# Blockchain and Security Services

Marcel Njighe-Tezeh

Cybersecurity, Wilmington University

Cyb8101: Research Seminar

Professor Maureen Mcwhite

Nov 27, 2022

**Introduction**

Blockchain technology is often hailed as a technology that will change the world, and in many respects, it will. However, contrary to what many evangelists would have you believe, it is not always the all-encompassing answer to the world's security problems (Marr, 2021). While the adoption of blockchain has skyrocketed, so has the number of attacks compromising the security and trust in the ecosystem. Smart contracts and decentralized applications are paving the way to new business models and a revolutionary new autonomous incarnation of the internet. And security must be ingrained from day one.

**Definition of the Problem**

This research will focus on the body of knowledge available on leveraging blockchain as an additional innovation for cyber security solutions. The major goal of this study is to provide a community-driven starting point for more extensive research in cyber security for blockchain technology. In this era of advanced technology, supported by data driven decisions, there is a need to review how blockchain security mechanisms can help reduce the gap that traditional security services face today.

Lack of regulation makes the blockchain dangerous and raises concerns about its cybersecurity models. This primarily affects Bitcoin and other value-based blockchain networks. But the reality is that it's an extremely volatile market, as many people who have just invested in Bitcoin or other cryptocurrencies for the first time have discovered to their cost. Scams and market manipulation are widespread because of the absence of governmental control. But with its decentralized, distributed, and consensus-based protocols, this study will seek to review how it reduces the issues we have in centralized systems.

Blockchain technology is the spine of Web3.0, crypto, NFTs, and the metaverse. Researching, developing, and implementing security measures to understand the security maturity of the blockchain technology and its distributed applications (dApps) is of the essence as their day-to-day importance has been fast growing. With this growth, a much need literature is needed to understand how its built-in security protocols can extend to addressing security in traditional services like authentication, data privacy, data integrity, data confidentiality, non-repudiation, data provenance, etc,.

**Research Question**

Innovative technologies strive to influence cyber-security innovation from a scientific and practical standpoint. The use of blockchain technology may change or eliminate security paradigms in traditional security services that are based on centralized models of access rights, models of computation, models of distributed computing, and or models with no specific theoretical definition.

A qualitative and systematic literature is required to examine how distributed blockchain security mechanisms can be used to close the gap that exist in security services such as authentication, data privacy, data integrity, data confidentiality, non-repudiation, and data provenance. A literature will help comprehend the change before its full acceptance because there hasn't been much research on blockchain technology in the context of its security. This study examines the development of Blockchain's security systems in a methodical manner. The rest of the literature is then reviewed based on the literature issue of how Blockchain, through its security mechanisms and characteristics, is the remedy to security services concerns, which is derived from the link between the mechanism and its key attributes.

The primary research question, which is based on the study objective, is:

* **Are blockchain security mechanisms an antidote to the gap and overhead that exist in cyber security?**

The following two sub-questions have been developed to help this research answer the main research question.

* **Are blockchain security mechanisms susceptible to any attacks?**

From the lens of security, this question will help look at the blockchain technology attack surface and potential attack vectors by applying a four-factor security model to cover the security aspects of the blockchain ecosystem and its consensus protocols, smart-contracts programming, and third-party services, such as wallets, exchanges, and Oracles. And finally, the end user.

* **How can blockchain technology influence the innovation of cyber security models?**

For this thesis, it is essential to develop a certain grasp of the possibilities and cooperativeness that blockchain technology offers because it is still a relatively new concept and has numerous definitions. I will use a range of technical and non-scientific materials from the previous questions to develop findings geared toward security models. This question is answered in the discussion of findings and recommendations.

**Problem Justification**

**To the best of my analysis, only a few Systematic Literature Reviews (SLR) have been conducted specifically about the use of blockchain to address the issue of cyber security. Salman et al. completed one of the most current surveys in the field of blockchain and cyber security. The paper emphasizes the difficulties and issues that come with using security services in centralized architectures across a range of application areas. They offer a thorough analysis of the most recent blockchain-enabled techniques for these security service applications (Salman et al., 2019b).**

**In order to find out what research findings have been published in respect to the overall idea of blockchain technology, Yli-Huumo et al. did an SLR in 2016. They concentrated on publications regarding blockchain technology, excluding studies on law, economics, and regulations (Yli-Huumo et al., 2016). In instance, they discovered that the common topics of security and privacy are discussed in 80% of the research articles about Bitcoin specific initiatives and not blockchain as an ecosystem. This research aims to ascertain what research works are already available especially in the fields of cyber security and blockchain applications given the diversification of blockchain applications since 2016 (Seebacher & Schüritz, 2017).**

**Conoscenti et al. performed an SLR in 2016 on the use and scalability of blockchain technology, particularly in regard to the Internet of Things and other peer-to-peer devices. They emphasized how the blockchain might be used to detect data misuse without a centralized reporting system (Conoscenti et al., 2016). This serves as the foundation for my analyses into the potential impact of blockchain on cyber security issues.**

In conventional centralized systems, the fundamental security services are expensive, prone to a single point of failure, and requires a trusted third party to implement authentication and encryption (Aste et al., 2017). These are the three of the significant obstacles that Blockchain mechanisms can address significantly.

Existing published research is limited to a few blockchain technology areas, making it difficult to determine industry-wide blockchain security protocols and vulnerabilities. Existing research has a narrow scope, focusing on the top-level layers such as smart contracts, oracles, end-users, etc., and not the effect of attacks on the entire blockchain infrastructure or the implementation of blockchain security mechanisms. Existing research also fails to address and analyze real-world incidents that evolve around existing technology weaknesses (Xu et al., 2014).

Many of the vulnerability types that exist in conventional software are listed in the Common Weakness Enumeration (CWE) dictionary, which is available online. A crucial resource is CWE. It serves as the foundation for the kinds of vulnerabilities that many code-scanning technologies attempt to find. CWE does not, however, specifically address blockchain or smart contracts (Seifried, 2021).

All of the aforementioned earlier studies provide answers to concerns about the more general application of blockchain technology, but they do not particularly look at how it may be used to enhance cyber security measures. Blockchain research is a relatively new area of study, but it is developing swiftly. In order to direct future research efforts, it is vital to present a current synthesis of the most recent research works, particularly in the fields of blockchain and cyber security.

.

**Methodology**

This study seeks to close a knowledge gap by investigating how blockchain technology can affect cybersecurity innovation in the context of a distribution system's operation. Because the phenomena being studied are extremely complicated, abstraction is utilized to keep the study's scope within the theoretical framework. Specifically, very novel blockchain technology phenomena are examined in the context of the security of the blockchain distribution system.

**Research Design**

The research statement problem is approached by first demystifying blockchain by providing an overview of what blockchain is, and its architecture. This study discusses security services based on blockchain technology. As a result, solutions like authentication, privacy, integrity, and confidentiality are reviewed. Since public key cryptography offers both authentication and confidentiality, these two are bundled in one chapter. The remaining chapters are devoted to privacy and integrity.

Authentication, privacy, decentralization, consensus, and cryptography are used in the fundamental design of blockchain technology to ensure that transactions are effectively tamper-proof, and meets confidentiality, integrity, and availability (CIA) requirements.

