# Blockchain Security

## A Framework for Trust and Adoption

Dutch Blockchain Coalition

connect and create

www.dutchblockchaincoalition.org

# Authors:

Nicolas Castellon, CGI Nederland
Peter Cozijnsen, CGI Nederland
Tjerk van Goor, CGI Nederland

Graphic design by Dune Pebbler
Graphic design of infographic by Elene Pacuk, CGI Nederland

The authors would like to thank the following people for their input in the different stages of defining this framework:

- Pawel Szalachowski, Singapore University of Technology
- Virgil Griffith, Ethereum Foundation
- Sofie Berns, Berenschot
- Tommy Koens, ING
- Tey El-Rjula, Tykn
- Idius Felix, Zorginstituut Nederland

We would also like to thank the partner organizations that have contributed content and analysis to this framework:

- TNO
- Delft University of Technology
- Pels Rijcken & Droogleever Fortuyn
- LedgerLeopard
- Amsterdam University of Applied Sciences
- ECP | Platform voor de InformatieSamenleving

This whitepaper was funded by the Ministry of Justice and Security for the Dutch Blockchain Coalition.

# Executive Summary

With the current rise in popularity of blockchain, more organizations are beginning to consider this technology to innovate their IT environments. With every new technology, security risks are amplified or diminished depending on its characteristics. This whitepaper provides a framework on the major security considerations to consider when adopting blockchain technologies. The framework was written to be used by decision makers in organizations that are planning to adopt blockchain technology. The framework is meant to be a high-level practical guide of the top security concerns an organization should consider when starting their own blockchain application or migrating a current application to this new environment.

The following are the top 18 security risks to consider when adopting the technology:

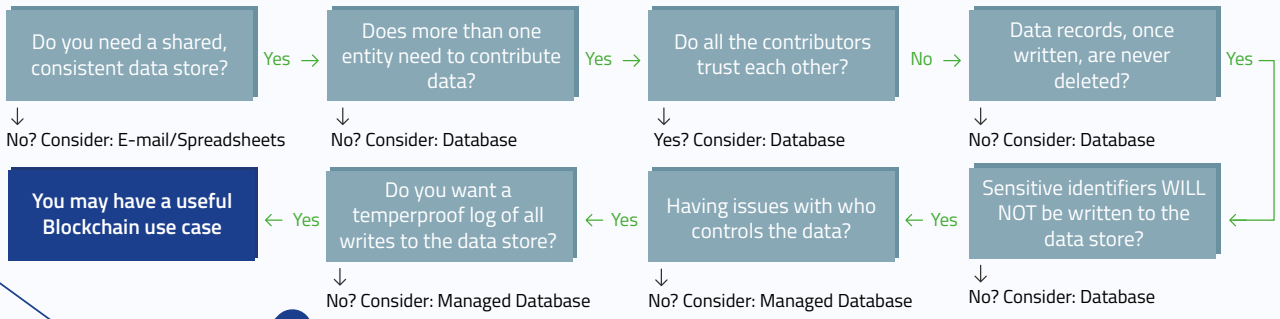
1. **Security of Smart Contracts**
2. **Forks**
3. **Crypto Algorithms**
4. **Cryptographic key management**
5. **Access Control**
6. **Scalability**
7. **Intrusion Detection**
8. **Targeted attach resistance**
9. **Data Propagation attach resistance**
10. **Operations & Communications security**
11. **System Acquisition, Development, and Maintenance**
12. **Asset management**
13. **Human resource security**
14. **Supplier relationships**
15. **Incident management**
16. **Organization of Information Security**
17. **Information Security Policies**
18. **External/Internal Compliance**

The following are the top 6 security risks to consider when migrating a current application to this new environment:

1. **Choosing the right blockchain**
2. **Special considerations for testing**
3. **Awareness and training**
4. **Contingency planning**
5. **Simplicity as a security measure**
6. **Privacy**

These considerations will offer organizations a strong base upon which to adopt blockchain technology and do so in a secure manner. With these 24 security recommendations, organizations can begin trusting this technology and find innovative ways to use it in their IT environments.

# Do you need Blockchain?




## Top Security Considerations

### Smart contracts

- **Risks** lie in life cycle of contract. Since code cannot be changed, through **testing** of the functionality is **required**.

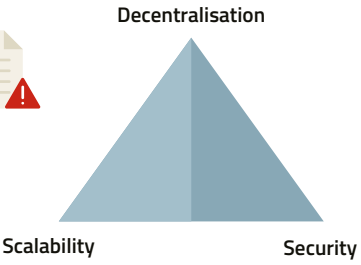
### Cryptography

- In **public blockchains**, the **algorithm** is **pre-determined** by the creators of the blockchain and will **rely** on the **community** using the chain.
- In private blockchain: adequate configuration, **control** of the **configuration**, including the **amount of miners**, the **distribution**, and the appropriate **hashing algorithm**.

### Privacy

- It is highly advised to **not** have any **personal user data** on the blockchain itself
- It is important to be **compliant** with the **General Data Protection Regulation** (GDPR).

## The Blockchain Trilemma




Remember to consider how decentralization and scalability affect the security of the application.

## Public vs Private

| Public | | Private |
|---|---|---|
| Commonly used are "Proof of Stake" and "Proof of Work" | **Consensus algorithm** | Agreed-upon with pre- defined rules. "Proof of Authority" mostly used in Netherlands |
| High | **Scalability** number of nodes | Low |
| In general slow | **Performance** transaction per second | In general high |
| Everybody is free to join | **Participation in the network** | Defined group of participants |
| Determined by the community | **Development** | Controlled by the participants |
| Not recommended | **Privacy when using personal data** | Generally not recommended. Implement high-levels of security if considered |
| Anonymous or Pseudonymous | **Identity of the nodes in the network** | Known identities |

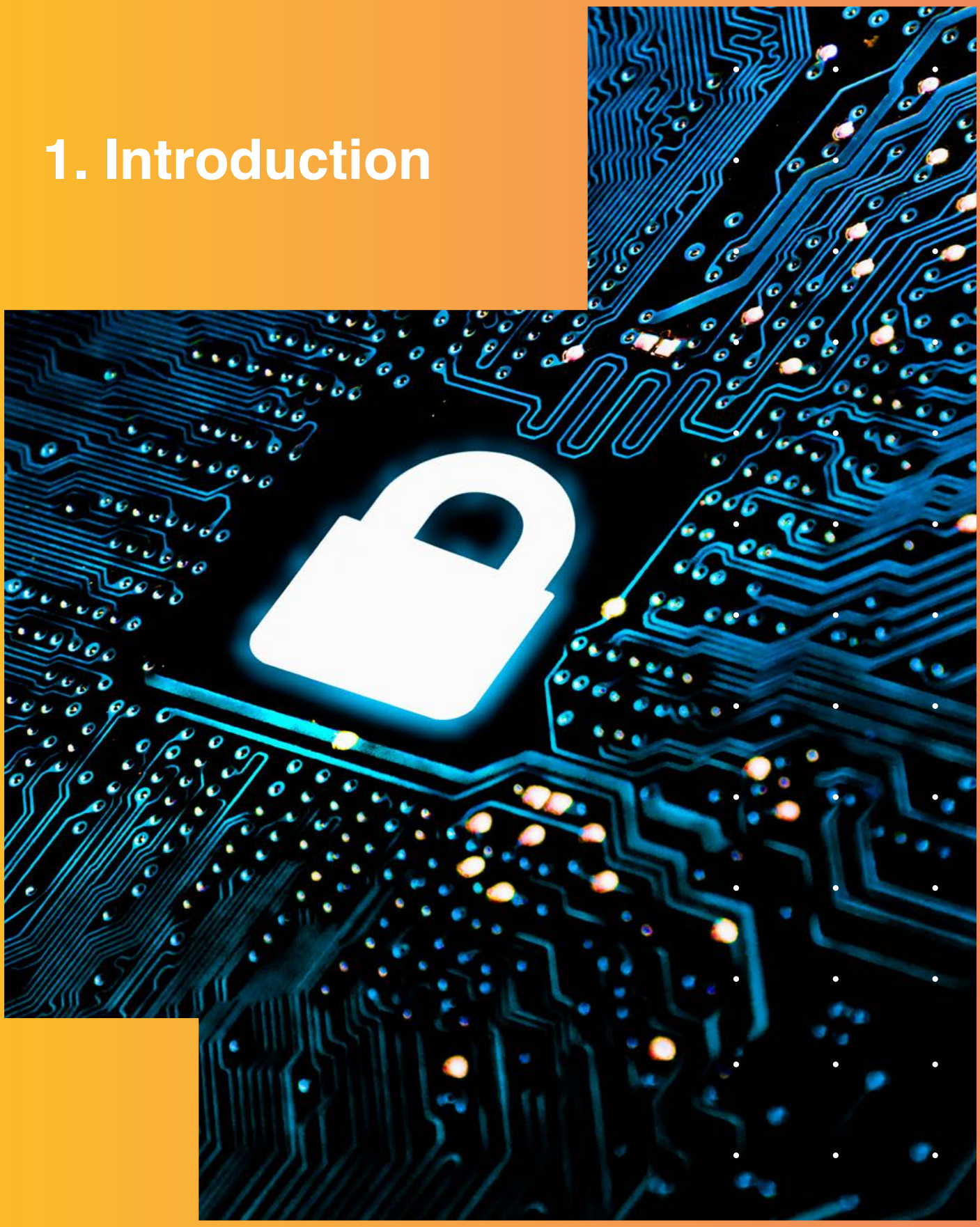
# Contents



**Abbreviations**

| | |
|---|---|
| 2FA | Two Factor Authentication |
| ABCI | Application Blockchain Interface |
| CPU | Computer Processing Unit |
| DLT | Distributed Ledger Technology |
| DPA | Data Protection Authority |
| GDPR | General Data Protection Regulation |
| KYC | Know Your Client |
| PIA | Privacy Impact Assessment |
| PKI | Public Key Infrastructure |
| PoA | Proof of Authority |
| PoS | Proof of Stake |
| PoW | Proof of Work |
| OPSEC | Operations Security |
| OWASP | Open Web Application Security Project |

# 1. Introduction



# Introduction

Blockchain has become a fast-rising technological trend. Though the origins of its popularity are in cryptocurrencies, we are now starting to appreciate this technology for the changes it can bring in our IT environments. Blockchain technology provides some advantages that are not available in conventional databases, IT systems or applications. Blockchain offers the possibility to avoid a central authority, eliminates intermediaries, provides real-time settlement, reduces operational costs, and has high levels of transparency. These are just some of the potential advantages that this new technology can contribute to our IT environments.

