Software Engineering Department
Ort Braude College
Course 61766: Extended Project in Software Engineering

Gambling Platform Based on Blockchain Technology

Authors: Aviv Rozia 201411477**,** Moshe Malka 204769426
Supervisor: Alexander Keselman

Abstract. *As a part of the big crush of the united states stock market at 2008, many people lost their trust in the common banking system, as a result, the need for a new platform arose, this platform called BLOCKCHAIN.*
A blockchain is a list of records (blocks) which are linked and secured using cryptography, each block contains a cryptographic hash of the previous block, a timestamp and transaction data, blockchain is resistant to modification of the data.
although there are many types of blockchain, on our project we will focus on blockchain 2.0 (Ethereum) that supports smart contracts, a huge improvement from version 1.0 that supports only 2 functions: send (), receive (), that focus mainly on money transactions such as "bitcoin".
Moreover, on our project we will allow people to gamble using the benefits of the BLOCKCHAIN system such as: Reliability, Transparency, Security, Anonymous.

Keywords: BLOCKCHAIN, Merkle tree, Ethereum, Gambling.

1. INTRODUCTION

In the late 1990s, online gambling gained popularity, by 2001 after several major changes in some federal laws the estimated number of people who had participated in online gambling rose to millions, since then the online gambling industry continue to grow. Until today, there have been various problems with the old approach:

1) The lack of privacy, a person who wants to gamble need to uncover his identity, he needs to create an account with his personal information, such as credit card number, name, address, social security number, etc.
2) The lack of reliability, in the modern gambling platforms, there is always a chance to a fraud, there is always a chance that someone will intervene in the game and will put the odds in his favor, in short someone might cheat.
3) The lack of transparency, there are many online casinos where data such as winnings, gaming results, payouts, and so on are deliberately hidden or partially obscured from public scrutiny.

These problems can be solved with the new BLOCKCHAIN technology. In the BLOCKCHAIN protocol each person has an encrypted hash number. Although everyone can see the hash number of the person, its identity remains hidden by the advanced encryption of the protocol. However, you never send your funds to any 3rd partied, there is no internal database guarded by some anonymous site owner, since BLOCKCHAIN technology relay on decentralized public database where everyone on the network can inspect. smart contracts are public, verified code that lives on the very public Ethereum BLOCKCHAIN network.

1.1 Organization of the Paper

In the first section, we introduce our project and explain the purpose of it. In the second section, we explain the background of the project: what is our project based on. Moreover, we define some terms that related to our project. In the third section the expected results of our project are given. In the forth section, the software engineering documents are placed: use-case diagram, UML diagrams and GUI. In the fifth section we gave references for the information we show in the book.

2. THEORY

2.1 Background and related work

2.1.1. Introduction to BLOCKCHAIN

A **blockchain**, originally **block chain**, is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.
Blockchains are secure by design and exemplify a distributed computing system with high byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This contributes a great deal to the security of blockchain and makes the network reliable, since the information isn't stored in one source, moreover by decentralizing data on an accessible ledger, public blockchains make block-level data transparent to everyone involved.
Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has been the inspiration for other applications.

2.1.2. Satoshi Nakamoto

In October 2008, an anonymous person who identified himself as Nakamoto published a paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" in which he explains how a peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. In fact, all we know about Nakamoto is that he identified himself as a Japanese man and that he was born on April 5th 1975, but all of that is probably false. Experts speculate that Nakamoto identity, bases of his expertise in number of cryptography and computer science, is not Japanese but a United States or Europe resident. To this day there is still doubt about the real identity of Satoshi Nakamoto.
Satoshi stats that his work on the writing of the code began in 2007, he kept with the agenda that due to its nature the code design would have to be able to support a broad range of transaction types.
On 3 January 2009, the bitcoin network came into existence with Satoshi mining the "genesis block of bitcoin"(block number 0), since then the blockchain technology has continued to evolve.

