POLITECNICO DI TORINO

Master's Degree in Computer Engineering

Master's Degree Thesis

Design of a mobile payment application and performance comparison with the Lightning Network

Supervisors:

Dr. Antonio Vetrò

Dr. Marco Conoscenti

Candidate:

Andrea Ciccarello

Academic Year 2020-2021

Summary

The events of 2020 have certainly led to an increase in the use of digital payments. The global pandemic phenomenon has led to the evolution of the processes that allow the digital exchange of money and the regulations associated with it. In this context, European Payment Service Directive (PSD) regulations assume a crucial role. PSD2 is in fact bringing important changes to the European digital finance sector. Among the most important innovations, the thesis focuses on those that impact the most on the development of a mobile application for digital payments:

- Stronger Security Requirements through multi-factor authentication.
- Implementation of an architecture that allows banks and financial institutions to share customer accounts information to third-party payment service providers.

In particular, the main purpose of this work is to examine the design and development process of a digital payment mobile application. The result was obtained in collaboration with a Turin IT company operating in the world of digital payment solutions. My contribution to the project has concerned the drafting of the Security Analysis document, and the implementation of Android modules that manage the user registration process for the mobile application. The thesis shows fundamentals factors taken into consideration during the software development process such as architectural patterns, actors involved, security requirements. The application allows to link up payment instruments from users' bank accounts, even from different banks, and to access banking operations. Its release is scheduled for summer 2021, with a development of six months.

The secondary purpose of the thesis is to compare the performance of the mobile payment application discussed in this thesis with the Lightning Network. The Lightning Network is a payment system for the Bitcoin cryptocurrency and is the most developed solution for the exchange of fast Bitcoin payments. Performance measures regarding the LN payments were computed running a simulation on CLoTH, a LN simulator. The simulation was executed on a snapshot of the LN captured on 17th December 2020. Performance measures regarding the mobile payment application were computed from an IT audit during the month of September 2020. The results show that the solution based on traditional payment methods has a higher success rate with respect to the Lightning Network (99.97% against 82.73%, respectively). The Lightning Network is still in an immature phase of development and the community is working on improving its performance.

The world of digital payments is experiencing a strong evolution, especially in the European context. In fact, regulations are pushing for more efficient and open approaches. These new architectures encourage financial institutions to leave closed banking applications in favor of community networks. In parallel, cryptocurrency-based solutions are arousing more and more interest in the social scenario. The possible adoption of this type of innovative payment encourages the development of increasingly reliable and effective solutions.

Acknowledgements

The author wishes to thank his supervisors, Dr. Antonio Vetrò and Dr. Marco Conoscenti, who gave him the opportunity to develop the Master Thesis, matching the work done in the company to a stimulating and constantly evolving context, which is the cryptocurrency reality. The author also wishes to thank his supervisors for the advice and support given to him during the writing of the thesis. The author thanks the company tutor and colleagues for the professional support and the opportunity to work in an innovative and engaging environment. Finally, special thanks go to the family, all the university colleagues and friends for their support and affection.

Table of Contents

List of figures VI

List of Tables VII

1. Introduction 1

1.1 Context 1

1.2 PSD2 Regulation 1

1.3 Goals and Contribution 3

2. Background on Digital Payments and Payment Channel Networks 4

2.1 Digital Payments - Introduction 4

2.2 Digital Payments – Requirements 5

2.3 Payment Services Directive 2 9

2.4 Bitcoin and blockchain 15

2.5 Payment Channel Networks 16

2.6 Lightning Network 18

3. Analysis of Digital Payment Application 25

3.1 Introduction – Multi Bank App 26

3.2 Stakeholders and Roles 27

3.3 Architectural Requirements 29

3.4 Strong Customer Authentication 31

3.5 Security Requirements 38

3.6 Main Features 44

4. Comparison between Traditional Application payments and LN exchanges 49

4.1 CLoTH Simulator 49
4.2 Simulation on the Lighting Network 54
4.3 Traditional Digital Payment Application Performances 57
4.4 Comparison of the results 59
5. Conclusions and future work 61
Bibliography 65

List of figures

Figure 1 - Two Factor Authentication 10

Figure 2 - Funding Transaction 19

Figure 3 - Commitment Transaction 19

Figure 4 - Routing Payment Schema 21

Figure 5 - Pre-Image Generation and Delivery 23

Figure 6 - HTLC Opening phase 23

Figure 7 - HTLC Closure 24

Figure 8 - Stakeholders scheme 27

Figure 9 - Architecture scheme 29

Figure 10 - Bank SCA, Redirect on Web App Sequence 33

Figure 11 - Bank SCA, Redirect on Bank Mobile App Sequence 34

Figure 12 - Bank SCA, Decoupled on the same device Sequence 36

Figure 13 - Bank SCA, Decoupled on a different device Sequence 37

Figure 14 - Certificate Pinning scheme 42

Figure 15 - Initial Configuration Sequence Diagrams 45

Figure 16 - Set Default Instruments Sequence Diagram 47

List of Tables

Table 1- CLoTH simulator input parameters 51

Table 2 - CLoTH Simulator output parameters 53

Table 3 - LN simulation results 55

Table 4 - P2P payments performance 57

Table 5 - P2B payments performance 58

Table 6 - Braavos App p2p / LN results comparison 59

1. Introduction

1.1 Context

Thanks to the adoption of emerging innovations that increasingly integrate with others and facilitate the development of novel payment mechanisms, the digital payment industry is expanding and thereby generating business opportunities. With the rising demand and usage of mobile devices, the production and use of mobile POS alternatives grows exponentially. Digital and mobile technologies have become real competitive resources in this context.

- According to the *Mobile Payment & Commerce Observatory of the Milan Polytechnic School of Management*, Mobile Payment and Contactless Payment surpassed EUR 46 billion in payments at the end of 2018, reflecting 21% of overall digital payments by wallet [1].

1.2 PSD2 Regulation

There is no question that the introduction of the Payment Services Directive 2 (PSD2), the regulation [2] that formally came into effect in January 2018, has led to the transformation of the sector. In particular, in order to benefit from a modern multi-channel consumer interface, regulation has incorporated several important reforms, first and foremost the idea of Open Banking, a user-centered environment. The PSD2 has decided to put the user and his experience at the center of the whole regulatory system by imposing a complete revision of the rules related to digital payments. More freedom and more choice are the two pillars of this great change. People must be able to use any digital tool to make transaction and payments. By implementing a

full revision of the rules pertaining to digital payments, PSD2 has agreed to place the customer and his experience at the center of the entire regulatory framework. The two foundations of this big transition are more rights and more options. People must be able to make purchases and transfers using any digital instrument.

The context of new and emerging cryptocurrencies has generated great interest.

- Bitcoin is the world's largest cryptocurrency by market capitalization [3]. It is a collection of nodes that run the Bitcoin's code and share information about transactions stored and traded thanks to the use of a decentralized ledger system known as blockchain. This technology has the capability of processing around 7 transactions per second. This represent one of the greatest problem of Bitcoin: the scalability. This problem is due to the fact that each committed transaction needs to be stored into the blockchain.
- The Lightning Network, is one of the solutions that were proposed in order to solve the scalability limit related to the blockchain. The main concept that stands behind this technology is that it enables parties to perform transactions off-chain, reducing the operations that involve the distributed ledger.

1.3 Goals and Contribution

The banking and finance sectors are forced to constantly understand the possibilities provided by emerging technologies, by adopting the best business solution in order to satisfy the customers' demands.

- The goal of this work is to examine the development of a Digital Payment Application by exploring its functionality, performances, involved actors and the overall project evolution.
- The thesis work was carried out in collaboration with a Turin IT company operating in the world of digital payment solutions.
- My contribution to the project concerns the support on analysis phase and the development of some modules of the Android mobile application regarding the users' initialization process.
- The result is a multi-bank and multi-IBAN application that allows user to link multiple bank accounts with multiple payment instruments on the same application. The great advantage is given by the possibility to access to money exchange and banking operation from the same interface, performing person-to-person and person-to-business payments instantaneously, even if parties belong to different banks.
- The possibility that new technologies based on cryptocurrency can replace the current paradigm is continuously emerging.
    - For this reason, a comparison between the actual digital payment solution and Lightning Network will be conducted.
    - The goal of this comparison is to illustrate the key architectural and practical discrepancies, in terms of performances and reliability, between these solutions

2. Background on Digital Payments and Payment Channel Networks

2.1 Digital Payments - Introduction

Digital payments are payments made over the internet and mobile channels, and any payment sent electronically or by mobile computing and internet-enabled devices should also be considered so.

This means that, for digital transfers to take place, the payment sender must have a bank account, a form of internet banking, a payment device and a means of transmission, which means that either he or she could have signed up with a provider or an intermediary, such as a bank or a provider of services.

The recipient of the payment must still have these forms to accept payments, aside from the sender possessing those means. This means that there must be a medium of transmission between the sender and the recipient. The former instead of paying the latter in cash and physical format, pays in digital format indicating that the exchange happens over the E-Commerce or M-Commerce modes.

The method of buying and selling on the internet applies to E-Commerce or electronic commerce. The birth of e-commerce is predicted to occur in 1994, with the first online transaction in Philadelphia. In general, e-commerce refers to internet shopping operations that take place on a tablet or laptop.

M-Commerce refers to online payment transfers that take place over a mobile device. The growth of mobile access, surveillance, and applications has enabled retailers to provide smartphone services, goods, and payment

gateways. The trend in m-commerce is also spurred by the rising population owning smartphones. [4]

2.2 Digital Payments – Requirements

2.2.1 Security

Without any uncertainty, the more comfortable the user feels, the sooner they can test new features. In order to ensure that personal information is not turned over to ensure that their money is in safe hands, banks need to announce proactively that their networks and procedures are absolutely safe. In this situation, research is immensely important, due to the enormous relief it will bring to banks seeking to follow the path of digital transformation. Security monitoring will guarantee that the introduction of software and products on the market is acceptable. Basic elements of secrecy, honesty, verification, availability, authorization and non-repudiation which contain typical security specifications. Clearly, it can be known that the effects of a security breach are important. There is a loss of profits, a loss of reputation and a loss of consumer interest as well.

