ethereum, two popular blockchain platforms and networks.

TABLE I. HYPERLEDGER AND ETHEREUM

Feature	Ethereum	Hyperledger
Purpose	run smart contracts	Businesses
Confidentiality	public network	limited access
Governance	Ethereum developers	Linux Foundation
Participation	permission-free	Only authorized members
Smart contracts	Yes	Yes using chaincode
Programming Language	Solidity	JavaScript, Java, etc
Consensus Mechanism	Yes, PoW,PoS, etc	No
Speed of Transactions	Low	High
Use	Public Applications	Private applications

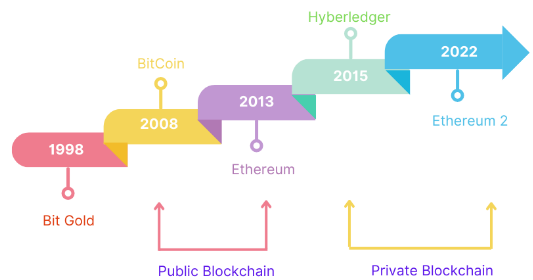

Fig. 1. History of blockchain.

III. BLOCKCHAIN TECHNOLOGY

A. Blockchain Layers

According to Melanie Swan, blockchain technology has passed through two stages. The first stage is blockchain 1.0 represented by Bitcoin, and the second stage is blockchain 2.0 represented by Ethereum. In general, blockchain-based technologies include Bitcoin, Ethereum, Hyperledger, etc [8]. Even though the implementations are varied, there are some similarities in the basic architecture.
Blockchain environments can be classified into five layers, as shown in Table II application, network, contract, consensus, and data layers.

TABLE II. BLOCKCHAIN LAYERS

Layers	Bitcoin	Ethereum	Hyperledger
Application layer	Bitcoin trading	Ethereum trading	Enterprise blockchain
Network layer	TCP	TCP	HTTP
Contract layer	Script	Script	Java
Consensus layer	PoW	PoW/PoS	PBFT/SBFT
Data layer	Merkle tree	Merkle patricia tree	Merkle Bocket tree

Consensus mechanisms are the main component of the consensus layer. In the contract layer, smart contracts are included. Various protocols for data transmission and verification are included in the network layer. In addition, it is pertinent to note that the blockchain is a typical peer-to-peer network. There is no central node and all nodes are connected through a planar topology [9]. It is possible to transact between any two nodes. Each node within the network is free to leave or join anytime. A number of applications are included in the application layer, such as Bitcoin, Ethereum, and Hyperledger.

B. Consensus Algorithms

Among the many desirable characteristics of blockchain technology, it is possible to verify the honesty of anonymous users when they enter transactions into the ledger. This is done by validating each transaction to ensure that it is legal before adding it to a block. Consensus algorithms are used to determine whether new blocks will be added to the blockchain and to ensure trust between parties involved in the blockchain system and to store transactions. As a result, consensus algorithms are the core of all blockchain transactions [10]. Every participant must follow a consensus protocol. There have been several consensus mechanisms developed for blockchains. This includes Proof of State, Delegated Proof of State, Proof of Work, Proof of Elapsed Time, Directed Acyclic Graph, and so on. We will take a look at the most common algorithms shown in Table III.

Proof of Work (PoW): The objective of this algorithm is to determine a problem that must be solved through guessing. Bitcoin and Ethereum employ PoW as the algorithm for their consensus. As a result of PoW requiring lots of electricity and time, it is not widely used [11].

Proof of Stake (PoS): It ranks second in popularity as a consensus algorithm, and it involves fewer computations than PoW. It minimizes the time and energy waste issues that PoW has. This consensus algorithm replaces the current method for reaching consensus in a distributed system, instead of solving a Proof-of-Work. BlackCoin was the first cryptocurrency to use a PoS [12].

Proof of Elapsed Time (PoET): It is a consensus algorithm for blockchain networks that keeps the process more efficient by avoiding over-utilization of resources and high-energy consumption. The PoET method resembles the proof of work method (PoW), but requires less power due to its ability to allow the processor to switch to other tasks after a period of time, which increases efficiency [13].

Byzantine Fault Tolerance (BFT): It is aimed at solving problems where there are untrustworthy parties, but they need to achieve consensus. PBFT is designed to improve BFT. With PBFT, if hostile nodes represent fewer than thirty percent of all nodes, then the current state of the blockchain will be agreed upon by all participants. Blockchain systems are more secure when there are more nodes involved. Currently, Hyperledger Fabric is based on PBFT [14].