2.1.3. Introduction to BITCOIN

Bitcoin is the first decentralized digital currency. It uses a BLOCKCHAIN technology to transfer digital currency in a peer-to-peer payment system. Using this system allows us to transfer currency without involving banks or any third-party member, insuring the legitimacy of the transactions and decreasing the fee. Several currency exchanges exist where everyone may buy and sell Bitcoins, for dollars, euros and more. The bitcoins are kept in digital wallets where the user can access them from

every computer or mobile device. The Bitcoin network is secured by individuals called miners, users with strong CPU power. The miners verify every transaction and after the verification they broadcast to a transparent public ledger which is fully distributed across the network. The bitcoin software is a completely open source code.
The programmable, open character of Bitcoin allows us to completely rebuild and innovate our financial sector and our administrative processes. Make them more efficient and transparent and significantly decrease bureaucracy.
Bitcoin is much more than simply money and payments. In fact, Bitcoins are created as a reward for the mining process, they can be exchanged for other currencies, products and services. Today many merchants and vendors accept bitcoin as payment.

2.1.4 Vitalik Buterin

Vitalik Buterin (1994) is a Russian- Canadian programmer. In Canada Buterin placed in class of gifted children and started to understand that he was drawn to math, programming and economics. Buterin learned about bitcoin from his father, a computer scientist, at age 17. In 2011 a person reached out to Buterin about a new publication called "Bitcoin Magazine" and later became a leading writer at the magazine and wrote hundreds of articles on cryptocurrency. Buterin argued that bitcoin needed a scripting language for application development. He proposed development of a new platform with a more general scripting language. The system was called Ethereum. For his work, Buterin was named a 2014 Thiel fellow, a contest that awards winners $100,000.

2.1.5 Vitalik's BLOCKCHAIN

In 2013 Vitalik Buterin released his version of the BLOCKCHAIN system, Ethereum. Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications. In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network. Before the creation of Ethereum, blockchain applications were designed to do a very limited set of operations, Bitcoin and other cryptocurrencies, for example, were developed exclusively to operate as peer-to-peer digital currencies. Either expands the set of functions offered by Bitcoin and other types of applications Ethereum allows developers to create whatever operations they want. This means developers can build thousands of different applications that go way beyond anything we have seen before.

2.2 Detailed Description

2.2.1. A deeper look into BLOCKCHAIN.

In the previous chapters we explained about BLOCKCAHIN and the set of problems it can solve. In order to really understand BLOCKCHAIN we must talk about the main parts of the system.

Transactions

We define a transaction as a chain of digital signatures. Each user who wishes to make a transaction of any kind has to digitally sign a hash of the previous transaction and the public key of the next user. The signatures can be verified by the chain of ownership.

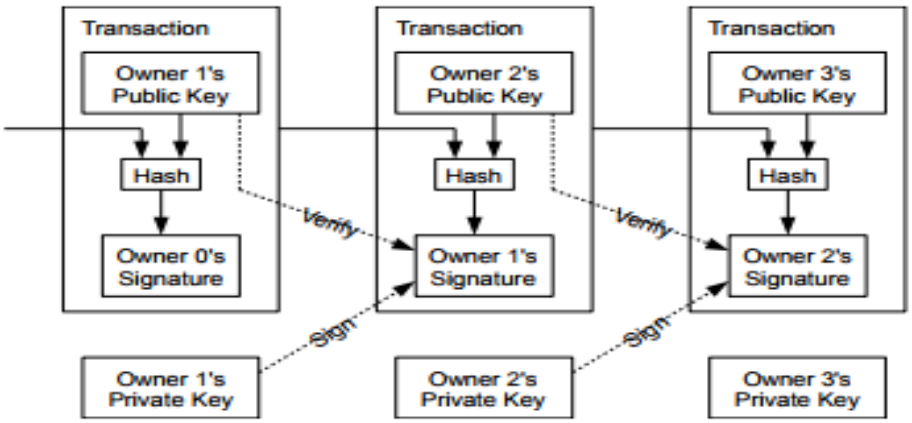

Fig.1: Transactions structure

However, there is a problem called "double-spending", this problem refers to the fact that a peer can try to spend the money he has more than once due to the fact that all the transactions has to be verified (this process takes some time).
The double-spending problem can be solved by the fact that the transactions must be publicly announced. The BLOCKCHAIN technique allows the participants to agree on a single history of the order in which the transactions were transferred. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend.

Timestamp Server

To support this technique, we need to use timestamps that is relied upon the previous timestamps in its Hash, thus forming a chain, with each additional timestamp reinforcing the ones before it.

