Chapter 1

Security, Privacy and Trust of Distributed Ledgers Technology

Saqib Rasool,[1] Muddesar Iqbal,[2] Shancang Li,[3] Tasos Dagiuklas,[2] and Saptarshi Ghosh[2]

[1]*Faculty of Computing and IT, University of Gujrat, Gujrat, Pakistan*
[2]*School of Engineering, London South Bank University, London, UK*
[3]*School of Computer Science and Informatics, Cardiff University, Cardiff, UK*

The Distributed Ledgers Technology (DLT) Sunyaev [2020] refers to decentralized technological infrastructure and protocols that allow all participants in the connected system to access, verify, and store updates in an immutable and traceable way across the whole decentralized system. Blockchain technology Nakamoto [2009] is a typical example of DLT that can record, validate, and store transactions using cryptographic Cho and Lee [2019] hash signatures. In DLT, each distributed participant, as a ledger, is able to process and verify every transactional item that can be processed based on a consensus of multiple participants. Unlike the central authority-based ledger systems, which need a central authority to validate the authenticity of transactions recorded in the ledgers, the DLT utilizes cryptography algorithms to automatically access, validate, and record transactions based on a specific consensus algorithm in the decentralized network Miraz and Ali [2018a].

As a typical DLT implementation, the blockchain bundles transactions into 'blocks' that are 'chained' together through their respective cryptographic hashes. Blockchain technologies have attracted much attention across industries and sectors, such as cryptocurrencies, supply chains, finance systems, banking systems, etc. Alladi et al. [2019] The DLT has great potential to improve the way of governance, instituting, and corporations work by offering a way to securely and efficiently create a tamper-proof record of sensitive actions and activities. In recent, DLT has been widely researched and several distributed ledger solutions have been developed, such as Hyperledger Fabric, Ethereum, Quorum, R3 Corda, etc.

The DLT is based on cryptography algorithms Miraz and Ali [2018b], decentralization networks Zwitter and Hazenberg [2020], and consensus protocols Wahab and Mehmood [2018], which ensure trust among participants through fair execution of transactions. Data in DLT is structured into chained blocks inherent security properties. Each new block is chained to all the blocks before it using a cryptographic chain in such a way that it is nearly impossible to tamper with the data stored in the ledger Zhao et al. [2019]. All transactions within the blocks are validated and agreed upon through a consensus mechanism, ensuring that each transaction is correct and true. According to the nature of the DLT, there is no single point of failure, and a single user cannot change the record of transactions. However, DLT based technologies are different with many critical security aspects. In DLT or blockchain, the data is organized by cryptographically connected chained blocks and each new block connects to the blocks chained before it in a cryptographic chain Li et al. [2019b]. In this decentralized system, a single point of failure at each participant cannot change the record of transactions.

This chapter has been divided into three distinct sections. Following is an overview of content covered in each section:

Section 1 explains the evolution of distributed databases into blockchain and DLTs (Distributed Ledger Technologies). It also elaborates the differences between distributed databases, blockchain, and DLTs. After presenting the idea of the CAP theorem Frank et al. [2014], it further elaborates the relationship of three basics pillars of the CAP theorem, viz. 1) Consistency (C), 2) Availability (A), and 3) Partition Tolerance (P). The first section also explains the constraints of DLTs for supporting only two of the three features of the CAP theorem and focuses on the three mechanisms of the POW (Proof of Work) Chepurnoy et al. [2017], PBFT (Practical Byzantine Fault Tolerance)Sukhwani et al. [2017], and TDAG (Transactions-based Directed Acyclic Graph) Yeow et al. [2017] for respectively achieving the AP, CP, and CA. This chapter will introduce the detailed DLT with respect to the CAP theorem along with its associated security and privacy issues. in the DLT.

1.1. CAP Theorem and DLT

Fig. 1.1 depicts the blockchain as a subset of the DLTs (Distributed Ledger Technologies) that is a further subset of the DDBS (Distributed Database Systems). However, the origin of DLTs lies in the blockchain and that of blockchain in the DDBS n14 [1992]. Hence, the DDBS initially evolved into the blockchains that further gave rise to the DLTs. Therefore, this section initiates by presenting the evolution of DDBS to the blockchain and then extends that discussion to the transformation of blockchains to the DLTs.

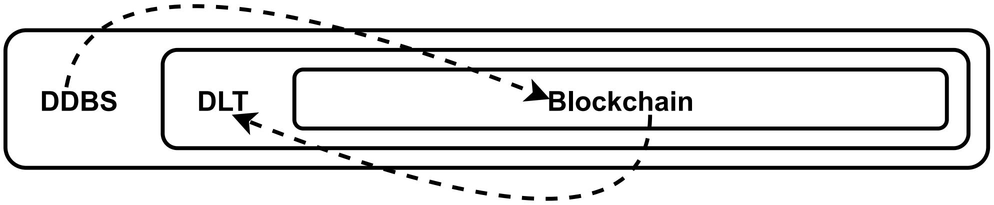


Figure 1.1: The Evolution of DLT (Distributed Ledger Technology) to Blockchain and Distributed Database System (DDBS) and Relationship of DDBS, DLTs and Blockchain

1.1.1. Distributed Database System (DDBS)

A database is an application that abstracts the operations of data handling of a system. With the tremendous growth in the data generation capabilities, databases encounter the requirement of data and computation scaling at a scale that can be tackled through vertical scaling only. Vertical scaling is a technique that refers to the improvements in the system capabilities that are hosting a database application. Hence, a horizontal scaling approach needs to be adopted for supporting the increasing burden of data management.

The horizontal scaling approach utilizes multiple computing nodes for distributing the computational load across multiple machines. The implementation of a horizontal scaling approach is comparatively simpler for stateless applications that only require the load balancing of the computation across different computational nodes. However, it is quite challenging for stateful applications that require the load balancing of both computation and storage. DDMS (Distributed Database Management System) Chen et al. [2019] comes in handy for the stateful application by supporting the horizontal scaling of data management on multiple nodes.

1.1.2. Evolution of DDBS to the Blockchain

A blockchain can be considered as an improved version of a DDBS with some extra constraints. A database offers all four CRUD (Create, Read, Update and Delete) operations while a blockchain only supports the create and read operations. We can also achieve the update operation in the blockchains by appending the new values in the ledger of the blockchain. However, the old values will also remain available in the ledger and new updated values will not be able to replace the old values in the ledger.

1.1.3. Public vs Permissioned Blockchains

Fig. 1.2 shows three broader categories of blockchain solutions, viz. 1) public, 2) permissioned, and 3) hybrid. Public blockchain solutions extend to the permission-less Helliar et al. [2020] (which is mostly interchangeably used for public blockchain) and public-permissioned blockchain that is a relatively new idea for referring to the **without barrier entry of identifiable nodes** in a public network. Similarly, permissioned blockchain solutions extend to the private (usually referred to as a read-only copy of a distributed database) and a consortium blockchain where a group of known members takes the administrative decisions of a blockchain.

The hybrid blockchain is a relatively new addition to the blockchain arena. It refers to a collection of multiple blockchain ledgers under a single umbrella. According to Fig. 1.2, a hybrid blockchain solution may access both public and permissioned blockchain solutions. Hence, a hybrid blockchain can simultaneously act as a public blockchain and a permissioned blockchain, depending upon the operational configurations at any specific time interval.

