How to Develop Secure Blockchain Applications

Author: Damian Rusinek

This article contains many useful recommendations and guidelines which should be implemented if you work with solutions based on blockchain.

We sorted out the most important issues related to blockchain and Smart contracts and dealt with popular myths about them. Then, we explained the difference between public and private blockchain in order to draw attention to security aspects of this infrastructure.

A separate chapter is devoted to Smart contracts, their limitations and security recommendations.

The summary contains the most important aspects of integration between applications and the blockchain. It will be interesting for cybercriminals, especially in the case of blockchains used by cryptocurrencies like Bitcoin or Ethereum.

If you have any comments, change request, want to provide any feedback or help with future versions of this document, please don't hesitate to contact us at info@securing.pl.

SecuRing Team

Table of Contents

Blockchain's key points

The blockchain technology is a storage technology that contains, as the name implies, the chain of blocks. They are connected with cryptographic functions in a way which makes it difficult to tamper a single record because it requires to change all blocks that were added to the blockchain after the record.

The main benefits that blockchain provides are:

- Decentralization
- Trustlessness
- Immutability
- High availability (DoS resistant)
- Cost saving

They are achieved by the architecture of blockchain which is a network of equal nodes which create and verify blocks. Nodes keep the copy of the whole blockchain and use the consensus protocol to argue its current state.

Decentralization makes the storage trustless, because there is no single authority that controls the whole blockchain. Also, the redundancy makes the blockchain highly available without one single point of failure. Last but not least, the architecture of blockchain removes the need of third party or clearing houses and so, decreases the cost.

Blockchain myths explained

There are a lot of myths about blockchain gossiped in the Internet. Here we explain the most popular ones.

- Blockchain is not a cryptocurrency, but a technology that cryptocurrency uses to store its ledger.
- Blockchain does not require high computing power to operate. That requirement applies only to one of many consensus algorithms known as Proof of Work.
- Blockchain does not need a huge network with many nodes. There is a rule that says the more nodes in a blockchain, the more secure (trustless) the blockchain is. However, a

small group of participants can create a small blockchain network to create a storage without trusted third party between them.

- There is no single blockchain. Everyone can create his own blockchain, which is unique in terms of configuration and use.
- Blockchain is not used only in the finance sector. Blockchain is a technology that brings immutable storage which is suitable for the ledger, but can have many other applications (e.g. a durable medium in the banking sector).
- Smart contracts are not legal documents. They are programs that can confirm and track occurrences of certain facts on the basis of which legal conclusions can be drawn.

Public and private blockchains

The first decision in the design phase is to select a proper type of blockchain for particular application. There are two types of blockchains: public and private. They have many similarities like decentralization, replication, and immutability however some differences can influence the security of the network. Public blockchains are typically designed to achieve anonymity, whereas private blockchains use identity to validate membership and access privileges. Therefore, in case of private blockchains, the participants know exactly who they are dealing with.

Public blockchain

Public blockchain allows anyone to join the network, verify, and maintain the shared storage. The biggest known public blockchain is Bitcoin with capitalization over 100 billion dollars and about 40% of the market share.

The advantages of public blockchain are the following:

- There exist many blockchains that have a ready-to-use architecture (e.g. Ethereum - the most common smart contracts platform). This removes the need to run your own blockchain.
- It is easy to create a network with many nodes, but you must employ an incentivizing mechanism to encourage more participants to join the network.
    - The more nodes are there in the network, the more decentralized and trustless it is. It is harder to perform an attack to tamper the current state of blockchain.

- Public chains can be verified in real-time by anyone who wants to run a node and control the network.

On the other side, a public blockchain introduces the following drawbacks:

- All data kept in the blockchain is public which means that everyone can access and read it. Imagine health data in a public blockchain. If you want to keep sensitive data in a public blockchain you must:
  - create an access control mechanism in your application,
  - consider how trusted participants can access this encrypted data,
  - remember that transaction which store data can also reveal some sensitive information.
- Everyone can add new data to the blockchain. It does not mean that someone can change your data, but malicious participants may try to perform a denial of service attack on blockchain by sending a huge amount of new data.
- Public chains due to their public nature can be attacked by anyone and are a tasty morsel for cyber criminals as they keep assets worth millions of dollars. Only in 2018 the public blockchains market has been robbed at over $ 1 billion.

Private blockchain

A private blockchain allows only invited user to join and operate the network. Businesses who run a private blockchain, usually set up a permissioned network. They allow to specify restrictions on who is allowed to participate in the network, and only in transactions of certain type. Participants need to obtain an invitation or permission to join.

By reducing their focus on anonymity, private blockchains prioritize transparency, efficiency, and immutability.

The advantages of private blockchain are the following:

- Permissioned network easily allows to define an access control mechanism, which defines who is allowed to participate in the network in certain transactions.
- Private blockchain allows to use many different consensus protocols including “selective endorsement”, where known users verify the transactions. This allows to highly increase the throughput of blockchain transactions.

