



**School of Engineering and Natural Sciences**  
**Graduation Project**  
**2022-2023**

<b>PROJECT TITLE</b>
<b>Pay With Crypto</b>
<b>FACULTY ADVISOR</b>
Prof. Reda Alhajj
<b>TEAM MEMBERS</b>
Emre Kaan Satış - 64190004 Mehmet Berat Öztürk - 64190003




## School of Engineering and Natural Sciences Graduation Project



<b>Project Code</b>
<b>Project Title:</b> Pay With Crypto
<b>Faculty Advisor:</b> Prof. Reda Alhajj
<b>Project Team Members:</b> Emre Kaan Satış Mehmet Berat Öztürk
<b>Sponsor Company (if any):</b>

BUDGET (TL)	PROPOSED	CONSENTED
IMU FUNDING	234000 TL	234000 TL
SPONSOR COMPANY FUNDING	-	-
TOTAL	234000 TL	234000 TL

PROJECT PLAN	PROPOSED	CONSENTED
PROJECT PLAN Duration in Weeks	09.01.2022	28 Weeks
STARTING DATE	09.01.2022	09.01.2022

## School of Engineering and Natural Sciences Graduation Project

Project Code	
ADVISOR	DEPARTMENT CHAIR
<b>Name:</b> Prof. Reda Alhajj	<b>Name:</b> Asst. Prof. Mehmet Kemal Özdemir
<b>Contact Information:</b> Tel : 05511418806 E-mail : ralhajj@medipol.edu.tr	<b>Contact Information:</b> E-mail : mkozdemir@medipol.edu.tr
<b>Signature:</b> 	<b>Signature:</b>

TEAM MEMBER	TEAM MEMBER
<b>Name:</b> Mehmet Berat Öztürk	<b>Name:</b> Emre Kaan Satış
<b>Contact Information:</b> Tel : 05394422776 E-mail : mehmet.ozturk2@st.medipol.edu.tr	<b>Contact Information:</b> Tel : 05063909957 E-mail : emre.satis@std.medipol.edu.tr
<b>Signature:</b> 	<b>Signature:</b> 

## School of Engineering and Natural Sciences Graduation Project

**Project Title:** Pay With Crypto

**Faculty Advisor:** Prof. Reda Alhajj

**Team Members:** Mehmet Berat Öztürk – Emre Kaan Satış

**Project Group Title:**

### **PROJECT OVERVIEW/SUMMARY/ABSTRACT**

In today's world, blockchain technologies are all around us. We are using them in our daily lives more and more every day. Right now, cryptocurrencies are one of the most used assets in trading. But their aim was to be a tool in the payment sector as it suggests in Bitcoin whitepaper. Pay with Crypto will offer a worldwide on-chain payment solution. This document provides high level information about Pay with Crypto POS and Pay with Crypto App. Pay with Crypto is the name of an infrastructure solution for the payment system which is designed to replace existing centralized payment methods for better security, low operational costs, faster transaction speeds, easier supervision for governments and reducing harm to the ecosystem. The project aims to have fast transactions, secure connection, and ease of usage.

The whole system can be used on all EVM based blockchains for transactions and has a new encryption solution for privacy concerns occurring with the usage of blockchain technology for payment systems. For the project, Avalanche Network can be used because of its high-speed transactions and low gas (transaction fee). During the tests, Fuji Test Network was used, as proposed.

In the first semester, the user interface was developed and waiting for actual blockchain integration for sending transactions via the app. Desired security algorithm was selected and ready to be implemented into the system. QR scanning is done. During the second semester, NFC implementation was successfully done, POS device app design was finished. Homomorphic encryption and zero-knowledge proofs were decided to be used for more security and privacy. Paillier encryption was selected because of its functionalities in homomorphic encryption. The whole system was tested with new additions and overall success criteria were achieved at the end.

**Keywords:** blockchain, payment, crypto, cryptography, NFC, QR, transaction

## School of Engineering and Natural Sciences Graduation Project

### 1. OBJECTIVE OF THE PROJECT

Blockchain represents a network, mainly consisting of ledgers, which works without any central authority, therefore being decentralized. One of the most important use cases of blockchain networks is payment. But there are some adjustments needed for the payment sector being the main aspect of them. The biggest problem is the extreme transparency that blockchain technology brings. The system acts as an intermediate layer for fixing privacy issues using the highest standard encryption method. With the usage of this revolutionary layer, only merchant owners and governments will be able to see the transactions and transaction history of a merchant.

Existing payment systems use centralized authority for approving or reviewing transactions. In today's world, almost all businesses use POS systems to take their payments. The system which customers use when paying via credit or debit cards is called a point of sale (POS). These systems are making up the most commonly used infrastructure in the world today. They became purely digital, taking payments from all around the world and help shop owners to track all the transactions easily. But this system has some major drawbacks, such as costly software upgrades, less convenience than web-based systems, problems caused by the hardware, not being secure enough, and don't have transparency. Unlike typical software updates that we use every day to applications in our mobile phones or computers, POS system's updates are not free. Also, centralized payment systems such as Visa and Mastercard cut fees between %1-2.5. This makes the payment processing services unnecessarily expensive and inconvenient.[1] Beside all these problems, today's payment system is extremely harmful to the world. Numerous servers, high number of credit card production and receipt usage resulting in depleting the earth's resources day by day. Given that the world's resources are limited, it is urgent to transition into a healthier system for everyone. Using blockchain technology in payment systems can help solve most of these problems.

Besides the technology behind the blockchains, there are other factors affecting the possibility of replacing traditional payment methods with cryptocurrency payments and adapting it to human lives. So, when designing the POS and mobile app, the user experience was one of the top priorities. As it is hard to change society's payment habits, the system is designed to offer very similar experience to using a contactless credit card.

Existing payment systems mostly rely on credit card usage. For instance, in Canada, %82.58 of the nation's population uses credit or debit cards for paying their daily needs. It is easy to comment about waste generated from unused credit cards plastics, but actual environmental damage made by credit cards are not caused by its plastic, but from their chips. A credit card chip is called EMV and is a semiconductor. This little semiconductor allows people to store their card info securely in their pockets. A semiconductor is basically a circuit consisting of multiple transistors. During the production of these a lot of water needs to be consumed. Since semiconductors are produced layer by layer, each layer added to the silicon water consumes enormous amounts of water to be rinsed. The main problem here is that the

## School of Engineering and Natural Sciences Graduation Project

water used in this process is called Ultra-Pure Water (UPW). 1400 – 1600 gallons of water are needed to produce 1000 gallons of UPW. [2]

Another serious issue with the traditional payment system is the number of servers used worldwide. The traditional system is centralized therefore, the credit card companies must store their customers' information in their servers. Today, major credit card companies have over 2000 servers around the world. These machines demand a high amount of electricity, and the workforce is to be able to work stable.

Pay with Crypto aims to have a solution to all these problems by offering a decentralized blockchain-based payment system, which also gives virtual receipts.

## 2. LITERATURE REVIEW

### 2.1. AES128 Reference Manual

This paper provides detailed information about the advanced encryption algorithm (AES). In the first chapter of the research, the authors give some brief information about the Rijndal algorithm and the need for a new encryption method. The Rijndal algorithm's implementation and the main components have been explained in detail. Substitution, ShiftRow, MixColumn, and KeyAddition are the four main parts of the algorithm's encryption section. All these operations are performed one after the other in each encryption round. Each step of the encryption process has an inverse operation for the decryption process. Since blockchain is a public database, Every transaction, address, and balance is transparent to everybody and cannot be changed. While developing a payment system with blockchain, nobody wants to know how much money they have or their transaction history. This privacy issue is the biggest problem for the payment infrastructure that uses on-chain payment. In summary, to make the application much safer, we need to add one more security layer to the application. [3]

The main contribution of such an encryption algorithm to the application is adding one more security layer to the infrastructure and solving the privacy concern that comes from the nature of blockchain technology. Before sending any transaction to the blockchain from the user's application, data will be encrypted, and cipher text will be given as a function parameter. Since cipher text is generated with randomly generated keys, different parameters will be sent to transaction data. [3]

## School of Engineering and Natural Sciences Graduation Project

### **2.2. Three QR Code**

Credit cards are used a lot in today's world. But they are very harmful for environment. Chips of credit cards need to be cleaned with fresh water. After this cleaning, all the used freshwater has been returned to the ground because it contains heavy metals that harm human life. To avoid environmental damage and to create a more secure payment system, we need another technology to replace credit cards. [4]