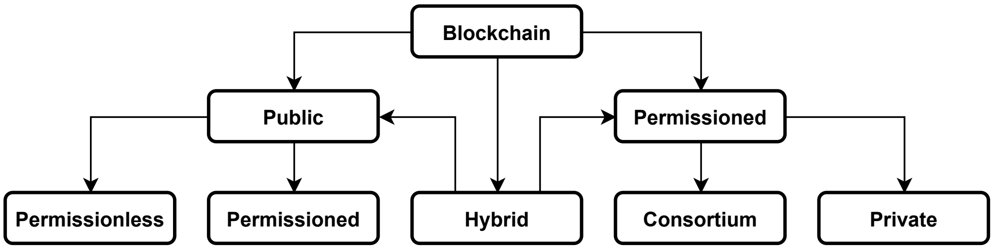


Figure 1.2: Types of Blockchains

1.1.4. Evolution of Blockchain to the DLTs

A blockchain is just like a data structure of a link-list where the blocks of data are linked in a chain and are secured through cryptographical hashes. However, more data structures are proposed for offering similar features to a blockchain system. These systems are known as the DLTs and are considered as the superset of the blockchain systems. IOTA is an example of such a system that uses the data structure of a DAG (Directed Acyclic Graph), instead of the link-list, to offer features similar to the blockchain. Section six of this chapter covers the DLT solution of IOTA in more detail.

1.2. CAP Theorem

Fig. 1.3 presents an overview of the CAP theorem De Angelis et al. [2018] that contains three competing properties of Consistency, Availability, and Partition tolerance. These three properties can be achieved in a centralized system but are not achievable in a distributed system. Only two of the three CAP properties can be strongly achievable in a distributed system. Hence, a trade-off for one of the properties is necessary to achieve for claiming the remaining two properties in one of the three pairs of CA, CP, or CA. The decision of this trade-off drastically affects the overall behavior of a distributed application. Therefore, the particular requirements of an application dictate the decision of this trade-off.

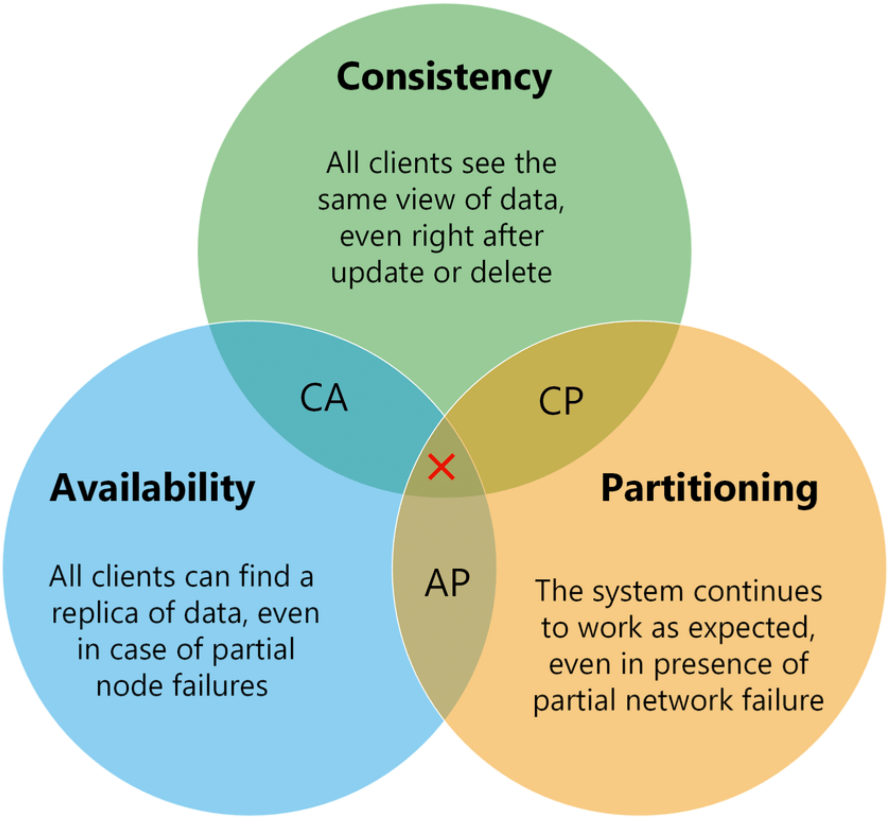

Consistency
All clients see the same view of data, even right after update or delete
CA
CP
✕
Availability
Partitioning
All clients can find a replica of data, even in case of partial node failures
AP
The system continues to work as expected, even in presence of partial network failure

Figure 1.3: An Overview of CAP Theorem

1.2.1. CAP Theorem and Consensus Algorithms

Fig. 1.4 shows a triangle with three properties of the CAP theorem. Each of these three properties can be combined in three different pairs that are reflected in the diagram. Each of the three dimensions of the CAP theorem refers to three different types of consensus algorithms. Each consensus algorithm further gives rise to a different set of properties that are covered in detail in the upcoming sections.

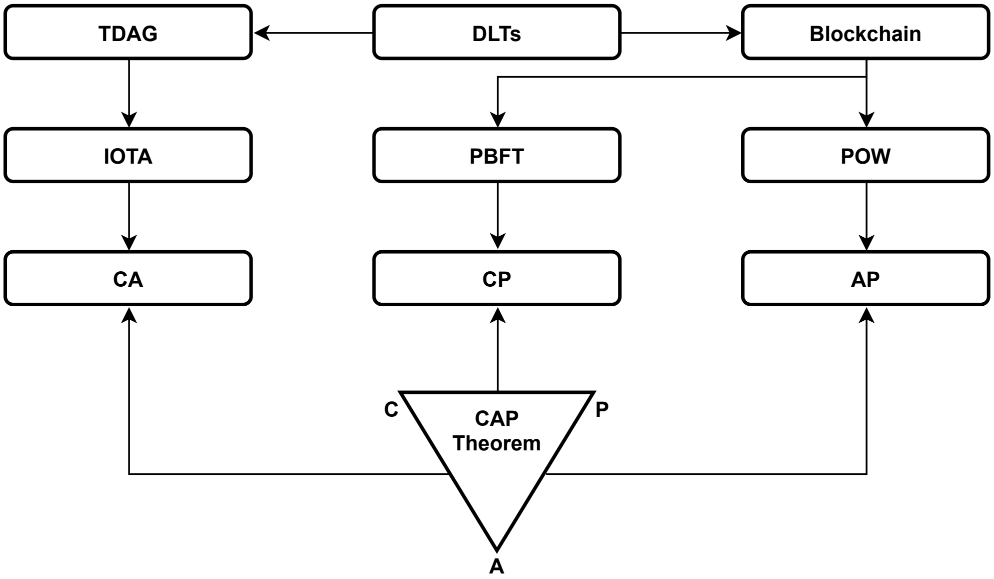


Figure 1.4: DLT solutions against each of the three compatible pairs of the CAP Theorem

1.2.2. Availability and Partition Tolerance (AP) through POW

The consensus algorithm Urban et al. [2004] used in the first generation of blockchain solutions is known as the PoW (Proof of Word). It follows the order-execute model which ensures the ordering of transactions before executing these. It was not only the pioneer consensus algorithm in the DLT world but also the most popular consensus algorithm to date. The consensus algorithm of PoW follows the properties of AP after compromising the property of consistency. More details of this consensus algorithm and associated properties are covered in section four.

1.2.3. Consistency and Partition Tolerance (CP) through PBFT

The consensus algorithm of PBFT (Practical Byzantine Fault Tolerance) achieves the CP properties after compromising the property of availability. It follows the execute-order-validate approach in which the execution of transactions takes place before the ordering of that transactions. This execute-order-validate approach was introduced in the Hyperledger Fabric first. More details of this consensus algorithm and associated properties of the Hyperledger Fabric 1.x and 2.x are covered in section five.