The drawback of private blockchain that must be considered are the following:

- Business must configure and maintain its own blockchain.
- Private blockchains are smaller than public ones and there exists a risk that after some nodes go offline the blockchain cannot continue its operation. This brings about the need to keep the nodes online.
- They are much less transparent (globally) and not designed for broad adoption, thus limiting their potential reach and application.
- Private blockchains mostly use effective consensus protocols that highly increase throughput of the network. However, it requires to lower the level of trustlessness to a trusted group of selected participants.

Infrastructure security

Regardless of the type of blockchain you choose, the following security aspects that concern the infrastructure should be considered.

- Prevent anyone — even administrators — from accessing sensitive information kept on the node.
- Deny illegal attempts to change data or applications on the nodes of the network.
- Guard encryption keys using the highest-grade security standards.

The above aspects apply to internal threats. Usually the applications integrate with one (random or selected) node. If an intruder can tamper the data on this node, the application will use this malicious data to operate.

Smart contracts

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the contract negotiation or performance. Smart contracts allow performance of credible transactions without any third parties. These transactions are trackable and irreversible.

This chapter defines the security aspects that must be considered when using smart contracts. We describe these aspects by the example of the most common platform for smart contracts – Ethereum.

Smart contract data is public

The Ethereum and other broadly adopted smart contract platforms are public blockchains. This allows intruders not only to read all contract data, but also to execute its public functions (functions are public by default).

History has shown that the problem of publicly accessible functions can led to million-dollar thefts.

Security recommendations:

- Set visibility to all variables and functions. That will minimize the risk of forgetting about a function that can perform critical operations and will become public by default.
- Do not keep sensitive information as plaintext in a smart contract. Use such protocols like blind commitments instead.

Smart contracts are programs with all its security consequences

Smart contract are programs stored and executed in a blockchain. It exposes them to the risks typical for classic programs such as overflows, underflows, insecure libraries and many others.

The insecure library was the cause of a half a million Ether (Ethereum's cryptocurrency worth about 220 million dollars at the time of writing) frozen, which basically means lost (Ethereum's Parity Hacked, Half a Million ETH Frozen).

Security recommendations:

- Use open source libraries to handle typical errors (e.g. SafeMath library which checks for underflow and overflow vulnerabilities).
- Verify the correctness of the libraries that you plan to use in your smart contract.
- Write tests for boundary conditions during a smart contract development.

Smart contracts and their limitations

Smart contracts, though very similar to typical programs, have specific limitations.

One of the most common limitation is the gas limit which defends the platform from denial of service attacks. The idea is that execution of smart contract cost some gas which must be paid by the executor. When he sends too less gas, the execution of smart contract is rejected.

However, this mechanism can be used as an attack vector when the programmer does not take into account the fact that certain operations may cost more gas when they are performed on different objects (e.g. other contracts). In this situation, the mechanism that was to defend against DoS attacks will be a vector for such an attack, when an intruder performs a smart contract on the "more expensive" object.

Another type of limitation is the randomness which is hard to achieve in a blockchain. Every operation on smart contracts must be executed in the same way on all nodes, thus there is no place for local pseudo-randomness. The blockchain-safe pseudo-randomness can be achieved easily by seeding deterministic pseudo-random function with any variable from global state of blockchain. However, such pseudo-random function is easy to crack because all seeds are publicly known.

Security recommendations:

- Learn the limitations of a smart contract platform.
- Learn how to bypass those limitations.
- Write tests for handling limitations during smart contract development.

Integration with blockchain

The blockchain technology delivers secure storage used by applications. The integration between applications and blockchain is a tasty morsel for cyber criminals, especially in case of blockchains used by cryptocurrencies, like Bitcoin or Ethereum. Intruders do not attack the blockchain itself,

but try to make the application execute malicious operations on smart contract or are deceiving people who use blockchain.

The applications that communicate with blockchain include:

- online wallets,
- crypto exchanges,
- or Initial Coin Offering (ICO) websites,
- and others.

All of the above applications are particularly vulnerable to attacks because they keep high volumes of money or store sensitive data, such as personal data. Furthermore, the security bugs in the applications integrated with blockchains led to millions-dollar thefts in cryptocurrencies:

- Detected vulnerability in Coinbase allowed to "extract" Ethereum.
- Simple Reflected Cross Site Scripting vulnerability on EtherDelta allowed to steal thousands of dollars (Hacker Uses Malicious Smart Contract to Trick EtherDelta Users).

Summary

Blockchain introduces an innovative approach to data storage in such a way that a trusted third party is not required. However, it introduces new threats to the technology itself, but also to applications that use this technology. The threats include both the well-known threats from typical applications, but also new ones specific for the blockchain.

When designing and implementing solutions that use blockchain, the following security recommendations must be considered.

Analyze the security of the solution in the design phase. In this way, you can avoid the situation where an application is exposed to threats, the removal of which will be difficult in a later phase.

Perform application security audits that integrate with blockchain as they can become an easy attack vector.

Revisit well-known web application vulnerabilities as they can have critical consequences.

All this comes from the fact that blockchain services (especially in the fintech sector) should have the same level of security and reliability that users expect of banks because millions of dollars are behind both.