

A survey on security and policy aspects of blockchain technology

Haider Hadi Abbas¹, Montadher Issam Abdul Kareem², Hassan Muwafaq Ghani³

¹Computer Technology Engineering Department, Al-Mansour University College (MUC), Baghdad, Iraq

²Business Management Department, Al-Mansour University College (MUC), Baghdad, Iraq

³Computer Techniques Engineering Department, Al-Mustaqbal University college, Hillah 51001, Iraq

Article Info

Article history:

Received Jan 11, 2022

Revised Oct 24, 2022

Accepted Oct 29, 2022

Keywords:

Bitcoin

Cryptocurrency

Digital mining

Encryption

Initial coin offerings

ABSTRACT

This survey talks about the problem of security and privacy in the blockchain ecosystem which is currently a hot issue in the blockchain community. The survey intended to study this problem by considering different types of attacks in the blockchain network with respect to algorithms presented. After a preliminary literature review it seems that some focus has been given to study the first use case while, to the best of my knowledge, the second use case requires more attention when blockchain is applied to study it. The research is also interested in exploring the link between these two use cases to study the overall data ownership preserving accountable system which will be a novel contribution of this work. However, due to the subsequent government mandated secrecy around the implementation of data encryption standard (DES), and the distrust of the academic community because of this, a movement was spawned that put a premium on individual privacy and decentralized control. This movement brought together the top minds in encryption and spawned the technology we know of as blockchain today. This survey explores the genesis of encryption, its early adoption, and the government meddling which eventually spawned a movement which gave birth to the ideas behind blockchain.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Haider Hadi Abbas

Computer Technology Engineering Department, Al-Mansour University College (MUC)

Baghdad, Iraq

Email: haider.hadi@muc.edu.iq

1. INTRODUCTION

Blockchain is at its heart, simply an immutable transaction log, often referred to as a digital ledger, which employs cryptographic hashing techniques in a distributed fashion to create a one-way transaction register which memorializes the characteristics of an interactions between parties and secures those actions with completed proofs of work and a distributed, decentralized, and public log as mentioned in [1]. The research proposed in this report may be broadly categorized as a problem related to networked and distributed systems. Specifically, the research that will be carried out will contribute to the topics of system design, consensus mechanisms, algorithmic efficiency, and machine learning methods powered by network measurement data as mentioned in [2]. The research will be borrowing a few concepts and established tools from the fields of security and (maybe also from the) game and optimization theories as well. Ideally, to design an efficient system that addresses the privacy issues in the existing blockchain-based systems while considering the use case of data ownership and provenance in an efficient and more systematic manner as mentioned in [3]. It was originally

designed to facilitate commerce on the internet without the need for a trusted intermediary such as a bank or a monopolistic computing company like Microsoft or Google overseeing and injecting itself into transactions.

Blockchain however, due to its robustness, versatility, and security, has been leveraged into a whole host of other applications for which trust, privacy, resilience, and security are necessities as mentioned in [4]. This survey will explore the distributed ledger technology known as Blockchain. In this survey we will cover what Blockchain is, the theories and technologies behind Blockchain, its strengths and shortcomings, as well as its current and possible future uses as mentioned in [5]. We will explain the different types of blockchains (public, private, and federated), and the pros and cons of each. This paper will conclude with a description of an emerging application of blockchain, BigchainDB, which is a NoSQL database augmented with the core strengths of blockchain, its decentralized nature, robustness to node failures, and its security as mentioned in [6].

This work will also try to facilitate a more systematic approach to study the effective integration of laws and policies with the blockchain technology in terms of smart contracts which is currently also a hot topic. After a preliminary literature review and following the development of a few blockchain-based projects the aspect of privacy by blockchain seems quite important and critical as mentioned in [7]. Privacy by a blockchain-based distributed system implies an efficient (in terms of time, storage, and computation) and trustful (i.e. in an immutable, transparent, auditable, and decentralized manner) solution to automate an application in terms of a contract among different non-trusting parties. Figure 1 shows the security requirement triad [8]. Such an automation ideally should have the capability to tackle a logical fallacy such as a bug in the code, a malicious activity by an adversary that can often lead to logical and legal ramifications, or a conflict among the members of the contract as well mentioned in [8].

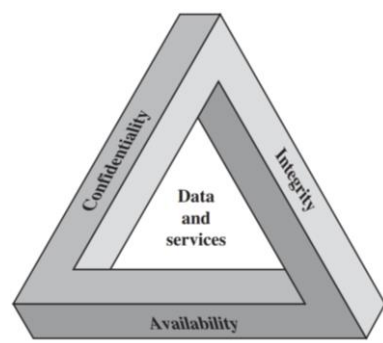


Figure 1. The security requirement triad [8]

Currently it seems that the way these such hacks were counteracted was by deploying a dedicated smart contract. As a result, the whole community was not taken on board during such events thus breaching the original idea of immutability and decentralization of the blockchain technology as mentioned in [9]. If, however, an efficient governance framework was existed to tackle this type of situation then such a split could have been avoided. This motivates me to study the aspect of governance by the blockchain in a more systematic manner. Similarly, another important aspect is of the governance of blockchain system itself. As an example, Bitcoin Cash was born when debate to upgrade the underlying Bitcoin system to make it more scalable arose as mentioned in [10]. This is different from governance by the blockchain as it deals with how to upgrade the underlying protocols and mechanisms of the blockchain technology itself. Here the vulnerability was in differential cryptanalysis that was discovered by digital currency initiative.