In our project, encrypted data will be transferred with a QR code from the POS device to the user application. Reading the QR code is as fast as contactless payment, so the user experience will also be protected. There are a bunch of packages for generating QR codes with values. As a result, QR codes provide us with a high-speed process and a much more environmentally friendly solution for credit cards. [4]

There are two technologies that we can use instead of credit cards. One of them is QR Code, and the other is NFC technology. QR integration would be so much easier than NFC. Since NFC technology has fewer implementations and the size of the data being transported is smaller, it is easier and more convenient to use QR in our project. While making the payment, the POS device will generate a QR code, and the payer will be able to make the payment by scanning this QR code.[4]

Developed by Denso Wave, a subsidiary of Toyota in Japan, QR Code is a 2D barcode system. QR code was developed in 1994 and can store 7,000 digits of characters at maximum, which is much more data than other barcode types like UPC code, Code 39, Code 49, etc. [4]

There are a couple of main characteristics of QR codes compared with other barcode types. Traditional barcodes are very hard to scan if the code is not straight. But in the QR code, the ratio between black and white patterns is always 1:1:3:1:1 from all sides. With that pattern, the scanner can easily scan the QR code from all sides.[4]

QR code scanners have multiple error correction percentages with a maximum of 30 percent. This error correction percentage is much higher than other types. Because the Reed-Solomon code, which is resistant to burst errors, is used in QR codes.[4]

QR codes can be divided by 16 at most, but scanners can scan them without looking at the order of the code. With this division, QR code also provides an advantage in the area range.[4]

### **2.3. Impact of Blockchain Technology on the Payment Management Systems – What Future Holds?**

Blockchain has become a matter of debate because of its potential to cause trouble in the business model (BMs), and its usefulness, advantages, disadvantages, and potential risks in payment depending on the utilization of the blockchain to both formal and non-formal credentials are taken into consideration in line with the purpose of this research.[5]

Blockchain is one of the potentially troublesome breakthroughs that has many effects

## School of Engineering and Natural Sciences Graduation Project

on numerous businesses. The first utilization emerged in the financial services sector with bitcoin placing the installment industry in the center of advances around blockchain technology, and it brought together a large group of experts and obtain a deeper understanding of the recommendations on BMs in the installments business for the first time. Present services have become out-of-date because of the initiation of new services that are used to promote peer-to-peer transactions. The results revealed that the financial structures of the current BM will become different in the future. These advances will be indicated in the evolution of new BMs while causing some of the present BMs to become obsolete. Moreover, these advances will give fintech the opportunity by making use of blockchain innovations to enter the market. In short, this research provides information about modifications in different sections that progress and what companies need to consider updating their BM thanks to blockchain innovation along with the improvements in BM literature as a consequence of examining the influences of new technologies. In addition, the results of the research provided new research opportunities that encourage an investigation of the field of blockchain.[5]

A Delphi study was carried out with experts who are well-informed about blockchain technology in parallel with the needs of multi-stage and group-oriented research. Since the Delphi technique is a typical tool for predicting and decision-making, as well as for measuring; it was seen as convenient for this research as an exploratory theory construction method by including new trends. A 3-round Delphi technique was preferred, and in the first cycle, experts were asked about their experiences and feelings. Next, the outcomes of the first cycle were evaluated by the experts and in the last cycle, they were requested to reconsider the results by taking provided input into account.[5]

This paper contributed to the project as we understand the necessities of blockchain technology in payment systems and what is waiting the World in future.

### **2.4. Online Payment Using Blockchain**

This research paper provides the main terminology of blockchain technology and how to implement a blockchain-integrated online payment system. Blockchain technology is based on three different components. These are "nodes," "blocks," and "chains." A chain is made up of blocks that are connected one after the other, and a block stores a packet of transaction data that is written into the blockchain. And after writing any kind of data to the blockchain, it becomes immutable, and no one can change it because blocks are connected by cryptographic hash functions. So whenever new data enters the block after packing it, the hash of the block changes, and the chain breaks.[6]



## School of Engineering and Natural Sciences Graduation Project

These blocks are stored in nodes; a node can be a computer or any other technological device that meets the minimum requirements of the chain. Each node stores all blockchain information. This is the crucial difference between centralized systems and blockchain. Because in today's world, every system has one large database that holds every kind of data, if this database gets corrupted or attacked by hackers, data will be lost forever. As I mentioned at the beginning, blockchain nodes store all information about the current state of the chain. So if something happens to one of the nodes, the chain can easily recover itself and continue to work.[6]

### **2.5. The Impact of FinTech and Blockchain Technologies on Banking and Financial Services**

This report delivers information about FinTech and the usage of blockchain technology in this area. We learned how to use our project in the field of FinTech as a result of this research. With the fast development of technology, it has become much easier for people to access the Internet. The field of finance has had to adapt, just like every other field, to the fast improvement of technology. Due to this, the term "FinTech" is introduced. FinTech is a new type of financial application that applies new technologies to the finance industry. Blockchain technology is transparent, secure, and immutable. With these characteristic features of blockchain, it can be easily implemented into traditional payment systems and banking, which is an important working area of fintech.[7]

In traditional payment systems, the sender and receiver always have to trust the service provider and any third parties that validate the transactions for them. But with blockchain, there will be no need for this middleman; cryptographic functions will validate the transaction and store it encrypted on the blockchain. This implementation will be faster and more budget-friendly than today's payment systems.[7]

Because blockchain is a decentralized system, no one can alter or influence the status of a transaction once it has been mined. This tells us that there will be no authority to control the system. Public, immutable code is going to have absolute authority.[7]

Blockchain has also been influenced by traditional finance. There is a very big and important field named Defi, which was introduced. Defi is a new area of the blockchain ecosystem where users can lend, borrow money, and exchange currencies, with their digital assets.[7]

## School of Engineering and Natural Sciences

### Graduation Project

#### **2.6. Blockchain in FinTech: A Mapping Study**

This paper gives general information about the vision of blockchain technology in Fintech companies, along with statistics. Research is based on 50 different scientific studies' results.[8] The authors first talked about what the blockchain is and smart contract. Smart contracts are the programmable part of the blockchain and can be developed in various programming languages. The authors also mentioned the importance of smart contracts for fintech, because companies can programs blockchain behavior with smart contracts for their needs. [8] In the fourth part of the paper, authors provide information about the blockchain's limitations and security problems. These concerns were given much attention in this research and discussed in very deep detail. As I mentioned earlier in this paper review, this research provides information and statistics about several scientific research about fintech and blockchain. And the "51%" attack, has been the most repeated topic among these studies. "51% Attack" is the most dangerous attacking vector in the blockchain.[8] Blockchain is a distributed system that decides the validity of the transaction with consensus. This consensus is formed by the votes of the nodes, and the result written into the blockchain changes the state of the chain. But if someone or some group takes control of 51% of the nodes, they can easily manipulate the chain and make fraudulent transactions. The authors also talked about wallet security and the difference between traditional banking systems.[8] In today's banking system, if someone's credit card or bank account got stolen, the authority froze the account and protects the victim's assets. Since there is no authority in the blockchain, if any private key is stolen, the user will lose all the digital assets owned by this account. Scalability is also a big problem for blockchain, as explained in the study. [8]

With this research, we learned about the boundaries of our project and the concerns of the fintech field to the blockchain.