With every new technology, also come new perspectives to security risks. In this way, blockchain technology is no different than any other modern technology- such as Cloud computing or the Internet of things. All technology is vulnerable to security risks.

Identifying risks for new technologies entails examining the technology and assessing how it can amplify or reduce certain risks. As more organizations begin to consider blockchain technology as a possible solution to innovate their IT infrastructure and applications, it is important to consider the security risks of this new environment. For blockchain, this will concern risks brought by its key characteristics. These characteristics are its distributed nature, its cryptographic seal, its immutability, and its transparency to name a few. These new characteristics are at the core to understand what the security risks are for this new technology.

This framework was developed in order to help organizations understand the security risks that come with blockchain technology. This framework was written for organizations that have made the decision to adopt blockchain technology and would like to be made aware of the security issues to consider in this new environment. It is meant to be a high-level guide that should be used as a reference point for decision makers speaking to suppliers, developers or integrators of this new technology. Though the content of the framework is meant for all organization sizes, we are aware that SMEs might not have the resources to have a team of researchers or experts dedicated to exploring the impact of blockchain technologies on the security of their organization. With this in mind, we have aimed to produce a practical and tangible list of recommendations to be considered. This framework will describe the current blockchain landscape, highlighting some of the major terms and concepts in this field, it will present the major security issues to consider when adopting this new technology, and it will present case studies that highlighted the security concerns.

It is important to note that blockchain technology is in its infancy, and we are only beginning to understand how its different characteristics can be used to innovate and improve our IT systems. This also means that we are only beginning to see the security implications that come with this new technology. We invite the reader to see blockchain as another information technology, and we aim to highlight the characteristics of this new technology that amplify or reduce certain security risks. No technology is 100% secure and this certainly also applies to blockchain. Understanding the security risks is a first step in instating trust in blockchain and therefore stimulating its further adoption.

# 2. Understanding the Technology

# Understanding the Technology

"Blockchain" is a term often used to describe distributed ledger technologies (DLT). Though distributed ledger technologies are not a new technology, the popularity of cryptocurrencies have revamped this technology into a new phase we have started calling blockchain. As there are various definitions and understandings of what this technology is, we will be defining it for the purpose of having a common understanding when applying this framework. This section will discuss definitions of the most commonly known attributes of the technology, it will define and identify consensus mechanisms, explain the types of blockchain, and illustrate how this would look in a corporate IT environment.

## 2.1 Defining the Technology

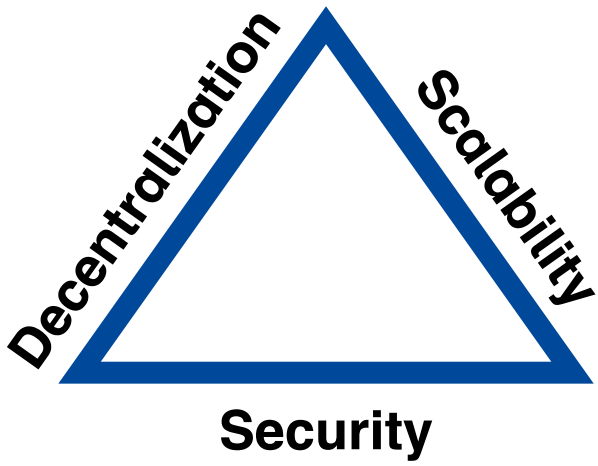
For the purposes of this framework, we have defined blockchain technology as an immutable distributed ledger of cryptographically signed sets of records or transactions that a number of parties want to continuously extend. These updates, or sets of updates, are saved on the ledger in the form of a "block". Each of the new updates to the ledger is linked to the preceding block and is timestamped, establishing an order for the records. Blockchain technology makes use of two proprietary characteristics - the use of validation rules and their enforcement. Validation rules define the conditions in which the records and blocks will be included in the blockchain and the enforcement of validation rules work in the way of an algorithm or protocol that enforces rules that have been entrusted by all parties that contribute data to the blockchain.

## 2.2 New Perspectives to Security Concerns

As previously stated, blockchain technology presents a new perspective on security issues. Two considerable attributes of this technology are it scalable and decentralized natures. These two characteristics of blockchain provide major advantages for its use. These advantages may also present strains on the security of the technology. The Blockchain Trilemma is a concept that exemplifies how the characteristics of this technology may pose a strain on its security. The blockchain trilemma is a concept that explains how there is a tension between the scalability, decentralization, and security of the technology. Though this concept is not widely agreed upon, it will be used as an analogy to explain how the different unique characteristics of this technology have consequences on the security of the application.

**Decentralization:** This is the attribute at the core of blockchain and the main tenant upon which communities around this technology were built. Its decentralized nature means there is no central body that is in control of the information being handled. This means it is censorship-resistance and allows for a nearly democratic participation of users in the ecosystem.

**Scalability:** This refers to the capability of a single node on a blockchain network to handle a growing amount of transactions per second and thus be enlarged to accommodate that growth. A node can be considered scalable if it is capable of increasing the total output under an increase in transactions per second when it is scaled horizontally or vertically. Scalability can be done horizontally, instantiating the same node again so two or more nodes can handle the increased load. Scalability can also be achieved vertically by adding more resources such as additional memory or Computer Processing Units (CPU) to the single node.




**Security:** This attribute concerns the risks that particular blockchain technology is susceptible to. In a general sense, the security concerns the Confidentiality, Integrity, and Availability of the technology. For blockchain, confidentiality means the authentication of the user or node on the chain; integrity means the data on the chain is immutable and authentic, and availability means the reliable use of the data stored and handled by the blockchain.

The blockchain trilemma suggests that increasing any two of these attributes will have a decrease on the third. Choosing to have a highly scalable blockchain may mean the widening of the attack surface, while decentralization means losing the control and authority over data. Though these are presented as security risks, these characteristics may make a chain more secure, such as scalability providing more resilience for the application and decentralization spreads the risk of a single point of failure. Taking this dilemma into account, we encourage the user of blockchain technology to use the security of the blockchain as a parameter to measure the attributes and characteristics of this technology, especially when using data linked to personally identifiable information.

## 2.3 Consensus Mechanisms

Blockchain technologies make use of consensus mechanisms to achieve an agreement on a single data value without a centralized authority. Two of the most prominent consensus mechanisms are known as Proof of Work (PoW) and Proof of Stake (PoS). There are many other widely used consensus mechanisms at the moment, including Proof of Identity, Proof of Capacity, Proof of Burn, and Proof of Authority (PoA). Consensus mechanisms ensure that all transactions within a block are agreed upon before adding a new block. As part of this wider verification, blockchain technology makes use of miners that create new blocks and to verify these transactions, very much in the same way we may hire an accountant to review financial information. Miners are selected in accordance with the chosen consensus mechanism, and the miners who successfully respond will verify transactions and also create new blocks on the blockchain. Various consensus mechanisms will do this in different ways.

**Proof of Work** does this by letting miners solve encrypted puzzles. The first miner to solve the encrypted puzzle will verify the transaction, create a new block, and announces the solution to the entire network. In return for this work, the miner gets a reward in the form of an amount of the crypto-currency being transacted. Without the reward system, miners would not be willing to solve the puzzles, so it is important to be aware of the importance of the reward system. Hardware to mine transactions is expensive and requires a significant amount of electricity to power. This leads to miners operating in consortiums known as Mining Pools. These offer miners the opportunities to pool resources to mine a block, spread the risks, and split the rewards.

**Proof of Stake** differs significantly from a proof of work system. Instead of building blocks through work output, the share or stake in a cryptocurrency determines the creator of a block. In other words, the bigger the share that a miner owns, the more mining capabilities a miner will have. This allows a miner to only mine a percentage of the transactions that are similar to its own share.

| | Public | Private |
|---|---|---|
| **Examples** | Bitcoin and Ethereum | Hyperledger-Fabric and R3 Corda |
| **Consensus algorithm** | Commonly used are Proof of Stake and Proof of Work | Agreed upon with pre-defined rules. Proof of Authority mostly used in the Netherlands |
| **Scalability of the network (Txs/second)** | Low | High |
| **Participation in network** | Mostly Permissionless. Users are free to join | Mostly Permissioned. A defined group of participants |
| **Development** | Determined by the community | Controlled by a central party |
| **Privacy when using personal data** | Not recommended. | Not recommended. Links to data through blockchain is safe up to a certain degree. |
| **Identity of the nodes in the network** | Anonymous or Pseudonymous | Known identities |

**Table 1: Differences between public and private blockchains**

## 2.4 Public, Private and Hybrid Blockchains

Blockchain technology can be explained in terms of access to a transaction, defining public, private, and hybrid blockchains, and can be defined by access to transaction processing creating the distinction between permission and permissionless blockchain network.

**Permissionless Blockchain:** In permissionless networks, any user is able to join and begin interacting with the network, such as submitting transactions, adding entries to the ledger, running nodes on the system, and verifying transactions.

**Permissioned Blockchain:** In a permissioned blockchain, the network owner decides who can join the network and only a few members are allowed to verify blocks.

**Public Blockchain**: A public blockchain has entirely an open read access and anyone can join and write in the network. Public blockchains often work with Proof of Work consensus mechanisms to incentivize participation.

**Private Blockchain:** A private blockchain often is the opposite of a public blockchain and only authorized participants have read access and can write and join the network. Often this requires an invitation to join, subsequently either the network starter or a set of rules put in place, determine if someone is fit to join.

**Hybrid Blockchain:** A hybrid blockchain, also known as a consortium blockchain, uses attributes of both private and public chains. It refers to a closed environment in which various parties work together in sharing data and transactions. Members can also determine which transactions can remain public and which have to be restricted to a smaller group of members.