Reading about this problem there seems to be a severe lack in the standardization of the cryptocurrency deployments as mentioned in [11]. Specially in security aspects of things. Take away message is that it is a good practice does not use custom cryptographic methods rather use the ones that have been in practice and vetted by the community over the years. Given the rapid growth of cryptocurrencies it is a daunting task for the community to vet all the code of such a system as mentioned in [12]. There might be a silver lining if a framework is developed powered by techniques such as formal verification of code like the one privacy uses in its system. The split in Bitcoin that resulted in new currency system called Bitcoin Cash was the result of a heated debate to address the scalability issue. In my opinion such a split can be avoided if decisions are made in a decentralized manner as well by automating an efficient voting process on top of blockchain itself as mentioned in [13]. This governance aspect is envisioned by privacy by introducing the concept of formal verification of code. The paper wants to extend this notion to build a more generic governance framework for blockchain as mentioned in [14]. Figure 2 shows the strengths of blockchain as emerging technology.



Figure 2. The strengths of blockchain as emerging technology

Several organizations are conducting paper on leveraging the blockchain technology, primarily used in electronic financial transactions, as the core principle to exchange information between these internet-of-things. Companies from various industries like healthcare, electronics, telecommunications, networks, transportation, and banking are coming forward to make this idea a reality. It is believed that the blockchain technology can be very efficient in exchanging information between devices and companies with minimal cost and complexity while maintaining trust, accountability, and transparency. However, the blockchain technology used in Bitcoins cannot be directly applied for internet-of-things. Depending on the type of company and the information being exchanged, there are many issues that need to be resolved. Following are some of them.

Unique identification for privacy: each device connected to the internet should have a unique identifier. This ID is used to track the device in the ledger. Usually, this is achieved by assigning a pair of keys (public and private) to each device. However, devices like lights and CCTV cameras might not have built-in capacity to manage these cryptography keys. IP address cannot be used for this purpose due to their dynamic nature and the presence of private IP addresses.

Double spending issue resolving: mining and proof-of-work functions are used eliminate the transactions involving double spending. This is only useful while transferring assets with monetary value. In other cases, involving the transfer of data, the same information from a device can be sent to different devices at any time. But there should be some protocol to build a blockchain and append blocks to it in a systematic manner.

Secure cryptographic computation: the devices in IoT may not have the computational capacity to perform complex cryptographic calculations involved in the blockchain model. Since it is estimated that 50 billion devices will be connected to the internet by 2022, there should be enough devices online at any point of time, to perform these calculations.

Secure information exchange: while it may be relatively easy to transfer the information and maintain a ledger for devices of the same type, IoT will have different types of devices and each device might store/process different kinds of information. Maintaining all this information in a single ledger might get complex and difficult to manage. Alternatives like sidechain can be utilized to solve this problem.

Trusting the private devices: more devices mean more risk. Each device might have different vulnerabilities and if they are exploited successfully by an attacker, it might lead to a complete takeover of the device. Blindly trusting all the devices in the blockchain might be a problem. Although there are many other issues and weaknesses surrounding this technology, it is believed that its advantages outweigh these issues by a large margin.

2. BLOCKCHAIN CONSENSUS ALGORITHMS

2.1. Early cryptography

In this paragraph will explain a short detail around early cryptography and how the story of early cryptography start. Until about the 1970s, cryptography was mainly the purview of state actors. However, in the 70s, two publications brought cryptography into the public eye the US government's data encryption standard (DES), the DES, and Whitfield Diffie and Martin Hellman's publication on public key cryptography as mentioned in [15]. Figure 3 shows an algorithm of blockchain consensus security [15].

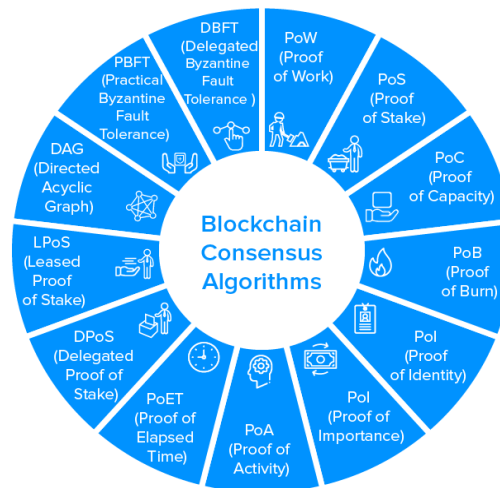


Figure 3. The algorithm of blockchain consensus security [15]

2.2. Data encryption standard (DES)

The data encryption standard is a symmetric-key, block cipher algorithm for the electronic data encryption first developed at International Business Machines Corporation (IBM), and then submitted as a candidate in an invitational study to the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), following the agency's invitation to help define a government wide standard encryption algorithm for the protection of sensitive, but unclassified electronic government data as mentioned in [16]. IBM's initial submission was modified to use S-blocks and to decrease the number of bits used for the key as suggested by the National Security Agency (NSA) before final ratification of the standard as mentioned in [17]. The final design was a symmetric key, 56-bit, block encryption algorithm using S-block, or substitution blocks.

2.3. Symmetric key algorithm

Symmetric-key or shared-key algorithms like DES are cryptographic algorithms that use the same or very mildly transformed keys for encryption and decryption of data. The keys enable the possibility of a secure communication link between 2 or more parties as mentioned in [18]. The requirement of this type of secure channel is that all parties to the communication need to know the secret keys. This fact represents the main drawback to symmetric key algorithms as the number of communicating parties increases it becomes exceedingly more complex to engineer a secure means of transferring the secret keys before the encrypted communication using the keys can begin as mentioned in [19]. Block ciphers, like DES, are cryptographic algorithms which deterministically encrypt fixed length groups of bits. In a typical block cipher implementation data is split into equal size blocks which are then transformed with a secret key seeding a mathematical transformation as mentioned in [20].