The study examines the key properties of blockchain.It further defines the implementation of blockchain security services, review mining on blockchain, and discuss the traditional security services with their issues and how the issues can be addressed by implementing blockchain security protocols.

**Research method**

This study is derived from a mixed method of research using Google Scholar, ScienceDirect, IEEE Xplore and Arxiv.org as primary search databases. The keywords were chosen to stimulate the creation of study findings that would aid in addressing the study's issues. Depending on the search platforms, the title, keywords, or abstract were used in the searches. In accordance with the recommendations provided by Kitchenham and Charters, an evaluation of the primary studies' quality was conducted. This made it possible to evaluate the studies' applicability to the areas of research while considering any indications of bias in the study and the reliability of the analytical outcomes.

Key search terms used were blockchain OR block-chain And security services OR cybersecurity OR cyber security to narrow down the data. With the use of the operators “OR, AND”, they further filtered out the most relevant data. Only information that complies with the following criteria was taken into account for extraction —requirements: research must convey scientific findings relating to the use of blockchain applications, constitute knowledge about blockchain or attributed distributed ledgers, and be a peer-reviewed work that has been accepted for publication in a symposium procedure or bulletin. These requirements were applied to the total number of 678 initial search results pulled for all the primary databases, which came out that 58 met the requirements for further analysis and use in this study.

**Literature Review**

This study intends to concentrate on the body of material that already exists on using blockchain as a supplementary innovation for cyber security solutions. This study's primary objective is to offer a community-driven launchpad for a more thorough research investment in blockchain technology’s cyber security domain. Salman et al. conducted one of the most current studies in the field of blockchain and cyber security about the usage of blockchain technology to address the issue of cyber security. In the research a possible research direction on the ability of Blockchain mechanisms to address services was raised.

This research reviews in a systematic design — the maturity of Blockchain’s security mechanisms. The rest of the literature from there is stemmed from the mechanism’s relationship with its key properties, and then, review based on the literature question of how Blockchain through its security mechanisms and properties is the antidote to security services problems.

1. **Demystifying Blockchain**
2. ***What is blockchain?***Blockchain is a distributed ledger with a cryptographic foundation that permits trusted transactions between network members who are not trusted (Taylor et al., 2019). Organizational bureaucracies operate to control the actions of social and economic communities in a centralized system. Blockchain makes it possible to create novel business models, inventive organizational structures, or new working and producing methods where access is valued over ownership and sharing of the property (Moudoud et al., 2019).

Blockchain is a technique that leverages user-to-user replication of ledgers to keep their contents synchronized (Aste et al., 2017). Blockchain is a fundamental technology that paves the way for the paradigm designed and engineered to trust people to trust nodes and from "centralized" to "decentralized" governance, regardless of its initial system solutions and use.

A new generation of intermediary-free decentralized applications could be made possible by blockchain (Taylor et al., 2019). which could also act as the framework for essential components of infrastructure for internet security.

1. ***Blockchain App*.** Bitcoin is a cryptocurrency that utilizes blockchain technology, its network, and specific protocols are example of distributed and decentralized systems.
2. ***Smart contracts and dApps.*** A "smart contract" is a computerized transaction protocol that executes the provisions of a contract, according to Nick Szabo, a computer scientist and legal researcher, who coined the phrase in 1994. A computer program called a "smart contract" is a grouping of data and code that is saved and run on the blockchain. They're put into use on the blockchain. Any user can engage with a smart contract and carry out its role by nature. Smart contracts are vulnerable to cyberattacks because of their distinctive property. (Szabo 1994).
3. **Blockchain Security Mechanisms and Security Services**

Authentication, data privacy, data integrity, data confidentiality, non-repudiation, and data provenance are the six security services that exist in the blockchain ecosystem (Salman et al., 2019). These services, implemented and mapped to the family of ISO/IEC 27001 security standards, set the basic foundation of Blockchain's security mechanism.

Blockchain's authentication mechanism ensures that only reliable nodes are utilized to offer services by detecting and removing unauthorized connections and requests (Akram et al., 2022). Only the verified nodes on a blockchain network are trusted. The immediate usefulness of data mining creates a serious problem with data sensitivity, integrity, confidentiality, non-repudiation, and provenance (Xu et al., 2014). As analyzed in subsequent stanzas, blockchain's encryption, data signatures, authentication by a private key, and role-based mechanisms are employed to mitigate and remediate these security issues. **Table 1**is a summary of these security services and their corresponding mechanisms.

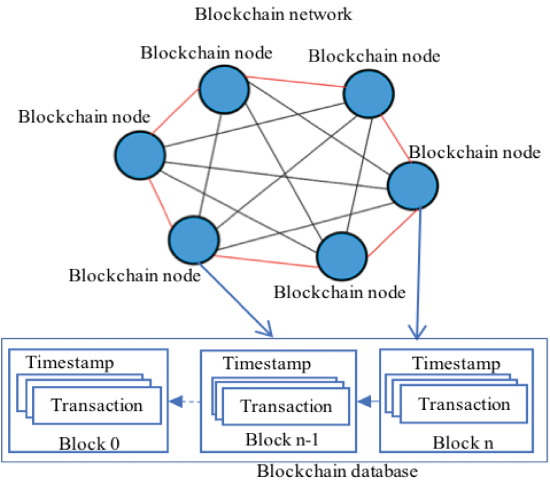
**Table I:** Security Services

|  |  |
| --- | --- |
| **Services** | **Security Mechanisms** |
| Data Confidentiality | Encryption and Public Key Cryptography |
| Data Privacy | Encryption, Access Control, and Public Key Cryptography |
| Data Integrity | Authentication code |
| Authentication | Encryption, Public Key Cryptography, and Digital Signature |
| Non-repudiation | Digital Signature and Public Key Cryptography |

1. **Blockchain Architecture**

Blockchain is a distributed system that enables the building of trust amongst untrustworthy people who communicate and do business with one another (Moudoud et al., 2019). The Blockchain architecture makes use of peer-to-peer network protocols to evaluate and validate communication among users, as shown in fig 1. It is made up of a network of connected nodes and a decentralized database.

**Figure 1:** Blockchain network, blocks, transactions, and database.



The blockchain platform is made up of a distributed ledger that records and manages transactions across blockchain networks (Saghiri, 2019). The platform is the backbone of the blockchain ecosystem. Its consensus protocol layer offers the capacity to validate transactions (Tabatabaei et al., 2022).

It is architected to accommodate external services and, thus, may be utilized by end users and decentralized apps. Users can store their cryptographic keys and cryptocurrencies with a third-party provider via host wallet services (Newell et al., 2021). Using programming languages like Solidity and Rust, Decentralized Applications (dApps) are engineered and deployed on the platform (Mamun & Islam, 2021). Consumed by users, this brings programmability and a new logical business model to the blockchain platform.

1. **Mining a Block in a Blockchain**

Blockchain blocks connected to the tamper-proof database are created through mining (Salman et al., 2019). A miner who generates the first legitimate block in various distributed ledgers, like Bitcoin, receives compensation. As discussed below, are details on three (Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), Measure of Trust (MoT), Proof of Work (PoW), Proof of Space (PoSpace), minimum block hash, and Proof of Importance (PoI) of the methods used by the platform to determine a miner who wins a block.