1.2.4. Consistency and Availability (CA)

The consensus algorithm used in IOTA n16 [2019] is based on a transactional graph known as TDAG or Tangle. It achieves the CA properties after compromising the property of partition tolerance. More details of its consensus algorithm and associated properties are covered in section six.

1.3. Security and Privacy of DLT

It is important to understand the security requirements of DLT and identify the type of vulnerabilities. This section, will introduce the basic security properties of DLT, specifically focuses on Blockchain.

1.3.1. Security differs by DLT

As one type of distributed ledger, blockchain networks may be different in the way that each participant access the data. Blockchain networks typically can be categorised into public network or private network depends on the permission and access the to network. Public blockchain networks allow anyone can join them and validate transactions, which allow anonymous public participants access, such as bitcoin networks. In private blockchain networks, only confirmed participants are permitted to maintain the transaction ledger and access the network and achieve consensus through a process called 'selective endorsement'. Both public DLT and private BLT can achieve greater decentralisation and distribution.

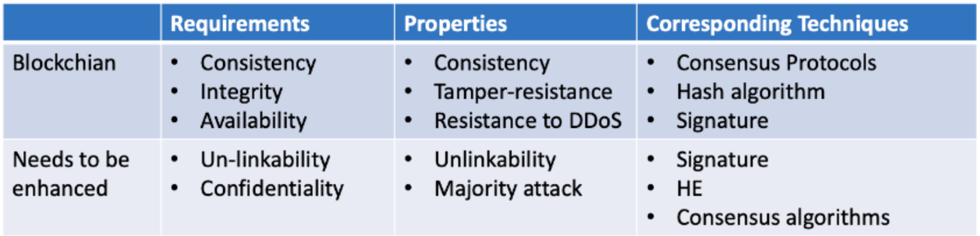
1.3.2. Security and requirements for transactions

The security and privacy requirements for transactions can be categorised into following aspects Putz and Pernul [2020a]:

- **Consistency** of Ledger across institution. Different institutions have their own requirement based on the architecture and business processes, however, the inconsistencies between ledgers may cause errors.
- **Integrity** of transaction, the blockchain system should be able to guarantee integrity of transactions and prevent tempering.
- **Prevention of Double-Spending**. Double spending is one of key challenges in DLT and a robust security mechanisms and countermeasures needs to be implemented in DLT to prevent spending a coin more than once.
- **Unlikability** of Transaction. In DLT, a participant should require that transactional records related cannot be linked to prevent inferring other information about the specific participant, e.g., account balance, user type and frequency of transactions, *etc.*

1.3.3. Security properties of DLT

A DLT system involves many security properties. Table. 1.5 summarised the security properties in DLT. Basically, the security properties in DLT can be classified into consistency, tamper-resistance, DDoS attack resistance, resistance to Double-Spending Attacks, Majority (51%) attack Resistance, Consensus Attack, and Pseudonymity Li et al. [2019a].



	Requirements	Properties	Corresponding Techniques
Blockchian	• Consistency • Integrity • Availability	• Consistency • Tamper-resistance • Resistance to DDoS	• Consensus Protocols • Hash algorithm • Signature
Needs to be enhanced	• Un-linkability • Confidentiality	• Unlinkability • Majority attack	• Signature • HE • Consensus algorithms

Figure 1.5: Security and Privacy Requirements, Properties, and Techniques in DLT Zhang et al. [2019]

Main security and privacy properties **?**Zhang et al. [2019] in DLT can be summarised as

- Consistency. In DLT, the consistency denotes to the property that all participants have the same decentralised ledgers when they access the DLT at the same time. The eventual consistency model is proposed to balance between availability (A) and consistency (C), in which the performance (e.g., latency/avaiability) is a key challenge.
- Tamper-Resistance. It means the resistance to the intentional tampering from the network to an entity by either the participants or the adversaries with access to the DLT entity. The tamper-resistance is usually used to guarantee that transactional data stored in DLT cannot be tampered during/after the process of block creation. Usually, there are two possible tampering ways for transactions: (1) attempts to tamper with information of received transactions; (2) attempts to tamper with the information stored on the DLT. Sun et al. [2020]
- Resistance to DDoS Attacks. Unlike the DoS attack, which refers to denial-of-service attack on a host, the DDoS refers to 'distributed' DoS attack to a victim. A DDoS attacker focuses on the avaiability of DLT and is related to

the question of whether a DDoS attacker can make the DLT unavailable by knocking out a partial or the whole network. Al'aziz et al. [2020] A cyber-attacker aims at making DLT offline by compromising the avaiability of computation resources of participants.

- Resistance to Double-Spending Attacks (DPA). In DLT and blocckhain, the double-spending is one of key attacks, in which an attacker can create/send a copy of the transaction to make it look legitimate Sai and Tipper [2019]. To prevent Double-Spending Attacks Zhang and Lee [2019], DLT and blockchain systems (e.g., Bitcoin) need to evaluate and verify the authenticity of each transactions using the transaction logs in its blockchain with a consensus protocol, in which all transactions are included in Blockchain and the consensus protocol allows every participant to publicly verify the transactions in a block before committing the block into the global block. By combining transactions signed with digital signatures Zhu and Zhu [2012] and public verification, DLT can be resistant to the DPA.
- Resistance to the Majority Consensus Attack (MCA) Zamani et al. [2016] . The MCA, also called 51% Attack, means the risks of cheating in the majority consensus protocol. If a powerful user/group is able to control the whole DLT network, then the consensus protocol will be compromised.
- Anonymity and Pseudonymity. In DLT systems, transactions are traceable, which may compromise the privacy of users. DLT uses pseudonyms for privacy to shield identity of user as part of self-sovereignty.
- Other security and privacy properties in DLT includes unlinkability, confidentiality of transactions and data privacy, etc.

1.3.4. Challenges and trends in DLT Security

It is a challenging task to achieve security and privacy protection in a DLT system that needs to meet multiple security and privacy requirements Li et al. [2018]. In this Chapter, we summarised three remarks to achieve this:

- To achieve security and privacy of DLT is a complicated task and appropriate techniques should be applied based on the security requirements and the context of applications. The security and privacy protection needs to combine multiple techniques, e.g., HE Tourky et al. [2016], ABE Qiao et al. [2014], SMPC Shukla and Sadashivappa [2014], etc.
- The efficiency and security needs to be well trade-off in complicated DLT systems, specifically at the 'thin node' and 'full node'.

1.4. Security in DLT

This section will introduce details of the security in DLT and blockchain. Basically, the DLT security involves the five aspects:

1.4.1. Governance Scenario Security

The DLT ecosystem rules and permission manage onboarding of participants into the network and the roles within the network, which involves following security features

- identity and access management
- key management over physical level security
- security guidelines and policies in organisations

- Security Information and Event Management (SIEM)

1.4.2. DLT Application Security

The DLT widely uses smart contract to conduct automatically agreements between parties to manage the access, application data, third-party apps, etc., over the platform. The related security features include

- DLT application security
- Code security
- Third-party application security and vulnerability assessment

1.4.3. DLT Data Security

Data generated in DLT is stored on the chain that can be encrypted individual and aggregated into the chain blocks, which involve following security features:

- data encryption and key management
- data privacy regulations and guidelines
- off-chain data security

1.4.4. Transactions Security

In DLT, each participants commit transactions to decentralised ledgers with consensus algorithms, in this end, the security considerations include:

- secure and reliable consensus algorithm against double-spending, sensorship
- fork management and maintenance

1.4.5. DLT Infrastructure Security

In a DLT ecosystem, participant nodes resident in blockchain networks and systems and communicate each other through the public or private connections.