#### **2.7. A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities**

This paper provides the advantages and risks of blockchain technology. At the beginning of the paper, the authors talked about general information about Ethereum and Bitcoin, their architectures, and the differences between these two types of blockchains. The main difference between Ethereum and Bitcoin is the type of account. The main component of Bitcoin's architecture is unspent transaction output (UTXO). In UTXO, the outputs of an existing transaction are used as the new inputs of the new transaction. As a result, it is extremely difficult to trace some address funds back to their Bitcoin transactions. But in Ethereum, every component has different kinds of accounts, one of which is the Ethereum external owned account (EOA). This is the wallet of the users; they can deposit or withdraw funds from this account. The other is the contract account (CA). Users can interact with a smart contract on the chain to execute unique logic on the blockchain. There is no concept of a smart contract in Bitcoin; users can only send funds to another wallet.[9] The authors also discussed common characteristic features between Bitcoin and Ethereum in the second part of the paper. In the third part, different types of consensus procedures are mentioned; this issue

## School of Engineering and Natural Sciences Graduation Project

is handled differently in these two chains. In Bitcoin, a consensus protocol named Proof-Of-Work is used to make decisions all over the chain. In POW, every transaction has a different problem to solve. Every node in the chain tries to solve this problem first to win the transaction fee. But this is a very old concept, in POW very powerful computers must be used as a node. These computers consume lots of electricity and are very harmful to the ecosystem. But in Ethereum, Proof-Of-Stake (POS) is used as a consensus protocol. POS is more eco-friendly and has minimum requirements of nodes that are not high as proof of work blockchain. Simply proof of stake is, users all stake their money to the nodes. It is a system where those who stake money have the consensus vote. At the end of the paper, the authors provide information about different areas of blockchain applications and the limitations of blockchain. With the help of this paper, we gained knowledge about various blockchain implementations and their architectures.[9]

### **2.8. Systematic Literature Review On Blockchain Adoption In Banking**

The paper discusses the future of blockchain in banking via pointing out the impact of distributed ledger technology. The main purpose is to gather various academic papers about blockchain in the banking sector and make a systematic literature review which includes a comprehensive and systematic search. By this way, the paper aims to become a starting point for the researchers in blockchain technology. The research consists of 22 different papers which give an insight into their general context, research area, output, challenges they try to overcome and the research gap.[10]

The authors believe that blockchain technology is going to be very successful in the future and is going to be widely used. Therefore, the banking sector will be under a critical transformation process. This transformation is also going to bring exciting advantages such as lower time, reduced operational cost and effort in bank to bank transactions. All the data may be under review of the miners within the consensus rules.[10]

In conclusion, this paper helps us find other sources about the blockchain infrastructure inside the banking sector which eventually leads to payment systems.

### **2.9. Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework**

The authors aim to give information about what decentralization is, how it is maintained in different systems and its implementation in blockchain technologies. They define decentralization as “distribution of power without central authority”. In blockchains transactions and codes in the network called smart contracts are kept as permanent and immutable records which can be seen by everyone inside the network. Therefore, there is no need for centralized authority to make sure of the truthfulness of these elements. In a such decentralized environment, everyone has a copy of all the data involved inside the chain which also makes everything more secure. [11]

## School of Engineering and Natural Sciences Graduation Project

In the end of the paper, authors deciding that there is no binary distinction between “decentralization” and “centralization”, at least in today’s world. It is not that easy to call a sociotechnical system with a binary decision. But little decisions given throughout the setup of the environment makes the system closer to one of them. [11]

This paper made us understand the effects of being centralized or decentralized in a financial system.

### **2.10. Online Payment Systems for E-Banking and Blockchain Technology**

With the improvements in electronic marketing, various electronic payment systems have also become quite popular so that they have begun to offer the required framework to simplify and speed the payment processes. Hence, many companies serve their customers via e-banking systems for different purposes, and blockchain and cryptocurrency are some of the fields that support electronic commerce.[12] Different perspectives about three important points are mentioned in this article. First, as one of the most important parts of an Ecommerce system, online payments consist of different means of payment such as mobile wallets, credit cards, and so on. Their usage for payments is increasing day by day since customers think that it is not as time-consuming as the traditional ways and bring along ease with it. However, the utilization of online payment systems is still not at the expected level since people living there are not accustomed to these new methods. Moreover, many people still believe that paying by cash after they take the delivery is safer than paying online even if they had no prior bad experiences.[12] On the other hand, despite the distrust of online payment systems, many customers also looking for other opportunities to pay for their transactions instead of using traditional payment methods. Furthermore, it has been thought by the majority that traditional payment is old-fashioned so some other virtual currency will be used in the following days rather than real money. Cryptocurrency, which is also called as virtual currency provides many opportunities by providing new payment options for people in the business world. However, the use of cryptocurrency in daily life is not as common as in the business world as a result of distrust, complexity, and unfamiliarity with this system. Additionally, blockchain is the reason for the creation of a new type of internet by spreading information but not being allowed to copy it. Thanks to the blockchain it is possible to do any kind of business without including third parties.[12] Moreover, in comparison with traditional ways, blockchain is more trustworthy with a higher speed of transfer and lower costs. Since it has more advantages than traditional methods, big companies like Mastercard and Visa started to use blockchain technology. In conclusion, with the improvements in technology, various new payment systems such as cryptocurrency and blockchain have come into our lives and provided convenience. They also offered many opportunities including not losing time while waiting in the bank queues, having a chance to do their payment whenever they want, high-quality customer service, getting rid of unnecessary paperwork, easy access to information and so on. Hence, it is an inevitable fact that these new technology and payment methods will change the transaction world.[12]

## School of Engineering and Natural Sciences

### Graduation Project

#### 3. ORIGINALITY AND ADDED VALUE

Few companies in the world make this kind of blockchain payment system. You can find additional information about these companies in the table below.

	Supported Networks	Receipt System	Decentralization	Payment Method
<b>Cyclebit</b>	All Networks	Paper Slip	Centralized	Only QR
<b>Pallapay</b>	All Networks	Paper Slip	Centralized	Only QR
<b>Monopayments</b>	-	Paper Slip	Centralized	Only QR

As seen in the table below all the solutions are centralized, and all the transactions are off chain. This means transactions are stored in a system centralized database for a while. This is a very big security concern from the user's perspective. Because if the hacker gets permission to modify the data, can change all the information about users' transactions before these transactions are written to the blockchain.

All the companies are using traditional receipt systems which has a very big negative impact on the ecosystem.

Lastly, mobile applications for companies using only QR technology while sending transaction.

Contrary to these features in Pay with Crypto, all transactions are on-chain and transparent for all the users, which are more secure than other payment solutions infrastructure. While using the word transparent, this is not mean you can follow other people's transactions. All the public data is encrypted, and cipher text is written into the blockchain. For the receipt part, in our project, all kinds of receipts are stored in a cloud server. Only we can allow institutions for investigating this transaction for several reasons. With that solution, we eliminate the damage of receipts to nature. Payment methods are a very important part of the user experience. Because the project appeals to everyone, so we do not want to replace society's old habits. For that reason, NFC is the new technology for contactless payment which currently using on credit cards.

Above companies offer blockchain payment systems to users. Although most of the companies supports all the networks, there are not any on-chain transactions in their system. All transactions are off chain. This means, the transactions are written to the blockchain after a while. This solution is fully centralized system product so in user perspective this is not different than a bank system.

## School of Engineering and Natural Sciences Graduation Project

### 4. SCOPE OF THE PROJECT AND EXPERIMENTS/METHODS

The smart contract was deployed on Avalanche mainnet. Transactions are created in the mainnet and being tracked and saved by both POS machine and the backend server. Just as the traditional payment methods, the price of the product will generate the data via POS machine. This data has 3 main values which are id, amount (price of the product) and a randomly generated alphanumeric string. This data will be encrypted using AES-128 algorithm and then will get encoded with Base64. Encryption generates a unique key for the data, which will be kept in the memory for later usage. Then, the POS machine sends this data via NFC to the app and a listener will start on the smart contract on blockchain. Mobile app will read the data using NFC from the POS machine to make a transaction with given amount and the data as the parameters. The listener on the POS machine will capture the transaction from the blockchain, a visual receipt will be generated in IPFS and displayed on both mobile app and the POS machine's screen. POS machine will send the key of the encrypted data, the transaction's hash and other required data to the backend server.

#### 4.1. Integration of Irish Recognition

Various physical features of the human body can be used for biometric authentication. The pattern of the iris can be obtainable from the human eyes, which is identical similar to fingerprints. The most common method is to work on either Iris localization or Iris pattern recognition. But in this approach, we are using the Wildes system which is a match quality-based system with the help of Fisher's linear discriminant for pattern identification.[13]

As can be seen in Figure 1, the iris recognition algorithm should firstly separate the outer limits of the iris and the pupil inside the given photos. Then, a pattern consisting of bits is created from the set of pixels which was forming the iris, preserving the data needed to make a statistically significant comparison between two iris images. This process results in a set of numbers that represents the information about the image of the iris. Using Daugman's algorithms, the remaining bits are transformed to represent the iris image which only includes Gabor-domain parts of the eye.[14] After the decision threshold is decided, Hamming distance is compared with it. If the distance is below this threshold, the recognition process is said to be successful. [14] The main problem with iris recognition is hardware limitations. When compared to built-in face recognition systems on today's phones. This system doesn't seem to be reasonable to use.