Table 1 provides a quick overview of the differences between public and private blockchain types and their characteristics.

## 2.5 Blockchain in your corporate network

When considering blockchain for your IT processes and application, it is important to have an understanding of how the blockchain network will relate to IT systems already in place. Diagram 1 exemplifies how multiple participants interact in a blockchain network and connect to a central application.

In case of a public blockchain, there will be several participants, shown in diagram 1 as participants A

and B in the network that connects their system with a blockchain infrastructure through an Application Blockchain Interface (ABCI). In the case of the Bitcoin network, a user installs the Bitcoin wallet software on their device, creating a transaction node and mining node that will allow the user to transact Bitcoins.

In case of a private blockchain or a hybrid blockchain, there can be a separate authority that can host a central application for an optional off-chain database. There is often an organization that initiates the blockchain, and can therefore be seen as the lead organization. This organization will also most likely be the host of the optional off-chain database. This optional off-chain database can be used as a backup system to verify data in relation to data that is stored on the blockchain when the gateway to the blockchain is not available for a moment in time and the business process cannot be halted. When there is an off-chain database used, there must also be a process in place to synchronize the blockchain with the off-chain database on a regular basis.
Blockchain technology is praised for the fact that there is no need for a lead organization. Nevertheless, in practice, hybrid or private blockchains often do have a lead organization. If an organization uses a private blockchain for the distribution of information across its suppliers, it can optionally host a central application on which all other users will connect to its server and then on to the central application. In this setup, an organization would then be able to store the data off-chain for the case as described above concerning the backup system. This authority may also host an optional mining node and a transaction node to contribute to the blockchain infrastructure itself.

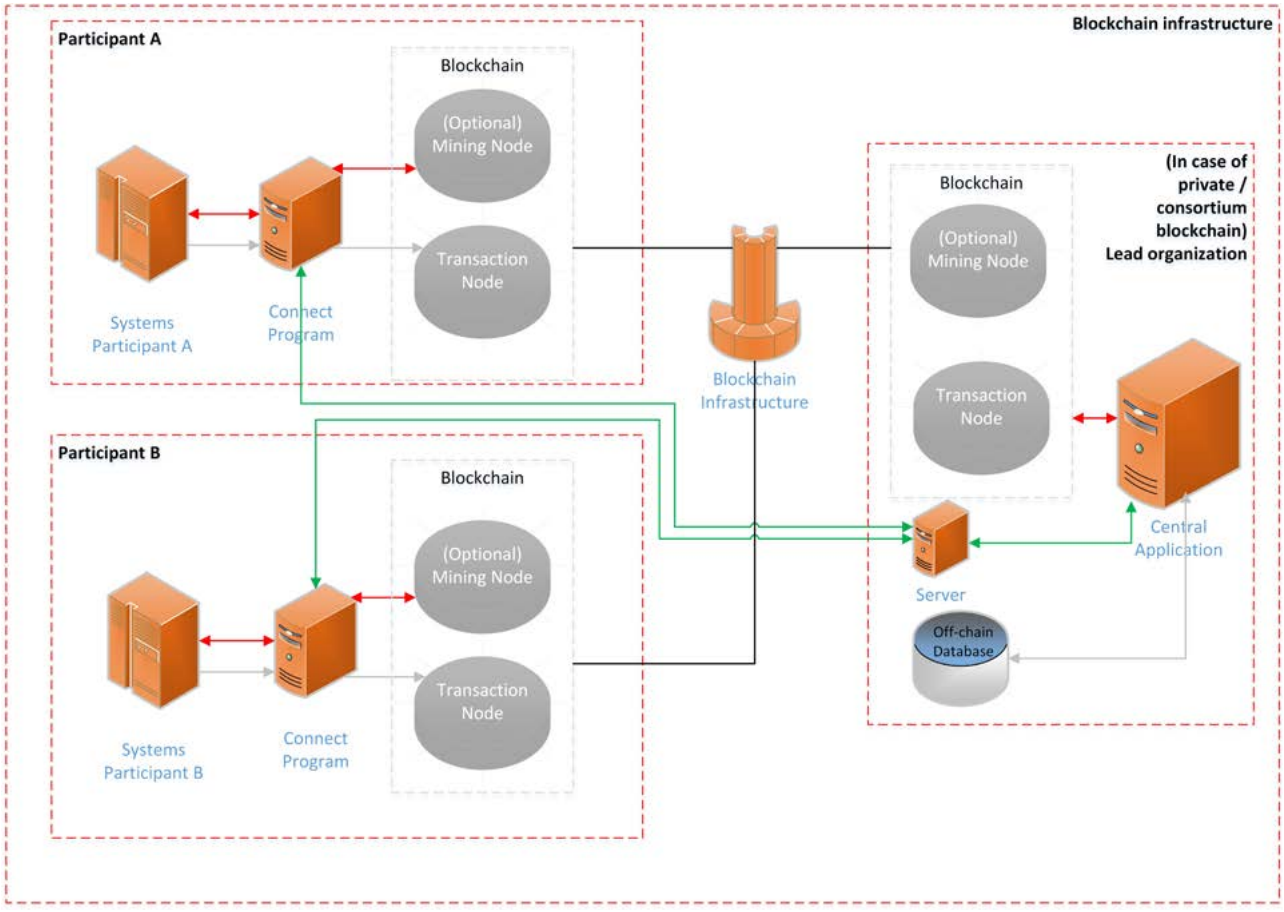



**Diagram 1: Example of private / hybrid blockchain infrastructure in corporate network**

# 3. Do you Really Need a Blockchain?

# Do you Really Need a Blockchain?

Blockchain can be simply described to be the orchestration of three technologies- the internet, private key cryptography and a protocol governing incentives.[1] This all results in a secure system for digital interaction without the need for a trusted third party to facilitate digital relationships. In this way, blockchain technology should be seen as a consortium of current technologies applied in a modern innovative way. As mentioned earlier, this technology is not suitable for all use-cases. In order to determine if blockchain technology is ideal for the IT system or process in question, we suggest using the diagram bellow developed by IEEE.[2]

This diagram will walk the user through the different considerations to take into account when wanting to adopt blockchain technology more generally. These considerations include the satisfaction with using traditional databases, the number of participants that will contribute data, the level of trust among participants, and the level of privacy and control needed over the data.

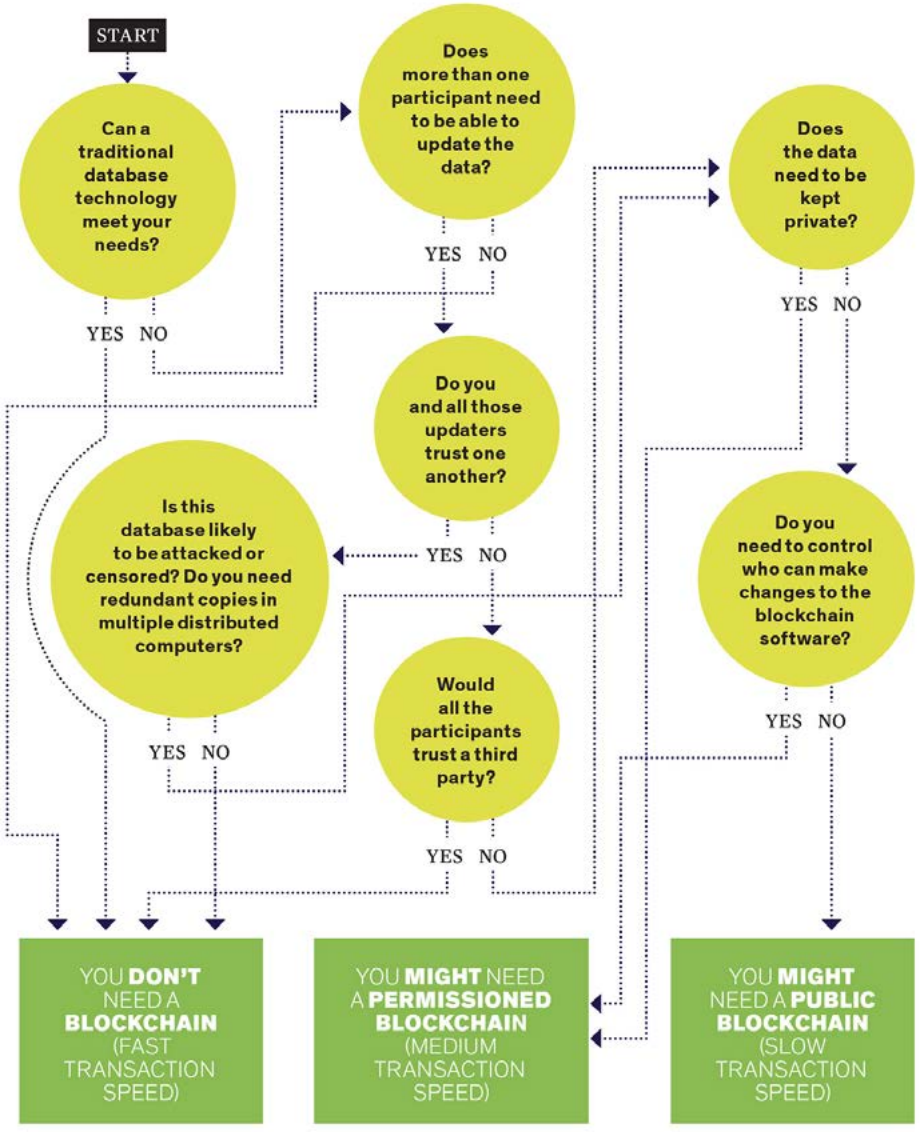



**Diagram 2: IEEE Blockchain Decision Tree, 2017**

# 4. Blockchain Security Framework

# Blockchain Security Framework

Like all other technologies, blockchain faces a number of security risks that are amplified and minimized accordingly to its unique characteristics. An example of this can be seen in blockchain's consensus mechanism, where it both amplifies and reduces different security risks. In terms of amplifying threats, consensus mechanisms may make certain types of blockchains vulnerable to a 51% attack where an attacker can overpower the network and effectively monopolize and control the application. By controlling the network, attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend cryptocurrencies. In terms of minimizing security risks, this attribute ensured that altering data on a chain is significantly more difficult as the data has been encrypted and cross-checked by other peers in the network. There are several more examples of this sort, where blockchains specific characteristics can reduce and at the same time increase security risks. For this reason, it is recommended to assess this technology with a minimum set of security controls.