- Auditing, monitoring, and logging
- node security and management
- network vulnerability assessment

1.5. Privacy issues in DLT

In DLT, privacy is the capability to choose whether information is disclosed to others and determine how it issues. This section raise the privacy questions and focuses on key features associated with DLT. The distribute aspect of DLT means that each participant that processes transactions and builds the blockchain necessarily has access to the data itself, which means the DLT is publicly available and every transaction/event can be trace back to the original genesis block.

Another issues is that the pseudonymous location of data makes it a big concern in terms of it is open for scrutiny by everyone. The public nature of DLT make the privacy-preserving very challenging. This section summarise the key data privacy issues in DLT.

- Many DLT applications are based on the mobile/IoT devices, in which sensitive data faces the threats of breaches and compromises by the third party apps that can collect and control massive amount of sensitive data Jurcut et al. [2020].
- Privacy issues in DLT systems, including smart contract, consensus mecha-

nism, data controller, data processor or service, etc.

- Privacy issues raised in the operation of DLT. The public or permission-less DLT applications allows everyone in any location to access and participate in the network, these actives may cause risks with traditional centrally administered mode.
- Recent data privacy law. In recent, a number of data privacy regulations have been proposed to address a general policy and regulatory concerns. Some key issues between DLT and data privacy requirements has been raised, e.g., how to identify data controllers and processors in DLT implementations, territorial implications, etc.

In recent, a number of privacy-preserving solutions have been proposed for DLT and its applications: Baskaran et al. Baskaran et al. [2020] introduced an access control moderator and off-blockchain solution to address the decentralising privacy and trust in a third party. In Dorri et al. [2017], local private blockchain is used to keep track of transactions and enforce nodes access control policy to address the data privacy in DLT. Kaaniche *et al.* proposed a cryptographic protocol between blockchain and users to preserve the transactional privacy of smart contract Kaaniche and Laurent [2017]. In Zyskind et al. [2015], the secure multi-party computation is used to address the privacy of raw data in DLT.

1.6. Cyberattacks and Fraud

The DLT technology is beleived a tamper-proof ledger of transactions, DLT networks are not immunute to cyberattacks and fraud. In this section, we will simply introduce the vulnerabilities in Blockchain infrastructures.

- Code exploitation,
- Stolen keys
- Employee computer hacked
- Data access and Disclosure

Cyberattacks have become increasingly targeted and complex due to more sophisticated malware

1.6.1. Challenges

The self-descriptive title of the Distributed Ledger Technologies (DLTs) depicts their inherent nature of distributed ledgers. Hence, it is crucial to assert strong security and strong privacy-preserving policies for gaining the trust of the stakeholders of a DLT solution. However, the data distribution through the shared ledger, makes it challenging to establish the security and privacy of a DLT solution. This chapter focuses on the stated challenge and presents an overview of the state-of-the-art mechanism of well-established solution DLT solutions in the market. It will be helpful for both academic researchers and industrial practitioners in understanding the current market trends for managing the security, privacy, and trust of a DLT solution.

1.6.2. Key Privacy and Security Techniques in DLT

As mentioned above, it is very important to leverage the security and privacy and the usability in DLT. This subsection will introduce the techniques to enhance the security and privacy of DLT.

- **Mixing**. The DLT usually does not guarantee anonymity for users (but provide traceability for transactions), in which transactions use pseudonymous addresses that could be publicly verified. Mixing (or tumblers) is a technique that random exchange of information between users to prevent users' addresses from being linked, which is widely used in the crypto-currencies. Typical mixing techniques include *Mixcoin, CoinJoin, etc.*
- Anonymous signature. In DLT, anonymous signature schemes (group signature, ring signature) were proposed to provide anonymity for the signer.
- **Homomorphic encryption (HE)**. HE has been significantly improved in recent and becomes a powerful cryptography that can perform computations directly on ciphertext without needing decrypt them. The DLT can use HE techniques to deal with data over the chain with no significant changes in the blockchain properties to ensure that the data on the chain will be encrypted. This could address the privacy concerns. The HE techniques provide privacy protection and allow access to encrypted data over public DLT.
- **Attribute-Based Encryption (ABE)**. The ABE is a public-key encryption method in which the secret key of a user and the cipertext are dependent upon attribute. In DLT, the decentralised ABE can be employed, in which the permissions could be represented by the ownership of access tokens.
- In DLT, the trusted execution environment (TEE) could provide a privacy-preserving running environment for smart contracts. However, it needs extra software support, such as the Intel software guard extensions (SGX), etc.

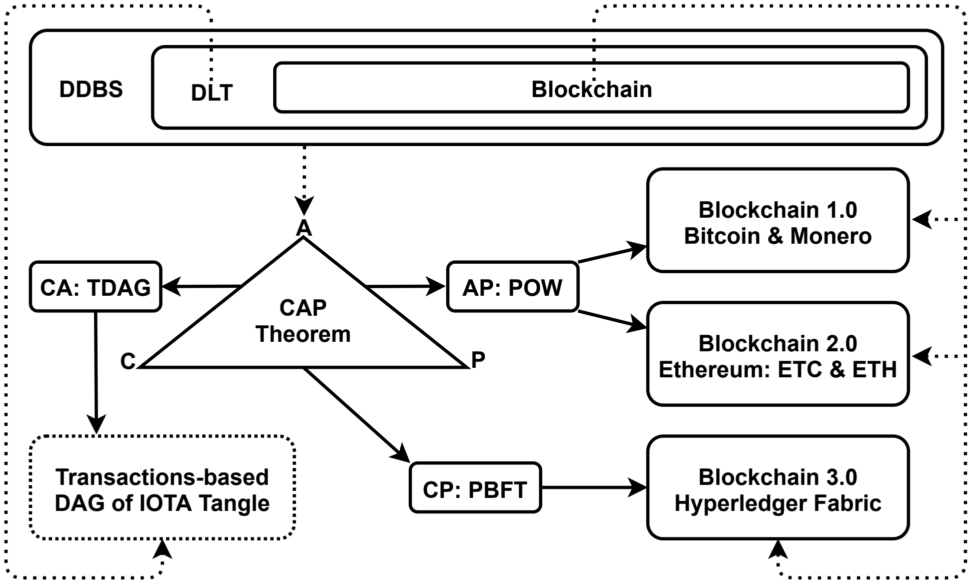


Figure 1.6: Flow of content for the section of implementations of different DLT solutions.

1.7. DLT Implementation and Blockchain

In this section, we are focusing only on the DLT solutions that have been well-established in the crypto market. We are not covering the solutions that are in the proposal or research phases. For example, a research project of zkLedger utilizes zero-knowledge proofs for the auditing of the private data stored on the ledger. However, we are not covering this project since it has to industrial footprint yet.

Similarly, from each discussed category of the DLTs, we are focusing on the most popular and successful DLT solution or framework. For example, there are many projects under the umbrella of hyperledger but we are only covering the most popular option of hyperledger fabric in the fifth section of this chapter.

1.7.1. Cryptocurrencies and Bitcoin

The first generation of blockchain solutions was focused only on a single application of financial services through virtual tokens that are known as cryptocurrencies. The consensus algorithm is the main contributing feature of the first generation of blockchain solutions and it provided the technical foundations for offering public blockchain solutions of cryptocurrencies. Thousands of different cryptocurrencies were launched to date. However, bitcoin was the first and most popular cryptocurrency that we are going to cover in this section. We will also cover the two privacy coins of monero and zcash in this section.