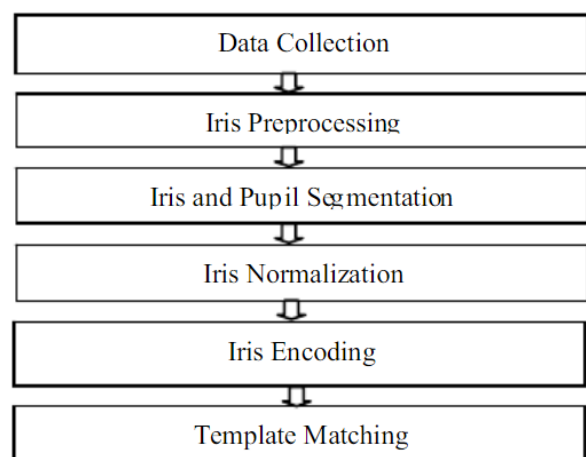


Figure 1: Iris Process[14]

## School of Engineering and Natural Sciences Graduation Project

### 4.2. AES Encryption Algorithm

AES is a symmetric block cipher standard. Algorithm inputs are plain text for encrypt and a secret password. The secret password and plain text must be 128 bits. The encryption part of the algorithm is based on four different components; Substitution, Shift Row, Mix Column, and Key Addition. At the beginning of the encryption operation, the secret key and plain text divide into 128-bit blocks and are added together. In the Substitution part, sixteen identical S-Boxes work in parallel, and these two matrix values are replaced with new values in the S-Boxes. After this adding operation, the algorithm will shift rows depending on the number of lines of the matrix. The next step of this encryption process is Mix Column, in this part, these 2 matrices are multiplied by each other. The last step is Key Addition, Key addition is the XOR of two 128 bits words. This flow is repeated 10 times. In the last iteration, the Mix Column operation was not performed.[15]

These are the advantages of AES over other encryption algorithms:

- Easier to implement than other encryption algorithms.
- Extendable to other keys and block sizes.
- Most efficient and secure way to encrypt data in today's world.

The main contribution of such an encryption algorithm to the application is adding one more security layer to the infrastructure and solving the privacy concern that comes from the nature of blockchain technology. Before sending any transaction to the blockchain from the user's application, data will be encrypted, and cipher text will be given as a function parameter. Since cipher text is generated with randomly generated keys, different parameters will be sent with transaction data.[15]

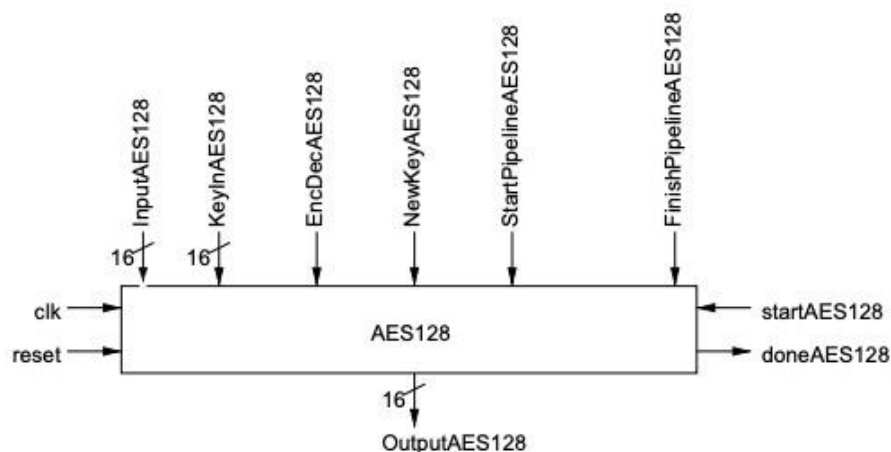


Figure 2: AES128 Top Level[15]

## School of Engineering and Natural Sciences

### Graduation Project

#### **4.3. Avalanche Network**

Avalanche is an open source blockchain platform for deploying applications with scalable and fast ecosystem. People can deploy their smart contracts with Solidity to C-chain easily since it is using Ethereum Virtual Machine (EVM). The main reason for us to use Avalanche over more popular ones such as Ethereum or Polkadot, is that the consensus mechanism of the network. It basically gives an advantage over others because of the transaction speed and scalability, which means that when the network reaches high numbers of users, it is still reliable and fast. [16]

Avalanche Network consists of 3 different chains, all of them have their own purposes, working parallel to each other. X, P and C chain. X chain consists of digital assets and mostly trading happens there. X and P chain are not supporting deployment of Smart Contracts. P chain coordinates the validators and subnets are created here. C chain has the EVM structure. In here Decentralized Apps, NFTs, Tokens and Smart Contracts are deployed. Therefore, we are going to use the Avalanche Network C-chain for the project.

When the blockchain structure is considered, someone or a group which controls the %51 of all the nodes can change the transactions, even the past ones. Someday you can wake up with no money. This is called %51 attack and almost all the networks are vulnerable to it. But when the scale comes to mind it is an extremely hard but not impossible thing to happen. Avalanche Network has a unique consensus mechanism which is also resistant to %51 attacks. In Avalanche, a node randomly selects a sub-group of nodes (e.g., 7 random nodes in the whole network), then considers these node's decision on a subject and change its own decision according to these groups'. This algorithm works very fast until %80 of the whole network decides on the same thing. On other networks such as Ethereum, nodes check all the other nodes not sub-groups, and this makes the transactions slower. Avalanche has a 2 second transactional finality compared to Ethereum's 6 minutes. Since the most important feature of the project is its being fast, we have selected to deploy our Smart Contract to Avalanche Fuji Testnet.

#### **4.4. Zero-Knowledge Proofs**

Zero-knowledge proofs are cryptographic techniques that let one party prove to another party the truth of a statement without revealing any further information. Zero-knowledge proofs were first proposed by Goldwasser, Micali, and Rackoff in 1985. ZKPs are growing increasingly well-liked in the context of blockchain technology due to their enhanced ability for anonymity and security. As an example, in a blockchain transaction, the sending party can use a the ZKP algorithm to show the recipient that they have the funds required to finish the transaction without exposing their actual balance or any other sensitive data. Zero-knowledge proofs come in a variety of kinds, including both interactive and non-interactive proof. Through back-and-forth communication, the prover and verifier engage in an interactive zero-knowledge proof to demonstrate the truth of a statement without disclosing any additional information. In a non-interactive zero-knowledge proof, the prover provides evidence that the verifier can separately check. For submitting the transaction through our platform, the user has to generate a non-interactive zero-knowledge proof. Many mathematical methods, including elliptic curves



## School of Engineering and Natural Sciences Graduation Project

and homomorphic encryption, among others, can implement ZKPs. They have numerous uses outside of blockchain technology, including safe multi-party computing, electronic signatures, and verification. The computational expense of generating and verifying proofs, as well as the need for reliable setup methods in certain circumstances, are some of the disadvantages of using ZKPs. Despite these disadvantages, ZKPs offer a potent tool for improving privacy and security in the field of blockchain technology as well as other cryptographic fields. We could see additional cutting-edge use cases for zero-knowledge proofs in the future as the field grows.

### 4.5. Homomorphic Encryption

Without the need for decryption, homomorphic encryption enables us to carry out mathematical operations on encrypted data. The term "homomorphic" signifies the transformation of data while preserving the relationships between its elements. This unique property enables mathematical operations to yield the same results in this transformed domain. As a result, we can perform desired operations on ciphertexts while maintaining privacy. In our project, achieving this objective was of utmost importance. We aimed to modify the user's balance by adding or subtracting the transaction amount, without exposing this information to anyone. To accomplish this, we opted for the Paillier Encryption scheme due to its extensive support for operations.[17]

The Paillier encryption is a partial homomorphic encryption method that allows two kinds of computations: addition and multiplying a ciphertext by a plaintext value.

The encryption process consists of two steps: key generation and encryption, as follows:

#### Key generation

1. Two random and independent large prime numbers  $p$  and  $q$ .
2. Confirm

$$\gcd(p * q, (p - 1) * (q - 1)) = 1$$

3. Define  $L(x) = x - 1n$
4. Compute  $\lambda = \text{lcm}(p - 1, q - 1)$
5. Random integer  $g$  in the set  $\mathbb{Z} * n^2$
6. Modular multiplicative inverse

$$\mu = \left( L(g^\lambda \text{ mod } n^2) \right)^{-1} \text{ mod } n$$

7. The public key which will be used in encryption is  $(n, g)$
8. The private key which will be used in decryption is  $\lambda$ .