2.2.2 User Experience

User experience is taken seriously by businesses, and quite a number of them are innovatively redesigning critical interfaces. While when a product or application is first introduced, the focus could be on receiving the basic concept, it has been validated over time and demonstrated that the application will launch the company to a whole new network with a better user interface. This is particularly true of banking services; even slight inconveniences will throw the masses off. Because of a confusing user interface, the inability to execute basic acts or the inability to concentrate on the appropriate action item due to interruption in the form of ads can both permanently throw off clients. The one thing that FinTech firms and financial institutions alike need to bear in mind is the simplicity of incorporation, when more retailers rely on becoming cashless in today's economy. Customers are far less passionate about the exclusivity of such payment demands. This is because the payment methods that a client may opt for are not approved by all merchants. This last statement is specifically related to one of the key goals of the regulation of PSD2, which will be further pointed out in the article. Indeed, Open Banking enables the collaboration and convergence of digital payment applications and organizations to be strengthened. Through making the payment hassle-free, smooth integration with the net-banking web application and e-payment gateways will significantly support cashless transactions.

Again, software testing is proving to be a solution in this respect. To guarantee that consumers find the program easy to maneuver, the whole user interface is also carefully tested.

2.2.3 Functionality

The standard of mobile banking apps will become a point of distinction for banks as more financial transfers move from bank offices to mobile phones. Value is defined by the application's functionality in such a scenario. Functional testing consists of testing for functionality, which is a feature that validates the whole system or part of your product. In order to ensure that the defect rates are minimized, software testing organizations have end-to-end research coverage, reaching straight from the requirements-gathering point. In an attempt to discover crucial flaws in the current structure, the coverage starts with the market requirement paper and continues to the end-to-end business scenarios. In order to ensure that the system meets all user expectations, the right methods always include any job from a user viewpoint.

2.2.4 Performance

Digital banking has to be very careful in terms of outcomes. Most consumers rely on their banking cards or digital applications to conduct transactions smoothly in the growing world of cashless transactions. There will be millions of clients executing multiple transactions at any given time. It becomes a matter of great annoyance if apps begin to crash and transactions begin to malfunction or be postponed. Unquestionably, success testing is important. Performance checking is important to measure that, ultimately, the software will respond as it was meant to, right from measuring the reaction time of the application to ensuring that the load and stress checking is completed. It is crucial that the finest approach and best technique for performance testing and its subsequent evaluation can be properly determined.

2.2.5 Data Integrity

The most significant service that operates exclusively on the topic of trust is banking. It is the duty of the customer to provide authentic information, while banks are responsible for retaining integrity and ensuring the security of customer funds. In such a situation, it becomes necessary to gather information that shows the financial details of a customer immediately and, in addition, spending patterns. Compromising such knowledge will have devastating repercussions. Software testing ensures the smoothness and reliability of internal systems and procedures and, most significantly, the protection of data privacy, especially under the threat of a possible breach.

2.3 Payment Services Directive 2

The PSD2 brings two major changes to the payments industry:

- It mandates stronger security requirements for online transactions through multi-factor authentication
- It allows banks and other financial institutions to offer access to customer bank accounts to third-party payment service providers when account holders offer their permission.

According to PSD2, anonymous transfers, such as card purchases conducted by European users with two-factor authentication, would need to be questioned by financial firms keeping payment accounts. This better authentication blends something that the user knows, such as a password or PIN, with something that the user has, such as a code created by a mobile app or something that the user is, such as a fingerprint or facial recognition biometric identifier. For any transaction that will connect the customer and the transaction number, this will result in specific authentication codes.

The goal of the European regulators was also to establish a competitive market for payment services in Europe and to allow new companies in this sector to innovate. PSD2 allows banks and other financial institutions that maintain payment accounts to offer third-party providers to consumers with access to those accounts in order to do this, provided that the account holders give their permission.

These third-party payment processing providers will be able to verify the availability of money, initiate transfers on behalf of account holders or access account details, such as details on purchases. Access can be provided in many ways, including by redirecting customers to the bank 's site for authentication.

2.3.1 PSD2 Strong Customer Authentication

Any elements of the latest authentication method adopted by the PSD2 need to be found out. How the Strong Customer Authentication (SCA) method is applied in a Digital Payment Smartphone Application will be discussed later in this article. One of the key facts of PSD2, as already explained in previous chapters, is the emphasis on enhancing protection in the payment space by stressing SCA. When the following circumstances emerge, PSD2 has required service providers to promote SCA:

- Access online payment accounts
- Initiate electronic transactions
- Action carried out through a remote channel that presents a risk of payment fraud
- Provision of information through a service provider

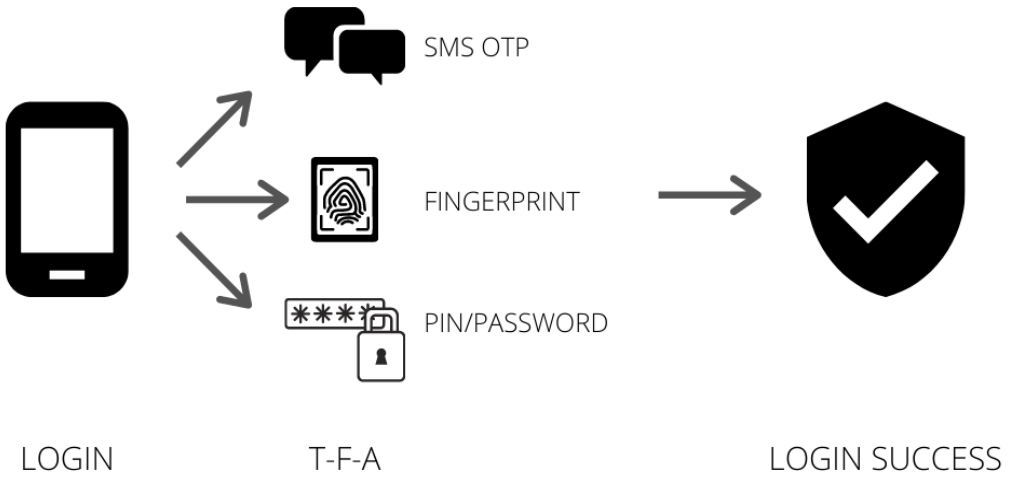

Figure 1 - Two Factor Authentication

There are common methods that various banks can adopt to introduce SCA. One of the most commonly used and simplest SCA methods to incorporate is Redirect. When the Payment Service Consumer (PSU) continues communicating with a third-party vendor, it is forwarded for authentication to an Account Serving Payment Service Vendor web interface / mobile device. It suggests that when a customer buys online in a banking situation and tries to make a payment, he is routed to his bank website / mobile application to authenticate himself by entering his credentials. In a mobile payment application scenario that allows a customer to connect one of their bank accounts to make digital payments, this procedure is likely to occur only during the account registration process, which is normally conducted as the first procedure. A great benefit of the Redirect strategy is that no more comprehensive usage knowledge is exchanged with the TPP.

The Decoupled method is another common solution. This technique is somewhat similar to that of Redirect. The key distinction is that the PSU will not be forwarded to the website / mobile device for authentication by the ASPSP. This authentication has to be performed from the end of the ASPSP from an individual program or computer. This suggests that the PSU should authenticate itself into a methodology that the primary authentication flow should be decoupled from. It is very easy to incorporate and makes it easier to provide a successful relationship between ASPASP and PSU, close to the Redirect method. [5]

The thesis would clarify in depth how these methods are applied during a digital payment application's authentication process. It will demonstrate how Redirect and Decoupled SCA can be used to authenticate the PSU in order to connect their bank accounts to the mobile application.

2.3.2 Main effects of PSD2

The efficacy of PSD2 will be expressed directly in the two main fields referred to in the Directive, namely 'Internal competitiveness in the European payments market' and 'User protection during online account monitoring and maintenance' respectively. The value of this Guideline is also related to the fact that its implications will have a concrete impact on individual consumers, who will see an improvement in identification and authentication processes, and on banks, as well as on any approved third party, who will have to reconsider their security mechanism and their strategic business place.

PSD2's first appreciable impact is attributable to rivalry. The Directive seeks to remove the monopoly on the management of online banking accounts by adding new third-party companies capable of providing comparable services to the European lawmakers. Indeed, today, parties other than banks may:

- Carry out payment ordered by the owner of a bank account held with another payment service provider
- Provide consolidated information on one or more payment accounts held by the user with another payment service provider or with more than one payment service provider
- In the case of payment service provider issuing debit card, to offer the possibility of receiving confirmation of the availability of funds in response to a request sent online

This would expand the number of players, thus improving the attractiveness of the services provided, both in terms of cost and quality. In addition, opening up the market to new entrants, especially in the start-up and Fintech industries, would enable established banks to continually develop their offerings, increasingly digital, which would definitely be beneficial for users

who, in terms of consumer experience, would benefit from creating more sophisticated systems.

Online shopping is another notable advantage, which can be appreciated by all consumers. Anyone shopping online was forced to trigger a double move before the launch of PSD2. If the order had been issued, the chosen merchant had to contact a credit institution inside particular payment circuits that had accessed the bank account of the customer and approved the operation. The law removes this intermediation, allowing parties other than banks to have access to users' current accounts and to dispose directly of the appropriate transaction. Not only does this make the whole payment process more agile, but also helps consumers to minimize the time and the fees for each operation in particular.

The enhancement of consumer service made possible by the legislation often relies on customers handling their accounts more effectively. Until PSD2, owing to the incompatibility of bank schemes, people of multiple accounts were obliged to handle them separately. It is easy to view all accounts from a single dashboard, even though they are in two or three separate banks, thanks to the crucial step towards Open Banking and Account Management Service Provider providers. It is also possible for consumers to use services that track their buying actions on the basis of bank movements and, as a result, identify the most competitive market offerings. PSD2 would potentially lead banks to vanish over time, as we know them today. The conventional credit institution would therefore surrender the proprietary aspect of the client partnership, i.e. the monopoly over the handling of its financial records. Indeed, the latest European regulation 'requires' all European banks to open up to all actors, and this represents a real shift in attitude when it comes to financial services management. In the Open Banking model, banks must, on the one hand, exchange all the financial details previously available only to them, while, on the other hand, they will

be motivated to turn themselves into a banking channel that, in addition to more conventional services, incorporates new and digital technologies to fulfill consumer needs and demands. This implementation is made possible by opening the API of the bank, which has the interfaces that allow users to interact more efficiently and rapidly with various systems. Banks will also benefit from this transition because it will improve the synergy between separate parties. It would be cheaper for conventional credit institutions, without even needing to build specialized in-house tech capabilities, to leverage start-ups in the Fintech industry to make the jump in technology innovation required to stay competitive.