1. **Proof of Work (PoW).** PoW was initially a Bitcoin mining method and is now utilized by several other blockchain systems (Yang et al., 2019). PoW requires all mining nodes to solve a mathematical challenge agreed upon by all miners (Sforzin et al., 2022). Upon successful verification, the newly mined block is uploaded to the original chain and the miner is rewarded. A consensus is a foundational principle on which the blockchain ecosystem operates. It is therefore challenging for bad intend miners unless they control more than 50% of the mining nodes (Natoli & Gramoli, 2016).

The issue with the PoW strategy is that significant computing resources are spent on the mathematical problem-solving challenge. Because Bitcoin's proof of work requires a lot of computing power, it is simple for network computing power to become centralized (Journal of L A T E X Class & Files, 2021). There's been considerable work invested toward finding more efficient algorithmically created problems, but not much progress has been made (Chaurasia et al., n.d.). Therefore, a challenge offered by anyone or an organization that the proposer may be ready to pay to have solved is a problem that is considered to be genuinely valuable.

1. **Proof of Stake (PoS).**Through the battle for computing power across all nodes, the POW consensus method delivers a conclusion that is challenging to calculate but simple to verify (Journal of L A T E X Class & Files, 2021). As a result of computing power wastage in PoW, Proof-of-Stake (PoS) was developed in 2011 with the premise that security on the chain is well maintained by equity owners than the miners.

The algorithm mandates that the method of calculating hash value depending on processing power in POW be replaced with the number of bitcoins possessed by nodes (Yan, 2022).

In the PoS 2.0 consensus mechanism, rights equity is inversely correlated with the amount of time a user is online (Schinckus, 2021). This incentive system significantly raises the difficulty for attackers to carry out 51% attacks and substantially improves the blockchain peer-to-peer network. Nonetheless, POS is susceptible to bifurcation, and blockchain's decentralization is less secure.

1. **Practical Byzantine Fault Tolerance (PBFT)**In contrast to previous consensus mechanisms, PBF makes use of the blockchain without using resources of any kind. In PBFT, a leader is first chosen and accepted by the nodes (Erbad & Samaka, 2019). The network's leader determines whether to validate the transactions and then broadcasts a block to every node. Due to the ensuing communication overhead, PBFT has scaling problems.

Any BFT protocol that is created must unavoidably deal with the FLP impossibility result (Oliveira et al., 2022). Even a single error makes it difficult to reach an agreement in an asynchronous system. For many years, employing a partial synchrony model was the nearly universally acknowledged technique to get over this obstacle (Chondros et al., 2011).

Most people believe that BFT and state-machine replication are ill-suited for scaling (Brewer, 2000). BFT protocols were created for fault-tolerant replication of established applications. There are perceived as being non-scalable due to their heavy network communication, which frequently requires as many as O(n2) messages in each block (Castro & Liskov, 2002).

**Table II: Blockchain Mining Techniques summary**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mining Approach** | **Needed Resources** | **Randomness** | **Implementation** | **Miner Reward?** |
| Proof of Stake | Stake | Blockchain randomized selection | Ethereum | No |
| Proof of Work | High computing resources needed | No randomness | Bitcoin | Yes |
| Practical Byzantine Fault Tolerance | No resources needed | No randomness | Hyperledger | No |

1. **Properties of Blockchains**

The five main properties of blockchain are cryptographic system, distributed, decentralized, trustless, and Non-repudiation (Ehmke et al., 2019). According to Nakamoto, these properties are the foundational principles on which technical security is built in blockchain architecture.

**Table III: Summary of Blockchain main Properties**

|  |  |  |
| --- | --- | --- |
| **Property** | **Problem to be solved** | **Blockchains' solution** |
| Decentralized  Consensus | A single point of failure might result from one controller's centralized choices. | Decentralized consensus, majority decides, and node consensus are used to make blockchain choices. |
| Non-repudiation  Guarantee | Users may reject engaging with the system. | Blockchains employ durable databases in conjunction to authentication of transactions and blocks to prevent subsequent denial of transactions. |
| Distributed  Nature | Due to the dispersed nature of modern systems, distributed control and security techniques are necessary.  For these applications, most of the viable security solutions now available are centralized and ineffective. | By their very nature, blockchains are decentralized. Therefore, distributed implementation of security services based on blockchain is possible. |
| Cryptographic  Security | Security algorithms should demonstrate that they are extremely tough to exploit. | Blockchains employ elliptic curve encryption, which is hard to crack. It is considerably more challenging to overturn because to the trustless system and decentralized consensuses. |
| Trustless System | If a third-party providing security is compromised, there may be security and privacy problems. | The majority vote trust imposed by blockchain technology is impermeable to breach unless attackers have complete system control. |

1. **Encryption and Authentication Security Services**

The two most valuable and required security services in every network are encryption and authentication (Salman et al., 2019b). When it comes to attack situations like physically compromised devices or tapped network links, encryption can reduce risk (Young, 2021). By guaranteeing that access privileges are role-based and managed consistently and dependably, the implementation of Central for Information Security (CIS) control 03 (IG3) will aim to safeguard enterprise assets (CIS Control 03: Data Protection | Tripwire, 2021).

To use public key cryptography solutions, organizations need both private and public information. A properly engineered infrastructure is required to produce, revoke, manage, distribute, utilize, and store the created keys (Kim et al., 2021). This chapter begins by talking about public key cryptography and how it is used in modern systems. The public key management strategies are then described, along with some of their difficulties. The usage of blockchains to address these issues is then briefly described, followed by a comparison of a few blockchain-based key management strategies.

1. **Public Key Cryptography.**A cryptographic technique that uses two separate keys in its encryption process. Public Key Cryptography is often called asymmetric (Lord, 2015). Cryptographic protocols in asymmetric encryption are based on algorithms defined to use private and public keys in the encryption and decryption of data.

Numerous security services, notably identity authentication and confidentiality, may be provided using public key cryptography (Yan, 2022). By evaluating the signature using the public key, one confirms or validates the sender of a transaction that has been authorized with that issuer's private key. Only the entity itself or a person with access to the private key may authenticate the communication since it is kept secret (Márton, 2010).

1. **Key Management by the Public Key Infrastructure (PKI).**

KPI is one of the many ways of ensuring and creating a standardized key management process for public key cryptography. On top of PKI, system, network, and application security components are deployed (Weise -Sunps, 2001). PKI is a crucial part of a comprehensive security plan that does indeed cooperate with other security measures, operational procedures, and risk management initiatives. A PKI is not a business function within an enterprise (Weise -Sunps, 2001). KPI makes the basic security mechanisms of IPsec, HTTPS, SSL, S/MIME, PGP, etc., possible to implement and manage.

The primary conventional means for implementing PKI are centralized by a certificate authority (CA) and decentralized through a web of trust (WoT) (Cooper et al., 2008). CA-based PKI implementation has been codified into many security standards like X.509.