## School of Engineering and Natural Sciences Graduation Project

### Encryption

Any  $m$  in the range  $0 \leq m < n$ .  $m$  is the message to be encrypted.

1. Random number  $r$  in the range  $0 < r < n$ .
2. Ciphertext

$$c = g^m * r^n \text{ mod } n^2$$

### Decryption

$c$  is the ciphertext created above, so that  $c$  is in the range  $0 < c < n^2$

- Plaintext

$$m = L(c^\lambda \text{ mod } n^2) * \mu \text{ mod } n$$

### Addition

Multiplication of two ciphertext results in addition of plaintexts:

$$c_1 * c_2 = m_1 + m_2$$

### Multiplication

A ciphertext raised to the power of a plaintext results in multiplication of these two:

$$c_1^{c_2} = m_1 * m_2$$

## 5. PROJECT TARGETS AND SUCCESS CRITERIA

The project consists of 5 highly important parts. These are integration of the blockchain technology, finding an efficient encryption method, finding a highly accurate security model, proposing a payment method, and creating the user interface.

The most vital part is the integration of blockchain technology. The main purpose of the project is to build a payment infrastructure based on blockchain since it provides an amazing opportunity for financial systems. Our aim is to change the people's habits of using

## School of Engineering and Natural Sciences

### Graduation Project

cryptocurrencies as a trade item to an everyday payment method.

Privacy is among the most crucial features of payment systems. Since blockchain is a transparent database, there is a need for an extra privacy layer. Being transparent in this kind of system is not a feature that people want. The objective of this layer is to encrypt the data written to the blockchain. This extra layer of encryption allows people to use such payment systems without compromising their personal information.

One of the biggest concerns that people have is the security of the apps they use. Therefore, finding a highly accurate security solution is a must. This method will aim to protect the people when their accounts are stolen, prohibiting the usage without the owner's presence.

Creating a user interface is one of the success criteria. The difference between these criteria and others is this one has a medium level importance on the study. It does, however, make usage easier for the people. Users can view their wallets and make their payments directly inside the mobile app. For the shop owners, POS machine app will be their key to take payments using cryptocurrencies.

Success Criteria	Effect on Project (%)
Integration of Blockchain Technology	%35
Finding an Efficient Encryption Method	%30
Finding a Highly Accurate Security Model	%15
Proposing a Payment Method	%10
Creating the User Interface	%10

## 6. RISKS AND B PLANS

Risk	B Plan
Higher requirements may be a killer for the NFC selection.	We are currently transferring encrypted data with NFC technology. There will be a problem if the user's phone does not support NFC technology. For this reason, we are planning to add it to the payment method with QR. Payment can be made easily from any phone with a camera without the need for more intermediate technology for NFC. In QR based payment system, POS will generate a QR code with transaction value and cipher text that POS is already generated.

## School of Engineering and Natural Sciences

### Graduation Project

	And these data will be transferred to the user's phone in JSON type.
<b>Iris Detection may not be implemented in real cases with high accuracy.</b>	The project is currently using iris detection for the security layer before payment. But this technology may not work properly with cameras in today's phones as it does not meet the minimum requirements. In our research, we found out that iris detection algorithms only give accurate results in datasets. In that case, we can replace Iris detection with face id. Face id is used much more than Iris detection, especially in IOS and Android phones. This is because the face recognition system is giving more accurate results than iris detection and supports current phone technology.
<b>Output of the AES-128 algorithm may not be a useful one.</b>	Because the encryption methodology of this project has not been done anywhere before. We are not sure 100% if this encryption technique works. So, if anything goes wrong in the encryption layer like the output of the encryption comes in a format or size we cannot use appropriately in our backend server, we are planning to change our encryption technique to Diffie-Hellman. The Diffie-Hellman method of securely exchanging private keys in the public channel. Due to this feature of the algorithm, we think that it can be integrated into the project very easily.
<b>Paillier Encryption limitations during calculations</b>	Even though Paillier Encryption is suitable for both the addition and multiplication, it has a value limitation in usage. If this limitation was not enough in the project, Twisted Elgamal Encryption will be used.

<b>Risks Occurred During Execution</b>	<b>Solution</b>
<b>The Web3 Library is not compatible with mobile applications.</b>	Web3.js is the most widely used blockchain library. Even though our application is directly compatible with JavaScript libraries and was created in React Native framework, some functions still need to be customized and overridden to make it suitable for mobile use.

## School of Engineering and Natural Sciences Graduation Project

<p><b>React Native Performance</b></p>	<p>React Native is a cross-platform framework, therefore it differs from native mobile applications in some ways. The most crucial downside is the performance. In our case, our JavaScript part is not fast enough in the context of generating zero-knowledge proofs. Because of that, we wrote our zero-knowledge proof generation-related code in Golang and compile it with the `gomobile` package.</p>
<p><b>POS Application NFC Implementation</b></p>	<p>In our POS application, we are using a library for handling NFC operations. Even though the library that we used in our project is the most famous one. It is outdated and not working at all. So, we need to change versions and other codes in the library's code to work properly.</p>

### 7. WORK TIME PLAN OF THE PROJECT

The tables at the end of the report templates provide the project's work schedule. The first semester is mainly about researching necessary technologies such as encryption algorithms and different networks to be used. At the end of the first semester, mobile app design is finished, and the app was created without any blockchain integration. In the middle of the second semester NFC integration to the system POS device app design was also finished. Encryption methodologies were added and started to implement. Lastly and most importantly testing and optimizing the process to make everything work better with each other.

Which work package is related to which part of the success criteria was noted in Table 4.

### 8. DEMO PLAN

The demo of the project will be held using a POS machine and mobile app. Teachers will make his payment using his phone via NFC or QR. Exact amount written to the POS machine will be taken from his account after the transaction. And this process will happen only in seconds using a public blockchain such as Avalanche Fuji Testnet. Teachers will be able to see their updated balance from their wallet and their transaction histories. Using Snowtrace block explorer of Fuji Testnet, all the transaction details will be seen. Also, in the demo two different accounts can send each other money. All this process is encrypted, therefore no other third party can access the data. All the functions proposed in Project 1 are included in the demonstration.

On the other hand, the system can also be tested in a local blockchain network using Hardhat and Truffle development environments. With the help of these tools, we can create our



## School of Engineering and Natural Sciences Graduation Project

private blockchain and some dummy wallets. Our system can be tested in this simulation to see the whole details of a transaction during the payment process.

### 9. FINANCIAL EVALUATION

On top of the report the Financial Evaluation Tables were presented. The proposed total budget is 234,000 TL. It was calculated considering a 28-week period of expenses. It mostly consists of the salary of the team.

For the final, only one POS machine was bought instead of one. All the tests were successful using these machines, therefore there was no need for the extra machines.

