**Blockchain Technologies**

**Research Report**

Contents

[1. Overview 1](#_Toc122606450)

[1.1 Main research question: 1](#_Toc122606451)

[2. Goal 1](#_Toc122606452)

[3. Sub-questions 1](#_Toc122606453)

[3.1 What Non-Functional Requirements are important for a payment system? 1](#_Toc122606454)

[Security 1](#_Toc122606455)

[Performance 1](#_Toc122606456)

[Availability 1](#_Toc122606457)

[3.2 What are the drawbacks and benefits of using cryptocurrencies as a payment method? 2](#_Toc122606458)

[3.2.1 Benefits 2](#_Toc122606459)

[3.2.2 Drawbacks 2](#_Toc122606460)

[4. Implementing a cryptocurrency payment system 4](#_Toc122606461)

[4.1 Coinbase 4](#_Toc122606462)

[Payment flow 5](#_Toc122606463)

[Implementation details 6](#_Toc122606464)

[Summary 7](#_Toc122606465)

[4.2 Comparison with Coingate 7](#_Toc122606466)

[5. Conclusion 10](#_Toc122606467)

[Bibliography 11](#_Toc122606468)

# 1. Overview

In this document I will describe the goal, the process, and the outcome of my research on the topic of “Blockchain technologies”. My research was conducted according to the research plan I have written in the first weeks of the semester.

## 1.1 Main research question:

*How can a payment system using cryptocurrencies be implemented in my marketplace website?*

# 2. Goal

My goal is to learn more about the blockchain by investigating cryptocurrency payment systems. In detail, my research is about how can such system be integrated in an enterprise application e.g., an online marketplace such as the one that I am currently building.

# 3. Sub-questions

## 3.1 What Non-Functional Requirements are important for a payment system?

Before implementing a payment system using cryptocurrencies, it is important to take note what the most important requirements for implementing a payment system are. This way, I can establish some baseline criteria for judging how reliable cryptocurrency payment systems are, as well as for listing their drawbacks and benefits.

I have performed **Literature study** to determine which NFRs are foundational when building a payment system. I will also investigate available payment services such as the ones used by banks to compare their characteristics to the ones of the cryptocurrency payment systems.

To get some examples of payment systems, I have used the **Available Product Analysis** research method. As it turns out, the most widely used implementation of payment software are banking systems. Therefore, the characteristics of those systems will be the most important criteria for judging a payment system.

### Security

According to multiple sources[[1](#_Bibliography)][[2](#_Bibliography)], security is the most important aspect of any payment provider or banking system. The reason being is that those systems operate with finances, which make them a common target for criminals.

Here, security is about protecting all sides of the transaction from potential exploits such as having their funds lost or sensitive information stolen by a bad actor and making sure transactions cannot be tempered with by a third-party (apart from the service provider e.g., the bank). Therefore, security is valued very highly in banking software and is incorporated by using secure encryption standards such as AES-256, network firewalls, automatic logout on inactivity etc.

### Performance

Performance refers to the time required to perform a financial transaction, as well as the ability of the system to handle multiple transactions at the same time. As any multi-client system, payment providers like banking systems need to be able to handle many simultaneous calls while resolving them within a reasonable response time and maintaining a certain number of transactions per second.

### **Availability**

Availability of a software system, banking software systems included, is achieved by having the system ready for use for as much time as possible during the day. Since there are multiple ways to spend money at any point of the day, a customer should always have access to their funds.

Banking systems should be up-and-running at least during the bank working hours. Mobile banking, online payment services and ATMs should work 24 hours a day with minimal maintenance time.

### **Summary**

Cryptocurrency payment systems, as any payment system, need to cover some Non-Functional Requirements, the most important of which are **Security**, **Performance** and **Scalability.** The next step of the research is to look at how well cryptocurrencies cover those NFRs as a payment method.

## 3.2 What are the drawbacks and benefits of using cryptocurrencies as a payment method?

Once again, I have performed **Literature Study** to gather information about Blockchain Technologies. Doing this, highlighted the most fundamental reasons to use this technology. Most of the benefits are taken into consideration from a merchant’s point of view, as implementing a cryptocurrency payment system is a concern of a merchant, and therefore their decision.