The CA method serves as a 3rd party organization that all design parameters trust. "Certificates" are documents that the CA produces to authenticate users and link each user to a cryptographic key (public key) (Maurer, 1996). A signed certificate linking a person to their public key will confirm that they are the rightful owner of that public key. In WoT, the keys are produced locally using a decentralized method and are only trusted if they have been validated by at least one other trusted person in the system.

1. **Problems With the Traditional PKI Systems**

Expenses, a single point of failure, and a trusted third party are three significant obstacles that the CA-based PKI faces. System users' dependability on the CA to create and manage public keys for them is a concern (Ellison et al., 2000). CA may face significant security concerns in the event of a breach. Additionally, it might be costly and ineffective for a single centralized CA to maintain the public keys.

Identity retention is not possible with either the CA or WoT PKI. Users can only join a network if another "trusted" member trusts them. This can make it difficult for new users to join the network. A number of solutions are proposed; however, they are mainly log-based (Ellison et al., 2000).

1. **Blockchain-Based PKI Concept**

The blockchain ecosystem is an ideal method for many apps due to its decentralized, event-recording, and non-reproducibility characteristics. These characteristics demonstrate the blockchain's appropriateness for PKI. The decentralized nature of blockchain-based PKI protocols eliminates any single point of failure. There is no one trusted third party and no prerequisite for system reliability (Salman et al., 2019). In table IV, the summary shows the blockchain-based solutions for conventional PKI issues.

**Table IV: Blockchain-Based PKI Concept**

|  |  |  |
| --- | --- | --- |
| **Conventional approach** | **Problem to be solved** | **blockchains solution** |
| WoT-based PKI | Credibility | Does not require any previous trust. Most votes are used to decide. |
| CA-based PKI | Third-party trust,  Single point of failure, and  Cost of implementation | Blockchains' distributed consensus feature. There is no central authority  Open-source deployment |
| CA-based and WoT-based PKI | Identity retention | The technology can determine whether the public key has previously been verified since it has an incident logging database. |

Blockchain employs several methods to achieve secure PKI.

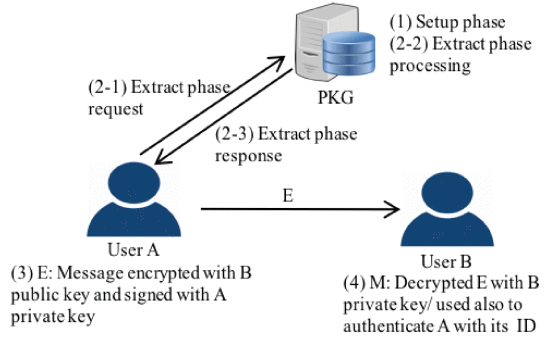
* **Blockstack.** Namecoin is used by Blockstack to develop a distributed PKI infrastructure. Namecoin is a Bitcoin derivative that enables information storage in blockchain operations (Kalodner et al., n.d.). Its implementation involves establishing a name-value pair for storing user credentials. It is one of the most powerful public key cryptography techniques available today because it bounds user identity to an elliptic curve public key in the Blockstack implementation. The open-source tool was developd and relased in 2014, being used by 55,000 users as a PKI solution (Salman et al., 2019). Namecoin has the benefit of already supporting name-value pairs in its transactions.

State changes operations are kept on blockchain in Blockstack. They are arranged in chronological order (Ravlija, 2018). Similarly, licensing of id and key combination is distinct from information storage and dissemination. Blockstack data is saved in zone files (4 KB per file) and on external drives such as IPFS. Blockstack is constructed on the blockchain in layers. Because it is not tied to the underlying blockchain technology, Blockstack has more freedom (Fromknecht et al., 2014).

### Identity-Based Cryptography (IBC)

IBC is a public cryptography technique in which data associated with an identity could function as a valid public key. A Trusted Third Party (TTP) server, also known as a Private Key Generator (PKG), initially holds a secret master key that is utilized to produce a set of public parameters and the private keys for the associated users (Mora-Afonso & Caballero-Gil, 2022). After registering, the user obtains the public and private keys. At this point even without PKG, a secure communication route is possible.

**Figure 3:** Identity-Based Cryptography



### Problems With the Current IBC-Based Approaches

PKG being required to create the private keys is the major problem that exist in IBC. Based on this requirement, the system is centralized. As most centralized systems, there is a single point of failure and the need to trust a third-party since the PKG is the sole authority with the ability to produce key pairs (Zhao et al., 2012). If the PKG is hacked, the entire system is at risk. The IBC shares the same limitations as the classic CA-based PKI solution.

### Blockchain-Based IBC

To alleviate the shortcomings of the conventional Identity-Based Cryptography, the Blockchain-based IBC just as blockchain-based PKI utilizes its decentralized advantage of distributed databases (Lewko & Waters, 2011). Blockchain uses a decentralized database to eliminate the issues of centralization and single point of failure. In this structure, users have the option to avoid trusting a third part by creating and managing their own master keys without dependability on PKG or any third-party. Users with limited resources to generate and manage these keys can easily delegate the task to other nodes it trusts (Fotiou & Polyzos, 2016).

1. **Data Privacy Services**

Data Privacy Services (DPS) are regulated security services aimed at mandating enterprises implement controls and data policies to safeguard users' privacy (Acquisti et al., 2012). These controls intend to give users the authority to choose how and when the network may access their personal identification information (PII) or system resources. With a definition of DPS in mind, this study reviews how access control lists (ACLs) are used to provide privacy, traditional methods for privacy, and issues with them, and the blockchain-based methods that serve as an antidote for data security.

1. **ACL role in Data Privacy**

A blueprint for creating a rigorous data management strategy with security at the center is provided by CIS Control 3. A successful data management strategy is built on an understanding of the "Five Ws" of the organization's data (Young, 2021). The "five Ws" are:

* What data does the company manage or process?
* Who can use it?
* Where is it kept or used?
* When should the data be disposed?
* Why does it require security?

CIS recommends the classifications "sensitive," "confidential," and "public," but businesses may require additional bespoke labeling. A data inventory and categorization intend to divide systems into groups according to the types of information they process and provide access privileges with a finer level of control to reduce data leakage (Goel, 2014).

In addition to being classified and kept separately the systems that host the data must be separated and only provide minimum access to users, with a process to request advance access as the need arises. ACL helps in the implementation phase by enforcing roles based on data classification (Ball, 2013). Every time data is gathered, kept, utilized, damaged, or discarded, there are privacy considerations (Dwork, n.d.). Both data in transit and at rest are protected by privacy. The healthcare information privacy regulations are only one example of the several federal laws that have been created to stop privacy violations.

1. **Data Privacy Traditional Methods**

Delegating the ACL definitions to the data owners and utilizing cryptography to restrict the information's access are two ways to ensure data privacy. One of the most active areas of research issues is the development and implementation of methods to provide privacy service. (Armknecht et al., 2012). One method of offering a data privacy service is through the use of homomorphic encryption, which enables calculation and analysis of encrypted data and provides encrypted outputs (Machanavajjhala et al., 2007).