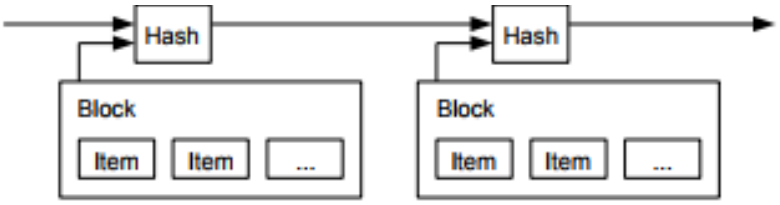

Fig.2: Timestamp Server structure

Proof-of-work

A proof-of-work (POW) system (or protocol, or function) is a means of proving data and preventing attacks and abuses such as spam on the network, the main use of this system is to avoid double-spending and add reliability to the system. What is special about this system is the fact that producing the code requires a lot of resources and takes a long time.
The key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle or CPU pricing function. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.
POW protocol is not a new idea, in fact it was invented by a person called Adam Back, Satoshi Nakamoto introduced a new way to implement this protocol inside the timestamp server in order to solve the double-spending problem. Satoshi combined this and other existing concepts- cryptographic signatures, Markle trees, and P2P networks into a viable distributed consensus system.

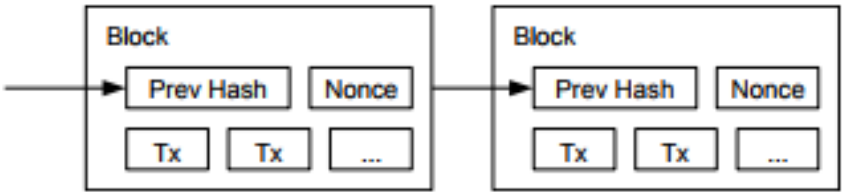

Fig.3: Proof-of-work structure

The idea is based on Hash code, the hash begins with a number of zero bits. In our timestamp network, we vary the string by adding an integer value to the end called a nonce and incrementing it each time until a value is found that gives the block's hash the required zero bits. This can be translated to CPU power. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it. Miners always consider the longest chain to be the correct one and will keep working on extending it. If two Miners broadcast different versions of the next block simultaneously, some miners may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer.

Network

The BLOCKCHAIN network requires the following steps:

1) New transactions are broadcast to all miners.

2) Each miner collects new transactions into a block.

3) Each miner works on finding a difficult proof-of-work for its block.

4) When a miner finds a proof-of-work, it broadcasts the new block to all miners.

5) Miners accept the block only if all transactions in it are valid and not already spent.

6) Miners express their acceptance of the block by working on creating the next block

In the chain, using the hash of the accepted block as the previous hash.

Decentralization

“Decentralization” is one of the words that is used in the crypto economics space the most frequently, it means that not one single entity has control over all the processing, this will keep the whole idea protected from fault tolerance, attack resistance and collusion resistance. Vitalik Buterin described in his article about three aspects of decentralization: Architectural Decentralization, Political Decentralization and Logical decentralization.
Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system behaves like a single computer). There is a common open ledger in the network that being kept by every miner, this will keep the network safe.