Although the above-mentioned method will also bring forward some negatives, the main disadvantages will be mostly discovered during a **Problem Analysis**. This method is useful to highlight the most important drawbacks of using cryptocurrencies as a payment method and of Blockchain Technologies overall. Finally, this will give more clarity on what is preventing the mass adoption of cryptocurrencies.

### 3.2.1 Benefits

As cryptocurrencies operate on decentralized systems, there is no single point of failure. This means that it is virtually impossible for the network to be down and payments to not be acceptable.

Depending on the specific network, payments using crypto usually take significantly less time to settle than traditional banking. This mostly benefits merchants, as the money that they are being sent will be received instantly rather than after a certain period of time.

Transaction fees are also a very important aspect of why a merchant would like to support crypto payments. Traditional payment providers charge the merchant a standard fee of 2.9% or higher, while a crypto payment fee will usually not exceed a fee of 1%, again, depending on the network. Examples of low transaction fee and high transaction speed networks are Stellar and Ripple.

Crypto payments also eliminate the risk of fraudulent chargebacks, which can occur in traditional payment providers when customers request chargebacks on their transactions. With blockchain, the transaction list, or a ledger, is public and completed transactions cannot be reversed, therefore invalid chargeback claims will no longer be an issue for the merchant[[4](#_Bibliography)].

### 3.2.2 Drawbacks

Cryptocurrencies are based on the blockchain technology and one of its main limiting factors is the transaction speed. Compared microtransaction providers such as Visa, currently existing cryptocurrencies can handle significantly less transactions per second. This could be a significant drawback in an enterprise environment, where depending on the number of users, payment services could be delayed significantly.

Figure 1 showcases the difference in the number of transactions per second, or throughput, that could be performed by VISA and PayPal, popular FIAT payment service providers, compared to that of the most popular cryptocurrencies.

Diagram

Description automatically generated

Figure - Transactions per second of different payment services

#### Blockchain Scalability Trilemma

The Blockchain Scalability Trilemma[[5](#_Bibliography)] is a concept, according to which blockchain can only achieve two out of either Scalability, Security, or Decentralization, but never all of them. Since decentralization is almost always the most important aspect of blockchain technologies, and security when it comes to financial transactions, compromises with scalability, and therefore speed, are inevitable.

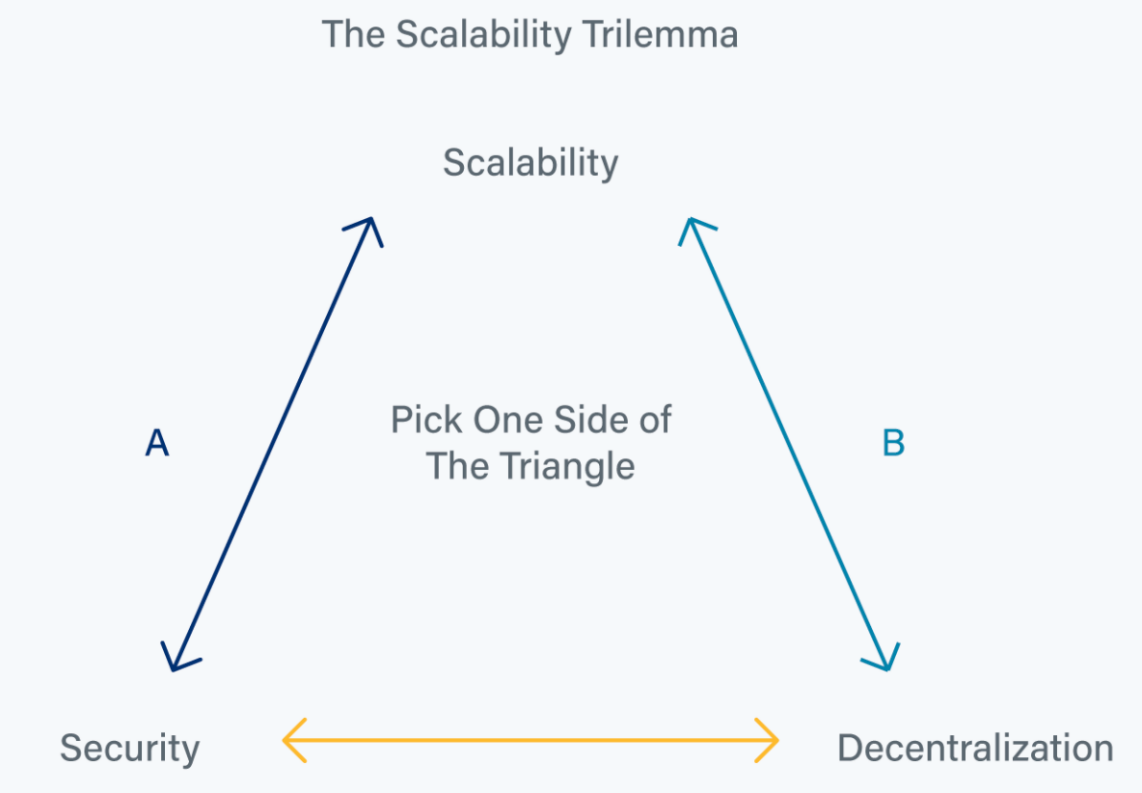
The Blockchain Scalability Trilemma relates directly to the NFRs listed in Chapter 3.1, where the *Performance* requirement is part of the *Scalability* aspect (how well does the system perform when it is upgraded), and Availability is part of Decentralization (absence of single point of failure, practically 0 downtime).