## School of Engineering and Natural Sciences Graduation Project

### 10. RESULTS

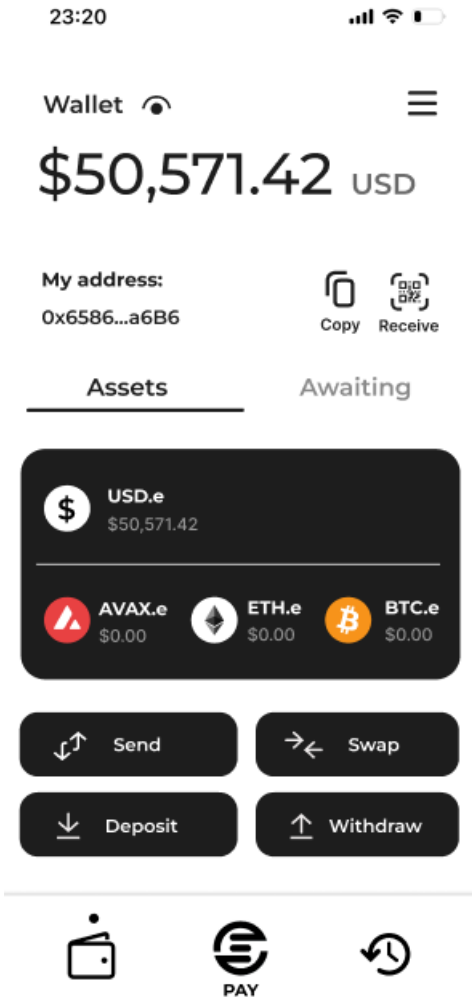


Figure 3: Dashboard

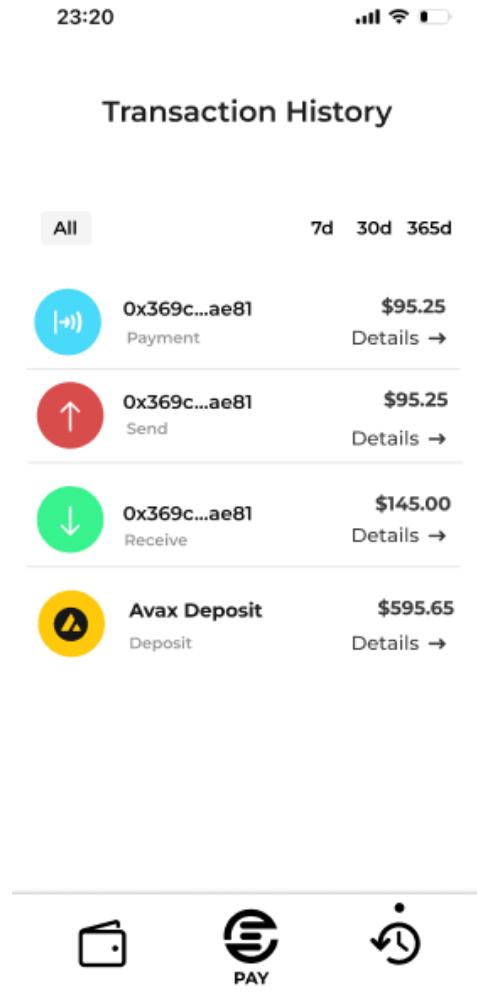


Figure 4: Transaction History

In Figure 3 and 4, Dashboard gives detailed information about the user's wallet. User can send-receive money, make deposit and payment, and withdraw coming transactions from this page. Using this page user can logout and reach his personal settings such as notifications.

Transaction History Page shows a history of the last payments. Users can see incoming and outgoing transactions. With a simple click, the user can access all the necessary information about a payment such as detailed date or virtual receipt.

## School of Engineering and Natural Sciences Graduation Project

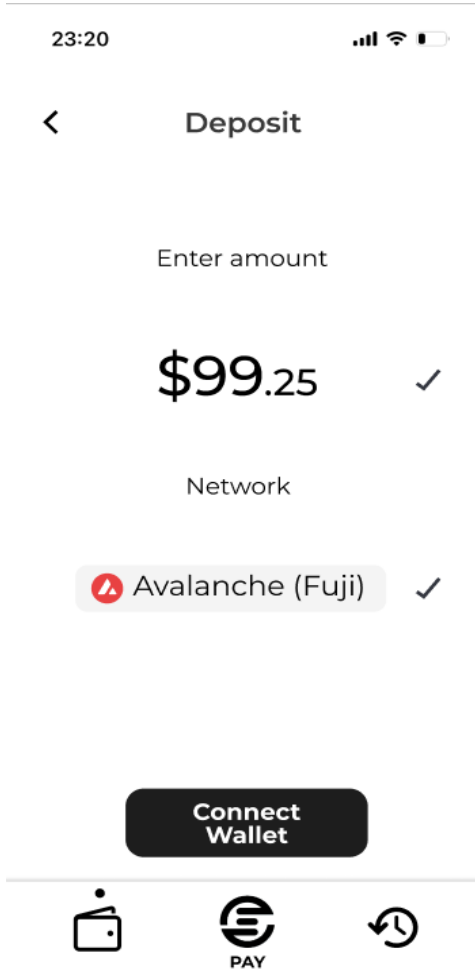


Figure 5: Deposit

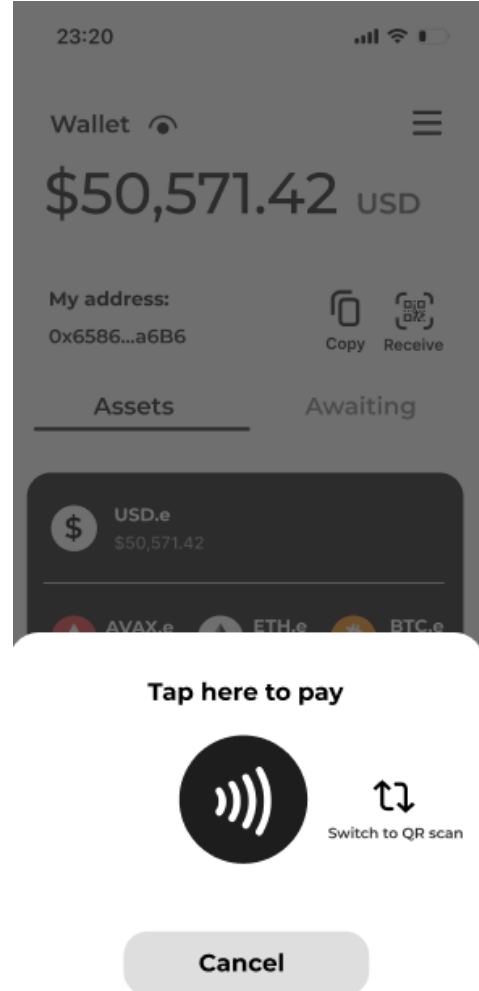


Figure 6: Payment Methods

User can deposit money to his account using the Deposit screen (Figure 5), accessible from the main menu. Money can be deposited into the system from any crypto wallet. Figure 6 shows the two different payment methods which the user can use. NFC scanning and QR code method are implemented inside the app.



## School of Engineering and Natural Sciences Graduation Project

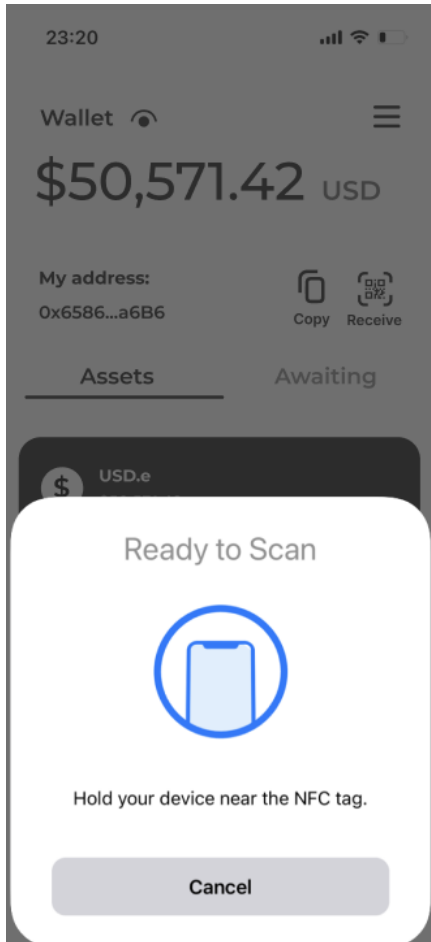


Figure 7: QR Code Scan

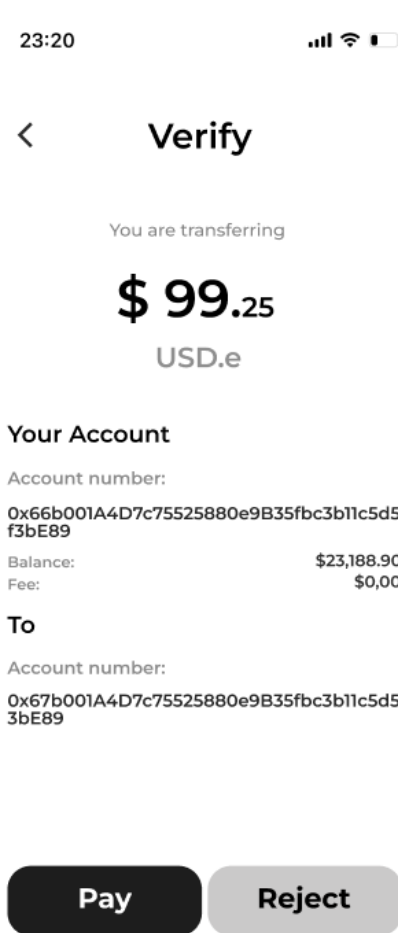


Figure 8: Payment Screen

As Figure 7 demonstrates the NFC scanning function, the user can select the NFC icon and then press the button. With a simple tap to the POS machine, the user will be able to start the payment process. Figure 8 shows the payment confirmation page. The user can see the exact amount of money demanded from him. By pushing the Pay button, he allows the app to initiate the payment process. After the confirmation phase is finished by the POS machine, the user can see the details of his payment, which also includes the virtual receipt uploaded to IFPS network. An example of a receipt can be seen in Figure 9.