Direct Acyclic Graph (DAG): It consists of vertices and edges, which differentiates it from various consensus algorithms. Transactions are represented by the vertices of the structure. A block is not referred to in this algorithm, nor do we need to use a mining process to add transactions. Each transaction is built upon the previous one rather than being grouped into a block. Several applications of DAG technology can be found in fields that require high speed and no fees, like Internet of Things (IoT) [15].

TABLE III. CONSENSUS ALGORITHMS

Algorithms	Speed	setup	Example of use
PoW	Low	Public/private	Bitcoin, Ethereum
PoS	High	Public/private	NXT
DPoS	High	Public/private	EOS, BitShares
DBFT	Very high	Public/private	NEO, TON
PBFT	High	Private	Hyperledger, Chain

C. Smart Contract

The smart contract also called chaincode is an essential feature of blockchain because it not only offers a distributed, immutable completion of all activities, but is also capable of allowing for the creation of a computer program that is non-subjective and specifies how the process will be implemented. In this contract, an important activity is addressed. More than two parties don't need to be involved in this contract. The Ethereum smart contract was designed to overcome some of the limitations of Bitcoin [16].

Enterprise blockchain applications are based on smart contracts, which will revolutionize the way businesses operate. Smart contracts can be developed by anyone without the need for an intermediary. Because of a smart contract, the process is autonomous, accurate, and cost-effective.

D. Cryptography of Blockchain

Blockchains enable confidential and secure transactions between anonymous parties. This trust is established through cryptography, thus eliminating the necessity for centralized institutions. By using cryptography, blockchain data is kept on the ledger. Cryptography building blocks are used in blockchain technology as follows [17]:

- Public Key Cryptography: Designed to create digital signatures and encrypt data.
- Zero-Knowledge Proof: Show that you know a secret without divulging it.
- Hash Functions: A mathematical function that generates pseudo-random numbers.

1) Public key cryptography: A transaction can be proven to have been created by the right user by this method. Using a private key, a user can sign a message, known as a digital signature. Digital signatures are used in Hyperledger and Ethereum transactions to verify the authenticity of the sender and that the information has not been changed since it was signed. The algorithm (ECDSA) is widely used to generate a combined set of private and public keys.

2) Zero-knowledge proofs: These are primarily used when users request to transfer money to other users. Before committing a transaction, the blockchain must verify that the participant who is transferring funds has enough to complete the transaction. However, the blockchain does not care about how much money he has in total or who is spending it so it has no idea who the user is or how much money he owns.

3) Hash functions: Hash Functions: Hash functions form an essential part of blockchain technology. There are five properties of a hash function that are critical for cryptography [18]:

Fixed size: The hash function can accept any input and create the output of a fixed size. In order to provide digital signatures, blockchains employ hash functions to condense messages.

Preimage resistance: When given a set of inputs, it is not challenging to produce a hash result. Despite this, reverse engineering the original input is mathematically impossible based on the hash output. The only way to achieve the same result is to randomly select data that should be entered into the hash algorithm.

2nd preimage resistance: Obtaining a secondary input that provides the same hash result is impossible given an input and its hash result.

Collision resistance: The same hash output cannot be produced from two distinct inputs.

Big change: An entirely different hash output will be produced if any single bit is changed in the input.

IV. Blockchain Applications

According to the survey, blockchain applications include cryptocurrency, Internet-of-Things (IoT), finance, reputation system, healthcare, security and privacy, advertising, copyright protection, society application, energy, mobile applications, defense, digital records, supply chain, digital ownership management, automotive, intrusion detection, agricultural sector, voting, identity management, education, law and enforcement, property title registries, asset tracking, and so on [19]. An illustration of the spiraling applications of blockchain can be found in Fig. 2.

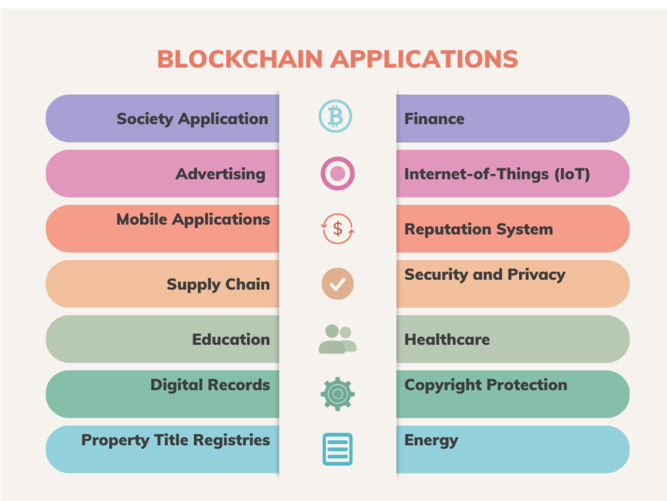

Fig. 2. Application of blockchain.