Figure - Blockchain scalability trilemma

The reason for this tradeoff is that in most blockchain networks having more participating hosts, or nodes, does not improve the actual performance of the network. It does contribute to it being more decentralized, as more are participating, and therefore more secure, as the risk of [51% attacks](https://www.investopedia.com/terms/1/51-attack.asp) and overall bad actors becomes significantly less severe.

However, to improve the performance of a such decentralized network, one would require to change the underlying software of the network, which can result in a less secure system ([Proof of work vs Proof of stake](https://river.com/learn/proof-of-work-pow-vs-pos-proof-of-stake/) mechanisms comparison).

### Summary

As blockchain technologies rely on a decentralized system of nodes, it provides high uptime and lower transaction costs without a single point of failure. However, this comes at a price of either lower transaction speed or a less secure network.

# 4. Implementing a cryptocurrency payment system

Payment functionality using cryptocurrency can be implemented with the help of a payment gateway. A payment gateway is a tool which allows implementation of crypto-to-crypto or crypto-to-FIAT payments. By applying **Available Product Analysis,** I determined what my options are for such service.

I will be building a prototype (**Prototyping** method) using one or more of those gateway providers. To successfully build a proof of concept, the main criteria will be ease of use of the provider gateway and of the payment service itself.

The first step in choosing a gateway is to look at the available ones. After taking a look at a [list of recommended gateway services](https://www.devteam.space/blog/10-best-bitcoin-payment-gateways/)[3], I decided to make my first prototype with the Coinbase one. The reason for this choice is that this is one of the leading crypto exchanges in the world and adheres to the U.S. laws on currency exchange, which makes it a trustworthy payment service provider.

## 4.1 Coinbase

To make a payment to someone using the Coinbase API requires the merchant to create a charge, which functions like a payment request. This is done by sending a request containing the amount to pay, description and name. Optional parameters can specify details such as pricing currency, but in this case, I am using the default currency which is USD.

### Payment flow

A screenshot of a computer

Description automatically generated with medium confidence

Figure - Creating a charge

After the request is done, a charge link is returned, prompting the user to make the payment.

A screenshot of a computer

Description automatically generated

Figure - Payment request

The link leads the user to the payment request page. The user is prompted to pay some amount (50 cent in the example) and can pay with their Coinbase wallet, or with an external one. This is one of the advantages of the Coinbase gateway – it has a large user base which allows many of the users to pay just by logging in.

The second option, payment with external wallet is also simple. The user selects a currency and is being presented with a QR code representing the merchant’s wallet address to scan with their wallet.