This minimum set of controls take care of common security risks ranging from operational such as access control and secure system development, to strategic such as security policies for your organization. If an organization is not developing or maintaining information systems, it is recommended to have a basic level of understanding of what are common security good practices. This understanding allows organizations to challenge IT suppliers on how they implement security controls for the applications that are requested. For a high-level overview of these security controls, it is recommended to use ISO/IEC 27001:2013 or NIST version 1.1 as a baseline. This framework presents 14 security considerations for secure blockchain applications, of which are divided into four categories:

- **Blockchain specific:**
This category will describe security issues that are most amplified by blockchain technology. The issues presented in this category are not unique to blockchain technology but are amplified by the technologies characteristics. These will include smart contracts, forks, cryptographic algorithms, and cryptographic key management.

- **Network and Infrastructure:**
This category will describe how blockchain should be considered for operations and the general IT infrastructure of an organization. These considerations will consist of access control, scalability, intrusion detection, targeted attack resistance, and data propagation attack resistance.

- **Operational and Organizational:**
This category will highlight security issues that affect an organization at an operational and organizational level. These security considerations are not unique to blockchain, but must not be forgotten when implementing or adopting this technology. These include operations and communications security, system acquisition, development and maintenance, asset management, human resource security, and supplier relationships.

- **Management-level:**
This category will highlight considerations for an organization's management level. They are also not unique to this technology but are crucial for establishing a culture of secure development,

| | | Public | Private |
|---|---|---|---|
| **Blockchain Specific** | | | |
| 1 | Security of Smart Contracts | + | + |
| 2 | Forks | - | + |
| 3 | Crypto Algorithms | - | + |
| 4 | Crypto key management | + | + |
| **Network and Infrastructure** | | | |
| 5 | Access control | - | + |
| 6 | Scalability | - | + |
| 7 | Intrusion Detection | - | + |
| 8 | Targeted attack resistance | - | + |
| 9 | Data Propagation attack resistance | - | + |
| **Operational and Organizational** | | | |
| 10 | Operations & Communications Security | - | + |
| 11 | System Acquisition, Dev and Maintenance | + | + |
| 12 | Asset Management | + | + |
| 13 | Human Resource security | + | + |
| 14 | Supplier Relationships | - | + |
| 15 | Incident Management | - | + |
| **Management Level** | | | |
| 16 | Organization of InfoSec | - | + |
| 17 | Information Security Policies | + | + |
| 18 | External/Internal Compliance | + | + |

implementation, and operation of this technology. These include organization of information security, information security policies, and external and internal compliance.

The table above gives an overview of the level of influence an organization can have in mitigating the security considerations listed below.

## 4.1 Blockchain Specific:

**1) Security of Smart contracts**

A smart contract is a computer program that acts as an agreement where the terms of the arrangement can be preprogrammed with the ability to self-execute and self-enforce itself. Smart contracts are available on both public and private blockchains. The main goal of a smart contract is to provide a superior system for contractual

agreements solely based on computer code as a set of instructions, possibly complementing or substituting current legal contracts.

A good example to illustrate what smart contracts do can be seen in the mortgage industry. Smart contracts can automate mortgage contracts by automatically connecting the parties, providing for a frictionless and less error-prone process. Smart contracts can automatically process payments and release liens from land records when the loan is paid. They can also improve record visibility for all parties and facilitate payment tracking and verification. They reduce errors and costs associated with manual processes. Digital identity, in this case, is a key requirement.

From the security point of view, this model has many important security risks to consider. First of all, the development life cycle of smart contracts is significantly different from the traditional software development life cycle, where testing, integration, and maintenance are repeatable. Since a smart contract's code is unchangeable after being appended to a blockchain, developers have to implement specific functionality if they wish to modify the behavior of their contracts later on. In that context, the development life cycle of smart contracts is much different from standard software that can be patched and fixed throughout its entire support-life.

Incidents with smart contracts occur when a smart contract does not work the way it was intended. Verification and testing are especially important in smart contract development and should be an integral part of the analysis and design steps. These practices may be perceived as contrary to traditional development life-cycles that may only follow implementation requirements.

If developers do not have much experience in working with smart contracts, it may be recommendable to build in functionality that is only accessible by an authorized party, possibly a third party to those getting into the agreement. This functionality would only be intended to be used in the case that an intervention is necessary.

The level of influence an organization can have in mitigating the smart contracts security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Smart Contracts | ⊕ | ⊕ |

**2) Forks**

At its most basic definition, a fork is what occurs when a blockchain diverges into two potential paths forward. This occurs either with the network's transaction history or a new rule in deciding what makes a transaction valid. Forks can be distinguished into hard and soft forks.

**Hard Forks:** A hard fork is a permanent divergence from the previous version of a blockchain in which a new set of consensus rules are introduced into the network that is

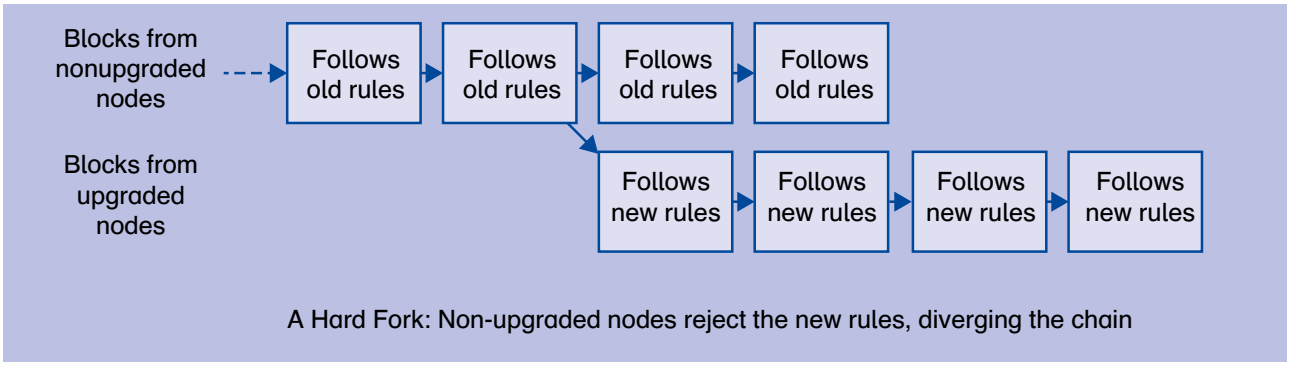



**Diagram 3: Investopedia description of Hard Forks.**

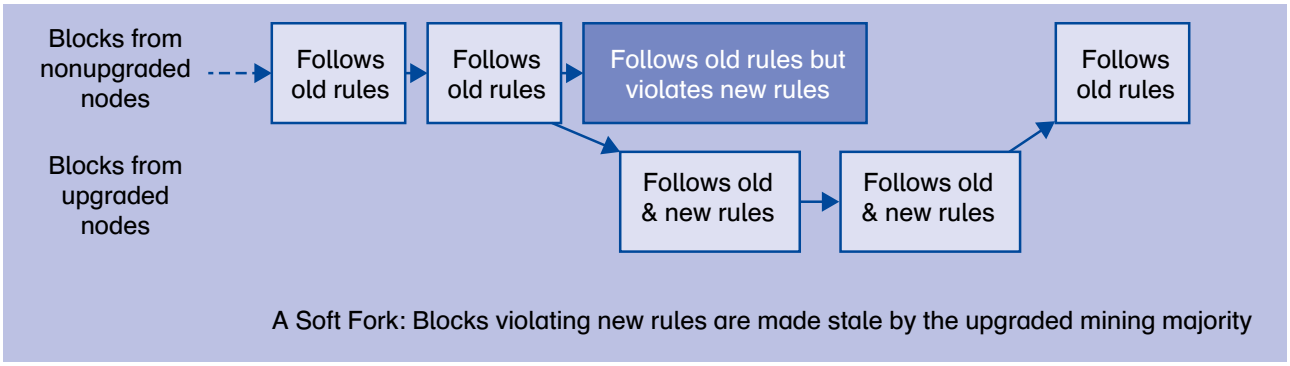



**Diagram 4: Investopedia description of Soft Forks.**

not compatible with the older network. In other words, a hard fork can be thought of as a software upgrade that is not compatible with previous versions of the software. All network participants are required to upgrade to the latest version of the software in order to continue verifying and validating new blocks of transactions. Under a hard fork, blocks that are confirmed by nodes that are not yet upgraded to the latest version of the protocol software will be invalid. Nodes running the previous version of the software will have to follow the new set of consensus rules in order for their blocks to be valid on the forked network. In the event of a hard fork, if there is still mining support for the minority chain, then two blockchains can continue to exist simultaneously.

**Soft Forks:** A soft fork is a backward compatible method of upgrading a blockchain. In other words, a soft fork is software upgrade that is backward compatible with previous versions of the software. Soft forks do not require nodes on the network to upgrade to maintain consensus, because all blocks on the soft-forked blockchain follow the old set of consensus rules as well as the new ones. Blocks produced by nodes conforming to the old set of consensus rules may violate the new set of consensus rules, and as a result, will likely be made stale by the upgrading mining majority. For a soft fork to work, a majority of miners need to recognize and enforce the new set of consensus rules. If this majority is reached, then the older network will fall into disuse, with the newer blockchain gaining recognition as the 'true' blockchain.

When two or more miners find blocks at nearly the same time, the blockchain temporarily diverges into two chains, which can also be seen as a soft fork. This ambiguity is resolved when subsequent blocks are added to one, making it the longest chain, while the other block gets "orphaned", or abandoned, by the network.