1.7.1.1. Origin of Blockchain

Bitcoin was the first project to initiate the idea of blockchain in 2009. It operates over the PoW (Proof of Work) that provides the basis for the collaboration of independent and non-trusted entities to execute the transactions in a distributed manner. Although PoW usually refers to serve as a consensus algorithm in theory. However, it is just a Sybil control mechanism that combines with the idea of the selection of the longest chain for practically serving as a consensus algorithm.

1.7.1.2. Bitcoin

Although bitcoin believe to be the most secure blockchain solution, it has the following shortcomings regarding security, privacy, and trust:

- **Security:** Bitcoin is the most secure blockchain solution. However, it operates over a very costly mining algorithm of the nonce (number of ones) finding. Furthermore, this PoW needs to combine with the selection of the longest chain to serve as a consensus mechanism. It results in some issues like selfish mining strategies, withholding, towing, and temporary shutdown tactics. These issues allow the groups with huge mining capabilities to influence the consensus algorithm for their interests. However, the number of minable coins is reducing over time and will eventually result in the depletion of all the minable coins. Hence, the severity of the listed problems will automatically keep on reducing.

- **Privacy:** Bitcoin offers pseudo-anonymity by representing users with unique arbitrary hashes that can be traced by linking multiple transactions listed in the ledger of bitcoin. Furthermore, the privacy of stored data is preservable through the PoE (Proof-of-Existence).
- **Trust:** Although bitcoin is the most trusted cryptocurrency, a few of the reported shortcomings may result in an uneven distribution of coins during the mining process that we discussed in the security issues. However, these minor issues are not well-known and thus the bitcoin is the most-trusted cryptocurrency to date.

1.7.1.3. Monero

Monero Wijaya et al. [2019] is a privacy coin that shines in handling the privacy of the end-users. It is the most popular cryptocurrency that ensures the anonymity of the stack-holders. Dash dashplatform and z-cashz cash are also the two privacy coins. However, the dash is lagging in popularity whereas the z-cash offers both open and stealth transactions. Hence, we are discussing the Monero and z-cash in this section. Details of Monero are given below:

- **Security:** Monero shifted to the mining algorithm of RandomX Monero in November 2019 that encourages CPU mining by resisting ASIC mining. A couple of vulnerabilities have been reported and successfully patched in Monero's algorithm before that. Monero is lesser mature since it was launched five years after the bitcoin in 2014. Its algorithm is also more complex than the bitcoin. Hence, there are more chances of zero-day vulnerabilities in Monero that makes it lesser secure than Bitcoin.
- **Privacy:** Monero is the most popular privacy coin on earth. It earned this title by offering full anonymity to the end-users performing transactions through this coin. Monero achieves this anonymity through Stealth addresses along with a non-interactive zero-knowledge proof (NIZKP) Tsai et al. [2019] protocol implemented as a bulletproofs algorithm. However, its privacy feature is only limited to the anonymity of the end-users. For the privacy of stored data, similar to bitcoin, Monero also depends on the PoE.
- **Trust:** Monero is well-trusted by the end-users. However, the regulatory bodies are not ready to trust Monero due to its non-compliance with AML (Anti-Money Laundering) laws since it resists the notion of KYC (Know Your Customer) by offering full anonymity to the end-users.

1.7.2. Blockchain and Smart Contracts

The second generation of blockchain is focusing on multiple applications based on cryptocurrencies. Smart contracts are the main contributing feature of this generation, which provides the technical foundations for offering public/permissioned blockchain solutions for DApps (Distributed Applications) only.

The second generation of blockchain solutions exploits the potential of smart contracts for innovating solutions alongside cryptocurrencies. Ethereum appeared in 2015 as a pioneer of the second generation of blockchain solutions by offering JavaScript-inspired programming language of solidity for writing smart contracts.

Forbes found more than 100 large American corporations that were actively exploring blockchain technology in 2019 and many of them were focusing on the ethereum network. Since ethereum was the first second-generation blockchain-solution, it presents few lessons that are adaptable in the feature versions of the second-generation blockchain solution. Hence, it was devised to proceed with two independent versions of ethereum classic (ETC) and ethereum (ETH). This section covers both of these versions of ETC and ETH in detail.

1.7.3. Typical Blockchain Systems

1.7.3.1. Ethereum Classic (ETC)

Ethereum Classic di Angelo and Salzer [2019] is an open-source solution that is powering the public blockchain network of ETC. It can also be used for establishing private blockchain networks. Next is the discussion on the security, privacy, and trust features of the first version of ethereum.

- **Security:** After the first year of its launch, the ethereum underwent a 51% percent attack on DAO (Decentralized Autonomous Organization) in 2016 that resulted in the splitting of ethereum into ETC (Ethereum Classic) and ETH (Ethereum). ETC has also gone through three consecutive 51% attacks in one month of August 2020. It reflects the vulnerability of smart contracts and ETH is shifting to POS in its next version of Ethereum 2. Unfortunately, ETC is not backward compatible with ETH, it will not be able to take advantage of ETH's migration to the POS.

- **Privacy:** Same like first-generation blockchain platforms, ethereum is pseudonymous and it also depends on the POE for ensuring the privacy of the stored data.
- **Trust:** Due to the hard-fork of ETH from ETC, the community has observed the vulnerability of taking drastic decisions by neglecting the opinion of others. This becomes a more serious concern in the next version of POS-based ETH where larger stakeholders can also influence the future decisions of the ETH that eventually leads to lesser decentralization.

1.7.3.2. Ethereum (ETH)

Ethereum (ETH) was originated as a result of a hard-fork of ETC. It has better than ETC and therefore more trusted by the industry as compared to the ETC. However, it has privacy controls similar to the ETC.

1.7.3.3. Extensibility of Blockchain and DLT

The third generation of blockchain is focusing on the interoperability of multiple applications without being dependent on cryptocurrencies. The flexibility for custom policies and consensus algorithms is the main contributing feature of this generation, which provides the technical foundations for offering permission blockchain solutions that can exist without cryptocurrencies.

1.7.4. Origin of Blockchain 3.0

The blockchain framework of fabric is operated by the Linux Foundation under the umbrella of the hyperledger ecosystem. The initial modular structure of hyperledger fabric Dabbagh et al. [2020] was contributed, in 2016, by IBM and digital assets for giving an improved version of blockchain solutions that are not primarily focused on the digital assets of tokens or cryptocurrencies. Hence, it inherently differs from the first two generations of blockchain as generation one was only based on cryptocurrencies while the second generation was an extension of the cryptocurrencies with an extra layer of smart contracts. However, the advent of third-generation, in the form of hyperledger ecosystem, was not targetting the cryptocurrencies. Hence, end-users can very easily develop tokenless blockchain solutions that can operate without the need for any cryptocurrencies. The hyperledger ecosystem contains many other tools, frameworks, and libraries while we will be targetting its most popular framework of hyperledger fabric.

1.7.5. Overview of Hyperledger Fabric

Ethereum (a public, permissionless blockchain) and Quorum (private, permissioned blockchain based on Ethereum code) are based on execute-order architecture. Some of the limitations that this introduces are sequential execution of all transaction which directly affects transaction throughput. The main concept that differentiates Hyperledger Fabric from other blockchains is its execute-order-validate architecture. Transactions in Hyperledger Fabric do need not be executed by each peer.