## School of Engineering and Natural Sciences Graduation Project



Figure 9: Virtual Receipt

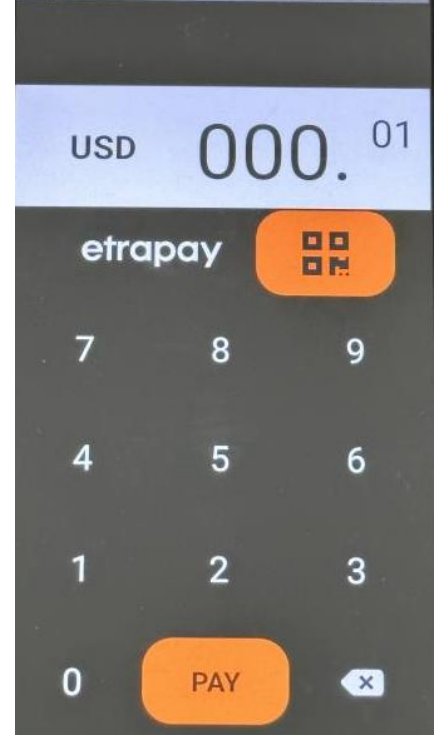


Figure 10: POS Device App

Figure 10 shows the POS device app design, the middle button enables and disables the NFC function during the payment. When the customer wants to pay with QR scanning, the right-most button enables the QR code generation.

Overall success criteria were achieved, all the transactions are encrypted, a secure application, NFC integration and an easy-to-use user interface were completed as proposed at the beginning.

## 11. DISCUSSION

As of the first semester, most of the success criteria proposed in Part 5 were completed as intended without any drawbacks. The encryption method to be used was found after deep research. When it comes to the security model, it was first proposed as iris recognition. But after some research and discussions, we have concluded that the risks are greater than the benefits. Therefore, we will stick with the built-in technologies such as FaceId and fingerprint scan. QR scanning was implemented inside the mobile app and NFC is the next one as proposed before. The overall app design was completed and can be seen in Part 10 screenshots. All the proposed features have their designs ready which, overall, makes us more than %50 percent ready for the future.

In the second semester, the POS device App was designed and coded. NFC and QR were implemented inside it to be used during payments. They are generating the correct data

## School of Engineering and Natural Sciences Graduation Project

that will be transferring the amount and the POS information to the user's app. Avalanche Subnet was created for the project and it works without a problem. Smart contracts were deployed to the subnet and various functions were called and the system was tested.

During the second semester, a new privacy method was proposed. Instead of encrypting the transactions with classical AES-128, we have decided to use newer, quantum-proof algorithms. Homomorphic encryption and zero-knowledge proofs were used in the development. In this way, sender-amount-receiver were hidden in a state-of-art manner. Paillier encryption algorithm was decided to be used in the project as the homomorphic algorithm. By using this encryption method, users' balances' will be updated without even a need of decrypting them. This whole new update to the project made it even more complex, more secure, and more private.

### 12. CONCLUSION

We have completed the designing mobile app and concluded our research about the current topics in the first semester. We have decided what we need to use and what we will use during the development. In the second semester, the POS device app and NFC function were finalized as proposed. The payment system is working in mockup local environments using Hardhat. In the last months, the blockchain integration to the mobile app and POS machine was finalized. In the very last step, testing is done and according to the results, the system is optimized. All the work is done according to the time plan proposed in Tables 1 and 2.

All the elements in the success criteria were completed as proposed before. The project implements a blockchain-based payment system utilizing an Avalanche Subnet, where all the transaction parties and the amount is private. The system also supports governmental policies by decrypting encrypted information.

### 13. ASSESSMENT OF ENGINEERING COURSES

One of the most important courses that we took throughout our education was "Data Structures". During the algorithm construction phase of the projects, we are always using the information that we got from it. Algorithm Analysis course carries the same importance level. Both of them helped us write the codes of Pay with Crypto App and improve the transaction speeds. Artificial intelligence-based courses such as Advanced Programming, Introduction to Machine Learning and Introduction to Deep Learning helped understanding the iris recognition part. Since the project is on the blockchain, the most important course is the "Blockchain Technologies" given by Dr. Aytunç Yıldızlı. We learnt a lot during his lesson about our project.

### 14. REFERENCES

## School of Engineering and Natural Sciences Graduation Project

- [1] “The Key Disadvantages Of POS Systems | National Processing.” <https://nationalprocessing.com/blog/the-key-disadvantages-of-pos-systems> (accessed Oct. 13, 2022).
- [2] “8 Things You Should Know About Water & Semiconductors - China Water Risk.” <https://www.chinawaterrisk.org/resources/analysis-reviews/8-things-you-should-know-about-water-and-semiconductors/> (accessed Jan. 09, 2023).
- [3] “View of A Study of Encryption Algorithms AES, DES and RSA for Security.” <https://computerresearch.org/index.php/computer/article/view/272/272> (accessed Nov. 14, 2022).
- [4] D. Pandey, A. Ansari, and T. J. Soon, “Three QR Code Related papers The Effective QR Code Development using VB.NET Manish Mathuria Quick Response Code and ITS Use in Libraries: A Recent Trend by Aslam Ansari and Mohd Nazim”.
- [5] “Impact of Blockchain Technology on the Payment Management Systems – What Future Holds?,” *European Journal of Economic Studies*, vol. 8, no. 1, Mar. 2019, doi: 10.13187/ES.2019.1.43.
- [6] K. Thanapal, D. Mehta, K. Mudaliar, and B. Shaikh, “Online Payment Using Blockchain,” *ITM Web of Conferences*, vol. 32, p. 03007, 2020, doi: 10.1051/ITMCONF/20203203007.
- [7] A. Kumari and N. C. Devi, “The Impact of FinTech and Blockchain Technologies on Banking and Financial Services,” *Technology Innovation Management Review*, vol. 12, no. 1–2, 2022, doi: 10.22215/TIMREVIEW/1481.
- [8] S. Fernandez-Vazquez, R. Rosillo, D. de La Fuente, and P. Priore, “Blockchain in FinTech: A Mapping Study,” *Sustainability 2019, Vol. 11, Page 6366*, vol. 11, no. 22, p. 6366, Nov. 2019, doi: 10.3390/SU11226366.
- [9] A. A. Monrat, O. Schelén, and K. Andersson, “A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities”.
- [10] A. Khatri and A. Kaushik, “SYSTEMATIC LITERATURE REVIEW ON BLOCKCHAIN ADOPTION IN BANKING,” *Journal of Economics, Finance and Accounting-JEFA*, vol. 8, no. 3, pp. 126–145, 2021, doi: 10.17261/Pressacademia.2021.1458.
- [11] M. R. Hoffman, L.-D. Ibáñez, and E. Simperl, “Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework,” *Frontiers in Blockchain*, vol. 3, p. 35, Aug. 2020, doi: 10.3389/FBLOC.2020.00035.
- [12] “ONLINE PAYMENT SYSTEMS FOR E-BANKING AND BLOCKCHAIN TECHNOLOGY,” *ECONOMIC VISION - International Scientific Journal in Economics, Finance, Business, Marketing, Management and Tourism*, vol. 7, no. 13–14, pp. 63–70, 2020.
- [13] R. Biswas, J. Uddin, and M. J. Hasan, “A new approach of iris detection and recognition,” *International Journal of Electrical and Computer Engineering*, vol. 7, no. 5, pp. 2530–2536, Oct. 2017, doi: 10.11591/IJECE.V7I5.PP2530-2536.
- [14] A. T. Kahlil and F. E. M. Abou-Chadi, “Generation of iris codes using 1D log-gabor filter,” *Proceedings, ICCES'2010 - 2010 International Conference on Computer Engineering and Systems*, pp. 329–336, 2010, doi: 10.1109/ICCES.2010.5674879.



## School of Engineering and Natural Sciences

### Graduation Project

- [15] C. O. Chițu, “Advanced Encryption Standard Technical Report 1 Electric Power Steering View project Advanced Encryption Standard View project”, Accessed: Nov. 14, 2022. [Online]. Available: <https://www.researchgate.net/publication/336126626>
- [16] “Overview | Avalanche Docs.” <https://docs.avax.network/intro> (accessed Jan. 09, 2023).
- [17] “What is the Paillier cryptosystem?” <https://blog.openmined.org/the-paillier-cryptosystem/> (accessed Jun. 22, 2023).