A fundamental factor in which directives interfere is the cybersecurity of the Transparent Banking system that is being implemented. Sufficient protection conditions for all entities must be ensured in order to maximize competitiveness and open up the market to other parties. PSD2 incorporated some significant developments for this purpose. The Dynamic Relation definition, which is an external protection element, is one of these. It is based on creating random authentication codes, subject to a specific collection of security criteria and based on the validation of encryption-based disposable keys, electronic signatures or other authentication. In fact, this ensures that when the user decides to execute some transaction, the user must approve the transaction by means of a special code explicitly identified with that transaction, for certain specific characteristics, for the specific sum and for the specific receiver. All this can help to remotely execute every operation, even those on social media. The SCA was also implemented in this field to increase consumer safety. Therefore, authentication schemes based entirely on a username and password request are no longer sufficient; the user would be forced to authenticate himself by means of knowledge that he alone recognizes, computers that he alone owns, or identifying elements.

2.4 Bitcoin and blockchain

Bitcoin is a decentralized banking mechanism and a currency that is decentralized. It is introduced by open software, and is open for all to download and use. A computer running the Bitcoin program is called the Bitcoin Node. It is connected to the other Bitcoin nodes and it is part of the Bitcoin peer-to-peer network. The blockchain is the database that records all Bitcoin transactions that have happened. Since the form is a sequence of blocks, it is called a blockchain. Each block includes a transaction group and has a connection to the previous block, thus forming a chain. The process that allows to maintain this public ledger is called *mining.* The mining process is conducted by nodes in order to record a new block of transactions into the blockchain. All the nodes that are involved into this process, are called to solve the "proof of work", a series of complex computational math tasks. The result of this operation makes two outcomes:

- The winner of the "proof of work" will be awarded with Bitcoins, in this sense it is possible to assert that new Bitcoins are produced.
- Solving the "proof of work" verifies Bitcoin payment network and makes it trustworthy and secure.

Scalability is the key limitation of this technology. Indeed, because of the blockchain transaction throughput limit, Bitcoin and blockchain-based cryptocurrencies don't scale. Payment Channel Networks are one of the most interesting options for tackling scalability, as they allow users to make off-blockchain payments.

2.5 Payment Channel Networks

This paragraph provides a background on Payment Channel Networks, in particular, it focuses on Lightning Network.

Payment Channel Networks are networks of payment channels that allow users to perform off-chain payments, therefore not subjects to the blockchain throughput limit. A payment channel is a direct, bi-directional payment connection between two nodes. Based on the balance and capacity of the channel, users can exchange off-chain commitments to each other outside of the Bitcoin blockchain. Payment within a channel are off-chain and do not require validation by or communication to the blockchain. Payment Channel are limited by three things:

- **Trip Time**: the time it takes for routing bytes of data that the protocol requires to move funds from one end of the channel to the other.
- **Capacity**: it is the capacity of the channel, meaning the amount of bitcoin that is committed by each node to the channel during the opening phase.
- **Size limit**: due to the maximum size limit of a Bitcoin transaction there is a limit on the number of in-progress routed payments that can be carried over a channel at the same time.

One of the greatest advantages of PCN is linked to the payment speed. The time to update a channel is, indeed, bound by the communication speed of internet. This allow payments very likely to be almost instant. Once a channel is open, there is no need to ask for confirmation of Bitcoin blocks in order to make a payment. This allow this solution to be enough independent from the Bitcoin Network, reducing the interaction of a node only with its channel partner. Smart Contract can be used also to solve trust problems. The cryptographic protocol that stands behind PCN allow nodes to perform

payment without any trust on the counterpart. If any node becomes unresponsive of tries to cheat, the blockchain can be called in order to resolve the smart contract agreed by nodes. Another important concept on PCN is related to Privacy. Bitcoin transactions are public, meaning that everyone as access to transactions blocks. Payment transactions on PCN are known only to nodes that perform transactions. Only the final balance, which is the aggregate of all payments in that channel, will become visible on the blockchain.

2.6 Lightning Network

Lightning Network (LN) is a peer-to-peer network of payment channels implemented as smart contracts on the Bitcoin blockchain as well as a communication protocol that defines how participants set up and execute these smart contracts. It is the most popular implementation of Payment Channel Networks based on Bitcoin. The motivation that stands behind the adoption and proposal of this solution is given by the Bitcoin scalability limit. Bitcoin technology doesn't allow more than seven transactions per second. Compared with standard payment systems, the number of transactions allowed by Bitcoin is near to the 0,01% with respect of standard payment circuits.

In order to perform a payment, a payment channel needs to be opened. This transaction is called *Funding Transaction*, and it is recorded on the Bitcoin blockchain. Each node decides the amount of BTC they want to allocate into the channel. The amount of funds own by each node is called balance. In this phase the input balance is given by the sum of nodes' BTC balances. The total amount deposited is called *channel capacity* and sets the maximum amount that can be sent across the payment channel.

Nodes are allowed to exchange off-chain payments with their partners only after they have committed their balances. The *commitment transaction* gives as output information about nodes' balances. By signing a commitment transaction, each node can get its funds even without the interaction of the other node. This is considered as protection towards any kind of unusual behavior, like disappearance, refusal to cooperate or attempt to violating the payment channel protocol. Let us provide a use case of a payment transaction.

1. Alice and Bob open the payment channel performing the funding transaction. They are allocating 50 Satoshi each.

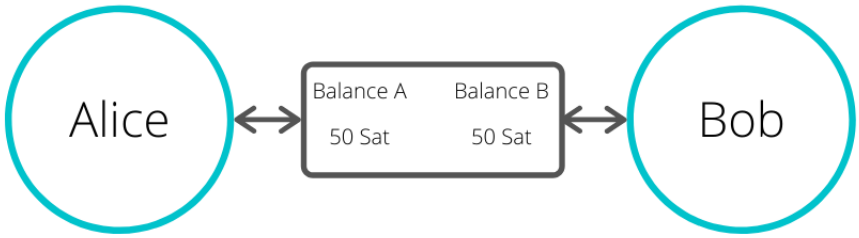

Figure 2 - Funding Transaction

2. In order to perform a payment, Alice and Bob, make a commitment transaction, updating their balances. Let assume that Alice wants to pay Bob 10 Satoshi. Alice and Bob will make a commitment transaction which have as result 60 Satoshi for Bob and 40 Satoshi for Alice. This operation is done off-chain, meaning that any interaction with the blockchain will be avoided. This allows LN to scale way better with respect of limited solution based on on-chain transactions.

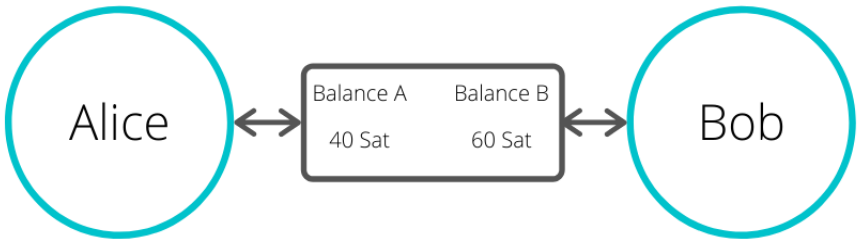

Figure 3 - Commitment Transaction

3. Last phase, in a simplified case, is the channel closure.
   There are 3 ways to close a channel:

   - Mutual close: both channel partners agree on the closure of the channel. When both side have decided to close the connection,

they have to send to the blockchain the last commitment transaction, stating the last balances state. This operation is called *close transaction*. The fee related to the on-chain transaction is paid by the node who opened the channel. Furthermore, channel partners need to agree on the appropriate fee and then sign the closing transaction.

- Force close: it happens when a node wants to close the channel without the other node's consent. Usually, this is the outcome for a connection in which there is an unreachable node, or a not responding node, so mutual close is not possible. In order to perform a force close, a node needs to publish itself the last commitment transaction.
- Protocol Breach: whenever a node violates the payment channel protocol. Generally, this happens when a node tries to cheat the counterpart, i.e. by publishing a not valid commitment transaction to the blockchain.

Opening and closing channels requires an on-chain transaction. As it is mentioned, this kind of transactions include also fees. The best way to avoid paying fees is to keep channels opens as long as possible. Channels cannot last open forever, sometimes a closure is necessary, i.e. some node wants to change its balance, a channel partner becomes not responsive for a long time, a node has finished its balance and it wants to perform a new payment etc.

2.6.1 Routing payments across channels

Another property of LN is Payment Routing. The network, indeed, allows its nodes to perform payments even if two nodes are not directly connected through a channel. Payments can also be forwarded from a payment channel to another payment channel, by following a path across the network connecting different payment channels. This scenario is shown in the figure 2.4. Alice can send money to David even if not directly opened a channel with him, by routing its payment through the channel opened with Bob.

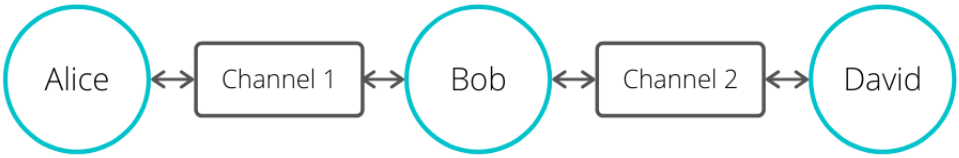

Figure 4 - Routing Payment Schema

The motivation that stands behind the routing is given by the great advantage toward chain fees. As it is described, opening a channel means performing an on-chain action, resulting in paying a chain fee. Routing allows node to perform payments by crossing payment channels already opened by other nodes, without the need to open a direct channel with the recipient. The challenge, is to implement this avoiding that intermediate nodes could steal money that the sender wants to send to recipient. Let assume that Alice wants to give 10 Satoshi to David, but does not have direct access to him. The shown schema allows Alice to perform a payment to David letting the money cross Bob's node. The payment will be delivered only if Bob can prove that he can truly forward the payment toward David. The proof that has to be given from Bod to Alice is called pre-image, and it represent a secret that only the recipient knows, in this case David. Once Alice has received the

proof from Bob, she can deliver the payment to Bob, who will deliver it to David.