We can define the endorsement policy that specifies which peer nodes have to execute the transaction and give their endorsement. This means that we can define a subset of peers to execute (endorse) a given transaction and satisfy the transaction's endorsement policy. Therefore, this allows for parallel execution of transactions and directly boosts performances of the system. Hyperledger separates transaction flow in three distinct steps:

- **Transaction Execution:** In this initial phase, the client collects the predefined number of endorsements from the nodes that are already designated as the endorser nodes. These nodes execute the corresponding smart contract and return a stamped version to the requesting client.
- **Ordering:** The same client again sends all the collected endorsements to the predefined orderer node that forwards it to random validating nodes.
- **Transaction Validation:** These nodes discard or successfully execute the transactions over the distributed ledger after validating that all the requirements of the consensus algorithms have been met. The collection of a specific number of endorsements in the first step is also dictated by the consensus algorithm.

1.8. DLT of IOTA Tangle

All of the previously discussed solutions are both DLTs and blockchain-based solutions. However, in this section, we are going to introduce the DLT solution of IOTA Tangle which is not a blockchain. It is a tailored solution for IoT devices that compromises the partition tolerance for achieving the consistency and availability features of the CAP theorem.

The solution of IOTA is based on a DAG (Directed Acyclic-Graph) Tangle technology. The word IOTA refers to both the parent organization as well as the associated token while the tangle is the protocol and the underlying ledger in the form of a graph. In this graph, the nodes at one end are not entirely aware of the state of the other end of the graph. This is in contrast to the blockchain where all the nodes have exactly similar views of the ledger.

In IOTA, the transactions of different sections of a graph are kept on synchronizing but time spent during this transaction results in the emergence of new transactions at the remote ends of the graph. Hence, different nodes are viewing the different states of the graph at a single time interval. Since IOTA is compromising the partition tolerance, therefore, thousands of transactions can be executed per second at different ends of the graph. IOTA is also a highly scalable solution as it requires every transaction initiation node to validate two other transactions, originated by the different nodes, for showing the PoW. This gives IOTA an option to operate with zero fees as compare to the other blockchain-based DLT solutions.

In terms of security, smart contracts are landed in the IOTA world recently in a pre-alpha release in October 2020. Hence, these will take time in getting mature and gaining the trust of the audience. Similarly, the IOTA is more vulnerable than the other discussed blockchain-based solutions because it only requires 34% of the total hashing power for taking the control of tangle which is 51% for the blockchain-based solutions. This is because each one node is validating the transactions of the two other nodes. Hence, almost one-third of the malicious nodes of the total nodes will be enough for performing the 51% attack in IOTA. In contrast to the blockchain solutions, IOTA claims to be the quantum resistance since it uses the trinary or balanced ternary computations while blockchain only uses the standard binary cryptographic computations.

1.9. Trilemma of Security, Scalability, and Decentralization

According to Vitalik Buterin, the founder of Ethereum, it is not possible to equally optimized the three crucial attributes of security, decentralization, and scalability in a blockchain system. Hence, more and more blockchain projects (like Cardano, Polkadot, etc.) are originating after tweaking different parameters for trying to optimize all of the features of security, decentralization, and scalability at the same time. Here we are going to explain it with the examples of first and second-generation blockchain solutions.

1.9.1. First generation solutions: BTC / BCH

The Bitcoin (BTC) operates with a block size of 1MB while a movement was started to increase the block size of BTC for improving its transaction rate. However, due to a disagreement in the bitcoin community, a hard fork of BTC happened with the title of Bitcoin Cash (BCH) at block number 478559. BCH increased the BTC block size from 1MB to 8MB which resulted in improving the transaction rate from 7 transactions per second for BTC to 116 transactions per second for BCH. Although BCH has achieved improvements in transaction rate, they compromised the decentralization but collecting more transactions at the same node. The tremendous popularity of BTC proves that decentralization is very important for winning the trust of the audience.

1.9.2. Second generation solutions: ETH / BSC

To reduce the higher gas price of Ethereum (ETH), Binance launched an exact clone of opensource code of ETH project with less gas price by compromising the decentralization, under the title of BSC (Binance Smart Chain). Again the tremendous popularity of ETH shows that the crypto community trusts decentralized solutions.

1.9.3. Threats in DLT and Blockchain networks

Like other DLT and blockchain networks, following threats are common Saad et al. [2020]:

- Spoofing. Malicious attackers pretend to be or impersonate an authentic user. The HLF attempts to mitigate this with having a high quality CA bult in using the highest quality certificates X.509.
- Tampering. The HLF uses the built-in encryption like sha-256 or elliptic curve cryptography algorithms.
- Repudiation. The HLF uses a built-in strict logs to track events that lead to ledger creation.
- Replay attacks. In some case, the replaying of events will corrupt the blockchain itself. The HLF has read/write sets to validate transactions and if transactions fail, read sets invalidate the transaction.

1.10. Security architecture in DLT and Blockchain

In many DLT application scenarios, the security standards and regulations are still in its infant stage. This section will introduce the security architecture in DLT and blockchain that can help to establish a secure environment by leveraging the cybersecurity risks, best practices, and risk mitigation. Basically, a DLT system requires assessment, authorisation, authority to operate processes to determine whether they comply with security regulation and privacy requirements (e.g., GDPR), and security on DLT entities (e.g., Blockchain networks, participants, actors, etc.).

Figure 1.7 shows an example of security architecture in a DLT application, which contains three key components Homoliak et al. [2019]:

- Risk management and scrutinising
- Threats analysis and model
- Security controls that mitigate the risks and threats

Physically, it can be implemented over a four-layer architecture:

- DLT Network Layer. It consists of data representation and network services planes, which deals with the storage, encoding, and protection of data, while the network services focus on discovery, communication with protocol peers, addressing, naming system, etc.
- Consensus Layer. This layer focuses on the dynamic protocol of reaching agreement in a group, which can be classified into three main categories according to the protocols: *Byzantine Fault Tolerant, PoR, PoS.*
- Application Layer. It contains the most common application/services.

- The state management machine (SMM). It deals with the interpretationof trasanctions.

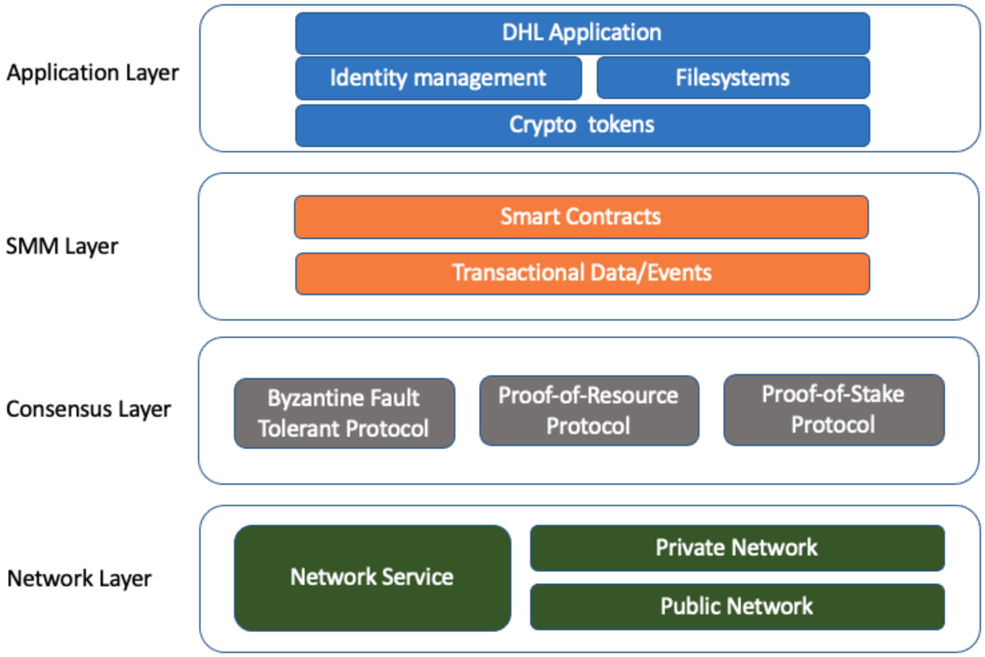


Figure 1.7: DLT security Architecture

1.10.1. Threat model in LDT

Together with the potential benefits, the DLT technologies are also facing a number of potential threats and attack vectors Putz and Pernul [2020b], as shown in Figure 1.8. Like other IT systems, the LDT security theats can also be mapped to the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service attacks, and Elevation of privilege (STRIDE) threat model developed by Microsoft [1]. The STRIDE model can be used to address the