Qr code

Description automatically generated with medium confidence

Figure Payment with BTC

### Implementation details

A screenshot of a computer

Description automatically generated with medium confidence

Figure - Create Charge endpoint implementation

Implementing this gateway was straight-forward. My application accepts a charge request and forwards it to the Coinbase Commerce API and then the response is sent back to the client.

In a production environment, the client will not be able to choose the amount to pay but will rather receive a charge based on the price of the product they have selected. As this is just for testing purposes, I am using the Postman application (*figure 3*) to simulate a client buying a product.

This workflow allows extra configurations to be added in the code to add options such as paying in different currencies. Security is handled by Coinbase and does not require the merchant to implement extra validation or security features.

### Summary

The Coinbase gateway provider fulfills the requirements to be both easy to use for the customer, as well as easy to implement by the merchant. It is also secure and has multiple options for payment. In addition, it offers additional functionality related to checkouts and payment invoices.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure - Coinbase Commerce API

## 4.2 Comparison with Coingate

I took a look at another payment gateway to compare its features with the one I implemented. My choice was Coingate, as it is also appeared to have good documentation. As I had already gone through the process of researching such service, I knew what to look for the second time.

Graphical user interface

Description automatically generated

Figure - Coingate API documentation

The overall payment flow here is similar, with the difference that here, a “receive\_currency” field has to be specified prior to creating the payment request. This is slightly more inconvenient in terms of implementing the API, as the merchant would need to implement their own menu to show the payment options.

Coingate also offers payment with 10 different cryptos, compared to the 12 of Coinbase.

Coingate however offer a [sandbox website](https://coingate.shop/ecommerce/checkout/), where the implementation of the payment service is implemented. For this reason, no implementation prototype is required to evaluate the ease of use of the service. The main downside here, is that an email is required for the purchase to go through, in contrast to the Coinbase gateway.

Graphical user interface, application

Description automatically generated

Figure - Coingate sandbox shop payment view

# 5. Conclusion

Based on my research, there are various reasons to implement cryptocurrency payments into one’s online marketplace, such as higher network availability, lower risk of scams, lower transaction fees.

Naturally, there are also drawbacks to using cryptocurrencies, as listed above. However, existing payment services called gateways solve most of those issues, for example by providing multiple currencies as options. This makes sure that more than one network is used for transaction, depending on the preference of the users, which makes sure a single blockchain network is not overused, therefore partially avoiding performance issues.

Finally, the most appropriate way of implementing a cryptocurrencies payment system in an online marketplace would be by using cryptocurrency payment gateways, as their services are conveniently exposed for usage and they solve some of the most critical cryptocurrency and blockchain problems, leaving a significant amount of benefits.

# Bibliography

1. *System Design of Bank Management System*. (n.d.). Retrieved 16.11.2022 from <https://iq.opengenus.org/system-design-of-bank-management-system/#nonfunctionalrequirements>
2. *NetCheque, NetCash, and the Characteristics of Internet Payment Services* (n.d.). Retrieved 16.11.2022 from <https://quod.lib.umich.edu/j/jep/3336451.0001.126/--netcheque-netcash-and-the-characteristics-of-internet?rgn=main;view=fulltext>
3. *10 Best Bitcoin Payment Gateways for 2022* (n.d.). Retrieved 16.11.2022 from <https://www.devteam.space/blog/10-best-bitcoin-payment-gateways/>
4. *Benefits of Accepting Cryptocurrency Payments 2022* (n.d.). Retrieved 16.11.2022 from <https://coingate.com/blog/post/why-should-business-accept-crypto>
5. *A Deep Dive Into Blockchain Scalability* (n.d.). Retrieved 16.11.2022 from <https://crypto.com/university/blockchain-scalability>
6. *51% Attack: Definition, Who Is At Risk, Example, and Cost.* (n.d.).Retrieved 16.11.2022 from <https://www.investopedia.com/terms/1/51-attack.asp>
7. *PoW vs PoS* (n.d.).Retrieved 16.11.2022 from <https://river.com/learn/proof-of-work-pow-vs-pos-proof-of-stake/>