More applications of blockchain systems are predicted to be developed in the future.To provide further information, we have selected the following 10 blockchain-based applications:

A. Healthcare

Prescription medications are being tracked and traced throughout supply chains using blockchain technology. The tool enables the easy and rapid prevention and regulation of counterfeit pharmaceutical distribution as well as the recall of ineffective and unsafe medications. Security of customer data is a primary goal in healthcare, as is the exchange of data between hospitals, governments, and research institutes, which facilitates the improvement of healthcare services.As part of this project, Nokia has used wearable devices to track daily steps and hours of sleep and stored the data on the Blockchain [20].

B. IoT

People, places, and products can be connected via the Internet of Things (IoT), providing new opportunities for the generation of value in products and business processes. On the other hand, implementing this technology on a large scale is fraught with security concerns. Combining blockchain and IoT offers the following benefits: To detect data manipulation quickly and accurately, blockchain technology can provide a robust framework for faster detection. Due to the size of IoT networks, it can be difficult to detect failure patterns. Each IoT endpoint is assigned a unique key by blockchain technology, which facilitates the identification of inconsistencies. By combining IoT with smart contracts, it becomes possible to authorize automated responses. Decentralization enhances security: Blockchain technology is decentralized, making it impossible for cybercriminals to hack and corrupt a single server. Additionally, the use of blockchain technology allows tracking of user actions to provide information on who, when, and how users have used a particular device [21].

C. Government

Blockchain technology can be used in the public sector to improve the quality and quantity of services. It can also be used to improve transparency and accessibility, as well as to share information between different organizations. In addition to being secure against online attacks, the blockchain is publicly available. Transactions are not editable or deletable once they have been added. This makes data transactions safe, secure, and accessible to anyone [22].

D. Power Grid

The development of blockchain-based smart grids is aimed at improving energy distribution on a large scale. There is a significant amount of inefficiency in electricity distribution at the retail level. The use of blockchain technology and Internet-of-Things (IoT) devices for these types of services can reduce electricity bills by bypassing retailers and directly connecting consumers to wholesale distributors. Consumers connected to the smart grid can also shop around for the highest rates from a variety of providers. This leveled the playing field in an industry that has traditionally been dominated by a single provider. Several projects are leading the way in this area, including Grid + and Energy Web Token [23].

E. Copyright and Royalties

Music, films, and other creative mediums are subject to copyright and royalties. These are artistic mediums and do not appear to be linked to Blockchain in any way. In the creative industries, however, this technology is quite critical in terms of ensuring security and transparency. It is common for music, films, art, etc., to be plagiarized without proper credit being given to the original creators. A detailed ledger of artist rights can be maintained on the Blockchain to rectify this issue. The use of blockchain technology can also provide a secure record of artist royalties and deals with large production companies, in addition to being transparent. Digital currencies, such as Bitcoin, can also be used to manage the payment of royalties [24].

F. Cryptocurrencies

In 2008, it was announced that Bitcoin would be the first cryptocurrency. It was launched in 2009. It is estimated that there are 21 million bitcoins in use today. The miner receives a transaction fee once he finds a value that matches the difficulty. Currently, about 90% of BTC is mined.

Ethereum (ETH) is regarded as the second largest cryptocurrency based on market capitalization after Bitcoin (BTC). According to Cryptoslate, [25] there are 2403 top cryptocurrencies ranked by market capitalization. Table IV below shows seven popular cryptocurrencies.

TABLE IV. Top Cryptocurrencies

No	cryptocurrency	Market cap
1	Bitcoin (BTC)	322.5 billion
2	Ethereum (ETH)	162.8 billion
3	Tether (USDT)	66.3 billion
4	Binance Coin (BNB)	44.0 billion
5	U.S. Dollar Coin (USDC)	43.9 billion
6	XRP (XRP)	17.66 billion
7	Binance USD (BUSD)	16.3 billion

Blockchain technology can be applied to the use of cryptocurrencies, thus taking full advantage of the features of this technology including:

- There is no intermediary involved in the payment process.
- Processing fees are low.
- Money can be sent at any time without delay or restriction.