This schema is possible due to the use of Smart Contracts, which protect the channel partners. It is possible to extend smart contracts which control the channel so that intermediate nodes have no possibility to perform malicious actions toward funds that are being forwarded through their channels. The smart contract is called *Hashed Time-lock Contract* (HTLC). The contract script is composed by two parts. The first, is the pre-image Hash. This is the proof that intermediate nodes have to forward in order to prove that they are belonging to the right path toward the recipient. The second, contains a time-lock, that implements a countdown (i.e. 24 hours). When the time runs out, if the intermediate node has not delivered the proof, the blocked funds will be released to the sender.

Another important concept that makes possible the cooperation between edges node and intermediate nodes is related to fee. In order to give an incentive to intermediate nodes, the sender, will pay a fee for each intermediate node that offers its balance to make possible the routing payment. Referring to the previous example, Alice will add to the payment amount a small quantity of money for Bob, compensating in this way, his collaboration.

HTLC will be signed for each channel crossed along the routing path. Each signed contract will require the same hashed secret in order to be satisfied. In particular, the actions order of the previous use case is the following:

- David will create the pre-image and he will deliver its hash over the internet to Alice.
- An HTLC will be employed between Alice and Bob.
- An HTLC will be employed between Bob and David.

At this point, David, has to show to Bob the pre-image hash in order to receive the funds from Bob. Bob will show the pre-image hash to Alice in order to receive the funds from Alice. At the end of these operation, funds from Alice to David will be correctly forwarded from sender to recipient.

If pre-image has would not be correctly forwarded, each HTLC would fail. This will result in an entire refund to Alice after the expiration of time-lock countdown.

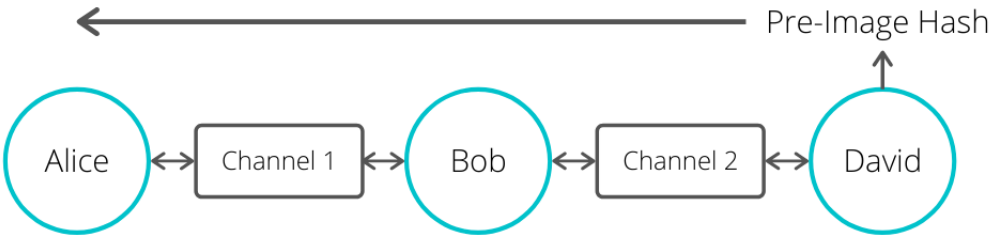

Figure 5 - Pre-Image Generation and Delivery

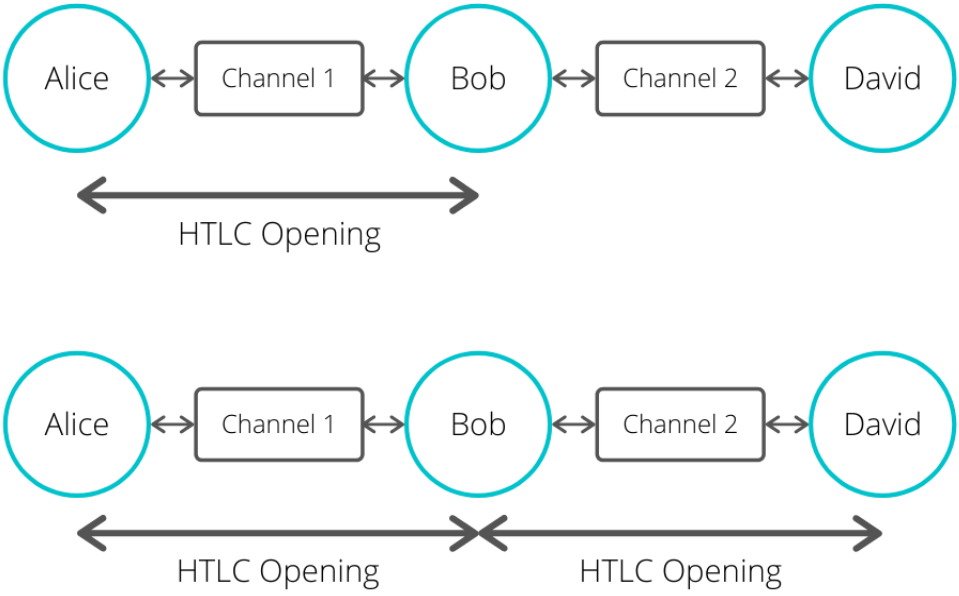

Figure 6 - HTLC Opening phase

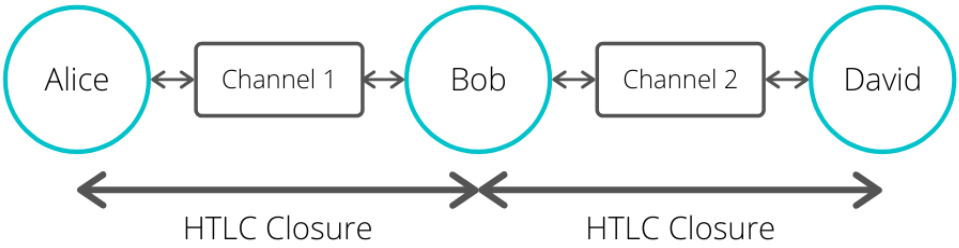

Figure 7 - HTLC Closure

3. Analysis of Digital Payment Application

The main focus of this chapter is on the production process and analysis of a Digital Payment Application. In particular, the chapter follows a procedural approach, by showing the entire process that is engaged to develop the Application. The work will focus its analysis on different aspects:

- Architectural Requirements
- Stakeholders involved and Roles
- Strong Customer Authentication
- Functional Requirements
- Security Requirements
- UX Flows

Each of these aspects will be treated independently of the target environment (iOS, Android, Windows Phone, HarmonyOS).

3.1 Introduction – Multi Bank App

As it is mentioned in previous chapters, digital payment applications try to help users to accomplish operations on money exchange in the simplest and useful way. From now on the application the thesis wants to describe will be mentioned as Braavos App, or only Braavos, for expression simplicity. A particular emphasis will be given to PSD2 effects in the development of Braavos, pointing out the aspects of SCA implementation. Summarizing what Braavos offers as service, it allows users to:

- Connect more than one bank account in a single Application
- Let users to switch between different IBANs linked to different bank accounts
- Make person-to-person, person-to-business, business-to-business payments
- Access all application functionalities by means of a phone number

Braavos is not only oriented to customers, but also to merchant. Indeed, two different version of the same application will be developed in order to allow customers to make payments toward merchants, and merchants to request payments from customers. As it is described, payments can be performed also between persons, and also between merchants, covering all the possible operations of money exchange between entities. Since all the characteristics the thesis wants to analyze are independent of the Braavos App versions, both versions will be treated as unique project, that embeds both builds.

3.2 Stakeholders and Roles

The first step before entering in more technical details, is to understand which Actors are involved in the development phase, and which stakeholders stand around the project. The scheme below shows which stakeholders are involved on Braavos project.

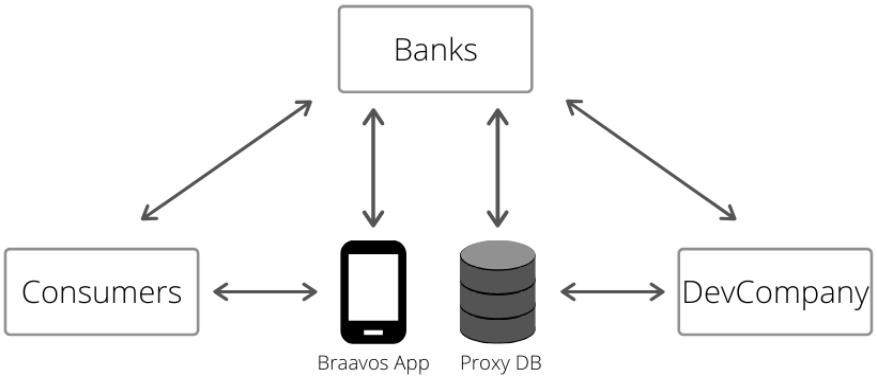

Figure 8 - Stakeholders scheme

Architectural details are not shown in this scheme; they will be treated further on the thesis work.

Let assume that there are not external entities interested as stakeholders. As it is shown, it is possible to reduce the number of effective Actors involved to 3.

Banks have a relationship both with their customers and DevCompany, that is in charge of developing Braavos. Contractual details between Banks and their Customers can be ignored in this analysis, it is enough to pointing out that in order to link a Bank Account with Braavos it is necessary to have at least one active signed contract with the enrolled Bank. At this point, it is needed to explain what is an enrolled bank, and which is the relation between

Banks and DevCompany. Braavos will include a set of Banks users can choose to perform the signup phase, and link their bank account in order to make payments. In this case, Braavos represents only a tool that users can use to manage their bank accounts collection, and decide time by time, which payment instrument they want to operate with in order to perform a money exchange.

DevCompany has the task of develop the mobile application, the back end proxy database, and interfacing Braavos with Banks APIs. As it was mentioned, PSD2 regulations, allow third-party institutions to access banks APIs in order to accomplish banks services without the need to develop or ask to banks specific interfaces. This represent a great advantage for DevCompany, that is in charge of developing only the white-label-app, leaving out of scope what regards the payment service complexity.

Consumers are the final users. They will use the application, by linking to Braavos one or more bank accounts they have signed with the enrolled banks. Consumers are also represented by merchant, that will sign up the same as buyers, by linking also the merchant activity. Later on, it will be described the set of operation allowed to users, merchant and buyers, describing the context in which Braavos operates.

3.3 Architectural Requirements

From the architectural point of view, it is important to describe which technical entities are involved and how they are related. It is possible to show how the entire system works by focusing on the relationship that are behind the scenes. The figure below, shows the architecture in question.