The user's identity is concealed using data security and confidentiality and privacy preservation techniques (Byun et al., 2007). K-anonymity demands that sensitive data be comparable to at least K-1 other entries. L-diversity ensures that private data is kept in the most "diverse enough" places. T-closeness employs noise addition or data modification strategies prior distributing the data (Li et al., 2007).

1. **Privacy Traditional Methods Problems**

Having been an area and topic of discussion lately, providing an effective data privacy solution remains problematic. Scalability, data ownership, efficiency, and an absence of a structured data lifecycle strategy are a few of the issues (Bertino & Ferrari, 2017). This study vividly reviews few of the issues with the conventional data privacy.

* 1. **Structured data lifecycle strategy.** To define a full lifecycle of data systematically, a strategy for privacy protection must be designed (Kalodner et al., n.d.). The stages should be identified, the privacy needs should be specified, and the lifecycle modifications should be flexible. These stages may entail the collection, exchange, and destruction of resources or the data itself. Majority of data privacy approaches that have been offered lack a systematic methodology (Yan, 2022).
  2. **Efficiency and Scalability.** Majority of data privacy strategies that exist today are inefficient and challenging to scale and manage with bigger apps since they rely on intricate cryptographic algorithms. Recent studies aim to simplify and boost the effectiveness of various cryptographic methods (Kreuter et al., 2013). The majority of the time, the suggested techniques still lack applicability. Additionally, most algorithms are unable to scale to the enormous volume of data needed in today's systems.
  3. **Data Ownership and Control.**Issues of data ownership and modification privileges are crucial to privacy. The person who chooses the data's access control procedures is often the owner (Bertino & Ferrari, 2017). Unfortunately, the conventional methods covered in the preceding paragraph are still unable to resolve the ownership issue.

### Blockchain-Based Data Privacy Concept

Blockchain replaces the traditional centralized model of trust with a completely distributed node-based network (Bernabe et al., 2019). This network is designed and implemented on a synchronous Distributed Ledger Technology (DLT), a decentralized database that maintains data replication and sharing between several nodes dispersed over numerous remote locations.

In order to increase privacy and enable transaction anonymity in blockchain, this section reviews and analyzes a blockchain privacy-preserving mechanism. This section discusses Zero-Knowledge Proof (ZKP) which is one of the many privacies preserving techniques in Blockchain's architecture.

1. **Zero-knowledge proof (ZKP).** This a cryptographic method uses for evaluating if the authenticator has enough events in its block without disclosing any private transaction information in a blockchain environment (Sun et al., 2021). A participant can demonstrate to another that a particular claim is true using the ZKP proof cryptographic technique without disclosing anything data (Goldwasser et al., 2019). For instance, a ZKP can be used to demonstrate the claim that one knows a secret value even after the ZKP has been completed. Zero-Knowledge, Soundness, and Completeness are three conditions to be met to consider a protocol ZKP.
2. **Soundness:**Soundness: With the exception of a little chance, a dishonest prover cannot convince the validator that a claim is correct if it is incorrect (Easttom, 2019).
3. **Zero-knowledge.** A polynomial-time constrained method that can produce excerpts of the protocol by itself and that are identical to a valid argument between a prover and a validator (Sun et al., 2021). The simulator is the name of this algorithm. It is Zero-Knowledge since neither the verifier nor an eavesdropper could learn any further details from an actual transcript if a third party (who does not know whether the assertion is true or untrue) can provide a legitimate transcript of the protocol (Bernabe et al., 2019).
4. **Completeness:**If the proposition being proven is accurate, the prover can always offer a convincing argument.

A formal proof in ZKP is one in which the prover constructs a proof by substituting a cryptographic hash for the verifier. Instead of depending on a single predictable matrix, the Fiat-Shamir heuristic overcomes this problem utilizing the random oracle model (Fiat & Shamir, 2019).

Perfect ZKPs are those in which the ensembles of the genuine excerpts and the modeled excerpts are comparable, and the prover is practically boundless (Miers et al., 2013). There are modifications, such as quantitative ZKPs or computed ZkPs, that ease the unreliable and inaccurate of ensembled samples with less stringent assumptions (Armknecht et al., 2012). There are additional variations that place limitations on the verifier, such as the honest-verifier ZKP, which limits the data that may be sent to and received from the device.

Enhanced privacy mechanisms in certain blockchain ledgers, as those in Hyperledger Indy 2, utilize decentralized identification (DIDs) (Camenisch & Lysyanskaya, 2001). ZKPs, authentication encryption, and a distinction between credentials and proofs are all used by DIDs. The use of ZKP in this kind of blockchain has no bearing on a transaction's legality. Instead, the credibility a verifier offers an issuer determines how much trust to place in it (Reed et al., 2018).

1. **Is Blockchain susceptible to Cyber Attacks?**

Aside from the vast array of advantages which blockchain brings, there are a few obstacles that limit its usefulness for many security applications (Bhushan et al., 2020). Blockchain networks are susceptible to fraud and hacking even though they provide a tamper-proof ledger of transactions. People with malicious intentions have successfully carried out several hacks and frauds over the years by manipulating known weaknesses in blockchain technology (IBM, 2021).

The fundamental structure of how this young technology operates—using decentralization, consensus, and cryptography—guarantees that transactions are essentially tamper-proof. Nevertheless, throughout time, hackers have nonetheless discovered ways to take advantage of the system. Twelve cryptocurrency exchanges were compromised in 2019 (How Safe Is Blockchain? 2021).

The development of distributed ledger technology led to the emergence of a broad spectrum of threats. These threats or vulnerabilities might be brought on by internal actors or outside parties. New privacy and security control requirements for data storage and transfer are being driven by the rising popularity of blockchain technology (Bhushan et al., 2020). Risks to double spending, networks, mining swarms, and wallet security make up the four main categories of existing blockchain cyberthreats.

Smart contracts are blockchain-based computer program code that execute themselves automatically to carry out all or a portion of an agreement (Levi et al., 2018). This agreement is embedded into the blockchain, which renders it irrevocable and immutable. They are typically used to automate the implementation of an agreement so that all parties are immediately certain of the outcome and no middlemen are required. A poorly written DAO smart contract that was instantiated on the Ethereum Blockchain to serve as a contract for users to vote on projects and funds to support and invest in potential profitable smart contract ventures led to a loss of $120 million to hackers (Asmakov, 2021).

The vulnerable parts of the multi-sig wallet library are within the initWallet () function and the "kill" function (Petrov, 2017). The purpose of implementing this sort of centralized architecture in a decentralized network is to save gas fees on deployment transactions when new wallets are created. A newly deployed multi-sig wallet can invoke the code from the already deployed library and not pay the extra gas fee on that EVM bytecode. However, because a new wallet that was created required interaction with this library, it created a single point of failure. This security issue led to a parity multisig wallet hack in July 2017.

The careful management of the risks connected to the blockchain is necessary for its adoption and functioning. The underlying architecture of every organization will eventually incorporate blockchain technology, which is more than just an application (Blockchain Security Risks for Financial Organizations | Deloitte US, 2017). A unique instance of distributed ledger technology is the blockchain protocol, in which the consensus protocol establishes a daisy-chain immutable ledger of all transactions shared among all participants.