A few disadvantages of cryptocurrencies include:

- Black money may be incurred due to a lack of control.
- Digital assets may be lost as a result of a security attack, which we will discuss in more detail later.
- Some commentators claim that investing in cryptocurrencies is highly speculative and risky. Tesla, for instance, advised investors to be aware of Bitcoin's volatility.

G. Dubai Blockchain Office

Strategy of Dubai Blockchain is the result of a collaboration between the Dubai Future Foundation and the Digital Dubai Office. The purpose of this initiative is to continuously explore and evaluate the latest technological innovations that can be used to enhance the quality of life in cities through seamless, efficient, safe, and impactful solutions [26].

The strategy represents a powerful and innovative tool to influence the future of the Internet through the provision of safe and simple transactions. This will help to achieve the vision of making Dubai the world's first blockchain-powered city. When this strategy is successful, Dubai will contribute substantially to the future economy.

H. Cloud Computing

Cloud computing has had a major impact on the software technology industry due to its impressive benefits. There are many uses for cloud computing among businesses worldwide, including data storage and backup, software development and testing, disaster recovery, and more. Many industries are using cloud computing to build innovative solutions, including healthcare, automotive, and retail. Even with the advantages of cloud computing, it has its limitations. Blockchain can help overcome these limitations. Due to its transparency, security, and decentralized nature, blockchain technology is being used by millions of businesses for a variety of industrial applications. The use of blockchain and cloud technology together, however, can further revolutionize industries. Even though blockchain technology provides better network security, privacy, and decentralization, cloud computing provides high scalability and elasticity. Therefore, cloud technology and blockchain technology can be combined to produce innovative solutions [27].

I. e-Commerce

Constant evolution is taking place in the e-commerce industry due to the development of new technologies and the creation of new ways to buy and sell products and services. Using blockchain technology, it is possible to create a decentralized database for storing information about products and customers. By doing so, customers would be able to obtain information about products, such as their origin and supplier, which would also reduce the possibility of fraud. A blockchain-based payment system can also ensure enhanced security and reduce the risk of fraudulent payments. As a distributed database, blockchain technology provides secure, transparent, and tamper-proof transactions. It is anticipated that this technology will revolutionize the e-commerce industry by improving the security of transactions and simplifying the fulfillment process. The system also enhances buyer-seller trust and transparency. Blockchain technology allows e-commerce businesses to track the history of orders and transactions to improve the customer experience. The customer would be able to track their orders easier and find information about previous purchases. Additionally, blockchain can reduce the risk of fraud and facilitate the tracking and verification of transactions more reliably and securely. The implementation of this technology could prove to be a game changer for the e-commerce industry, which is currently plagued by issues of fake reviews, fraudulent transactions, and other security risks. Businesses that use blockchain technology can reduce costs associated with processing transactions and shipping products, as well as improve the speed at which new products are introduced to the market [28].

J. Advertising

A blockchain advertising application is a type of distributed ledger technology that promotes decentralization with the highest level of security and transparency. On the blockchain, digital records are immutable, which means that individuals have access to read but cannot amend the records. Blockchain can allow advertisers to track their advertising expenditures in real time since it stores information and transactions. it provides a level of transparency that cannot be achieved with existing systems. Transparency is not the only advantage. In advertising, speed is crucial, as it is difficult to track inventory and ensure high-quality products. Blockchain technology has the capability of keeping up with these challenges [29].

V. Attacks and Security Measure on Blockchain

A. Attacks on Blockchains

Blockchains are distributed so it makes sense to conduct research on their security. In this section, we will discuss the security risks associated with this technology. In order to gain a deeper understanding of blockchain security, it is essential to first understand the differences between private and public blockchain security, particularly regarding data access and participation capabilities, as we mentioned above.

The following are the top security issues associated with blockchains [30]:

1) Sybil attack: In this attack, several fake network nodes are generated by hackers. Through the use of these nodes, it will be able to gain majority agreement and interrupt transactions.

2) Endpoint vulnerabilities: Another vital concern in the security of blockchain is the vulnerability of endpoints. Electronic devices such as mobile phones and computers are used to interact with the blockchain network. Observing the behavior of users and targeting their devices will allow hackers to steal the user's key. Perhaps this is one of the most prominent security issues associated with blockchain technology.