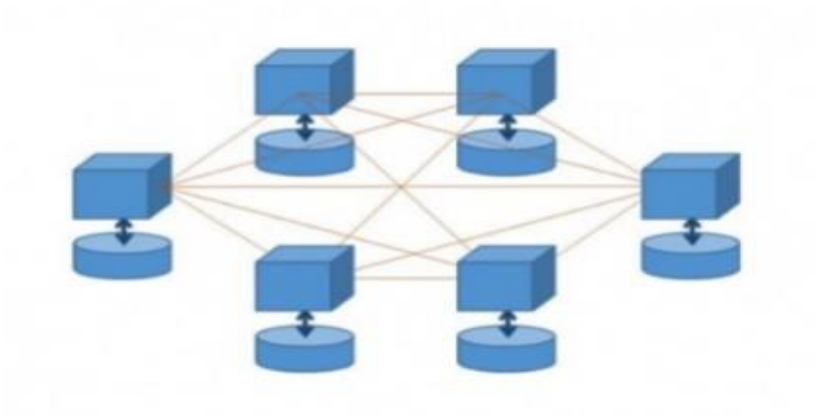

Fig.4: Decentralized network

Merkle Trees

Merkle tree is a hash-based data structure that is a generalization of a hash list. It is a tree structure in which each leaf node is a hash of block of data and each non-leaf node is a hash of its children. Typically, Merkle trees are implemented as binary tree, which means that each node can have 0,1 or 2 children, although it can be implemented as an n-ary tree. Merkle trees are used in distributed and peer to peer systems for data verification. Suppose you want to check if a file is same everywhere and nobody has tampered with its contents. For doing this, we can use Merkle trees. Instead of sending the entire file from point A to point B and then comparing it with a copy of it, we can send the hash of the file from A to B. This hash is then checked against the root of the Merkle tree. If the hash matches then we can be sure that the data in the file was not modified in any way. Merkle trees can be used to check for inconsistencies in more than just files and basic data structures like the blockchain. Apache Cassandra and other NoSQL systems use Merkle trees to detect inconsistencies between replicas of entire databases.
So where does this hash-based tree fit into the world of blockchain? Each block typically contains a hash pointer to a previous block, a timestamp, and transaction data in a permanent manner. The transaction data can be stored in blocks, which are actually the leaf nodes of a Merkle tree. The root hash can then be stored in the block. So, the blocks of a blockchain hold valid transactions that are hashed and encoded into a Merkle tree.

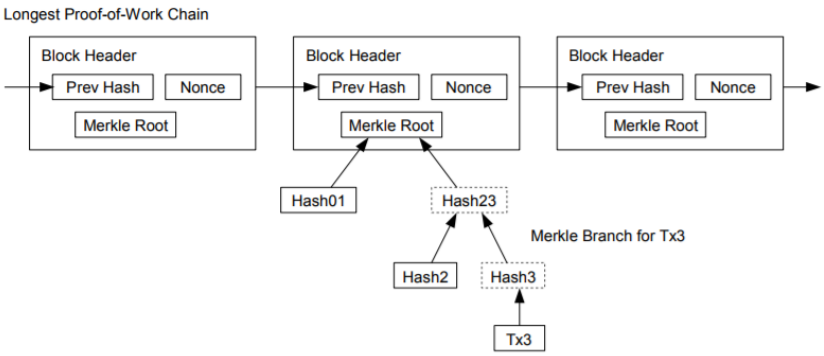

Fig.5: Merkle Trees

Pruning

The pruning method was described first in Satoshi Nakamoto's Article, this technique will provide the user more disk space. Let's keep in mind that miners save all the transactions history is their computer, each transaction has a size, a small size, but if we add lots of transactions together we get a huge file. Here is where we need some technique to help us save

disk space without harming the proof-of-work because in few years this file will grow bigger and bigger and miners won't be able to save it as a whole.
In 2017 a solution was activated that called Segregated Witness, SW is the process by which the block size limit on a blockchain is increased by removing signature data from Merkle Trees. When certain parts of a transaction are removed, this frees up space or capacity to add more transactions to the chain, then when a miner want to verify a new block he has to check only the witness blocks instead of the whole tree.

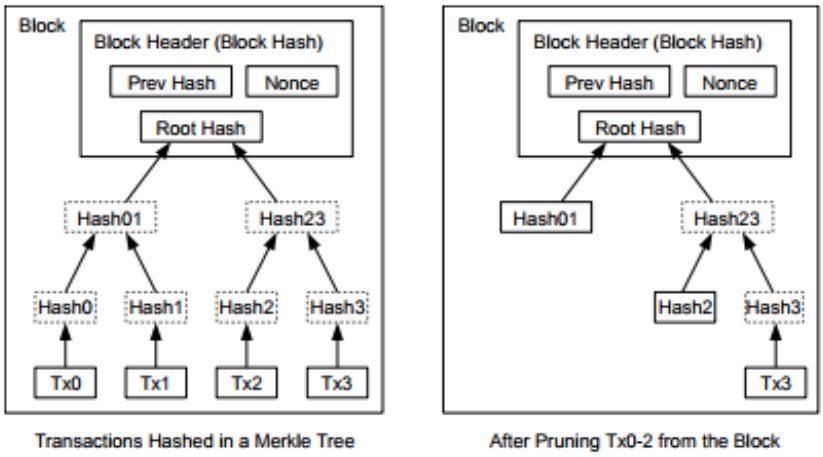

Fig.6: Pruning

Privacy

Blockchain technology fulfills its mission and enables the transfer of funds between two parties without the need for a third party. Furthermore, this technology does not link user information to currencies and transactions, it keeps public keys anonymous, thus maintaining maximum privacy.
Privacy is achieved by allowing the public to see if someone has sent a certain amount to someone else, without additional information linking the traffic to someone specific. The level of privacy is similar to the level of information published by stock exchanges - the time and size of individual transactions - is the link itself performed publicly but without telling the parties. In addition, for each account we will use a new pair of keys to prevent affiliation to the same owner.