However, since each block is deterministic and unwavering, block ciphers are susceptible to an exploit called differential cryptanalysis in which output blocks are scanned for evidence of non-random behavior caused by some repeating value in the plaintext, and that information is used to reverse engineer the encryption keys. Substitution blocks, at the time a new feature in cryptography is a cryptographic algorithm in which an input of n bits is transformed into an output of m bits, and where n and m are not necessarily alike as mentioned in [21]. DES incorporated the first widely used implementation of substitution blocks in its 6×4 s-blocks in which 6 input bits were transformed to 4 output bits. S-blocks serve to obfuscate the deterministic regularities arising from simple block ciphers thus making them more resistant to differential cryptanalysis as mentioned in [22].

2.4. Early DES opposition

During the DES public comment period, parts of the proposed standard were deemed classified, and thus could not be vetted by researchers in the field. Also, it was made known that the NIST enlisted the help of the NSA in modifying the initial IBM proposal, and that made people a little bit wary. Due to the partially classified nature of the publication, the involvement of the NSA, and the introduction of heretofore unknown features in the design called S-boxes, the initial specification was immediately met with wide skepticism in the academic realm. Velliangiri and Karthikeyan [23] panned the standard in an "exhaustive cryptanalysis of the NBS data encryption standard". Primarily their concern was that the 56-bit key proposed by the standard was too short to be secure as mentioned in [24]. There was also public skepticism that the classified

implementation of the S-boxes, now known as substitution boxes, in the design represented some sort of backdoor introduced by the NSA to allow it to decrypt secure communications as mentioned in [25].

It wasn't until years later when S-boxes were rediscovered, that it was determined that the inclusion of S-boxes in the DES standard made it more secure against differential cryptanalysis. However, the NSA did push for a reduction of the key size from the originally proposed 64 bits to 48 bits. IBM pushed back and the IBM and the NSA eventually compromised on a 56-bit key. However, this weakened the standard so much, according to [26], that state actors and other organizations with deep pockets could theoretically build a computer to crack DES encryption through brute force. In [27], an early public shaming of DES they made this point in their opening introduction. Fittingly, in 1998, the electronic frontier foundation built a \$200,000 machine, well within the financial means of companies and especially governments, that cracked DES in a few days. The project was headed by John Gilmore, a founder of the cypherpunk movement and a cryptographic academic and activist as mentioned in [28]. The goal of the project was to demonstrate that DES was insecure, and that the US government had been telling deliberate lies about the security of DES for some time.

2.5. Public key cryptography

The public key cryptography is used to advocate for an asymmetric encryption algorithm with greater complexity of the 56-bit DES and the ability to agree upon a shared key over an unsecure channel. This process became known as public key encryption, and they went on to eventually patent this concept as given in [29]. The key exchange protocol is what can become to be named. Interestingly though, the concept was actually first conceptualized and secretly described in a now unclassified paper in [30]. The private key must remain secure, but the public key can be widely disseminated without fear that the encrypted data will be compromised. The security of this cryptographic system is hinged on the sheer complexity and time it would take to factor the product of the two very large prime keys with current technology.

2.6. Cypherpunks

Blockchain technology grew out of the tenants of a group of hightech privacy enthusiasts calling themselves cypherpunks. The term cypherpunk is a compound word combining root words cypher or cipher, a coded message, and punk, in this instance referencing a member of a rebellious counterculture group advocating the widespread use of cryptography to social and political change as mentioned in [31]. The cypherpunk movement traces its roots to the early days of public key cryptography. With the initial academic uproar surrounding the distrust of the NSA's involvement in the manipulation of DES, and the secrecy in which the implementation of the algorithm was shrouded in, there began the seeds of dissent and the onus for the beginnings of the cypherpunk movement. The eerily prescient early focus of the small, mostly online group was on discussing individual privacy in a digital world, government monitoring, and central authority control of information, all issues which are in national conversation today. The cypherpunk group began a meeting of tech-minded individuals with developmental leanings founded by Eric Hughes, Tim May, and John Gilmore. These three together with 20 of their friends began meeting regularly in the offices of John Gilmore's company, Cygnus, a stalwart of the burgeoning opensource community, in the early 1990s as mentioned in [32]. Their meetup shortly morphed into a mailing list to broaden its appeal and to attract likeminded individuals from around the world. One of their primary concerns was that of governments and large powerful corporate entities capturing information, as described the problem in a speech at the first association for computing machinery (ACM) conference on computers.

"In most of Europe, phone companies don't record the phone numbers when you call, and they don't show up on your bill. They only tick off the charges on a meter. Now, I was told that this is partly because the Nazis used the call records that they used to have, to track and identify the opposition after taking over those countries in World War II. They don't keep those records anymore."

The mailing list's topics and tenor favored privacy in communications, self-revelation, financial privacy, anonymity, and pseudonyms. It also derided and actively opposed government data collection, forced self-revelation, and censorship as mentioned in [33]. It is notable that an early and very active, member of the cypherpunk mailing list was infamy, who has made it his life's mission to expose corruption and abuse of power. However, since each block is deterministic and unwavering, block ciphers are susceptible to an exploit called differential cryptanalysis in which output blocks are scanned for evidence of non-random behavior caused by some repeating value in the plaintext, and that information is used to reverse engineer the encryption keys. Privacy in communication was a primary concern of the movement, but equally important to the movement were discussions around financial privacy, as Eric Hughes, one of the founders, puts it in his cypherpunk manifesto as given in [34].