[1] https://www.howardposton.com/blog/threat-modeling-for-the-blockchain

relationships between entities in LDT, review threats and weakness related to these relationships, and propose appropriate mitigation.

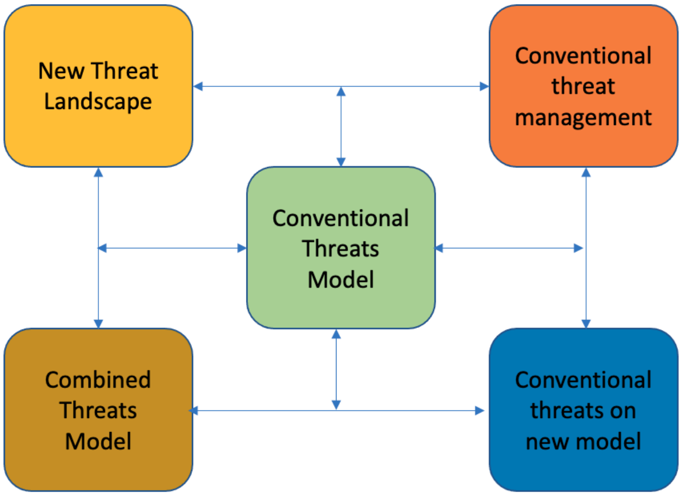

New Threat Landscape
Conventional threat management
Conventional Threats Model
Combined Threats Model
Conventional threats on new model

Figure 1.8: Threat model in DLT [2]

The DLT applications often incorporate with existing IT systems, such as authentication, identity management systems, access control system, regulatory, log and auditing system, public crypto key system, etc. Aligning with existing system, threats needs to be addressed in the DLT system, as shown in Figure 1.8[2], in which it is important to fully understood the *new threat landscape*, new vulnerabilities in DLT infrastructure and tempering with smart contract. For a DLT application, it is not infeasible to build a universal threat model, and specific threats analysis should be conducted based on the application. Also, it is necessary to ensure a secure system environment for a DLT application to use corporate security standards.

[2] https://developer.ibm.com/technologies/blockchain/articles/how-to-secure-blockchain-solutions/

1.11. Research Trends and Challenges

One of challenges that the DLT is facing is lack of clarity on the terminology. The DLT has been discussed for a long time, however there a big gap between the technical implementation of DLT and businesses model, which makes it difficult to understand how DLT operates in real world industry. The DLT undoubtedly benefits the existing business processes, however it is still an open question how to integrate DLT into existing legacy system without disrupting to existing industry practices Wustmans et al. [2021]. In recent, many research efforts focus on the governance of DLT to establish liability among partners in both permissioned and permissionless systems to reduce potential operation failure or compromises.

One of the research trends is to integrate blockchain with an already well-established solutions. For example, DocsChain is a solution that integrates the image processing and blockchain for offering the degree verification Rasool et al. [2020b]. Docs.vet is an improved form of the DocsChain that extends it for the verification of identity documents. Another solution of MultiCoT integrates the blockchain within the osmotic computing to offer the Multi-Cloud of Things solution Rasool et al. [2020c]. Another project integrates the blockchain in the MEC (Multi-access Edge Computing) to offer the reliable resource sharing for supporting a mobile ad-hoc cloud at the edge of the network Rasool et al. [2020a].

Bibliography

Iee colloquium on 'distributed databases' (digest no.229). In *IEE Colloquium on Distributed Databases*, pages $0_1 - -$, 1992.

Consensus in the iota tangle — fpc, August 2019. URL https://blog.iota.org/consensus-in-the-iota-tangle-fpc-b98e0f1e8fa/.

Tejasvi Alladi, Vinay Chamola, Reza M. Parizi, and Kim-Kwang Raymond Choo. Blockchain applications for industry 4.0 and industrial iot: A review. *IEEE Access*, 7:176935–176951, 2019. doi: 10.1109/ACCESS.2019.2956748.

Bram Andika Ahmad Al'aziz, Parman Sukarno, and Aulia Arif Wardana. Blacklisted ip distribution system to handle ddos attacks on ips snort based on blockchain. In *2020 6th Information Technology International Seminar (ITIS)*, pages 41–45, 2020. doi: 10.1109/ITIS50118.2020.9320996.

Hasventhran Baskaran, Salman Yussof, and Fiza Abdul Rahim. A survey on privacy concerns in blockchain applications and current blockchain solutions to preserve data privacy. In Mohammed Anbar, Nibras Abdullah, and Selvakumar Manickam, editors, *Advances in Cyber Security*, pages 3–17, Singapore, 2020. Springer Singapore.

Yun Chen, Hui Xie, Kun Lv, Shengjun Wei, and Changzhen Hu. Deplest: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks. *Information Sciences*, 501:100–117, 2019.

Alexander Chepurnoy, Tuyet Duong, Lei Fan, and Hong-Sheng Zhou. Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake. *IACR Cryptol. ePrint Arch.*, 2017:232, 2017.

Sunghyun Cho and Sejong Lee. Survey on the application of blockchain to iot. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, pages 1–2, 2019. doi: 10.23919/ELINFOCOM.2019.8706369.

Mohammad Dabbagh, Mohsen Kakavand, Mohammad Tahir, and Angela Amphawan. Performance analysis of blockchain platforms: Empirical evaluation of hyperledger fabric and ethereum. In *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, pages 1–6, 2020. doi: 10.1109/IICAIET49801.2020.9257811.

dashplatform. Dash platform developer documentation. URL https://dashplatform.readme.io/.

Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. 2018.

Monika di Angelo and Gernot Salzer. A survey of tools for analyzing ethereum smart contracts. In *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, pages 69–78, 2019. doi: 10.1109/DAPPCON.2019.00018.

Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pages 618–623. IEEE, 2017.

Lars Frank, Rasmus Ulslev Pedersen, Christian Havnø Frank, and N. Jesper Larsson. The cap theorem versus databases with relaxed acid properties. In *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication*, ICUIMC '14, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450326445. doi: 10.1145/2557977.2557981. URL https://doi.org/10.1145/2557977.2557981.

Christine V Helliar, Louise Crawford, Laura Rocca, Claudio Teodori, and Monica Veneziani. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54:102136, 2020.

Ivan Homoliak, Sarad Venugopalan, Qingze Hum, and Pawel Szalachowski. A security reference architecture for blockchains. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 390–397, 2019. doi: 10.1109/Blockchain.2019.00060.