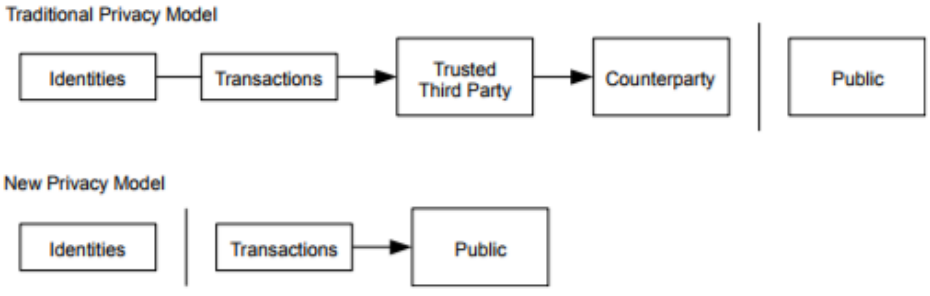

Fig.7: The new Privacy model

2.2.2. Smart Contract

The concept Smart Contract was first introduced in 1996 by Professor Nick Szabo. A Smart Contract is a computer protocol designed to facilitate, verify, and enforce a negotiation or execution of a contract.
One of Vitalik Buterin's goals, in the creation of Blockchain 2.0, was to realize Nick's vision and to create a basis for creating smart contracts on the Blockchain, and so it happened.
In creating a smart contract, you can enter terms and conditions such as a standard contract (such as sending a minimum or maximum amount of money or sending money only at certain times). The significant difference, however, between a normal contract and a wise contract, is that there is no need for a third-party mediating between the two parties who signed the contract in order to carry out the actions or to decide whether the two parties were in a deal. In a wise contract, the terms and conditions actually occur automatically and immediately, and if someone does not meet the terms of the contract, there will be no need for a court to rule and decide, but the contract will automatically reject it.
Because the need for an intermediary becomes redundant with regard to the validity of a wise contract, many risks associated with dishonesty and fairness among the parties involved in the contract are avoided; The diversion of the law, the falsification of facts, bribery and, consequently, harming weak people are nullified by the execution of the contract by an inhumane party. Accordingly, such contracts will increase the level of credibility and confidence in creating transactions between people.
Note: Today this technology is still young, and most of today's contracts are relatively simple, but there are a large number of projects to create reliable and complex contracts.

2.2.3. Lightning networks

In order to talk about our solution, first we need to understand the concept of the lightning networks. It's important to note that using the main BLOCKCHAIN network gives a dissent optimization for the online gambling already, however there is another big improvement that has been set in the last year the Lightning networks.
The Lightning Network is another layer that is based on the BLOCKCHAIN protocol. This layer creates a secondary map of nodes and allows money to be transferred between the nodes much faster than the main network, thanks to a significant reduction in the number of nodes. This has been touted as a solution to the bitcoin scalability problem. It features a peer-to-peer system for making micropayments of digital cryptocurrency through a network of bidirectional payment channels without delegating custody of funds and minimizing trust of third parties.
In order to use this network, one must join the payment channel by committing a funding transaction to the relevant blockchain. When a transaction occurs only the lightning network is being updated without broadcasting to the main BLOCKCHAIN. optionally followed by closing the payment channel by broadcasting the final version of the transaction to distribute the channel's funds.

2.2.4. Proposed Solution.

With our solution we will create a simple and convenient gambling system based on the BLOCKCHAIN under lightning network. The gamblers will be able to access the system through a web-based interface, thus allowing it to be accessible through out all of the platforms and all of the devices like iOS, android, windows and etc.
Any gambler who wants to use the platform must connect to the MetaMask plug-in in order to link his digital wallet to the site in a completely anonymous manner, after that the gambler must deposit funds in the Liquidity lightning network. The gambler must choose a game from among the games offered on the site, after selecting a game the gambler must enter the address of his MetaMask, the address of the game and the amount of the bet in the relevant range, the MetaMask plug-in will jump and ask for

confirmation of the transaction, if the balance in the wallet allows this. In case the gambler wins, the smart contract processes the bet and returns the win directly to his wallet.
NOTE: Once the transaction is approved, the transaction will be processed and then added to the off-chain BLOCKCHAIN where the bet cannot be changed or interfere, after a certain of time the off-chain blocks will be alter to the on-chain main network to update the gambler wallet.