An example of a soft fork would be the implementation of a new consensus rule changing the network block size from 1MB to 500KB. Nodes that have not upgraded will continue to see incoming transactions as valid, as these nodes follow the old set of consensus rules as well as the new (500KB is less than 1MB). Mining nodes that have not upgraded to the new consensus rule and attempt to mine new blocks will have these blocks rejected, as it does not conform to the new set of consensus rules (block sizes of 500KB). Thus, the blockchain with 1MB sized blocks is likely to fall into disuse as miners enforce the new consensus rule of 500KB.

**Forks can lead to the following risks:**

- When a soft fork is supported by only a minority of the nodes in the network, it could become the shortest chain and consequently become orphaned by the network.

- In the case of a hard fork, the chain can be split

off and create two separate chains. This may be acceptable for cryptocurrencies, but this may be become unwanted in business processes as it may cause fragmentation or loss of control.

- Hard forks are also susceptible to political impasses, caused when a portion of the community decides to not abide by new rules, and decide to keep implementing older consensus rules.

- When forks are unmanaged, the risk of attacks could involve inconsistency of data stored in the ledger.

All major issues with forks occur mostly in public blockchains. For this reason, it is important to take this into consideration when considering a public or private type of blockchain. The level of influence an organization can have in mitigating the forks security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Forks | - | + |

**3) Cryptographic algorithms**

One of the basic elements of blockchain technology is the use of cryptographic algorithms and protocols. When a cryptographic algorithm is broken, the blockchain cannot be continued and therefore will be stopped. Although it is very difficult to break a cryptographic algorithm, it has been done in the past and certainly will be done in the future, especially as computer power keeps getting exponentially higher. For public blockchains, it is nearly impossible to influence this matter, as one must rely on the wider community. In the case of private blockchains, it is possible to be in control of the following aspects:

- Proper configuration, including attributes such as the number of miners to prevent attackers from taking over the majority before the algorithm is changed.
- The desired distribution of miners.

- Processing power of a hash-function to provide a sufficient level of protection.

- Monitoring of the used algorithms and take action when one is broken.

- Make sure controls are in place in the case at the blockchain technology provider.

The level of influence an organization can have in mitigating the crypto algorithms security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Crypto algorithms | - | + |

**4) Cryptographic key management**

Blockchain technology, whether it be in a private or public chain, makes use of public and private keys. A private key can represent a natural person or an organization and is used to sign a transaction on the blockchain. The following example of transferring cryptocurrency explains the use of public and private keys.

When a user sends cryptocurrencies over the blockchain, they are actually sending a hashed version of what is known as the “Public Key”. The other key, which is only known by the individual user, is known as the “Private Key.” When receiving the currencies, the recipient will “unlock” the sender’s Private Key by using the known public key. This way the recipient can verify the authenticity of the transaction.

For an organization considering adopting blockchain, it is essential to have a process in place for key management, addressing concerns such as what to do if private key gets

compromised or lost. It is important to note that blockchain technology is not similar to Public Key Infrastructure Architecture (PKI) where a private key can be easily replaced. In PKI architectures, an old key can be placed on a Certificate Revocation List. In blockchain architecture, this process of revoking keys is not possible. When a private key used for accessing cryptocurrencies is lost, the cryptocurrency may often also be considered lost.

The level of influence an organization can have in mitigating the crypto key management security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Crypto key management | + | + |

## 4.2 Infrastructure and Network

**5) Access control**

Using private blockchain allows for the regulation of different types of permissions, such as how to add a node to the blockchain network, and what kind of transactions can neb performed on the network and by which users. In regards to access controls, the following aspects should be considered:

- The assigning of authentication and authorities to employees that need access to a node or nodes on the blockchain network.
- Implementation of separation of duties. An organization should have several levels of authorization, based on the different roles that need to be in place. It is not advised for every employee to have all possible authorizations.
- Authorizations must be regularly reviewed, at least with a minimum of once a month, and withdrawn from users when applicable.
- Controls need to be in place to prevent the access of non-authorized users or system-to-system connections that request access to applications and information of the organization.
- Special thought is needed for the joiners and leavers of the organization. Withdrawing access rights of people leaving the organization is essential.
- The implementation of access control allows an organization to mitigate unauthorized use of applications or information.

The level of influence an organization can have in mitigating access control security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Access control | - | + |

**6) Scalability**

The nodes in the blockchain network need to be scalable. If an application of the blockchain network generates more transaction then was foreseen, the nodes in the network must have the availability to easily scale up their computing power. This should be done to prevent the blockchain network to become very slow, or even come to a halt. When using a private blockchain, this can be achieved by making contractual agreements with the participants of the private blockchain and a constantly monitor the nodes in the network. When using a public blockchain, one must rely on trusting the wider community.
The level of influence an organization can have in mitigating scalability security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Scalability | - | + |

**7) Intrusion Detection**

In public and private blockchains, intrusions can lead to unauthorized modification of data or disruption of a service. The main functionality of blockchain technology is in guaranteeing data consistency across all involved nodes

and consequently guaranteeing that such data is protected from unauthorized modification. If unauthorized modification happens, it would lead to loss of reliability and consistency of data across involved nodes, and therefore loss of immutability and loss of trust. The level of influence an organization can have in mitigating intrusion detection security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Intrusion Detection | - | + |

**8) Targeted attack resistance**

For blockchain technology, this form of attack is called a 51% attack. This form of attack refers to an attack on a blockchain network by a group of miners controlling more than 50% of the network's mining hash-power. The attackers would then be able to prevent new transactions from gaining confirmations, allowing them to halt payments or other transactions between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend cryptocurrencies. 51% attacks are mainly an issue for public blockchains as the nodes are accessible to everyone. In the case of private blockchains, this is less of a risk as they run on controlled networks, and may also be run on private networks. The level of influence an organization can have in mitigating targeted attack resistance security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Targeted attack resistance | - | + |

**9) Data propagation attack resistance**

Using the same 51% attack described in the previous point, malicious users try to stall the distribution of the transactions among the nodes to reach consensus. With that, the blockchain does not function and it would lead to a loss of reliability. The level of influence an organization can have in mitigating data propagation attack resistance security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Data Propagation attack resistance | - | + |

## 4.3 Operational and Organizational

**10) Operations & communications security**

Operations Security (OPSEC) is a process that classifies information assets (see control 8 on asset management) and determines the controls that are required to protect those assets. According to research done by TNO on security aspects of the blockchain, the majority of incidents investigated indicate a lack of OPSEC measures in about 66% of the cases.[3] To prevent OPSEC type of incidents, standard cybersecurity solutions are available. The investigated incidents are mainly found in public blockchains, with a few cases found in private blockchains. It is therefore important to note that OPSEC issues are easier to oversee and mitigate in private blockchains. The level of influence an organization can have in mitigating operations & communications security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Operations & Communications Security | - | + |

**11) System acquisition, development, and maintenance**

This aspect of information security controls can be brief. Security by design must be common practice. Either if the organization develops and maintains the IT facilities itself, or if it is outsourced to an outsourcing partner. Detecting vulnerabilities in a timely matter can be done by implementing security by design at all stages, from the first development until maintenance. Organizations must ensure that the blockchain specific security risks are addressed in the design, whether it is developed in-house or outsourced to

a contractor. The level of influence an organization can have in mitigating system acquisition, dev and maintenance security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| System Acquisition, Dev and Maintenancet | + | + |

**12) Asset management**

All organizations should have a clear overview of its crucial assets, material and in terms of the information it collects and processes. For information used by the organization, it is important to enforce classification levels on that information. By classifying the information, the risk of sharing information with others who have do not have access rights can be mitigated. Classifying the information can help an organization to determine what type of blockchain can be used and what information to publish on the blockchain. For example, classifying information as "confidential" might be a good deterrent from choosing a public blockchain, and thus provide a better argument for using a private blockchain. The level of influence an organization can have in mitigating asset management security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Asset Management | + | + |

**13) Human resource security**

The most important part of human resource security is the screening of an organization's staff and the continuous process of training and creating awareness of security risks to information. This security control should be seen as an entry point to establish a secure foundation in the organization. Employee screenings are an important process when developing smart contracts, as their development relies on security and privacy by design. Once a smart contract has been written, it is unchangeable and therefore cannot be fixed retroactively. Smart contracts are also susceptible to back-doors that may provide an advantage to a party in the contract (see section 4.13 for smart contracts). The level of influence an organization can have in mitigating human resource security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Human Resource security | - | + |

**14) Supplier relationships**

An organization's security policy and security controls should also be implemented by its suppliers. This is especially true when personally identifiable data is involved. It is encouraged for organizations to request suppliers to present proof on how they handle information security.
The different security controls of this chapter can be used as a starting point to question suppliers or outsourcing partners involved in the development and maintenance of blockchain application on both public and private blockchains. Take into account that when a supplier is using a public blockchain, it is not always clear where responsibility resides. It is therefore advised to use a private blockchain as a starting architecture as it is possible to define responsibilities with external partners. The level of influence an organization can have in mitigating supplier relationships security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Supplier Relationships | - | + |

**15) Incident management**

When it comes to security incidents, it is important to take immediate action. It is also important to be able to identify them appropriately as security incidents. This means that staff should be trained and informed about guidelines that allow them to identify security incidents. This includes knowledge on how to react and how to report on a security incident. This security control is a general good practice for your information systems. For blockchain environments, this would mean to report security incidents

as soon as they happen. This is a good safeguard to prevent escalations of incidents and may be a good way to detect information breaches that may need to be reported to a data protection officer. The level of influence an organization can have in mitigating incident management security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Incident management | - | + |

## 4.4 Management Level

**16) Organization of information security**

Organization need to have an effective governance structure detailing how information security management is organized, what are the roles in the organization, and who is the end-responsible for security affairs. Knowing the security organization entails knowing who the Chief Information Security Officer (CISO) is, and who is responsible to determine if applications meet the desired security levels. An effective governance structure will help the organization to implement a "Plan, Do, Check and Act" cycle to measure the effectiveness of information security. It is important to consult any security risks concerns regarding the adoption of blockchain technology with the person responsible for security in an organization, especially when considering to use a private or public blockchain. The level of influence an organization can have in the organization of information security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Organization of InfoSec | - | + |

**17) Information security policies**

A document that describes how the organization protects their information, their ITS assets, and how to be compliant to existing laws and regulations. A document that is shared with all employees of the organization and can be shared with suppliers. In this way, an organization can show they value information security and therefore promote its awareness among employees. Without needing to specify the type of blockchain being considered, it is important that information security policies be updated for the use of blockchain technology. The level of influence an organization can have in mitigating information security policies security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| Information Security Policies | + | + |

**18) External and Internal Compliance**

Information security should be compliant internally to company policies, and externally to legal and industry requirements. This being said, information security needs continuous attention and a certain level of control. An example of this can be seen in carrying out regular audits to ensure that policies and procedures are respected within an organization. One of these such audits can be in the form of a Privacy Impact Analysis (PIA) to make sure that the implementation of blockchain technology will lead to compliance for the organization.