Anca Jurcut, Tiberiu Niculcea, Pasika Ranaweera, and Nhien-An Le-Khac. Security considerations for internet of things: A survey. *SN Computer Science*, 1(4):193, Jun 2020. ISSN 2661-8907. doi: 10.1007/s42979-020-00201-3. URL https://doi.org/10.1007/s42979-020-00201-3.

Nesrine Kaaniche and Maryline Laurent. A blockchain-based data usage auditing architecture with enhanced privacy and availability. In *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, pages 1–5. IEEE, 2017.

S. Li, Q. Sun, and X. Xu. Forensic analysis of digital images over smart devices and online social networks. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1015–1021, 2018. doi: 10.1109/HPCC/SmartCity/DSS.2018.00168.

S. Li, K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao. Iot forensics: Amazon echo as a use case. *IEEE Internet of Things Journal*, 6(4):6487–6497, 2019a. doi: 10.1109/JIOT.2019.2906946.

S. Li, T. Qin, and G. Min. Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Transactions on Computational Social Systems*, 6(6):1433–1441, 2019b. doi: 10.1109/TCSS.2019.2927431.

Mahdi H. Miraz and Maaruf Ali. Applications of blockchain technology beyond cryptocurrency. *Annals of Emerging Technologies in Computing*, 2(1):1–6, Jan 2018a. ISSN 2516-0281. doi: 10.33166/aetic.2018.01.001. URL http://dx.doi.org/10.33166/AETiC.2018.01.001.

Mahdi H. Miraz and Maaruf Ali. A survey on cryptography algorithms. 8(7): 495–516, July 2018b. ISSN 2250-3153. doi: 10.29322/IJSRP.8.7.2018.p7978. URL http://dx.doi.org/10.29322/IJSRP.8.7.2018.p7978.

Monero. What is randomx mining algorithm in monero? URL https://academy.bit2me.com/en/which-mining-algorithm-randomx-monero/.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

Benedikt Putz and Günther Pernul. Detecting blockchain security threats. In *2020 IEEE International Conference on Blockchain (Blockchain)*, pages 313–320, 2020a. doi: 10.1109/Blockchain50366.2020.00046.

Benedikt Putz and Günther Pernul. Detecting blockchain security threats. In *2020 IEEE International Conference on Blockchain (Blockchain)*, pages 313–320, 2020b. doi: 10.1109/Blockchain50366.2020.00046.

Zhi Qiao, Shuwen Liang, Spencer Davis, and Hai Jiang. Survey of attribute based encryption. In *15th IEEE/ACIS International Conference on Software*

Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pages 1–6, 2014. doi: 10.1109/SNPD.2014.6888687.

Saqib Rasool, Muddesar Iqbal, Tasos Dagiuklas, Zia Ul-Qayyum, and Shancang Li. Reliable data analysis through blockchain based crowdsourcing in mobile ad-hoc cloud. *Mobile Networks and Applications*, 25(1):153–163, 2020a.

Saqib Rasool, Afshan Saleem, Muddesar Iqbal, Tasos Dagiuklas, Shahid Mumtaz, and Zia ul Qayyum. Docschain: Blockchain-based iot solution for verification of degree documents. *IEEE Transactions on Computational Social Systems*, 7 (3):827–837, 2020b.

Saqib Rasool, Afshan Saleem, Muddessar Iqbal, Tasos Dagiuklas, Ali Kashif Bashir, Shahid Mumtaz, and Sattam Al Otaibi. Blockchain-enabled reliable osmotic computing for cloud of things: Applications and challenges. *IEEE Internet of Things Magazine*, 3(2):63–67, 2020c.

Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and David Mohaisen. Exploring the attack surface of blockchain: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 22(3):1977–2008, 2020. doi: 10.1109/COMST.2020.2975999.

Kuheli Sai and David Tipper. Disincentivizing double spend attacks across interoperable blockchains. In *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 36–45, 2019. doi: 10.1109/TPS-ISA48467.2019.00014.

Samiksha Shukla and G Sadashivappa. Secure multi-party computation protocol using asymmetric encryption. In *2014 International Conference on Computing* *for Sustainable Global Development (INDIACom)*, pages 780–785, 2014. doi: 10.1109/IndiaCom.2014.6828069.

Harish Sukhwani, José M Martínez, Xiaolin Chang, Kishor S Trivedi, and Andy Rindos. Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). In *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pages 253–255. IEEE, 2017.

Jianfei Sun, Hu Xiong, Shufan Zhang, Ximeng Liu, Jiaming Yuan, and Robert H. Deng. A secure flexible and tampering-resistant data sharing system for vehicular social networks. *IEEE Transactions on Vehicular Technology*, 69(11): 12938–12950, 2020. doi: 10.1109/TVT.2020.3015916.

Ali Sunyaev. Distributed ledger technology. In *Internet Computing*, pages 265–299. Springer, 2020.

Dalia Tourky, Mohamed ElKawkagy, and Arabi Keshk. Homomorphic encryption the “holy grail” of cryptography. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pages 196–201, 2016. doi: 10.1109/CompComm.2016.7924692.

Ya Che Tsai, Raylin Tso, Zi-Yuan Liu, and Kung Chen. An improved non-interactive zero-knowledge range proof for decentralized applications. In *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, pages 129–134, 2019. doi: 10.1109/DAPPCON.2019.00025.

P. Urban, N. Hayashibara, A. Schiper, and T. Katayama. Performance comparison of a rotating coordinator and a leader based consensus algorithm. In *Proceedings of the 23rd IEEE International Symposium on Reliable Distributed Systems, 2004.*, pages 4–17, 2004. doi: 10.1109/RELDIS.2004.1352999.

Abdul Wahab and Waqas Mehmood. Survey of consensus protocols, 2018.

Dimaz Ankaa Wijaya, Joseph K Liu, Ron Steinfeld, Dongxi Liu, and Jiangshan Yu. On the unforkability of monero. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 621–632, 2019.

Michael Wustmans, Thomas Haubold, and Bennet Bruens. Bridging trends and patents: Combining different data sources for the evaluation of innovation fields in blockchain technology. *IEEE Transactions on Engineering Management*, pages 1–13, 2021. doi: 10.1109/TEM.2020.3043478.

Kimchai Yeow, Abdullah Gani, Raja Wasim Ahmad, Joel JPC Rodrigues, and Kwangman Ko. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access*, 6:1513–1524, 2017.

z cash. z-cash documentation. URL https://zcash.readthedocs.io/en/latest/.

Mohsen Zamani, Alireza Khosravian, and Brett Ninness. Compensation of attacks on consensus networks. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3491–3495, 2016. doi: 10.1109/ICASSP.2016.7472326.

Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3):1–34, 2019.

Shijie Zhang and Jong-Hyouk Lee. Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*, 15(10):5715–5722, 2019. doi: 10.1109/TII.2019.2921566.

S. Zhao, S. Li, and Y. Yao. Blockchain enabled industrial internet of things technology. *IEEE Transactions on Computational Social Systems*, 6(6):1442–1453, 2019. doi: 10.1109/TCSS.2019.2924054.

Likun Zhu and Lizhe Zhu. Electronic signature based on digital signature and digital watermarking. In *2012 5th International Congress on Image and Signal Processing*, pages 1644–1647, 2012. doi: 10.1109/CISP.2012.6469828.

Andrej Zwitter and Jilles Hazenberg. Decentralized network governance: Blockchain technology and the future of regulation. *Frontiers in Blockchain*, 3:12, 2020. ISSN 2624-7852. doi: 10.3389/fbloc.2020.00012. URL https://www.frontiersin.org/article/10.3389/fbloc.2020.00012.

Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.