Blockchain technologies present sophisticated technologies that companies must account for. These technologies expose institutions to threats that are like those connected to traditional enterprise processes. Since blockchain enables peer-to-peer value transfer without the requirement for a central middleman, value transfer dangers exist. The transferred value may take the shape of assets, identities, or data. Due to this new business model, the interacting parties are now subject to new risks that were previously controlled by central intermediaries (Yan, 2022).

1. **Security model.**

Networks, information systems, computing techniques, and security and privacy are the four criteria used by the ACM Computing Classification System, which is extensively used in the field of computer science, to characterize technology maturity (Wang et al., 2016).

**Figure 4:** Threats can emerge from traditional and well-known attack vectors or due to a new breed of attacks unique to blockchain. All threats fall into the four-factor security model. Each factor comprises a set of security controls that work to protect the ecosystem.

1. Securing the foundations of the blockchain. This includes its transactions, distributed ledger, and consensus protocol.
2. Smart contract security. This factor includes secure design principles and secure coding practices, especially targeted for smart contracts and testing strategies to discover bugs before deploying contracts.
3. Securing the crucial ecosystem players, such as wallets, providers, exchanges, and Oracles.
4. End user and security control to protect the interactions of the users with the blockchain ecosystem.

**Attack surface and vectors**

The attack surface simply means the areas of a system that are vulnerable and can be exploited.

**Figure 4**

Graphical user interface, application

Description automatically generated

* The concentration of consensus power. Malicious miners and transaction validators can collude to manipulate the consensus protocols.
* Nodes on the blockchain network can become rogue, assume civil identities, and compromise trust in the blockchain. These weaknesses can cause a ripple effect and lead to 51% attacks and double spending attacks.
* Vulnerabilities in the blockchain platform can also lead to an attack on the promise of privacy that the blockchain technology is founded upon.
* Smart contracts are also vulnerable to attacks such as reentrancy attacks, front-running attacks, and denial of service attacks.
* Ecosystem enabler services such as wallets and exchanges can also be compromised due to phishing attacks, denial of service attacks, other insider threats, and conflicts of interests.
* The end user and client apps running on devices are also prone to well-known attacks such as malware infections, threats of private keys, and a host of other attacks that are possible due to application-level vulnerabilities also defined by OWASP Top 10.

**Results**

Blockchain and its related systems cannot solve all cybersecurity issues. They only support current initiatives for secure systems, connectivity, and information sharing. Blockchain stores immutable records via encryption and hashing, and a large number of current cyber security measures also make use of similar methods for data security.

The two most valuable and required security services on every network are encryption and authentication. When it comes to attack situations like physically compromised devices or tapped network links, encryption can reduce risk. Blockchain-Based PKI is designed to address the risk of single point on failure that exist in centralized systems.

The blockchain ecosystem is an ideal method for many apps due to its decentralized, event-recording, and non-reproducibility characteristics. These characteristics demonstrate the blockchain's appropriateness for PKI. Blockchain adopters can use Namecoin, which is a Bitcoin derivative that enables information storage in blockchain operations. Its implementation involves establishing a name-value pair for storing user credentials. It is one of the most powerful public key cryptography techniques available today.

The IBC shares the same limitations as the classic CA-based PKI solution **(Table IV)**. As with most centralized systems, there is a single point of failure and the need to trust a third-party. If the PKG is hacked, the entire system is at risk since it is the sole authority with the ability to produce key pairs.

To alleviate the shortcomings of conventional IBC, the blockchain-based IBC utilizes its decentralized advantage of distributed databases, just as the blockchain-based PKI does. Blockchain users create and manage their own master keys without relying on PKG or any third-party. Users with limited resources to generate and manage these keys can easily delegate the task to other nodes they trust.

Data ownership, scalability, and efficiency are just a few of the privacy issues improved by blockchain. In order to increase privacy and enable transaction anonymity in blockchain, this literature reviews and analyzes a privacy-preserving mechanism. It discusses Zero-Knowledge Proof (ZKP) which is one of the many privacy-preserving techniques in Blockchain's architecture. ZKP is a cryptographic method use for evaluating if the authenticator has enough events in its block without disclosing any private transaction information in a blockchain environment. A ZKP can be used to demonstrate the claim that one knows a secret value even after the protocol has been completed. Zero-Knowledge, Soundness, and Completeness are three conditions to be met to consider a protocol ZkP.

Aside from the vast array of advantages which blockchain brings, there are a few obstacles that limit its usefulness for many security applications. Blockchain networks are susceptible to fraud and hacking even though they provide a tamper-proof ledger of transactions. People with malicious intentions have successfully carried out several hacks and frauds by manipulating known weaknesses in the technology. Risks to double spending, networks, mining swarms, and wallet security make up the four main categories of existing blockchain cyberthreats. A poorly written DAO smart contract that was instantiated on the Ethereum Blockchain led to a loss of $120 million to hackers. The careful management of the risks connected to the blockchain is necessary for its adoption and functioning. Since blockchain enables peer-to-peer value transfer without the requirement for a central middleman, value transfer dangers exist.

**Discussion & Conclusion**

**Summary**

The implementation of blockchain security mechanisms may change, improve, or eliminate security paradigms in traditional security services. This literature review examines and presents how distributed blockchain security mechanisms can be used to close the gap that exists in security services such as authentication, data privacy, data integrity, and data confidentiality.

**Discussion**

In centralized systems, a single trusted authority is used by the majority of currently implemented security procedures to validate and store encrypted data. This approach leaves systems open to attacks, and several criminal actors might concentrate their resources on the trusted authority to launch attacks like denial-of-service operations, introduce harmful code, and extract data via extortion (Huang et al., 2017). In a blockchain infrastructure, this type of operation is not possible because there are no centralized systems. Blockchains are decentralized and distributed by nature. Thus, there is no single point of failure.

Since every node has a replica of the entire historical data, the blockchain system doesn't require trust. Data is only added to the chain of previous data by gaining a majority consensus. The key point is that a group will be much more reliable if several nodes have access to the same data than if there is only one master and a large number of nodes that depend on the master for data (Pinno et al., 2017). This is especially true when bad actors could masquerade as group nodes or masters themselves.

These findings are intended to provide answers to the literature questions by investigating how blockchain can be used to improve cyber security based on the security services evaluated. They are a meta-analysis of the current situation with relation to the use of blockchain-based techniques to increase the security of current and future applications.