When an organization subcontracts their blockchain activities to an outsourcing partner, the "right to audit" that partner should be part of the contract. But, even when this is part of the contract, audits can only be done upon a certain level. When the partner is using a public blockchain, the audit cannot be done on that part of the solution. The level of influence an organization can have in mitigating external/internal compliance security considerations for public and private blockchains are:

| | Public | Private |
|---|---|---|
| External/Internal Compliance | + | + |

# 5. Risks when Migrating

# Risks when Migrating

Migrating an application or process to a blockchain architecture will require an additional list of topics to be considered. Though this new technology has attributes that make it different than other architectures, it should be assessed like any other technology. The following is a list of comprehensive operational security risk considerations. It is important to note that the considerations have been formulated under the assumption that organizations will be adopting a blockchain technology and not developing a proprietary chain.

## 5.1 Choosing the right blockchain

As previously described in chapter 2 of this framework, there are different sorts of blockchain and different consensus mechanisms to consider. When an organization is engaging with blockchain for the first time, it is highly recommended to start with a private blockchain.[4] In private blockchains, the organization has full control of the architecture, nodes, and access to the blockchain. This type of blockchain is recommended so that in the case of a security breach, the organization can still have an overview of everything under control, and quickly identify the origin of the breach. Asides from the Grain Initial Coin Offering, all other uses cases described in chapter 7 are implemented on a permissioned blockchain.

## 5.2 Special considerations for testing

Testing is an essential part of ensuring the reliability and security of an application. In non-blockchain technology environments, it is a normal practice to carry out further testing while the application is in production environment. This means bugs can be fixed and a new version can be released. With blockchain technology, this is not possible. Once a chain is started, there is no possibility to test the code further to weave out bugs. In the case of private chains, it is conceivable that a central authority tests the chain and periodically moves over to a newer version, consolidating all previous transaction in the new chain.

Application testing should be considered one of the most important considerations when migrating a process to a blockchain architecture. It is a good organizational practice for organizations to have testing procedures and methodologies in place. In order to enhance the security of the testing, it is highly recommended for organizations to use frameworks such as the Open Web Application Security Project (OWASP) to make sure all industry standards are considered and covered. Organizations have less control over the entire infrastructure when they use public blockchain, and testing might become difficult. In that case, it's recommended to implement extra monitoring and control on business processes. This can be done to ensure that abnormal behaviors are detected in time.

For one of the uses cases in chapter 7, load-testing was executed to test the boundaries of the architecture. For two other uses cases, external expertise was brought in to review and audit.

## 5.3 Awareness and Training

Security training is critical for any user. While there are some security capabilities inherent in blockchain technologies, it is important to have a training plan to ensure users understand what they are permitted to do with the solution. A training plan likely exists for most environments; while users may not know that they are using a solution that runs on the blockchain, the security training plan may need to be updated to include unique aspects of the blockchain implementation.

Organizations should consider whether there is any training in place to educate system owners and users on blockchain technology and the security risks that come with it.

## 5.4 Contingency planning

Organizations should develop a contingency plan for information systems that meet the following criteria:

- Systems that identify essential missions and business functions and associated contingency requirements.
- Provide recovery objectives, restoration priorities, and metrics.
- Address contingency roles, responsibilities, assigned individuals with contact information.
- Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
- Address eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

## 5.5 Simplicity as a security measure

When smart contracts are used, create guidelines that will help the developers keep the smart contracts as simple as possible. This will prevent security breaches that may result from too much complexity in the code of smart contracts. Organizations should be sure to have a review process in place, starting with peer-reviews.

For two uses cases described in chapter 7, external expertise was brought in to review the blockchain code and perform audits.

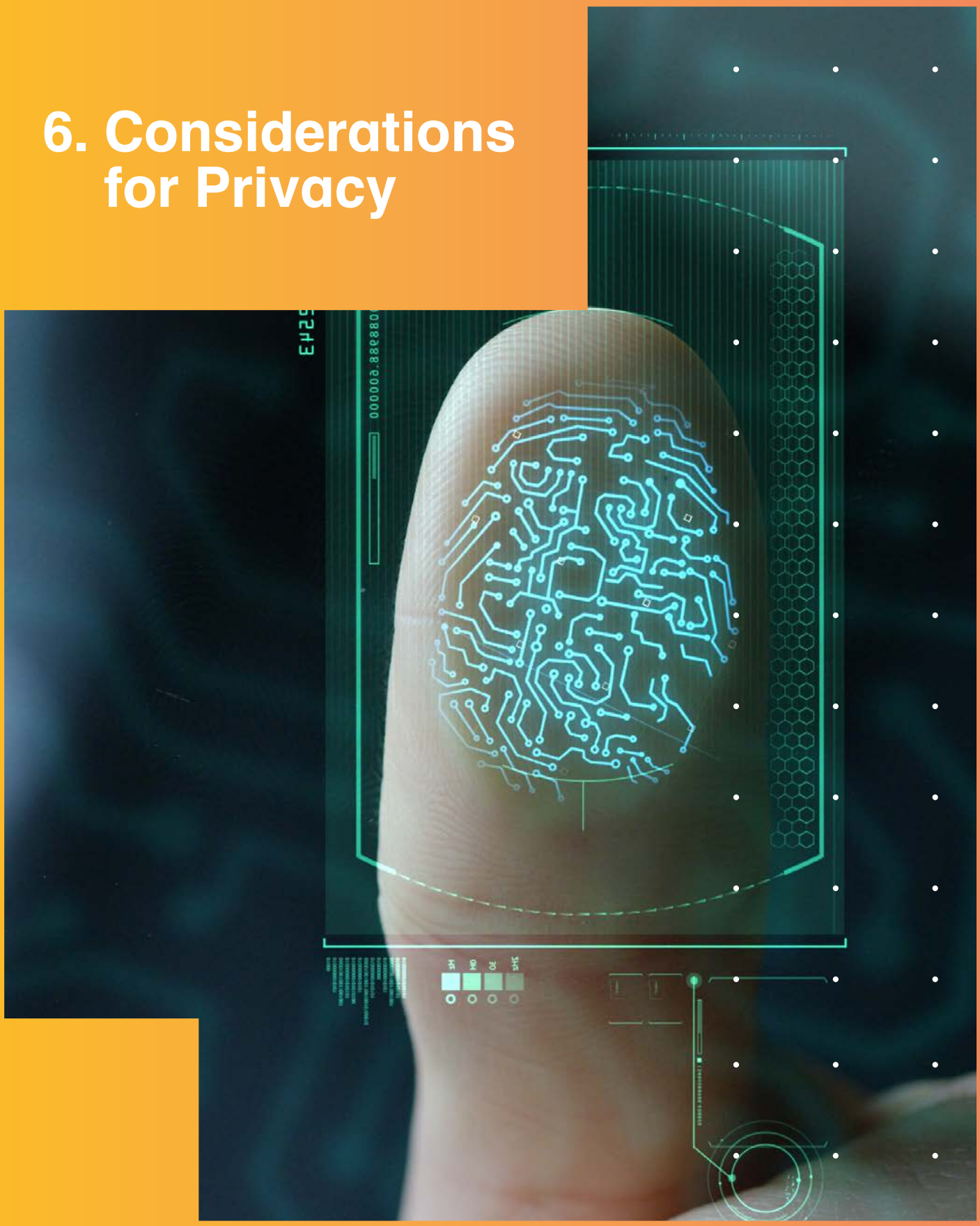
## 5.6 Privacy

Organizations considering to use blockchain to process attributes of personally identifiable information must ensure to have a mature level of information security. It is highly recommended for organizations to not keep any personally identifiable information on a blockchain, whether it be public or private. For private blockchains, storing the personal information off-chain and using the blockchain to reference the data is conceivable under certain circumstances. There are three main privacy considerations to take into account when moving a process to a blockchain environment:

- Inform the users of how their data will be processed and by what organization if a new supplier has been sought.
- Inform users of how their rights will be considered in regards to the right to erasure, right to be forgotten, and right to correct their data.
- Use the most modern and applicable cryptographic technology to secure the user's data attributes.

For all uses cases described in chapter 7, privacy was an important security consideration. These were implemented in the form of hashes for documents or encrypted external file storage connected to the blockchain application. The next chapter will elaborate further on privacy implications related to the General Data Protection Regulation.

# 6. Considerations for Privacy



# Considerations for Privacy

It is a current trend for privacy concerns in Europe to be automatically linked to the General Data Protection Regulation (GDPR), which became directly applicable in all member states on 25 May 2018. Given its importance, we will focus on illustrating the applicability of the GDPR, understanding the roles of Data Processor and Data Controllers in this context, and the risks to personal data.[5] This chapter will take a closer look at the roles of the data processor and data controller, the preferred type of blockchain in terms of privacy, the rights of the data subjects in the context of a blockchain application, and will discuss hashes in the context of the GDPR.

The GDPR poses serious challenges for organizations that have to comply in order to avoid fines. Blockchain technology is not exempted from this obligation if personal or pseudonymous data is involved in the process. One has to be aware of the fact that the GDPR still causes uncertainty about the interpretation of certain articles in it. Organizations face the same challenges with blockchain applications. When considering blockchain technologies, it is important to consider the relationship between controller and processor and the user's rights.

## 6.1 Controller vs. Processor

The first main concern lies in defining the roles of controller and processor for the blockchain application. In the GDPR the controller is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[6] The processor can be defined as the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[7] The processing of personal data within a blockchain presumes that there is no hierarchical relationship between the participants. Each participant is therefore equal and able to contribute and make use of the date as seen fit.[8] If there are other agreements in place, this could prove to be the exception.