“When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.”

2.7. Directed acyclic graph (DAG) in Bitcoin

In this section given detail about the DAG in Bitcoin, From this primordial stew of technologist, university researchers, cryptographers, a love of privacy in communication and in financial transactions, and a general mistrust of central authorities an anonymous, short but groundbreaking paper, was mailed to the cypherpunk mailing list in 2008 by Satoshi Nakamoto, fittingly an alias, describing an electronic currency, Bitcoin, based upon cryptographic principals akin to asymmetric encryption, one-way functions, but in reverse using the DAG as mentioned in [35]. While Bitcoin was not the first digital currency created, it was the first to solve the problem of double spending and the first to do it without the need for a central authority regulating the transaction. Figure 4 will show the major characteristics of blockchain in terms of transaction [35].

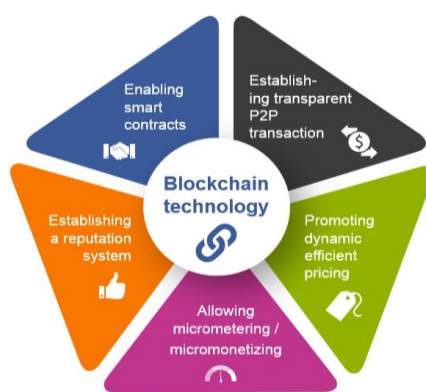


Figure 4. The major characteristics of blockchain in terms of transaction [35]

2.8. Secure hashing algorithm (SHA)

Hashing algorithm in blockchain can be considered for the motivation is a simple sign up process on securing the application with hashing function. If a user, along the way, does not feel comfortable with the type of personal information sharing she agreed on while sign up the only choice that remains with her is to re-sign up as mentioned in [36]. The hashing structure is presented as an access control manager. A user's data sits in an off-blockchain storage and permissions related to access of this data by any sort of third parties is set by a user by making a transaction to the blockchain. This way the data access information for a piece of user data is mined in a distributed and trusted manner in a block of a blockchain as mentioned in [37]. Such as an access control system provides long chain for blockchain for the owners of the data to either modify or completely revoke the permissions related to their data. These permissions can be modified/revoked in a per-service manner or in a collective way (same action that affects permission level of all the services at the same time).

One extension to the work can be to only return the computation nodes on one's data and record it on top of blockchain as mentioned in [28]. This means third parties are not given access to the raw data of a user (which they can store locally for later use) rather only the result of using this data is published and recorded on blockchain. This way if a third party tries to behave maliciously the record of this computation may be presented in a court of law to prove this behavior.

A mismatch final output between the record extracted using a blockchain receipt and the corresponding provenance data stored in a separate database, then the output can raise an alarm for a possible break in [38]. The blockchain can never be attacked the cloud service provider with one application on the wallets of users for taking the coins out of it. There should be a system that allows users to control and own their data all the time yet at the same time giving third parties a set of permissions to use their data. This set should be modifiable on the go with the extreme case of this set being empty, i.e., a user can revoke a service/application's right to access her data at any time she wants. Figure 5 shows the blocks that have been created by encryption and Figure 6 shows the secure hash algorithm works on choosing the longest chain with hash function [37]. Figure 7 shows the secure hash algorithm works on choosing the longest chain with hash function [38] and Figure 8 show an example of secure hashing being performed on text [39].



Figure 5. The blocks that have been created by encryption

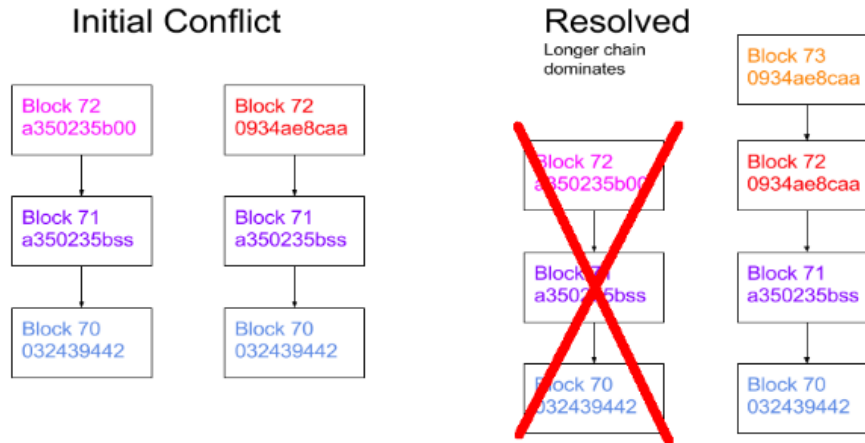


Figure 6. The secure hash algorithm works on choosing the longest chain with hash function

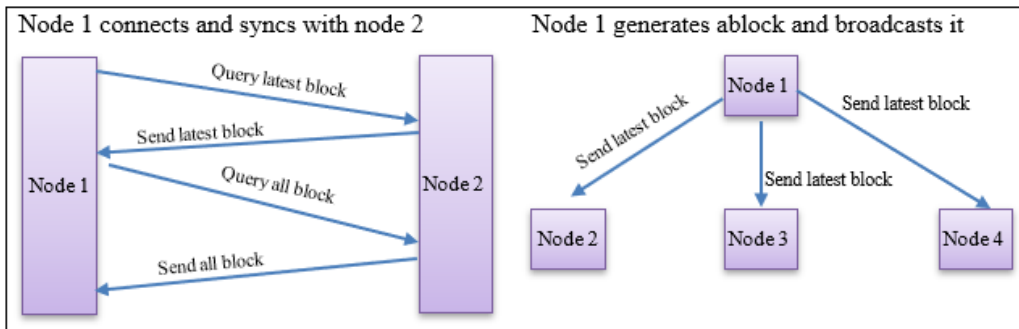


Figure 7. The secure hash algorithm works on choosing the longest chain with hash function



Figure 8. Example of secure hashing being performed on text

2.9. Digital signature algorithm (DSA)

The digital signature algorithm minimizes the attacks that have been carried out on the blockchain network with a system that allows malicious users to control and own blockchain data all the time yet at the same time giving third parties a set of permissions to use unauthorized blockchain data as mentioned in [40].