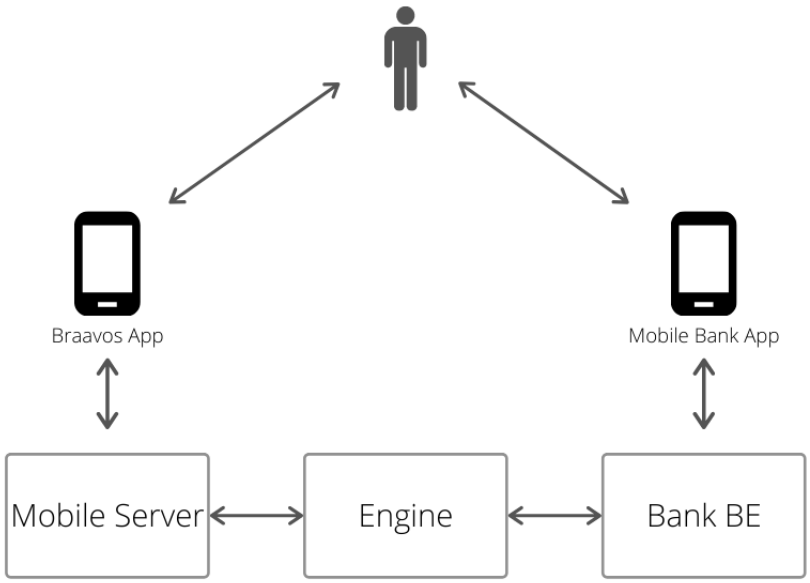

Figure 9 - Architecture scheme

A new entity needs to be introduced at this point. The mobile bank app will have a crucial importance during the bank SCA process, but it is dutiful to mention this actor, as it is part of the system's architecture. The SCA process will be described in details further, by showing the different scenarios in which it operates and which actors are involved into it.

The Mobile Server is in charge of processing requests coming from the Braavos App and deliver them to the Engine. It is also responsible of

maintaining data that is necessary for the correct operating of the mobile application. No further data will be stored into the Mobile Server database. This is possible because all the other operations, such as the payment one, are achieved by delivering a request to the Bank Back End Server through the Engine.

The Engine acts like a proxy Server. It takes all the requests coming from the Mobile Server and it delivers them towards the Bank BE, waiting for its response. The Bank BE response will come back to the Mobile Server, passing always by the Engine.

The Bank BE offers to Braavos App all the banking services. It allows to let the user to register a new bank account, to perform payments, to check the banking analytics etc. All of these operations are possible thanks to a series of APIs offered by the BE that can be called by the Mobile Server through the Engine.

3.4 Strong Customer Authentication

As already mentioned, SCA is the process that allow a user to authenticate himself by means of a two-factor authentication. It is required by the PSD2 regulation, so it is necessary to implement it as a primary step. The regulation provides three stages of "compliance":

- Payment Initiation, a service to arrange a payment from an entity to another entity, even if they belong to a different payment service.
- Account information, a service that provides data related to the bank account associated to the user.
- Funds checking, a service offered by a payment service provider that allows to check information related to active user's funds.

Any operation that involves these three actions needs to be conducted through the SCA. Indeed, once the user has installed the application, he can attach the first bank account by accomplish the authentication through SCA. The outcome of this operation, in the scope of Braavos, will be a correct attach of a bank account and its available IBAN, selected as default payment instrument. This paragraph will describe in details how SCA is performed in Braavos, which are the actors involved, technical and not.

There are different ways to perform SCA. The thesis describes the approaches that are used in Braavos to accomplish the user authentication: Redirect SCA and Decoupled SCA. Each of this ways are analyzed in order to describe how the SCA process it's technically integrated in Braavos during the Bank Account Connection phase. As it is mentioned, this is not the only operation in which SCA is involved. Other use cases in which SCA is performed, such as money transfer, will be described further in the thesis document.

3.4.1 Redirect SCA on Web App

Pre-Condition

- The customer must have downloaded the Braavos app and started it
- The customer must be successful enrolled with the mobile number

Post-Condition

- The customer has attached with success a new bank account with its relative IBAN as a default payment instrument

Sequence Description

1. User selects bank from the list of enrolled banks
2. API request delivery from the mobile App to the Mobile Server with the mobile phone and the bank ID
3. Mobile Server sends the request to the Engine
4. Engine checks if the mobile number is present in the proxy DB, if success, it invokes the relative bank API in order to start the SCA process
5. The bank SCA is triggered with the Redirect method
6. Braavos App creates a Deep Link in order to redirect the user to the bank Web App
7. User is redirected to the Browser Online Banking; in which it will perform the authentication with the selected bank
8. On success authentication, the bank Web App performs a redirect through Deep Link toward Braavos App
9. SCA outcome is positive, user has successfully linked a new bank account on Braavos

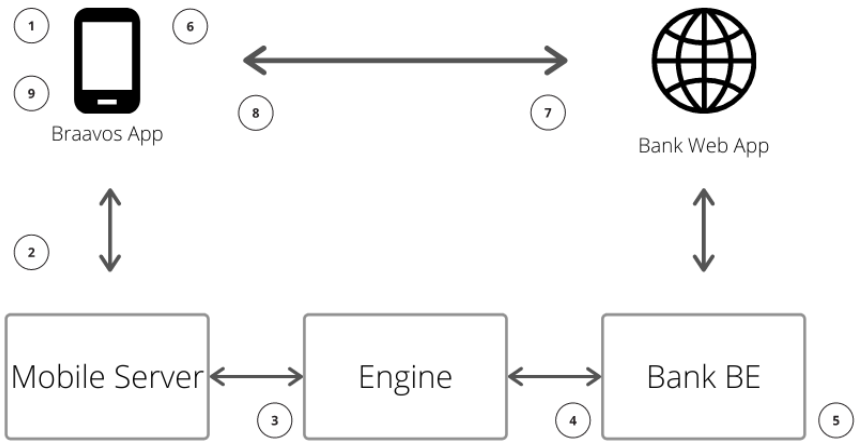

Figure 10 - Bank SCA, Redirect on Web App Sequence

3.4.2 Redirect SCA on Bank Mobile App

Pre-Condition

- The customer must have downloaded the Braavos app and started it
- The customer must be successful enrolled with the mobile number

Post-Condition

- The customer has attached with success a new bank account with its relative IBAN as a default payment instrument

Sequence Description

1. User selects bank from the list of enrolled banks
2. API request delivery from the mobile App to the Mobile Server with the mobile phone and the bank ID
3. Mobile Server sends the request to the Engine
4. Engine checks if the mobile number is present in the proxy DB, if success, it invokes the relative bank API in order to start the SCA process

5. The bank SCA is triggered with the Redirect method
6. Braavos App creates a Deep Link in order to redirect the user to the bank Mobile App
7. User is redirected to the Mobile Bank App; in which it will perform the authentication with the selected bank
8. On success authentication, the bank Web App performs a redirect through Deep Link toward Braavos App
9. SCA outcome is positive, user has successfully linked a new bank account on Braavos

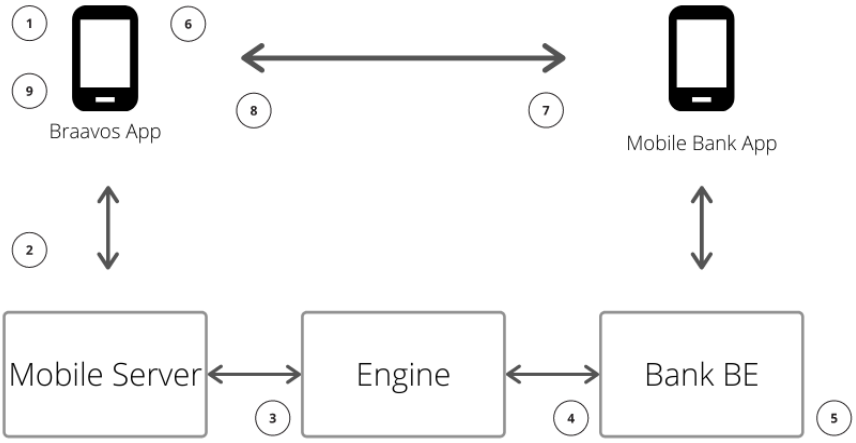

Figure 11 - Bank SCA, Redirect on Bank Mobile App Sequence

3.4.3 Decoupled SCA on the same device

Pre-Condition

- The customer must have downloaded the Braavos app and started it
- The customer must be successful enrolled with the mobile number

Post-Condition

- The customer has attached with success a new bank account with its relative IBAN as a default payment instrument

Sequence Description

1. User selects bank from the list of enrolled banks
2. API request delivery from the mobile App to the Mobile Server with the mobile phone and the bank ID
3. Mobile Server sends the request to the Engine
4. Engine checks if the mobile number is present in the proxy DB, if success, it invokes the relative bank API in order to start the SCA process
5. The bank SCA is triggered with the Decoupled method
6. The Mobile Bank App receives a push notification from the Bank BE in order to let the user accomplish the bank SCA directly on the Mobile Bank App
7. On success authentication, the Mobile Bank App performs a redirect through Deep Link toward Braavos App
8. SCA outcome is positive, user has successfully linked a new bank account on Braavos

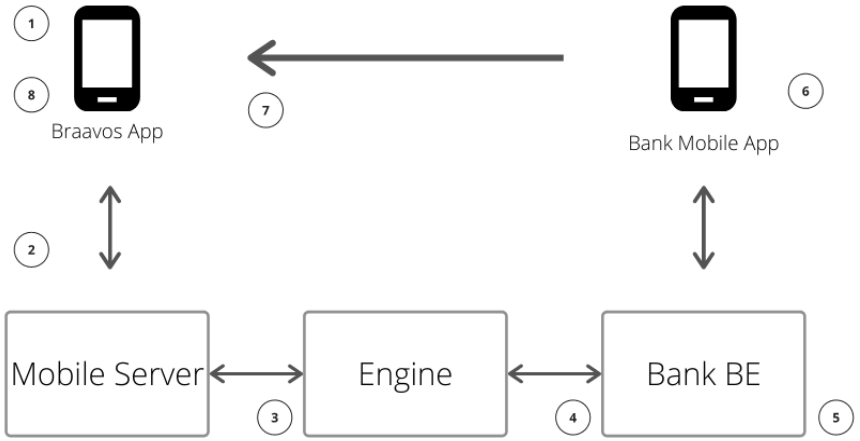

Figure 12 - Bank SCA, Decoupled on the same device Sequence

3.4.4 Decoupled SCA on different device

Pre-Condition

- The customer must have downloaded the Braavos app and started it
- The customer must be successful enrolled with the mobile number

Post-Condition

- The customer has attached with success a new bank account with its relative IBAN as a default payment instrument

Sequence Description

1. User selects bank from the list of enrolled banks
2. API request delivery from the mobile App to the Mobile Server with the mobile phone and the bank ID
3. Mobile Server sends the request to the Engine
4. Engine checks if the mobile number is present in the proxy DB, if success, it invokes the relative bank API in order to start the SCA process
5. The bank SCA is triggered with the Decoupled method

6. Braavos App starts a polling phase in order to catch the final status of the bank SCA
7. The Mobile Bank App (installed on a different device) receives a push notification from the Bank BE in order to let the user accomplish the bank SCA directly on the Mobile Bank App
8. On success authentication, Braavos App catches the success status of SCA
9. SCA outcome is positive, user has successfully linked a new bank account on Braavos.