For blockchain applications, a controller can be defined as the participants of a blockchain who have the right to write on the chain and who decide to send data for validation by the miners.[9] More specifically, a controller can be more closely defined as a participant that is seen as a natural person that processes personal data related to a professional or commercial activity or when a participant is a legal person that registers personal data in a blockchain.[10] In other words, the participants that define the purpose and means of processing are the controllers, thus excluding miners from being a controller. The controller has different obligations under the GDPR, such as reporting a data leak. If a group of participants decides to carry out processing operations with a common purpose, this would lead to practical issues with regard to governing these responsibilities. This should be addressed in various ways. One way to do this is by identifying one participant as the decision maker by reaching an agreement on how to govern as joint controllers. Another way to achieve this is by creating a legal persona such as an economic interest group or association.[11] This issue can likely be solved within a blockchain that is governed by one or a few parties.

If parties that do not necessarily exchange personal data, but are contributing as nodes to the blockchain network, it can be assumed that these parties can be considered processors.[12] In other words, one could say that all the nodes that are not specifically defined as being controllers could be considered processors since they all

contribute as a node to the processing, creation, and maintenance of the data on the chain. Consequently, all the controllers have to enter into a processing contract with the processors. In a small private blockchain this is quite manageable, yet in a larger private or public blockchains, this is a more complicated matter. Organizations should be aware that there is no legal precedence on this matter, thus European case law could lead to different interpretations. For this same reason, it is currently unclear what the definition of processors could mean for public blockchains and what legal obligations controllers have with regard to processors.

From a privacy perspective, permissioned and private blockchain applications are the safe choice for organizations wanting to adopt this technology. These two types of blockchain make it easier to identify controllers and processors. In return, this makes the governance of legal obligations for controllers and processors more manageable, as well as taking care of the contractual obligations between controllers and processors. It is very difficult to identify all the controllers and processors in a public blockchain, making it questionable if it is legally possible to adhere to the GDPR when using a public blockchain.

## 6.2 Data Subject Rights

An important component of the GDPR concerns the data subject rights. A data subject has six different rights under the GDPR: the right of access and rectification, the right of erasure, the right to restrict processing, the right of data portability, the right to object, and the right to not be subject to automated processing.[13]

We will be focusing on three of these rights and how they present challenges to the use of blockchain technology. These three rights are the right to erasure, the right to rectification, and the right to limit processing. Data subject rights are at the core of the GDPR and present the biggest concerns as there are no exemptions to their compliance.

**Right to Erasure**

The right to erasure is the first data subject right that becomes complicated when approaching blockchain applications. It is an inherent feature of blockchain applications to ensure that data cannot or should not be deleted. In a way, this undermines the actual purpose of a blockchain solution, making it impossible to adhere to the right of erasure. In a private blockchain, it is possible to make arrangements with participating organizations to make erasure technically feasible, yet again undermining the characteristics of blockchain. For the right to erasure, an organization should try to delete as much as possible and take proper steps to mitigate risks for the data subject as much as possible, within the boundaries of blockchain. Consequently, for blockchain solutions that are programmed to not enable removal, this means that they should pursue this. This can be done by encrypting the personal data, deleting the original data, and throw away the key. A log file that the data is actually encrypted can be added to provide proof. Assuming that an advanced form of encryption is being used and thus deemed most adequately secure, this could be a reasonable solution for the right to erasure.[14] Nonetheless, taking the inherent features of blockchain into account, it is not recommended to store personal data in plain-text on a blockchain.

**Right to Rectification**

The right to rectification also poses a problem with regard to blockchain applications. Similar to the right to erasure, this undermines the whole idea of blockchain. This leads to the question of how you can do this if you want to completely rectify the information without keeping the original faulty information. In other words, blockchain applications usually will allow rectification, yet the

faulty information will also remain on the chain. In order to solve this, the same reasoning can be used as discussed in the previous paragraph on the right to erasure. A new log file can show that the data is rectified, while the old incorrect information is encrypted and the key is thrown away.

**Right to limit processing**

In order to limit the processing of personal data on a blockchain application, it is necessary to identify how the access rights are arranged. To limit processing, the access to personal data should be restrained by denying some nodes in the blockchain network access to that information. In return, this can limit controllers and processors to adhere to the right to erasure. Henceforth, there should also be agreements on this matter in case of the limitation of processing. This also seems to contradict the fact that a blockchain solution should be decentralized since this construction can be considered as a centralized solution. This is only manageable when a private blockchain is used in which a single party has control over the majority of the nodes or when a few parties can come to a set of predefined rules on this matter. This may be very difficult to adhere to when using a public blockchain solution.

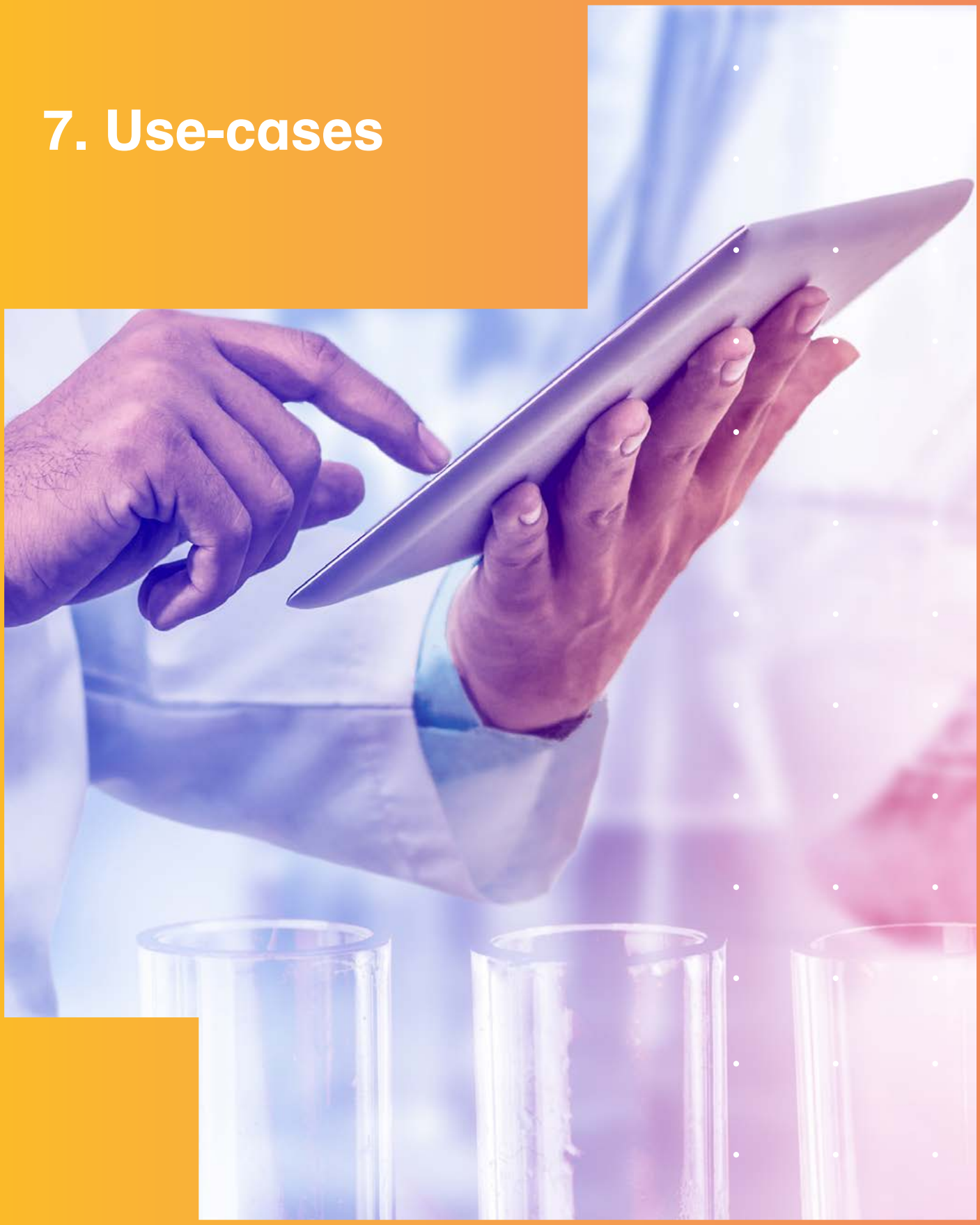
## 6.3 Regarding Hashes and Personal Data

It is worth mentioning that at this moment, a hash is considered to be personal data. The Dutch DPA provides three important reasons why a hash is considered as personal data.[15] Firstly, because the source data is often still available and the hash is then used in combination with a linking table; this leads to pseudonymization and not anonymization of the data. Secondly, it is theoretically feasible that hash values can be reproduced using a brute-force attack. Although it is rather difficult to brute-force a hash value back to the original data, this notion postulates that is technically possible. Thirdly, organizations often store the hashes with other additional information. The combination of those two could make it possible to link a person to a hash. Two of the three mentioned factors can be limited by fully separating the hash from the source information and other additional information, which is a measure that is mentioned before when discussing the data subject rights.

## 6.4 Compliance Beyond the GDPR

All in all, this section highlights some specific issues to be taken into account when discussing personal data processed on a blockchain application. Besides GDPR compliance, there are also other legal considerations that should be taken into consideration when working with a blockchain application in general. A whitepaper from Pels Rijcken & Droogleever highlights a few of these legal considerations, such as how to define the applicable national law for an international blockchain, how to define legally the ownership of a blockchain, legal issues with regard to identity within a blockchain – which especially applies to public blockchains, legal issues with regard to smart contracts, and legal issues concerning the monitoring of blockchains.[16] It is sensible to delve into this matters, to make sure that a blockchain adheres to certain legal obligations. In addition, it is crucial to always take specific legislation into account, which is already applicable to the sector in which the blockchain will be used.[17] Taking these considerations into account will bring organizations one step closer to adhere to its legal obligations when using a blockchain application.