Tracking the attacks is a piece of techniques can help detect different anomalies, break ins and data access violations thus improving users' privacy and integrity of data. Blockchain attacks particularly important to control in current age of cloud computing where most of users' data sit in a storage facility of third parties. Even if the thirdparty cloud storage providers implement a data provenance system the users still have to trust the third parties in their claim that such a system is trustworthy as given in [41]. If, however, we apply the blockchain paradigm to implement a data provenance system then a distributed and trusted data provenance system might be possible.

- Distributed denial of service
- Transaction malleability attacks
- Timejacking
- Routing attacks
- Sybil attacks
- Eclipse attacks
- Long range attacks on proof of stake networks
- User wallet attacks
- Selfish mining

A separate routing attack attacks the database is also maintained to record all of these operations on a file object. A Blockchain transaction begins with two willing parties to a transaction. The payer's equity stake, or coin, is recorded as a transaction in a chain of cryptographic blocks secured with his public key, a hash, and the private key of the person he bought his equity stake from and embedded in a "proof of work" block. There might be a silver lining if a framework is developed powered by techniques such as formal verification of code like the one privacy uses in its system as mentioned in [42]. The split in Bitcoin that resulted in new currency system called Bitcoin Cash was the result of a heated debate to address the scalability issue. An auditor is then provided with a blockchain receipt containing the information of block number and a transaction ID that tracks a certain set of operations that the auditor is interested in. Since Sybil attacks the block that is mined using a distributed consensus protocol a user does not have to trust a third party for the integrity of blockchain data. Figure 9 shows the encryption is done with digital signature using secure private key [42].

Paper intends to study its extension to multiple security providers with different applications in combination with the data ownership use case as discussed in the last section to study the overall ownership/privacy preserving auditable system as mentioned in [43]. Besides this digital signature algorithm to block the attacks are malicious types of attacks on blockchain network that studies the verifiable cloud computing using smart contracts in blockchain networks. These types of attacks make use of game theoretic techniques to study the aspect of collusion between two cloud providers for a same computation task. When both the providers return result a cross check can establish the existence or absence of collusion between them. Studying how efficient, in terms of overhead, it is to implement these systems alongside simple cloud storage and computing. Figure 10 shows the decryption is done with digital signature using secure public key [42].

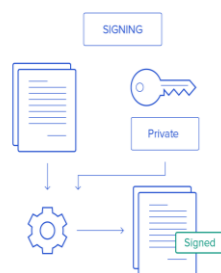


Figure 9. The encryption is done with digital signature using secure private key

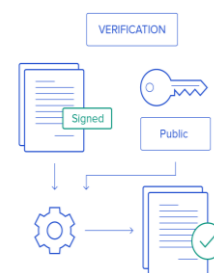


Figure 10. The decryption is done with digital signature using secure public key

2.10. Proof-of-Work (PoW) algorithm

This PoW algorithm portion of the framework manages the protocols and decisions related to the underlying blockchain security system. These could include the block size or which consensus protocol to use. An informed decision could be made by a policy-making body in an iterative manner. Each iteration can consider the feedback from the underlying blockchain network as given in [44]. This feedback can be in the form of smart contract execution data stored on blockchain. This can lead to a more systematic approach of development i.e., a system prototype that can be tested and improved in an iterative manner, like described above, before deploying it into the real world. Figure 11 shows the topologies of proof of work algorithm [44].

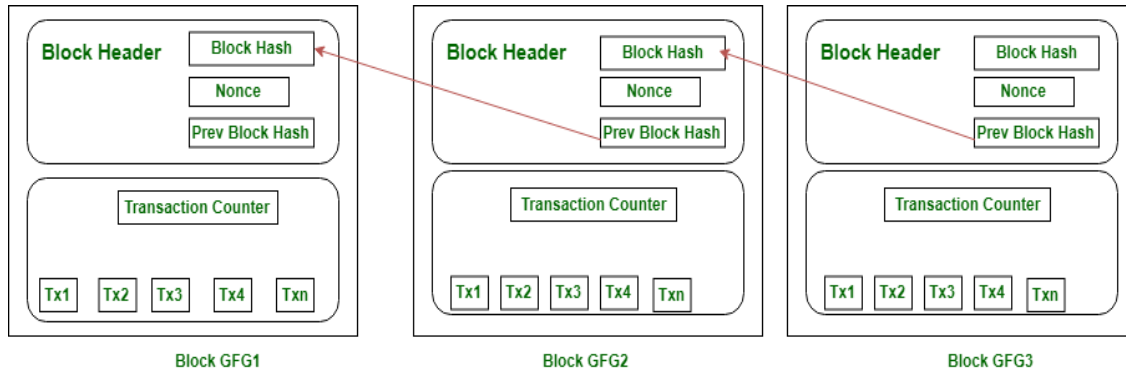


Figure 11. The topologies of proof of work algorithm

The PoW cryptography in blockchain is envisioned by encryption/decryption the sequences, this cryptography technique can be implemented to attach certain guarantees to the smart contract code developed after the deliberation on human-policy making level. The main aim of cryptography is to decouple, as much as possible, the human logic and decision making to its implementation in the form of smart contract code as given in [45]. The purpose is to make the code development as trustworthy as possible while mostly holding the actual human thinking accountable.