1. Most of the work in network security leverage containers for authentication and blockchains to improve Software Defined Networks (SDNs), allowing for the decentralized and secure storage of vital data (Basnet & Shakya, 2017). Such efforts employ an SDN controller architecture with blockchain support that uses a cluster configuration. In order to make the blockchain suitable for solving network security challenges, the design employs SDN controllers and both public and private blockchains for P2P communication between network nodes (Alvarenga et al., 2018).
2. In data storage and sharing, distributed ledgers are leveraged to remove a single point of failure and safeguard the data from manipulation. In other words, hash lists allow querying of data that could be preserved and saved anonymously, and data shared may be validated as being the same from dispatch to reception. Blockchain also ensures that data stored in the cloud stays resistant to unlawful alterations (Ali et al., 2016). Blockchain increases the security of data exchange and storage by establishing a decentralized network that employs client-side encryption and allows data owners to have auditable control over their data (Yue et al., 2017).
3. Data privacy. Compared to other sections, little has been published on the potential of blockchain to enhance data privacy. The explanation might be that blockchain is difficult to employ for privacy purposes, especially in data security, due to its irreversibility (Fu & Fang, 2016). Current strategies encrypt and store users' normal device choices on the blockchain so that they can only be accessed by them. Additionally, they examine the distinctions between proof-of-work (PoW) consensus processes on blockchains and proof-of-credibility techniques, in which nodes are awarded scores based on the number of connections to other trustworthy nodes to assess their credibility (Cha et al., 2018).
4. Authentication. To effectively manage data processing and restrict any unauthorized access, major private blockchains like Hyperledger Fabric should be used to create approved security controls for nodes in the network (Dorri et al., 2017). Blockchain can utilized it to enable nodes' identity, authentication, and frictionless anonymous data transmission via peer-to-peer protocols and to maintain security firmware upgrades (Kshetri, 2017). Based on this literature, the architecture proposed in these works is as follows: the blockchain protocol should reside between the application and transport layers of the network and employs token incentives similar to bitcoin but regards them as units of the voting power.

**Conclusion**

Blockchain is a distributed ledger with a cryptographic foundation that permits trusted transactions between network members who are not trusted. This literature review examines how blockchain consensus mechanisms can change or improve authentication, data privacy, data integrity, and data confidentiality security services. To understand how blockchain should be implemented to improve the security of data, this study has reviewed the issues with traditional data security and contrasted them with blockchain security protocol solutions.

Blockchain enables a new breed of decentralized, intermediary-free applications. This eliminates organizational bureaucracies that operate in centralized systems to control the actions of social and economic communities. This research discusses blockchain mining and its PoW, PoS, and PBFT, which are three of the many methods used by the platform to determine a miner who wins a block. It discusses Zero-Knowledge Proof (ZKP), which is one of the many privacy-preserving techniques in the architecture of the Bitcoin network.

From the literature, it's evident that blockchain adoption will play a role in improving security. But blockchain and its related systems cannot solve all cybersecurity issues. While this study presents blockchain-based solutions to traditional security services, the blockchain itself is also vulnerable to several cyberattacks.

**References**

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, *49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215

Akram, J., Akram, A., Jhaveri, R., Alazab, M., & Chi, H. (2022). BC-IoDT: Blockchain-based Framework for Authentication in Internet of Drone Things ACM Reference Format. *2022 ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, *22*. https://doi.org/10.1145/3555661.3560874

Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). *Blockstack: A Global Naming and Storage System Secured by Blockchains*. Www.usenix.org. https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali

Alvarenga, I. D., Rebello, G. A. F., & Duarte, O. C. M. B. (2018, April 1). *Securing configuration management and migration of virtual network functions using blockchain*. IEEE Xplore. https://doi.org/10.1109/NOMS.2018.8406249

Armknecht, F., Katzenbeisser, S., & Peter, A. (2012). Group homomorphic encryption: characterizations, impossibility results, and applications. *Designs, Codes and Cryptography*, *67*(2), 209–232. https://doi.org/10.1007/s10623-011-9601-2

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer*, *50*(9), 18–28. https://doi.org/10.1109/mc.2017.3571064

Basnet, S. R., & Shakya, S. (2017, May 1). *BSS: Blockchain security over software defined network*. IEEE Xplore. https://doi.org/10.1109/CCAA.2017.8229910

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for Blockchain: review and challenges. *IEEE Access*, *7*, 1–1. https://doi.org/10.1109/access.2019.2950872

Bertino, E., & Ferrari, E. (2017). Big Data Security and Privacy. *Studies in Big Data*, 425–439. https://doi.org/10.1007/978-3-319-61893-7\_25

Bhushan, B., Sinha, P., Sagayam, K. M., & J, A. (2020). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897

Brewer, E. (2000). *Towards Robust Towards Robust Distributed Systems Distributed Systems Inktomi at a Glance Inktomi at a Glance Company Overview Company Overview “INKT” on NASDAQ “INKT” on NASDAQ Our Perspective Our Perspective*. PODC Keynote. https://sites.cs.ucsb.edu/~rich/class/cs293b-cloud/papers/Brewer\_podc\_keynote\_2000.pdf

Byun, J.-W., Kamra, A., Bertino, E., & Li, N. (2007). Efficient k-Anonymization Using Clustering Techniques. *Advances in Databases: Concepts, Systems and Applications*, 188–200. https://doi.org/10.1007/978-3-540-71703-4\_18

Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. *Lecture Notes in Computer Science*, 93–118. https://doi.org/10.1007/3-540-44987-6\_7

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, *20*(4), 398–461. https://doi.org/10.1145/571637.571640

Cha, S.-C., Chen, J.-F., Su, C., & Yeh, K.-H. (2018). A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things. *IEEE Access*, *6*, 24639–24649. https://doi.org/10.1109/access.2018.2799942

Chaurasia, Y., Subramanian, V., & Gujar, S. (n.d.). *PUPoW: A FRAMEWORK FOR DESIGNING BLOCKCHAINS WITH PRACTICALLY-USEFUL-PROOF-OF-WORK & VanityCoin*. Retrieved October 28, 2022, from https://arxiv.org/pdf/2210.06738.pdf

Chondros, N., Kokordelis, K., & Roussopoulos, M. (2011). *On the Practicality of “Practical” Byzantine Fault Tolerance*. https://arxiv.org/pdf/1110.4854.pdf

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. https://doi.org/10.1109/aiccsa.2016.7945805

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. https://doi.org/10.17487/rfc5280

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. https://doi.org/10.1109/percomw.2017.7917634

Dwork, C. (n.d.). Differential Privacy: A Survey of Results. *Lecture Notes in Computer Science*, 1–19. https://doi.org/10.1007/978-3-540-79228-4\_1

Easttom, C. (2019). Computer Security Fundamentals. In *Google Books*. Pearson IT Certification. https://books.google.com/books?hl=en&lr=&id=erauDwAAQBAJ&oi=fnd&pg=PT34&dq=+Computer+Security+Fundamentals&ots=F26rzTkKzh&sig=WoV3F4FGG-sU3HKg2fg\_MTMhdnA#v=onepage&q=Computer%20Security%20Fundamentals&f=false

Ehmke, C., Blum, F., & Gruhn, V. (2019). *Properties of Decentralized Consensus Technology -Why not every Blockchain is a Blockchain*. https://arxiv.org/pdf/1907.09289.pdf

Erbad, A., & Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 858–880. https://doi.org/10.1109/comst.2018.2863956

Fiat, A., & Shamir, A. (2019). How To Prove Yourself: Practical Solutions to Identification and Signature Problems. *Advances in Cryptology — CRYPTO’ 86*, 186–194. https://doi.org/10.1007/3-540-47721-7\_12

Fotiou, N., & Polyzos, G. C. (2016, April 1). *Decentralized name-based security for content distribution using blockchains*. IEEE Xplore. https://doi.org/10.1109/INFCOMW.2016.7562112

Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). A Decentralized Public Key Infrastructure with Identity Retention. *Cryptology EPrint Archive*. https://eprint.iacr.org/2014/803

Fu, D., & Fang, L. (2016, October 1). *Blockchain-based trusted computing in social network*. IEEE Xplore. https://doi.org/10.1109/CompComm.2016.7924656

Goel, V. (2014). *Facebook Tinkers With Users’ Emotions in News Feed Experiment, Stirring Outcry*. https://cs.wellesley.edu/~cs110/assignments/a03/Facebook-Privacy.pdf

Goldwasser, S., Micali, S., & Rackoff, C. (2019). The knowledge complexity of interactive proof-systems. *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. https://doi.org/10.1145/3335741.3335750

Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Xie, L. (2017). A decentralized solution for IoT data trusted exchange based-on blockchain. *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*. https://doi.org/10.1109/compcomm.2017.8322729

Journal Of L A T E X Class, & Files. (2021). *Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake 1*. *14*(8). https://arxiv.org/pdf/2209.11545.pdf

Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J., & Narayanan, A. (n.d.). *An empirical study of Namecoin and lessons for decentralized namespace design*. Retrieved November 2, 2022, from https://allquantor.at/blockchainbib/pdf/kalodner2015empirical.pdf

Kim, H., Kim, K., Park, S., & Sohn, J. (2021). *E-voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data*. https://arxiv.org/pdf/2111.05096.pdf

Kreuter, B., Shelat, A., Mood, B., & Butler, K. (2013). *{PCF}: A Portable Circuit Format for Scalable {Two-Party} Secure Computation*. Www.usenix.org. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/kreuter

Kshetri, N. (2017). Blockchain’s roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Lewko, A., & Waters, B. (2011). Unbounded HIBE and Attribute-Based Encryption. *Advances in Cryptology – EUROCRYPT 2011*, 547–567. https://doi.org/10.1007/978-3-642-20465-4\_30

Li, N., Li, T., & Venkatasubramanian, S. (2007). t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. *2007 IEEE 23rd International Conference on Data Engineering*. https://doi.org/10.1109/icde.2007.367856

Lord, N. (2015, October 5). *What is Public Key Cryptography?* Digital Guardian. https://digitalguardian.com/blog/what-public-key-cryptography

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity. *ACM Transactions on Knowledge Discovery from Data*, *1*(1), 3-es. https://doi.org/10.1145/1217299.1217302

Mamun, Q., & Islam, M. Z. (2021). A Generalised Logical Layered Architecture for Blockchain Technology. *ArXiv:2110.09615 [Cs]*. https://arxiv.org/abs/2110.09615

Márton, G. (2010). Public-key cryptography in functional programming context. *Informatica*, *2*, 99–112. https://arxiv.org/pdf/1003.1387.pdf

Maurer, U. (1996). Modelling a public-key infrastructure. *Computer Security — ESORICS 96*, 325–350. https://doi.org/10.1007/3-540-61770-1\_45

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *2013 IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/sp.2013.34

Mora-Afonso, V., & Caballero-Gil, P. (2022). Using identity-based cryptography in mobile applications. *Arxiv.org*, *V1*. https://doi.org/10.1007/978-3-319-01854-6\_54

Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2019). An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain. *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, *v1*. https://doi.org/10.1109/pimrc.2019.8904404

Natoli, C., & Gramoli, V. (2016). The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example. *ArXiv:1612.09426 [Cs]*, *v1*. https://arxiv.org/abs/1612.09426

Newell, J., Mamun, Q., Rehman, S. ur, & Islam, M. Z. (2021). A Generalised Logical Layered Architecture for Blockchain Technology. *ArXiv:2110.09615 [Cs]*, *v1*. https://arxiv.org/abs/2110.09615

Oliveira, A., Moniz, H., & Rodrigues, R. (2022). Alea-BFT: Practical Asynchronous Byzantine Fault Tolerance. *ArXiv:2202.02071 [Cs]*, *V1*. https://arxiv.org/abs/2202.02071

Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. E. (2017, December 1). *ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT*. IEEE Xplore. https://doi.org/10.1109/GLOCOM.2017.8254521

Ravlija, D. (2018). *PKIs based on Blockchains*. https://elib.uni-stuttgart.de/bitstream/11682/10588/1/Bachelorarbeit\_Damir\_Ravlija\_2019.pdf

S Charters, B. K. (2007). *Google Scholar*. Scholar.google.com. https://scholar.google.com/scholar?cluster=4761353793292081832&hl=en&as\_sdt=0

Saghiri, A. M. (2019). Blockchain Architecture. *Studies in Big Data*, 161–176. https://doi.org/10.1007/978-981-13-8775-3\_8

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 858–880. https://doi.org/10.1109/comst.2018.2863956

Schinckus, C. (2021). Proof-of-work based blockchain technology and Anthropocene: An undermined situation? *Renewable and Sustainable Energy Reviews*, *152*, 111682. https://doi.org/10.1016/j.rser.2021.111682

Seebacher, S., & Schüritz, R. (2017). Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review. *Lecture Notes in Business Information Processing*, *279*, 12–23. https://doi.org/10.1007/978-3-319-56925-3\_2

Sforzin, A., Maso, M., Soriente, C., & Karame, G. (2022). On the Storage Overhead of Proof-of-Work Blockchains. *ArXiv:2205.04108 [Cs]*, *v1*. https://arxiv.org/abs/2205.04108

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network*, *35*(4), 198–205. https://doi.org/10.1109/MNET.011.2000473

Tabatabaei, M. H., Vitenberg, R., & Veeraragavan, N. R. (2022). Understanding blockchain: definitions, architecture, design, and system comparison. *ArXiv:2207.02264 [Cs]*, *v1*. https://arxiv.org/abs/2207.02264

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2019). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2). https://doi.org/10.1016/j.dcan.2019.01.005

Weise -Sunps, J. (2001). *Public Key Infrastructure Overview*. http://highsecu.free.fr/db/outils\_de\_securite/cryptographie/pki/publickey.pdf

Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information Security in Big Data: Privacy and Data Mining. *IEEE Access*, *2*, 1149–1176. https://doi.org/10.1109/access.2014.2362522

Yan, S. (2022). Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake. *ArXiv:2209.11545 [Cs]*, *v1*. https://arxiv.org/abs/2209.11545

Yang, X., Chen, Y., & Chen, X. (2019). Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information. *2019 IEEE International Conference on Blockchain (Blockchain)*. https://doi.org/10.1109/blockchain.2019.00041

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Young, C. (2021, September). *CIS Control 03: Data Protection | Tripwire*. Www.tripwire.com. https://www.tripwire.com/state-of-security/cis-control-3

Yue, L., Junqin, H., Shengzhi, Q., & Ruijin, W. (2017). Big Data Model of Security Sharing Based on Blockchain. *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*. https://doi.org/10.1109/bigcom.2017.31

Zhao, S., Aggarwal, A., Frost, R., & Bai, X. (2012). A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks. *IEEE Communications Surveys & Tutorials*, *14*(2), 380–400. https://doi.org/10.1109/surv.2011.020211.00045