# 7. Use-cases



# Use-cases

This section will exemplify various cases of security considerations in real blockchain use cases. These use cases span across the healthcare sector, real estate, and financial sectors. Every use-case will describe the use for blockchain, the organizations participating as nodes, and the security considerations for every case.

## 7.1 "Mijn zorg log": Blockchain baby

**Market: Healthcare**
The maternity care blockchain system "Mijn zorg log" was developed to connect clients, parents, maternity care providers, and insurance companies. This supply chain benefits from the optimization and trust that the blockchain technology brings. This project was started by healthcare insurance company VGZ, and the National Healthcare Institute (Zorginstituut Nederland), in partnership with the maternity care organizations Liemerscare, Kraamzorg Zuid-Gelderland, and Kraamzorg VDA.

In February 2018, the first "blockchain baby" was born. On this blockchain application, maternity care workers and young mothers keep a record of the number of maternity care hours provided on Mijn Zorg Log using their smartphones. This means that the hours of care provided are recorded and can be viewed directly by the various parties involved. Mothers have the choice to decide which parties have access to their data. They will also have real-time information at their disposal regarding how many hours of maternity care are left in their budget. This application created efficiency for all user involved as very little auditing and checks will need to be performed after the service has been provided.

This blockchain architecture consists of a permissioned Ethereum blockchain using Proof of Authority The nodes are operated by the following organizations:

- Healthcare providers
- Insurance company
- National Healthcare Institute
- LedgerLeopard

**Security Implications**
Handling the data of mothers, babies, healthcare providers, and an insurance company presents a lot of risk and room for potential breaches. The following security implications need to be considered for a blockchain use case such as this one:

- Compliance and adherence to the GDPR (sections 4.3, 4.4 and 7 of the framework).
- Place security measures to secure personally identifiable information on the chain or linked to the chain (sections 4.3, 4.4 and 7 of the framework).
- Carry out load-testing to determine the borders of the defined system (section 6 of the framework).

For this use-case, the development company was assisted by an external company to perform security audits on the blockchain architecture. This is also recommended for organizations considering their first blockchain application.

## 7.2 Microbiome center Nederland

**Market: Healthcare**
The microbiome center blockchain system was implemented to connect and optimize the microbiome supply chain. This microbiome supply chain consists of the following parties:

- Patients
- Doctors
- Laboratories
- Pharmacies
- Personal healthcare environments

In the process, a patient visits the doctor, who advises on a performed feces analysis. This analysis is then sent to a laboratory after being paid by the patient. When the analyses report is ready the patient and doctor receive a notification with the results. The doctor and patient meet again and the doctor creates a personalized prescription, that is sent to the pharmacist once it has been paid. The pharmacy creates the prescription and sends the patient a notification with a tracking code. This complete flow is managed by a blockchain application, as the agreements are handled by smart contracts.

The system is a permissioned Ethereum blockchain, using PoA. The nodes are run by the following stakeholders:

- Doctors
- Pharmacists
- Laboratories
- Microbiome center Nederland
- LedgerLeopard

**Security Implications**
Having had the experience of developing the "Mijn Zorg Log" application, the developers had an idea of what security considerations to take into account. The new challenge in this project was the security of the following external connections linked to section 4.2 of this framework:

- Laboratory API
- Payment systems
- Pharmacy API

Besides the secure connections we added the following security precautions:

- Only use hashes and pointers in transactions (section 4.3 of the framework).

- Authentication/Authorization (2FA) handled by Microsoft Azure B2C (section 4.2 of the framework).

- All data that is passed to the backend systems are to be sanitized in order to prevent NoSQL/ SQL injections (section 4.2 of the framework).

As an addition to the security audit on the system from an external company, the development team hired internally an experienced cyber security specialist to their development team in order to review system components.

## 7.3 Loek! Real estate management

**Market: Real estate**
The Loek blockchain system was implemented to connect data from multiple sources and grant the authenticity of building dossier documents. The focus of the Loek application is to focus on the management of buildings. The different application users store all information regarding a building from a single online location, which is a designated digital building file. As a result, the user has all the relevant information at hand at all times. Loek is connected to a blockchain in order to generate hashes and reference points to the digital building dossier. The system creates a "fingerprint" to prove the structure of a document on a specific moment and a hashed pointer to the location, for role-based access.

The system is a permissioned Ethereum blockchain using PoA, where the nodes are run by:

- Loek
- Connected buildings

**Security Implications**
The security part of the blockchain focused on the

protection of the building dossier files and access for users and roles. This expressed itself in the following security precautions:

- Hashed pointers (section 4.3 of the framework).
- Hashes for documents (section 4.3 of the framework).
- Encrypted external file storage connected to blockchain (section 4.3 of the framework).

This usage of the blockchain creates a digital trust layer with a decentralized register of the building dossier, where security and integrity of data plays an important role.

## 7.4 Grain Initial Coin Offering

**Market: Financial, ICO**
The Grain Initial Coin Offering is blockchain solution where developers wrote smart contracts to be able to whitelist investors and distribute cryptocurrencies. Grain processes write agreements on the blockchain and have an instant payment mechanism. It helps companies save billions of euros annually in middleman-services and payment processing costs. Grain is a backend solution that allows labor management systems and freelancer platforms to integrate smart contract and financial transactions on the blockchain.

For this project, smart contracts were created for the cryptocurrency usage on the grain blockchain platform. For the ICO of grain, the developers created a smart contract to whitelist the keys of investors as result of a knowing your client (KYC). The developers also implemented the smart contract that handled the distribution of the cryptocurrency as a result of a payment.

The smart contract was created to be used on the public Ethereum blockchain where the nodes are run by participants of the public blockchain network.

**Security Implications**
The Security of a cryptocurrency exchange is the key component for the creation of a smart contract. When attackers find any flaw in the contract, money and trust may be lost. The developers considered the following when developing the smart contracts:

- To make use of smart contract security tools (section 4.1 of the framework).
- Work according to financial market authority security guidelines (section 4.4 of the framework).
- Use the audited code (section 4.1 of the framework).
- External smart contract company audit (section 4.1 of the framework).

For ICO smart contracting security, it is highly recommended to do research on the latest practices, use the proven code, and work with experienced developers.

## 7.5 Consentus

**Market: Healthcare**
The Consentus blockchain system was implemented to handle the consent of patients for handling their data by hospitals in a generic and private way.

One of the limitations that always comes back with the exchange of medical data, is the process of obtaining and recording permissions from the patient. Permissions from the patient are required before a source file holder can share data from this patient with other healthcare professionals, even if they already had a treatment relationship

with the patient. This simply means that if a patient in hospital X has data, for example of an antibiotic allergy, this fact is not readily available if the patient unexpectedly reaches the emergency department of hospital Y. in addition to this, the patient would also need to provide consent in advance to hospital X.

Each hospital must request permissions from the patient in their own way. There is no integral overview of the permissions already granted and the patient has very limited means to change that permission. In addition, there are several types of permission that a patient can give, each of which is separately requested and stored.

The Radboud UMC has designed a solution that answers the problem outlined above. By using Blockchain technology, this smart architecture can be used to set up a system that enables the patient to manage all permissions themselves, from a PC or mobile phone. This data is cryptographically encrypted on the blockchain and it is up to hospitals to check whether they have permission to request this information.

- The system is a permissioned Ethereum blockchain using PoA, the nodes are run by the connected hospitals

**Security Implications**

The major security risk identified for this application concerns the possibility of a breach that may cause a change in the consent for medical data between the patient and the hospital. For handling the consent of the users, the developers took the following security precautions:

- Authentication/Authorization to be handled by the proven systems used by hospitals. (section 4.2 of the framework)
- Secure external connections with hospital systems. (section 4.2 of the framework)
- Hashes and pointers for users and system connections. (section 4.2 of the framework)

# 8. Endnotes

# Endnotes

1. For more on this definition of blockchain, see Nolan Baurle's article on CoinDesk titled "What is blockchain?"
2. For the full context of the IEEE decision tree for adopting blockchain technology, see Morgen E. Peck's article: **https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain.**
3. For more information regarding TNO's research on blockchain security, see their research paper "Rethinking Blockchain Security: Position" (IEEE Blockchain, 2018).
4. This recommendation was provided by Dr. Griffith from the Ethereum Foundation. In an interview, he recommended any organization beginning to adopt blockchain technology to begin with a permissioned blockchain that would allow the organization to have ample control over the blockchain.
5. When discussing legal matters such as the GDPR, it is useful to comment that one should also look at other applicable legislation when using blockchain applications. It is advised to not simply focus on the impact of the GDPR.
6. For more information see GDPR art 4 (7).
7. For more information see GDPR art 4 (8).
8. For more details on this case, see the white paper by Pels Rijcken titled "Legal aspects of blockchains" page 9.
9. This is also the position of the French national commission on communication and liberties (CNIL) as it can be seen on page 1 of their report: **https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf.**
10. Ibid.
11. Ibid page 2.
12. See also **https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf**, page 3.
13. For more information see GDPR Art. 12-23
14. For more information see Pels Rijcken article, pages 10-11. And see Opinion 05/2014 on Anonymization Techniques from the Article 29 Data Protection Working Party (WP216): "Neither encryption nor key-coding per se lends itself to the goal of making a data subject unidentifiable: as, in the hands of the controller at least, the original data are still available or deducible. The sole implementation of a semantic translation of personal data, as happens with key-coding, does not eliminate the possibility to restore the data back to their original structure - either by applying the algorithm in the opposite way, or by brute force attacks, depending on the nature of the schemes, or as a result of a data breach. State-of-the-art encryption can ensure that data is protected to a higher degree, i.e. it is unintelligible for entities that ignore the decryption key, but it does not necessarily result in anonymization. For as long as the key or the original data are available, even in the case of a trusted third party, contractually bound to provide secure key escrow service, the possibility to identify a data subject is not eliminated."
15. For further details on the stand point of the Dutch DPA, see: **https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens**
16. For more details see the Pels Rijcken article, pages 4-8
17. As is the case with the NEN 7510 security standard for Dutch healthcare organizations.

Dutch
Blockchain
Coalition

connect and create

info@dutchblockchaincoalition.org

**www.dutchblockchaincoalition.org**