3. BLOCKCHAIN TECHNOLOGY

One of Blockchain’s core strengths is its ability to allow for a verifiable transaction to take place without the need for central database or oversight authority. Traditional transactions require a central authority overseeing or simply recording the transaction to prevent fraud and to provide a verifiable record of has transpired as mentioned in [46]. Blockchain supplants this requirement with “cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party”. The consequences of this breakthrough are hard to overstate. A Blockchain transaction begins with two willing parties to a transaction. The payer’s equity stake, or coin, is recorded as a transaction in a chain of cryptographic blocks secured with his public key, a hash, and the private key of the person he bought his equity stake from and embedded in a “proof of work” block. The payer then digitally signs a hash of this prior transaction and the public key of the next owner with his private key and then adds this to the end of the coin as mentioned in [47]. The payee can then verify the signatures to verify the chain of ownership. However, since each block is deterministic and unwavering, block ciphers are susceptible to an exploit called differential cryptanalysis in which output blocks are scanned for evidence of non-random behavior caused by some repeating value in the plaintext, and that information is used to reverse engineer the encryption keys. This one-way cryptographic hash is computationally impractical to reverse, and thus this interaction secures the ownership chain; however, it doesn’t provide a means to prevent a bad actor from duplicating (double spending) or reversing a transaction. Table 1 shows the comparison of blockchain usage with different prescribed algorithms.

Table 1. The comparison of blockchain usage with different prescribed algorithms

Articles	Purpose	Algorithm
[48]	Cross-border payments	DES
[49]	NFT marketplaces	PoW
[50]	Secure sharing of medical data	RSA
[51]	Personal identity security	SHA-256

4. CONCLUSION

The world is fast approaching a time as a society in which ownership of an asset like a bicycle or a car, or any other type of asset need not be represented by a signed piece of paper which can be lost stolen or forged. Ownership can be represented as a digital asset in an immutable cryptographically secured database in much more secure and verifiable manner than traditional means. Our team has prepared a demonstration of a simple blockchain network hosted in the world. In this demonstration we take some liberties and we do not follow the best practice of diversifying the nodes as they are all going to be hosted on the same provider,




and obviously controlled by the same users, us. However, these are reasonable simplifications for a development or demonstration environment. This paper assignment is intended to describe the blockchain algorithm with the prerequisite knowledge of the field and the use cases for securing the blockchain. This paper extensively looked at different use cases of data ownership and provenance with security. Studying the implications that may arise after blockchain is implemented for a particular use case. Other purpose is to compare the exiting state-of-the-art techniques that try to solve the issues such as scalability, regulation and data ownership and provenance in blockchain-based ecosystems. The work to write a paper based on this plan is already underway. As a result, the whole community was not taken on board during such events thus breaching the original idea of immutability and decentralization of the blockchain technology. If, however, an efficient hashing and transaction framework was existed to tackle this type of situation then such a split could have been avoided. This motivates me to study the aspect of governance by the blockchain in a more systematic manner.