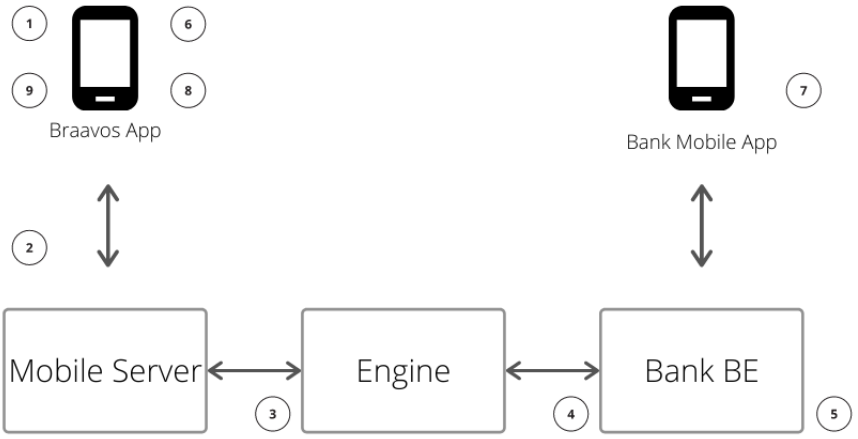

Figure 13 - Bank SCA, Decoupled on a different device Sequence

3.5 Security Requirements

This paragraph is in charge of describing all the security requirements adopted on the Braavos project. As it was stated in this thesis, security is one of the most important requirement for a digital payment application. Both server and app side measures need to be employed to guarantee the appropriate security level. Further in this paragraph will be described some of the most used approaches and tools in the field of security. Some of the proposed solutions are differently treated depending on the operating systems in which they operate.

3.5.1 Key Chain & Key Store

These tools are used in iOS and Android respectively in order to store and retrieve key, password and other sensitive credential. They are composed by a set of API that allows to process all the request to store or retrieve keys.

Key-Chain tools are encrypted using two different AES-256-GCM keys: one key for the metadata table and one for each row, which represent the secret value key. The metadata are encoded with the appropriate key to speed up searches, while the secret values are encoded with the secret value key. The metadata's key is protected through the Secure Enclave, that it's stored into the processor cache to allow quick key-chain searches.

Key-Store tools store keys in a container to make it more difficult to extract form the device. Once keys are in the Key-store, they can be used for cryptographic operations with the key material remaining not-exportable. Moreover, it offers facilities to restrict when and how keys can be used, such as requiring user authentication for key use or restricting keys to be used only in certain cryptographic modes.

Key-store system protects key material from unauthorized use. Firstly, it mitigates unauthorized use of key material outside of the device by preventing extraction of the key material form application processes and from the Android device as a whole. Secondly, it mitigates unauthorized use of key material on the device by making apps specify authorized uses of their keys and then enforcing these restrictions outside of the apps' processes.

Braavos integrates these approaches in order to store and retrieve all the cryptographic information and keys used to authorize operations on behalf of the user.

3.5.2 Fingerprint reader handler

This sub-paragraph describes the common used techniques regarding the setup and use of a fingerprint reader as alternative authorization method (with respect of device PIN).

As previously stated, in order to accomplish the bank SCA, it is needed to perform a two-factor authentication. Fingerprint reader is used by Braavos together with the device PIN as an authentication factor, by asking a pre-stored fingerprint (some the users is), or to insert a pre-stored device PIN (some the user knows).

Fingerprint setup

Braavos app allows the user to setup the fingerprint reader to be used, in order to authorize transactions, login operation and other minor operation, such as settings preferences. During the setup phase, Braavos app asks the user to enter the device PIN.

Fingerprint use

During the transaction confirmation phase or app access phase, if the user has setup the fingerprint reader as authorization method, Braavos App asks

the user to place his finger to the reader. In case of successful verification, Braavos app is able to unlock the key-chain/key-store safe memory area, in which are stored the keys needed for the correct user authentication.

3.5.3 Protection and Obfuscation

Digital payment applications usually adopt tools for advance protection and code obfuscation as DexGuard in order to improve the overall security measures.

DexGuard is specifically designed to protect and optimize Android applications. The multilayered protection provided is adapted to the distributed and quickly evolving environment in which mobile applications are used. Hackers try to gain access to the source code of the application by using decompilers and they monitor the behavior of the application at runtime. DexGuard hardens the source code of the application using a multitude of obfuscation and encryption techniques and also integrates a series of runtime security mechanisms into it. These mechanisms check the integrity of the application and of the environment in which it is running and enables the application to react whenever suspicious activity is detected. DexGuard obfuscates names of classes, fields, methods and also arithmetic and logical expressions in the code and the control flow of the code inside methods. In addition, it encrypts strings and classes and adds reflection to access-sensitive APIs.

3.5.4 Antiroot tools

Rooting is a computer process that allows users running Android OS to obtain privileged controls on various sub-systems. It is generally used to bypass the limitations that developers have set on the device. In this way the user is able to perform any operation otherwise inaccessible to a normal user. This could be a potential risk for any kind of application in the mobile realm. In order to avoid any kind of attack based on root operations, Braavos app adopts AntiRoot measure by means of tools and libraries.

3.5.5 Certificate Pinning

In order to increase the connection security, mobile apps rely on the certificate pinning. This technique consists in verifying that the server contacted by the client is the desired one in order to avoid any kind of attack towards the client.

The certificate pinning consists in checking the correspondence between the public key of the certificate and the key that the client knows. If the correspondence is verified, then the connection is considered as reliable, otherwise, it is considered as not reliable and therefore it is stopped.

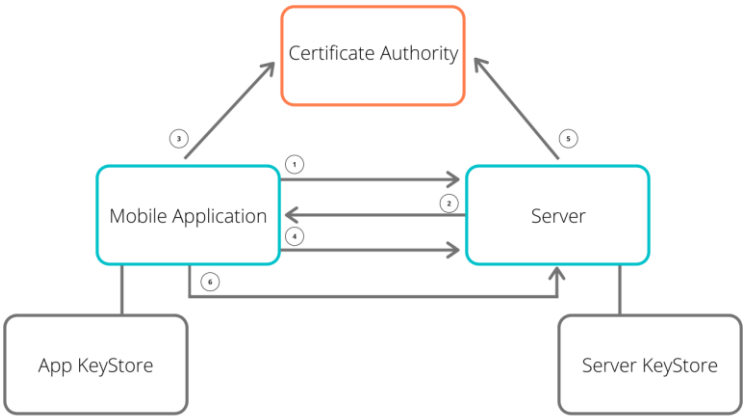

Figure 14 - Certificate Pinning scheme

The steps involved during the process of authenticating and establishing an encrypted channel using certificate pinning are the following:

1. The mobile application accesses to a protected resource.
2. The server presents its certificate to the application.
3. The application verifies the server's certificate by asking confirmation to the superior CA.
4. If successful, the application sends its certificate to the server.
5. The server verifies the application's certificate performing the same steps performed by the application on point 3.
6. If successful, the server authorizes the access to the protected resource requested by the application.

3.5.6 App Link & Universal Link

As in the case of Key-Chain and Key-Store tools, these approaches are differently adopted dependently of the operating system in which they need to be implemented.

Android App Links allows the application to designate itself as the default handler of a given type of link. In term of security, App Links use HTPP URLs that link to a developer's website domain, meaning only the developer can make use of those links. They also require developers to verify their ownership of a domain.

As in the case of App Links, Universal Links is the Apple's method of launching apps on iOS when linked from a website. When users tap or click a Universal Link, the system redirects the link directly to the app without routing through Safari.

Both App Links and Universal Links allow Braavos app to prevent any kind of attack disclosed by using Deep-Link approach (i.e. Deep-Link Phishing).

3.6 Main Features

The aim of this paragraph is to describe how the main features of Braavos are designed and implemented. One of the main features as it was mentioned at the beginning of this chapter, is the Multi Bank one. This feature allows users to activate and operate with multiple Bank Accounts within the same App. The first step to accomplish is the App initialization by means of the user's mobile phone number. This configuration allows the user to be enrolled and to access to the Braavos' features.

3.6.1 First App Initialization

App installation and initialization has been thought to be fast and smooth, but also secure. In order to be correctly enrolled in the App, the user has to perform these steps:

1. Launch the Braavos App
2. Select the country code prefix and enter the mobile number
3. Receive the OTP via SMS and enter the code for authentication
4. Enter passcode/biometrics ID

At the end of these steps, the user will be correctly activated. At this stage, the App is initialized with no connected Bank Account. The user will be asked at this stage to perform the Bank Account connection by means of Bank SCA. The sequence diagram below shows how this operation is performed and which actors are involved.