3) 51% attack: An attack of 51% occurs when one user or institution controls half of the hash rate and takes control of the entire system. Transactions can be modified by hackers and prevent them from being confirmed. They will even reverse transactions that have already been completed, leading to double spending.

4) Phishing attacks: Phishing attacks are designed to steal user credentials. An email will be sent to the wallet key owner that appears to be legitimate. A fake hyperlink is attached to the email that requires the user to enter their login details. By gaining access to a user's credentials and private information, it is possible to cause damage to the user and the blockchain network as a whole.

5) Routing attacks: In this attack, participants are usually unaware of the threat because the transmission of data and the conduct of operations continue as usual. A potential danger is that such attacks could reveal sensitive information or generate revenue without the user's permission.There is a critical reliance on the movement in real time of enormous amounts of information in a blockchain application and network. Due to the anonymity of an account, hackers may be able to intercept information transmitted to Internet service providers by using it.

6) Private keys: You will need a private key in order to access your funds. A hacker can easily guess the private key if it is weak. Your funds could be accessed as a result. Keeping your private key secret is extremely critical, and it should be strong enough not to be guessed easily.

7) Malicious nodes: Additional security problems related to blockchain technology include the threat of malicious nodes. An attempt to disrupt the network will occur once a dishonest actor has joined the network. In order to accomplish this, they will attempt to reverse transactions or flood the network with transactions.

B. Security Measures of Blockchain

To ensure the security of blockchain applications, security must be considered at all layers, including permission management through several security measures [31]. The following are some of the security measures of blockchain:

1) Blockchain governance: Determining how existing organizations or users leave or join the network, and providing mechanisms to prevent malicious actors, manage errors, secure data, and address issues between parties.

2) Data security: While data compression is generally regarded as the most effective method for identifying what data should be kept on-chain, additional privacy measures should be implemented to hash data, cloud storage, and data in transit.

3) Security of blockchain network: Blockchain is a distributed system, which requires network connections from various participants beyond a single organization to interact. All of these factors have the potential to introduce security exploits or flaws. Part of governance, therefore, includes reviewing security protocols for users [32].

4) Blockchain application security: Security applications are vulnerable points and should be protected with effective user identification and endpoint security measures. For private blockchains, where access and use are limited to authorized participants, it may be necessary to provide different levels of authorization that may change with time.

5) Smart Contracts Security: Smart contracts consist of a set of codes within the blockchain, triggered by a set of programmed conditions. This presents another point of vulnerability as their reliability determines whether the operation and the results can be trusted.

6) Use of trusted third-parties: Security evaluations, penetration checks, and reviews of the source code of smart contracts and blockchain implementations should be performed only by trusted individuals. Use these to protect against new security threats, such as unauthorized access to cryptographic algorithms [33].

VI. Conclusion

During the past few years, blockchain technology has attracted a great deal of attention due to its advanced characteristics of decentralization, autonomy, integrity, immutability, verification, and fault tolerance. In terms of the future scope, the primary priority will be addressing the security concerns arising from the various types of blockchain networks. Furthermore, consensus algorithms such as PoW implemented on blockchain have several drawbacks. Thus, the development of a consensus algorithm that is more efficient will result in more cost-effective blockchain networks. This survey introduces an in-depth overview of blockchain technology. A brief historical overview of blockchain was presented, followed by a comparison of the most widely used consensus algorithms. It has been discussed in detail how public key cryptography and hash functions applied to blockchains can be used for security, identification, and non-repudiation purposes. In addition, it provides detailed information and comparisons of some cryptocurrencies used in blockchain. Also, we focus on various categories of top security risks associated with blockchain technology. Finally, by making this effort, we hope that someone will gain a deeper understanding of blockchain technology. We also hope that individuals will give more focus to the safety of the blockchain

ACKNOWLEDGMENT

This research is financially supported by the Deanship of Scientific Research at King Khalid University under research grant number (R.G.P.1/188/41).

REFERENCES

[1] Kumar, S., Kumar, A., and Verma, V. (2019). A survey paper on blockchain technology, challenges and opportunities. Int. J. Comput. Trends Technol.(IJCTT), 67(4), 16. ISO 690

[2] Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document (pp. 437-455). Springer Berlin Heidelberg.

[3] Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375. ISO 690

[4] R. Sharma, Bit gold, Investopedia, 2021. Available online: https://www.investop edia.com/terms/b/bit-gold.asp.

[5] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. https://bitcoi n.org/bitcoin.pdf, October 2008.