REFERENCES




- [1] H. Chauhan *et al.*, "Blockchain Enabled Transparent and Anti-Counterfeiting Supply of COVID-19 Vaccine Vials," *Vaccines*, vol. 9, no. 11, 2021, doi: 10.3390/vaccines9111239.
- [2] I. Al Barazanchi *et al.*, "Blockchain Technology - Based Solutions for IOT Security," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp. 53–63, 2022, doi: 10.52866/ijcs.m.2022.01.01.006.
- [3] S. Sharma, A. Kumar, M. Bhushan, N. Goyal, and S. S. Iyer, "Is Blockchain Technology Secure to Work On?," *Blockchain and AI Technology in the Industrial Internet of Things*, IGI Global, 2021, pp. 66–80, doi: 10.4018/978-1-7998-6694-7.ch005.
- [4] R. Al-Amri, R. K. Murugesan, E. M. Alshari, and H. S. Alhadawi, "Toward a Full Exploitation of IoT in Smart Cities: A Review of IoT Anomaly Detection Techniques," *International Conference on Emerging Technologies and Intelligent Systems*, pp. 193–214, 2022. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-85990-9_17
- [5] H. R. Hasan and K. Salah, "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts," in *IEEE Access*, vol. 6, pp. 65439–65448, 2018, doi: 10.1109/ACCESS.2018.2876971.
- [6] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *International Conference on Principles of Security and Trust*, vol. 10204, pp. 164–186, 2017, doi: 10.1007/978-3-662-54455-6_8.
- [7] Y. K. Salih, O. H. See, S. Yussof, A. Iqbal, and S. Q. M. Salih, "A proactive fuzzy-guided link labeling algorithm based on MIH framework in heterogeneous wireless networks," *Wireless Personal Communications*, vol. 75, no. 4, pp. 2495–2511, 2014, doi: 10.1007/s11277-013-1479-z.
- [8] A. Moghimi, G. Irazoqui, and T. Eisenbarth, "Cachezoom: How sgx amplifies the power of cache attacks," in *International Conference on Cryptographic Hardware and Embedded Systems*, 2017, pp. 69–90, doi: 10.1007/978-3-319-66787-4_4.
- [9] I. Al Barazanchi *et al.*, "Blockchain: The Next Direction of Digital Payment in Drug Purchase," *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022, pp. 1-7, doi: 10.1109/HORA55278.2022.9799993.
- [10] M. Shuaib, S. M. Daud, S. Alam, and W. Z. Khan, "Blockchain-based framework for secure and reliable land registry system," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 18, no. 5, pp. 2560–2571, 2020, doi: 10.12928/TELKOMNIKA.v18i5.15787.
- [11] J. Li *et al.*, "Internet of things assisted condition-based support for smart manufacturing industry using learning technique," *Computational Intelligence*, vol. 36, no. 4, pp. 1737–1754, 2020, doi: 10.1111/coin.12319.
- [12] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on bitcoin, and how to protect against them," *Quantum Science and Technology*, 2017, doi: 10.48550/arXiv.1710.10377.
- [13] E. Kiktenko, *et al.*, "Quantum-secured blockchain," *Quantum Science and Technology*, vol. 3, no. 3, 2018, doi: 10.48550/arXiv.1705.09258.
- [14] A. Aborujilah, M. N. M. Yatim, and A. Al-Othmani, "Blockchain-based adoption framework for authentic land registry system in Malaysia," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 19, no. 6, pp. 2038–2049, 2021, doi: 10.12928/TELKOMNIKA.v19i6.19276.
- [15] E. B. -Sasson, Y. Bentov, Y. Horeish, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," *IACR Cryptology ePrint Archive*, 2018. [Online]. Available: <https://eprint.iacr.org/2018/046.pdf>
- [16] O. O. Malomo, D. B. Rawat, and M. Garuba, "Next-generation cybersecurity through a blockchain-enabled federated cloud framework," *The Journal of Supercomputing*, vol. 74, pp. 5099–5126, 2018, doi: 10.1007/s11227-018-2385-7.
- [17] A. Adebayo, D. B. Rawat, L. Njilla, and C. A. Kamhoua, "Blockchain-enabled information sharing framework for cybersecurity," *Blockchain for Distributed Systems Security*, pp. 143–158, 2019. [Online]. Available: https://books.google.co.id/books?hl=id&lr=&id=dhaMDwAAQBAJ&oi=fnd&pg=PA143&dq=Blockchain-enabled+information+sharing+framework+for+cybersecurity&ots=QU4fddNupv&sig=edpKP3Rd4F_gOMzdyIjhjVLb4fw&redir_esc=y#v=onepage&q=Blockchain-enabled%20information%20sharing%20framework%20for%20cybersecurity&f=false
- [18] Divya M. and N. B. Biradar, "IOTA-next generation block chain," *International Journal of Engineering And Computer Science*, vol. 7, no. 4, pp. 23823–23826. [Online]. Available: <https://ijecs.in/index.php/ijecs/article/view/4007/3798>
- [19] S. R. A. Ahmed, I. Al Barazanchi, Z. A. Jaaz, and H. R. Abdulshaheed, "Clustering algorithms subjected to K-mean and gaussian mixture model on multidimensional data set," *Periodicals of Engineering and Natural Sciences*, vol. 7, no. 2, pp. 448–457, 2019. [Online]. Available: <http://pen.ius.edu.ba/index.php/pen/article/view/484/297#>
- [20] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new-type of blockchain for secure message exchange in VANET," *Digital Communications and Networks*, vol. 6, no. 2, pp. 177–186, 2020, doi: 10.1016/j.dcan.2019.04.003.
- [21] T. A. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations," in *IEEE Access*, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.
- [22] I. Al-Barazanchi, Z. A. Jaaz, H. H. Abbas and H. R. Abdulshaheed, "Practical application of IOT and its implications on the existing software," *2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI)*, 2020, pp. 10-14, doi: 10.23919/EECSI50503.2020.9251302.
- [23] S. Velliangiri and P. Karthikeyan, "Blockchain Technology: Challenges and Security issues in Consensus algorithm," *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020, pp. 1-8, doi: 10.1109/ICCCI48352.2020.9104132.