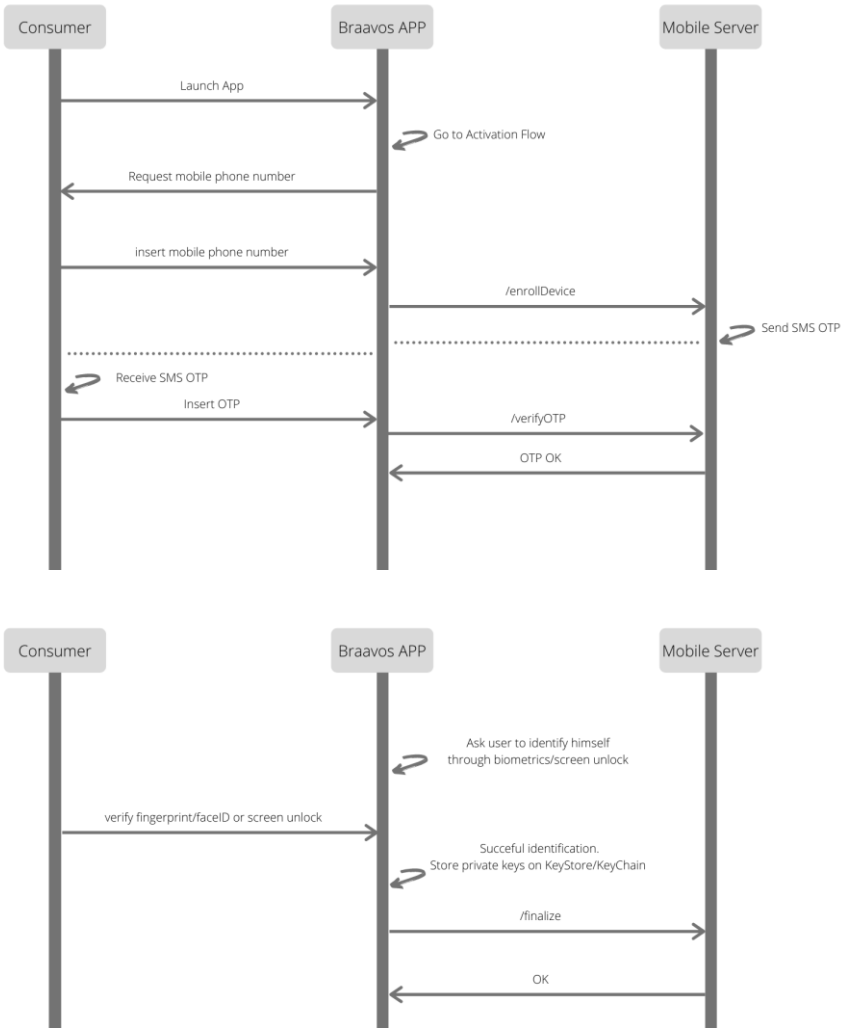

Figure 15 - Initial Configuration Sequence Diagrams

If the user reaches the end of the initial configuration process, by correct inserting biometry or phone passcode, a list of enrolled banks will be shown. At this point, the user has to select the bank which it wants to link to Braavos, and the SCA process will take place.

3.6.2 Activation failure cases

- After receiving the OTP via SMS
    - If the user enters an incorrect verification code, an error is shown
- After receiving the OTP via SMS
    - If the user enters an expired verification code, an error message is shown
- After reaching the maximum number of verification codes attempts
    - Error message is shown
- After reaching the maximum pin/smartphone lock attempts
    - Error message is shown and the user has to start the activation process again

3.6.3 After Bank SCA Features

Once the Bank SCA is accomplished and at least one Bank Account is connected to the Braavos App, the user is enabled to execute the following operations:

- Synchronize the phonebook with the Braavos enrolled users
    - This feature helps the user to have an updated list of contacts which are enrolled to the Braavos App.
- Switch between accounts from different Banks within Braavos App
    - This is essentially the main feature. Once the user has connected more than one Bank Accounts, it is able to switch the accounts at any moment within the App. This allows the

user to schedule which payment instrument to use operation by operation.

- Select default bank account
    - This operation allows the user to design the payment instrument that is in charge of receive or send money by default. This process is described in the following sequence diagram. The orange part has to be considered as an optional operation. Indeed, it is related to the attachment of a default receiver instrument. This step is performed only in case the user has more than one bank instrument attached to the account.

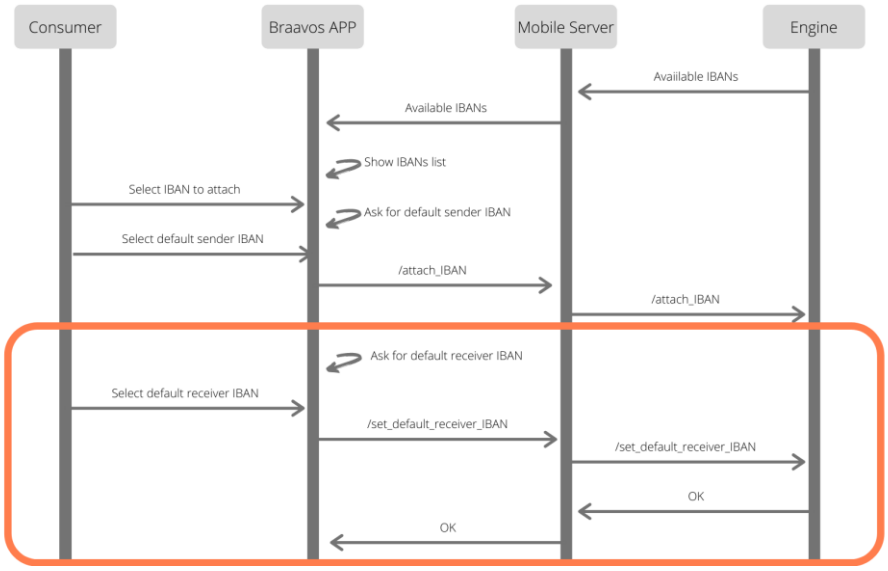

Figure 16 - Set Default Instruments Sequence Diagram

- Access the transaction history list
    - This feature allows user to keep track of performed transactions, with access to their status.
- Visualize the available balance
    - This feature is possible thanks to the possibility to interface the Braavos App directly with the bank's APIs, allowing the

retrieving of bank account's information, such as the current balance.

- Execute P2P transfer 24/7
    - In particular, the user can access to P2P payment with enrolled users, he can also request a P2P payment from another user.
- Receive payments 24/7
- Split Bill
    - This feature allows the user to split a bill among multiple users. Once a payment is done, it can be split among different users. The user who wants to split a bill, can select the transaction and then select from the contact list the users with whom he wants to split the bill.
- Block and unblock contacts for R2P
    - It is possible to block some contact to send request for payments to the user. It is also possible to disable the receiving of R2P at all.

4. Comparison between Traditional Application payments and the Lightning Network

In this Section, a description of a comparison between traditional mobile payments and LN payments is provided.

A simulation on the Lighting Network exchanges was carried out using the CLoTH simulator in order to collect payment-related performance measures. Data regarding the traditional paradigm of digital payments were collected by an audit company.

4.1 CLoTH Simulator

In this paragraph, a description of the CLoTH simulator is provided [6]. CLoTH is a Lightning Network simulator that takes as input a payment-channel network and payment script to be played during simulation. The simulator is used in order to compute payment-related performance measures on LN, such as probability of payment success and average payment time. This information is employed on a comparison with the performances of a traditional digital payment system. The computation flow of the simulator is constituted by three phases: Pre-Processing phase, Simulation phase and Post-Processing phase.

4.1.1 Pre-Processing Phase

The pre-processing phase consists in generating the payment network and the payments which are executed in the network during the simulation phase. This information is given as input to the simulator in order to start the simulation process, and are represented in the simulator by using data structures. There are two possible input modes:

- By providing some input parameters (e.g. number of nodes, average channels number per node, average channel capacity etc.). In this case, the simulator, randomly generates the network and payments.
- By directly providing a complete specification of each attribute belonging to the network and payments.

First mode input parameters symbols are explained in the table 1.

The simulation of this study was implemented using both input modes as follows:

- First mode for the payments, by providing to the simulator the number of payments, average payments rate, average payments amount.
- Second mode for the network, by giving to the simulator a precise specification of the Lightning Network.

Symbol	Definition
Nn	Number of nodes
Nch	Number of channels
Cch	Average value of channel capacity
Pr	Payment rate
Pa	Average payment amount
Pn	Number of payments

Table 1- CLoTH simulator input parameters

4.1.2 Simulation Phase

During the simulation phase, the simulator runs a discrete-event simulation by simulating the execution of the input payments in the input network; the simulation time, that is the time represented in the simulation, advances through discrete steps from one event to the next. Each event represents a state of a payment; it is generated each time a payment changes its state.

The simulator implements some functions that process each event:

- *Find_route*: simulates the search for a payment route from the payment sender.
- *Send_payment*: simulates the sending of a payment by the payment sender.
- *Forward_payment*: simulates the forwarding of a payment by an intermediate hop in the payment route.
- *Receive_payment*: simulates the reception of a payment by the payment receiver.
- *Forward_success*: simulates the forwarding of a payment success by an intermediate hop of the payment route.
- *Forward_fail*: simulates the forwarding of a payment fail by an intermediate hop in the payment route.
- *Receive_success*: simulates the reception of a payment success by the payment sender.
- *Receive_fail*: simulates the reception of a payment fail by the payment sender.

4.1.3 Post-Processing Phase

Once the simulation is over, all the collected data on payments are transformed in order to achieve statistically meaningful measures through the *batch-means* technique. This method allows to compute performance results of the output analysis of a steady-state simulation. Each performance measure has statistical mean, variance and 95% confidence interval.

Performance measures that have been computed during the simulation are listed in the table 2.

Symbol	Definition
Ps	Probability of successful payment
Pnp	Probability of failure due to missing route
Pnb	Probability of failure due to no balance
Po	Probability of failure due to offline node
Pt	Probability of failure due to timeout
T	Average time of payment
Na	Average number of taken attempts for a successful payment
Lr	Average route length traversed by a successful payment

Table 2 - CLoTH Simulator output parameters

4.2 Simulation on the Lighting Network

As already mentioned, a simulation was run in order to compute performance data regarding LN payments. The simulation was executed on a snapshot of the Lightning Network captured on 17th December 2020 which had the following features:

- *Number of nodes*: 6006;
- *Number of channels*: 30457;
- *Channel capacity*: 0.03 BTC;
- *Standard deviation*: 0.09 BTC;

The payment input attributes that were given to the simulator, with the relative values are the following:

- Pr: 100 payments per second;
- Pa: 0.0001 BTC, equivalent to 3€ at the time of simulation [8];
- Pn: 50000;

At the time of simulation was not possible to simulate payments with more of the stated Pa, because larger payments would tend to fail due to the limited capacity of Lightning Network payment channels.

The simulation output results are collected in the table 3.