[6] Vujičić, D., Jagodić, D., & Randić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE.

[7] A. Groetsema, A. Groetsema, N. Sahdev, N. Salami, R. Schwentker, F. Cioanca, Blockchain for Business: an Introduction to Hyperledger Technologies, The Linux Foundation, 2019.

[8] Sarmah, S. S. (2018). Understanding blockchain technology. Computer Science and Engineering, 8(2), 23-29. ISO 690

[9] Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In Journal of Physics: Conference Series (Vol. 1168, No. 3, p. 032077). IOP Publishing.

[10] Chaudhry, N., and Yousaf, M. M. (2018, December). Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In 2018 12th International Conference on Open Source Systems and Technologies (ICOSST) (pp. 54-63). IEEE. ISO 690

[11] Nguyen, G. T., and Kim, K. (2018). A survey about consensus algorithms used in blockchain. Journal of Information processing systems, 14(1), 101-128. ISO 690.

[12] Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). International Journal of Innovative Computing, 10(2).

[13] J. Frankenfield, Proof of Elapsed Time (PoET) (Cryptocurrency), Invest, October 16, 2020. Available online: https://www.investopedia.com/terms/p/proof-elapse

[14] Zhang, Z., Zhu, D., & Fan, W. (2020, December). Qpbft: practical byzantine fault tolerance consensus algorithm based on quantified-role. In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 991-997). IEEE. ISO 690

[15] Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. arXiv preprint arXiv:2001.07091. ISO 690

[16] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

[17] R. Santos, K. Bennett, E. Lee, Blockchain: Understanding its Uses and Implications, The Linux Foundation, 2021. Available online: https://www.edx.org/course/b lockchain-understanding-its-uses-and-implications.

[18] Wang, M., Duan, M., & Zhu, J. (2018, May). Research on the security criteria of hash functions in the blockchain. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts (pp. 47-55). ISO 690

[19] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., and Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys and Tutorials, 21(2), 1676-1717.

[20] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain technology in healthcare: a systematic review. In Healthcare (Vol. 7, No. 2, p. 56). MDPI.

[21] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. Sensors, 18(8), 2575. ISO 690

[22] Alketbi, A., Nasir, Q., & Talib, M. A. (2018, February). Blockchain for government services—Use cases, security benefits, and challenges. In 2018 15th Learning and Technology Conference (L&T) (pp. 112-119). IEEE.

[23] Foti, M., & Vavalis, M. (2021). What blockchain can do for power grids? Blockchain: Research and Applications, 2(1), 100008.

[24] Kim, A., & Kim, M. (2020, October). A study on blockchain-based music distribution framework: focusing on copyright protection. In 2020 International conference on information and communication technology convergence (ICTC) (pp. 1921-1925). IEEE.

[25] Aggarwal, S., & Kumar, N. (2021). History of blockchain-Blockchain 1.0: Currency. In Advances in Computers (Vol. 121, pp. 147-169). Elsevier. ISO 690

[26] Avan-Nomayo, O. Dubai's Economic Department to Roll Out Blockchain-Based Corporate KYC. Available online: https://cointelegraph.com/news/dubai-s-economic-department-to-roll-out-blockchain-based-corporate-kyc.

[27] Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain meets cloud computing: A survey. IEEE Communications Surveys & Tutorials, 22(3), 2009-2030.

[28] Zhou, Z., Wang, M., Yang, C. N., Fu, Z., Sun, X., & Wu, Q. J. (2021). Blockchain-based decentralized reputation system in an E-commerce environment. Future Generation Computer Systems, 124, 155-167.

[29] Chen, W., Xu, Z., Shi, S., Zhao, Y., & Zhao, J. (2018, December). A survey of blockchain applications in different domains. In Proceedings of the 2018 International Conference on Blockchain Technology and Application (pp. 17-21).

[30] Aruba, 10 Blockchain and New Age Security Attacks You Should Know, January 22, 2019. Available online: https://blogs.arubanetworks.com/solutions/10-bloc kchain-and-new-age-security-attacks-you-should-know/.

[31] Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. Blockchain: Research and Applications, 3(2), 100067.

[32] D. Wang, J. Zhao and Y. Wang, "A Survey on Privacy Protection of Blockchain: The Technology and Application," in IEEE Access, vol. 8, pp. 108766-108781, 2020, doi: 10.1109/ACCESS.2020.2994294.

[33] Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Materials Today: Proceedings, 37, 2653-2659. ISO 690