- [24] N. B. Somy *et al.*, "Ownership Preserving AI Market Places Using Blockchain," *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 156-165, doi: 10.1109/Blockchain.2019.00029.
- [25] S. Vyas, M. Gupta, and R. Yadav, "Converging Blockchain and Machine Learning for Healthcare," *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 709-711, doi: 10.1109/AICAI.2019.8701230.
- [26] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, 2020, doi: 10.3390/electronics9091338.
- [27] V. Shrivastava and S. Kumar, "Utilizing Block Chain Technology in Various Application Areas of Machine Learning," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 2019, pp. 167-171, doi: 10.1109/COMITCon.2019.8862203.
- [28] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *International Conference on Financial Cryptography and Data Security*, 2015, pp. 112-126, doi: 10.1007/978-3-662-48051-9_9.
- [29] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *International Conference on Financial Cryptography and Data Security*, 2016, pp. 43-60. [Online]. Available: <https://eprint.iacr.org/2016/056.pdf>
- [30] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," *arXiv preprint*, 2017, doi: 10.48550/arXiv.1708.04748.
- [31] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 15-29, doi: 10.48550/arXiv.1405.7418.
- [32] S. Noether, "Ring signature confidential transactions for monero," *IACR Cryptology ePrint Archive*, 2015. [Online]. Available: <https://eprint.iacr.org/2015/1098.pdf>
- [33] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *2015 IEEE Symposium on Security and Privacy (SP)*, 2015, pp. 122-134, doi: 10.48550/arXiv.1410.6079.
- [34] Z. A. Jaaz, S. S. Oleiwi, S. A. Sahy, and I. Albarazanchi, "Database techniques for resilient network monitoring and inspection," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 18, no. 5, pp. 2412-2420, 2020, doi: 10.12928/TELKOMNIKA.v18i5.14305.
- [35] E. -R. Latifa, E. K. M. Ahemed, E. G. MOHAMED, and A. OMAR, "Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures," *Journal of Internet Banking and Commerce*, vol. 22, no. 3, pp. 1-29, 2017. [Online]. Available: <https://www.icommercentral.com/open-access/blockchain-bitcoin-wallet-cryptography-security-challenges-and-countermeasures.php?aid=86561>
- [36] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, "A first look at the usability of bitcoin key management," *arXiv preprint*, 2018. [Online]. Available: https://www.researchgate.net/publication/300925188_A_First_Look_at_the_Usability_of_Bitcoin_Key_Management
- [37] A. H. Mohammed and R. M. A. Hussein, "Security Services for Internet of Thing Smart Health Care Solutions Based Blockchain Technology," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 20, no. 4, pp. 772-779, 2022, doi: 10.12928/TELKOMNIKA.v20i4.23765.
- [38] X. Wang *et al.*, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10-29, 2019, doi: 10.1016/j.comcom.2019.01.006.
- [39] Z. Zheng, S. Xie, H. -N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352-375, 2018. [Online]. Available: https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey
- [40] A. Panarello, N. Tapas, G. Merlino, F. Longo and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, 2018, doi: 10.3390/s18082575.
- [41] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653-659, 2017, doi: 10.6633/IJNS.201709.19(5).01.
- [42] O. W. Purbo, S. S. Riyanto, Suhendro, R. A. Aziz, and R. Herwanto, "Benchmark and comparison between hyperledger and MySQL," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 18, no. 2, pp. 705-715, 2020, doi: 10.12928/TELKOMNIKA.v18i2.13743.
- [43] A. Narayanan, J. Bonneau, E. Felten, A. Miller and, S. Goldfeder, "Bitcoin and Cryptocurrency Technologies," *Curso Elaborado Pela*, 2016. [Online]. Available: https://www.lopp.net/pdf/princeton_bitcoin_book.pdf
- [44] S. Q. Salih, A. R. A. Alsewari, and Z. M. Yaseen, "Pressure vessel design simulation: Implementing of multi-swarm particle swarm optimization," *ICSCA '19: Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 2019, pp. 120-124, doi: 10.1145/3316615.3316643.
- [45] J. C. Augusto, V. Callaghan, D. Cook, A. Kameas and I. Satoh, "Intelligent environments: a manifesto," *Human-centric Computing and Information Sciences*, vol. 3, no. 12, 2013, doi: 10.1186/2192-1962-3-12.
- [46] L. Roalter, M. Kranz and A. Möller, "A middleware for intelligent environments and the Internet of Things," *International Conference on Ubiquitous Intelligence and Computing*, 2010, pp. 267-281, doi: 10.1007/978-3-642-16355-5_23.
- [47] M. Ryu, J. Kim, and J. Yun, "Integrated semantics service platform for the Internet of Things: a case study of a smart office," *Sensors*, vol. 15, pp. 2137-2160, 2015. [Online]. Available: https://www.researchgate.net/publication/271222532_Integrated_Semantics_Service_Platform_for_the_Internet_of_Things_A_Case_Study_of_a_Smart_Office
- [48] W. -T. Tsai, R. Blower, Y. Zhu, and L. Yu, "A System View of Financial Blockchains," *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2016, pp. 450-457, doi: 10.1109/SOSE.2016.66.
- [49] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016. [Online]. Available: <https://eprint.iacr.org/2016/555.pdf>
- [50] L. Luu, D. -H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 254-269. [Online]. Available: <https://eprint.iacr.org/2016/633.pdf>
- [51] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 839-858, doi: 10.1109/SP.2016.55.




BIOGRAPHIES OF AUTHORS

Haider Hadi Abbas    received the B. Sc. degree in electronics and communication engineering from Baghdad University in 1994, Baghdad, Iraq, the M. Sc. degree in electronics engineering from University of Technology in 1997, Baghdad, Iraq, and Ph. D. degree in communications engineering from Baghdad University, Baghdad, Iraq in 2001. He has been an assistant professor of data and information security since 2014. He has authored more than 25 refereed journal and conference papers. His research interest includes data and information security, machine learning, internet of things, cloud related issues. He can be contacted at email: haider.hadi@muc.edu.iq.



Montadher Issam Abdul Kareem    received the B. Sc. degree in computer science from University of Technology in 2009, Baghdad, Iraq, the M. Sc. degree in Computer science and communication from AUL University in 2013, Beirut, Lebanon. He has been an assistant Teacher of data and information security since 2018. He has authored more than 2 refereed journal and conference papers. His research interest includes data and information security, machine learning, cloud related issues, computer applications, and networking. He can be contacted at email: montadhar.issam@muc.edu.iq.



Hassan Muwafaq Gheni    received his Bachelor (B. Sc) of Electrical and Electronic Engineering from Department of Electrical Engineering, Babylon university-Iraq-hilla in June 2016. In February 2018, he entered the master's program at the Faculty of Electrical and Electronic Engineer, Universiti Tun Hussein Malaysia. He is a lecturer at Al-Mustaqbal university college/ Department of Computer Techniques Engineering His research interest is optical communication, IoT, Wireless sensor Network, Communications, V2V system, Artificial intelligent. He can be contacted at email: hasan.muwafaq@mustaqbal-college.edu.iq.