	Mean	Variance	ConfidenceMin	ConfidenceMax
Ps	82,73%	0.001	82,69%	82,77%
Pnp	4,46%	$1.881e^{-4}$	4,45%	4,48%
Pnb	12,79%	$5.239e^{-4}$	12,77%	12,82%
Pt	0.0	0.0	0.0	0.0
T	857.98 ms	2171.015	857.439 ms	858.533 ms
Na	1.8859	0.0491	1.8833	1.8885
Lr	3.2711 $hops$	$5.655e^{-4}$	3.2709 $hops$	3.2714 $hops$

Table 3 - LN simulation results

Some considerations about the computed results are listed here.

- The probability of obtaining a successful payment, taking in consideration the pull of payment belonging to the case study, is near to 82,7%;
- The probability of obtaining a failure due to a missing path from sender to recipient is near to 4,5%. For some payments (usually the larger ones), channels don't have enough channel capacity to forward the payment and for this reason these payments fail for no path;
- The probability of obtaining a failure due to no balance is near to 12,8%. This failure is caused by the channels unbalancing. A channel is unbalanced when one balance is much higher than the other. In this case, payments going from the lower balance to the higher one tend to fail due to no balance availability.
- There are not cases in which the failure is due to an expired timeout;
- The average time of a successful payment is 857,98 ms.

- The average number of taken attempts for a successful payment is 1,88;
- The average route length traversed by a successful payment is 3,27 *hops*;

The simulation in Lighting Network shows that 12,8% of transactions fail due to no balance and 4,4% of transactions fail due to no path. These represent the biggest problems that LN developers are trying to solve. Rebalancing approaches can be used in order to mitigate failures due to no balance. CLoTH simulator supports a mode called *multipath payment* that allows to lower the probability of failure due to no path. If activated, when a transaction is stopped due to no path, the transaction's amount is halved and a new path will be found for each half.

4.3 Traditional Digital Payment Application Performances

Dataset regarding transactions' performances was provided by an auditing company, by performing an official audit on a digital payment application. Three performance measures were extracted from the dataset in order to make the comparison with the Lightning Network:

- Probability of success, expressed in percentage;
- Probability of failure, expressed in percentage;
- Payment time, expressed in seconds;

The application is architecturally designed as the Braavos APP, so it is assumed that the performances are the same of our case study.

The audit test was conducted during the month of September 2020 in order to check the average process time of end-to-end transactions. The audit considered both person-to-person and person-to-business transactions, making possible a distinction between the different solutions. The obtained results are shown in tables 4 and 5.

	Value
Probability of success	99,97%
Probability of failure	0,03%
Payment time	$1 \pm 0{,}5\ s$

Table 4 - P2P payments performance

	Value
Probability of success	99,91%
Probability of failure	0,09%
Payment time	$1 \pm 0{,}5\ s$

Table 5 - P2B payments performance

Also in this case, it is possible to make some considerations on the computed results. Regarding the person-to-person transactions:

- The 99,97% of person-to-person transactions were successful;
- The 0,03% of person-to-person transactions failed due to transaction's timeout;
- The payment time ranges between 0,5 and 1,5 seconds;

Regarding the person-to-business transactions:

- The 99,91% of person-to-person transactions were successful;
- The 0,09% of person-to-person transactions failed due to transaction's timeout;
- The payment time ranges between 0,5 and 1,5 seconds;

4.4 Comparison of the results

In this Section an explanation of the comparison is provided. The main objective of this experiment is to understand how much these different solutions could be compared from a performances point of view.

The obtained results show the different nature of the two solutions and underline that these realities can be used at the moment to accomplish different purposes. The major differences are highlighted in the table 6. With regards of Braavos transactions, only person-to-person ones are considered in this context, since Lightning Network payments are person-to-person too.

	Braavos App (p2p)	**Lightning Network**
Probability of success	99,97%	82,73%
Probability of failure	0,03%	17,27%
Payment time	$1 \pm 0{,}5$ s	0,85 s

Table 6 - Braavos App p2p / LN results comparison

The comparison highlighted the major differences between the two solutions:

- *Payment Success Rate*: Braavos person-to-person payments had a success rate of 99.97% against the 82.73% belonging to Lightning Network payments.
- *Payment Failure Rate*: Braavos person-to-person payments had a failure rate of 0.3% against the 17.27% belonging to Lightning Network payments.
- *Payment time*: Braavos person-to-person payments had a duration between 0,5 and 1,5 seconds; Lightning Network payments have lasted on average 0,85 seconds.

Although the average payment time resulted slightly lower in the Lightning Network than in the mobile payment app, the obtained results show that at the moment the best performing solution in terms of probability of success is the mobile payment app. The Lighting Network is currently in an immature state of development (the software is still a beta) and, as stated in Section 4.2, the community is working on solutions to improve payment success rate (such as the multi-path-payment feature and rebalancing approaches).

5. Conclusions and future work

The events of 2020 have led to a significant increase in digital payments. The global pandemic crisis has changed the overall environment for businesses. Digital payments trends and statistics show that the use of this expedient will likely continue to grow at the expense of cash payments [10]. The purpose of the current work was to design and show the development phase of a mobile application for digital payments, covering the analysis of:

- Stakeholders and Roles
- Architectural Requirements
- Security Requirements
- Main Application Features
- Authentication process

The development analysis was done in collaboration with a Turin IT company operating in the world of digital payment solutions. My contribution to the project has concerned the drafting of the Security Analysis document, and the implementation of Android modules. The project is currently under development and each requirement module is under implementation. The final transition to production, meaning the release of the mobile application to the market, is scheduled for summer 2021 with an estimation of six months of development. The mobile application introduces some innovative features currently not available in other digital payment mobile applications, such as *Multi-IBAN/Multi-accounts*. The application allows user to link multiple bank accounts with multiple payment instruments on the same environment. Customers have access to digital banking operations, such as person-to-person and person-to-business

payments, having the possibility to switch from a bank account to another instantaneously.

The secondary goal of the proposed study was to examine the Lightning Network solution comparing its performance measures to those belonging to the traditional digital payment application analyzed in this work. Lightning Network is a peer-to-peer network of payment channels built on top of the Bitcoin blockchain. It introduces itself as one of the most promising and developed solutions that aim to solve the blockchain scalability problem. Performance measures were computed running a simulation on CLoTH, a Lightning Network simulator. The simulation was executed on the Lightning Network on 17th December 2020. Performance measures regarding a traditional mobile digital payment application were computed from an IT audit during the month of September 2020.

The comparison has highlighted the major difference in terms of performance between the two solutions. The results show that the mobile payment app has a higher success rate, 99.97% of success rate with respect of 82.73% belonging to LN payments. The Lightning Network, in fact, is still in an immature phase of development, and the community is constantly working on improving this technology.

Leaving apart performance, there are two main reasons that may encourage the use of Lightning Network in place of traditional payment applications: low fees and privacy. Transactions are subject to very low fees, thus allowing to perform micro-transactions (of the order of a cent fraction). The architecture design of LN and its implementation allows edge nodes to preserve their identity towards the intermediate nodes along the routing path.

Moreover, solutions based on BTC, like the LN, allow users to accomplish payments without requiring for the *Know your customer*[1] process [9].

Finally, with regards to the traditional payment systems, the future of these technologies is in constant evolution. PSD2 regulations are bringing critical changes to the payment industry, such as:

- Stronger Security Requirements for online transactions through multi-factor authentication.
- Implementation of a structure able to allow banks and other financial institutions to offer access to customer bank accounts to third-party payment service providers.

New businesses are investing more and more on a user-centric model and the instauration of a collective customer network is evolving the current business core paradigm on digital finance services. Traditional banks must have a response to these challenges. New players, indeed, are pushing their business models on the existing ones.

[1] Known your customer is a recognition process, performed by companies in order to verify their customers' identities. By carrying out this technique, it is possible to evaluate potential risks that may arise during professional relationships.

Bibliography

[1] IQUII, "Digital Payments: a growing trend with a focus on Customer Experience" Medium, 28/11/2018. [Online]. Available: https://medium.com/iquii/digital-payments-a-growing-trend-with-a-focus-on-customer-experience-d31fa69664bc.

[Accessed 04/10/2020].

[2] European Commission, "Payment services (PSD 2) - Directive (EU) 2015/2366," 2015. [Online]. Available: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

[Accessed 15/09/2020].

[3] "Coin Market Cap," [Online]. Available: https://coinmarketcap.com/. [Accessed 12/11/2020].

[4] Prachi Juneja, "Digital Payments: what they are, how they work, and their benefits and problems." [Online]. Available: https://www.managementstudyguide.com/digital-payments-pros-and-cons.htm.

[Accessed 04/10/2020].

[5] Divya Premanantha, "Strong Customer Authentication and Dynamic Linking for PSD2." 19/06/2019. [Online]. Available: https://wso2.com/library/articles/2019/06/strong-customer-authentication-and-dynamic-linking-for-psd2/.

[Accessed 07/10/2020].

[6] M. Conoscenti, Capabilities and Limitation of Payment Channel Networks for Blockhain Scalability, Turin: Politecnicno di Torino, 2019.

[7] 1ML, "Real-Time Lightning Network Statistics" . [Online]. Available: https://1ml.com/statistics.

[Accessed 10/12/2020].

[8] DannetStudio, "a Web Analysis | Crypto". [Online]. Available: https://awebanalysis.com/it/convert-satoshi-to-euro-eur/.

[Accessed 14/01/2021].

[9] Wikipedia, "Know your Customer," 20/06/2019. [Online]. Available: https://it.wikipedia.org/wiki/Know_your_customer.

[Accessed 14/01/2021].

[10] McKinsey & Company, "The 2020 McKinsey Global Payments Report," 2020.

[11] Lucian Constantin, "What is PSD2? And how it will impact the payments processing industry." 13 09 2019. [Online]. Available: https://www.csoonline.com/article/3390538/what-is-psd2-and-how-it-will-impact-the-payments-processing-industry.html#:~:text=What%20are%20the%20strong%20consumer,%2Dfactor%20authentication%20(2FA).

[Accessed 06/10/2020].

[12] Andreas M. Antonopoulos, Olaoluwa Osuntokun, Rene Pickhardt, "Mastering the Lightning Network" 28/08/2020. [Online]. Available: https://github.com/lnbook/lnbook.

[Accessed 10/10/2020].