## School of Engineering and Natural Sciences

### Graduation Project

#### 15. PROJECT ACTIVITIES AND WORK PLAN

*Table 1 The Work-Activity Plan for Project 1*

Work and Activity	Responsible Group Member	Timeline													
		1. week	2. week	3. week	4. week	5. week	6. week	7. week	8. week	9. week	10. week	11. week	12. week	13. week	14. week
1.Literature Review	Emre - Berat														
2.Basic Terminology Research	Emre - Berat														
3.Research of Iris Recognition Algorithm	Emre - Berat														
4.Comparing Encryption Algorithms	Emre - Berat														
5.Researching Blockchain Networks	Emre - Berat														
6.Deciding the user interface	Emre - Berat														
7.Development of IOS app	Emre - Berat														

*Table 2 The Work-Activity Plan for Project 2*

Work and Activity	Responsible Group Member	Timeline													
		1. week	2. week	3. week	4. week	5. week	6. week	7. week	8. week	9. week	10. week	11. week	12. week	13. week	14. week
8.Implementation of NFC	Emre – Berat														
9.Building the smart contract	Emre – Berat														
10.Implementation of HE&ZKPs	Emre – Berat														
11.Development of POS machine app	Emre – Berat														
12.Testing the System	Emre – Berat														

## School of Engineering and Natural Sciences Graduation Project

### 15.1. LIST OF WORK PACKAGES

*Table 3 Detailed Definition of Work and Activity*

WP No	Detailed Definition of Work and Activity
1	Investigating and analyzing related articles
2	Researching related basic terminology
3	Research about Iris recognition algorithm
4	Comparing different encryption algorithms
5	Researching Blockchain networks
6	Deciding the user interface
7	Development of IOS app
8	Implementation of NFC technology
9	Building the smart contract
10	HE & ZK-Proofs
11	Development of POS machine app
12	System Test and Optimization

*Table 4 Work package targets, their assessment, and the contribution of each work package to the overall project success.*

Work package	Related Success Criteria	Target	Measurable outcome	Contribution to overall success (%)
1	1-2-3	Investigate different methods and their implementations	Analyzing at least 8 articles	<b>%5</b>
2	1-2-3	Examine the related terminology of the fields of the project	Getting general knowledge about related terminology	<b>%2</b>
3	3	Researching Iris recognition algorithms	Feasibility of the algorithm	<b>%8</b>
4	2	Comparing and testing various encryption algorithms	Selecting the optimal encryption method	<b>%8</b>
5	1	Getting information about the different blockchain networks	Selecting the most suitable network for the project	<b>%5</b>
6	4	Deciding the most user-friendly interface	Creation of design template	<b>%10</b>
7	3-4	Developing and testing the IOS app	Finalizing the mobile app	<b>%10</b>
8	4	Research and implementation of NFC technology to POS machine	Transferring the data via NFC	<b>%12</b>

## School of Engineering and Natural Sciences Graduation Project

9	1	Development of smart contract of the project	Deploying the smart contract to the network	<b>%13</b>
10	2-3	Implementation of HE & ZK-proofs	Hiding both parties in sub 2 seconds proof generation	<b>%11</b>
11	3-4	Developing and testing the POS app	POS machine app created	<b>%10</b>
12	1-2-3-4	Overall System Testing	<5 sec transaction time	<b>%6</b>
				<b>Total:100</b>

*Table 5 The work package distribution to project team members*

WORK PACKAGE DISTRIBUTION												
Project Member	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	WP 10	WP 11	WP 12
Emre	50	50	90	50	60	50	20	50	30	60	30	50
Berat	50	50	10	50	40	50	80	50	70	40	70	50
Total	100	100	100	100	100	100	100	100	100	100	100	100

## 16. BUDGET

*Table 6 Proposed Budget in TL*

	ITEMS				
	PEOPLE*	MACHINE-INSTRUMENT*	MATERIALS	SERVICE	TRAVEL
<b>IMU FUND</b>	210000 TL	24000 TL	0	0	0
<b>SPONSOR COMPANY FUND</b>	-	-	-	-	-
<b>TOTAL</b>	210000 TL	24000 TL	-	-	-

- 2 People, 15000 TL month/per person, 7 months
- 4 different POS machine for testing, 6000 TL per machine



## School of Engineering and Natural Sciences Graduation Project

### 17. CURRICULUM VITAE

# MEHMET BERAT OZTURK

## SOFTWARE ENGINEER

---

### CONTACT

+90539 442 27 76

mehmetberatozturk@outlook.com

https://github.com/BeratOz01

Istanbul / Turkey

---

### SKILLS

Javascript

Typescript

ReactJS

NestJS

SQL / NO-SQL Databases

Blockchain Development

Solidity

Python

Java

CSS

---

### EDUCATION

Computer Engineering

**Medipol University**

2019-2023

Full scholarship

Language: English

---

### LANGUAGES

English ◆◆◆◆

### PROFILE

I am a 4th-grade computer engineering student at Medipol University with a full scholarship. I am highly skilled in Javascript frameworks such as NestJS and ReactJS, and have hands-on, work experience in these frameworks. For the past year, I have been working on blockchain development. Currently, I am trying to improve my skills in the blockchain area.

---

### WORK EXPERIENCE

#### Intern

New Mind, Istanbul / Turkey Apr 2020 - Nov 2020

- Hands on experience on smart contract developments
- Worked as database engineer with SQL

#### Full Stack Developer

ErgoVisio, Istanbul / Turkey Oct 2021 - Dec 2021

- Develop ReactJs front-end & Python backend applications with SQL database for Image Processing tool.

#### Blockchain Developer

NextDream, Istanbul / Turkey Nov 2021 - Apr 2022

- Maintained and extended client-side and server-side applications.
- Brainstormed and evaluated applications for new tools and technologies.
- Develop vesting and launchpad contract which is currently online on Binance smart chain
- Develop NFT Marketplace contract

#### Blockchain Developer

XYZ Technology, Istanbul / Turkey

- Maintained and extended client-side and server-side applications.
- Develop front end application with ReactJS
- Develop server side application with NestJS & TypeORM
- Build crowd-funding application with ReactJS & Solidity

## School of Engineering and Natural Sciences Graduation Project



# EMRE KAAN SATIŞ

### PROFILE

Experienced member with a demonstrated history of working in the non-profit organization management. Highly interested in Object-Oriented coding languages and blockchain technologies. Working on bachelor's degrees in Computer Engineering and Biomedical Engineering.

### CONTACT

PHONE:  
0506-390-99-57

LINKEDIN:  
[linkedin.com/in/emrekaan/](https://www.linkedin.com/in/emrekaan/)

EMAIL  
[emrekaan1999@gmail.com](mailto:emrekaan1999@gmail.com)

### SKILLS

- Data Science
- Artificial Intelligence
- Machine Learning
- Object-Oriented Programming
- Blockchain
- Problem Solving
- Teamwork

### PROGRAMMING LANGUAGES

- Python
- Solidity
- Javascript
- Java
- C++

### EXPERIENCE

**Internship – Blockchain Developer**  
TUBITAK BILGEM UEKAE

July 2022 – August 2022

- Done research about blockchain technologies and developed cryptography algorithms.

**Internship - Data Engineer**  
Path | Product & Software House

July 2021 – August 2021

- Processed complex data and increased readability.
- Created a machine learning algorithm to increase the stability of a shopify system.

### VOLUNTARY JOBS

**Board Member**

Medipol Blockchain Community

2022 - 2023

- Community management and algorithm development in Ethereum Blockchain Environment

**Core Team Member**

Google DSC Medipol University

2021 - 2022

- Management in university-based community supported by Google

### EDUCATION

**Bachelor's Degree**

Istanbul Medipol University (Full Scholarship)

2019 – Present

- Computer Engineering – 4<sup>th</sup> year (gpa 3.46)

**Bachelor's Degree – Double Major**

Istanbul Medipol University (Full Scholarship)

2021 – Present

- Biomedical Engineering – 3<sup>rd</sup> year (gpa 3.53)

### CERTIFICATION & COURSES

- Certificate of Participation - Erasmus+ Bulgaria
- Certificate of Appreciation - Google Developer Student Clubs
- Certificate of Completion, Introduction to AI, Robotics and Data – Global AI Hub