2.2.5. Pros and Cons of the proposed solution.

Pros:

1. The BLOCKCHAIN protocol gives us a high-level build-in encryption level, stronger than any other system that is in use today.
2. In the solution we suggested, the user can enjoy complete anonymity because it is necessary for him to connect to the MetaMask system in order to play on the site.
3. There is no trust involved, the user will always control his own funds since the smart contract will process the bets.
4. On the smart contract we can program terms of use for example the minimum and maximum amount for bets.
5. Our system offers full transparency without the risk of frauds, since the smart contract is public, verified code, that lives on the very public Ethereum blockchain.
6. Our system provides the users to play from anywhere they are on any platform.
7. Our system works on the lightning network, this fact provide the gamblers with incredibly high transactions speed compared to the main network.

Cons:

1. Bets are processed slower the with centralized database, it takes around 15s to process bets in a decentralized way.
2. Our solution will only be available for people with technological means, people without internet access will not be able to play in our website.
3. The majority of governments, offices, retailers and everyone who deal with money, still don’t accept cryptocurrencies as valid payment.
4. Today there are still many people who oppose the use of cryptocurrencies.

2.2.6. Alternative approach to address the issue

Today there are many ways to gamble, some are private illegal places, some are public legal places and some that using BLOCKCHAIN.
We won't talk about the private illegal places since those places are managed by unauthorized people.
In the past when a gambler wanted to gamble he needed to go directly to the casino, risking himself by revealing his identity and trust the casino that the games will be fair. Then the online casinos aroused in order to deal with those problems, however, this problem was partially solved. The gambler didn’t have to reveal his identity; instead he needed to revel his personal information such as: credit card number, security number and id. He had to trust the credibility of the website, the fairness of the games and the fact that the owners had to pay back. In addition, the casino infrastructure was maintained on a single database, all the money saved in one place, all the games were managed from one place, this reveal the gambler for frauds and theft problems.
There are websites that use BLOCKCHAIN technology, although these sites try to overcome the problems presented above, these sites suffer mainly from development problems, they are very slow because they use the main network, most of them unclear and it's very difficult to play through them. In addition, in most of the sites it's hard to find who the owner is and it's very hard and even impossible to find and inspect the smart contracts.

2.3 Philosophy of BLOCKCHAIN

2.3.1. How are we benefiting from the Blockchain?

Finance

Our global financial system moves trillions of dollars every day and serves billions of people, but the system is rife with problems; adding costs through fees and delays and opening up opportunities for fraud and crime. 45% of financial intermediaries, such as payment networks, stock exchanges, and money transfer services, suffer from economic crime every year. The Blockchain is capable of recording anything of value. Money, equities, bonds, titles, deeds, contracts, and virtually all other kinds of assets can be moved and stored securely, privately, and from peer-to-peer because trust is established not by powerful intermediaries, like banks and governments, but by network consensus, cryptography, collaboration, and clever code. For the first time in human history, two or more parties, be them businesses or individuals who may not even know each other, can forge agreements, make transactions, and build value without relying on intermediaries (such as banks, rating agencies, and governing bodies) to verify their identities, establish trust, or perform the critical business logic — contracting, clearing, settling, and recordkeeping tasks that are foundational to all forms of commerce.

Middleman

The Blockchain has the potential to reinvent any transaction that now requires going through a middleman. Before the Blockchain, buying and selling required an intermediary, a bank or broker who housed your financial data on their servers. When you transfer funds or make a purchase, a banker connects to the bank's system to record the change. The Blockchain replaces this central system with a decentralized ledger of chained records. Each record is connected to the one before and the one after it, yielding a traceable history of every transaction. No record can be deleted and no existing records can be altered.

Identification

The greatest obstacle for migrating many services online is the ability to secure the data and verify the identity of the users of that service. Currently, online authentication relies on a password, or on rare occasions dual-factor authentication. The problems with these methods are that passwords are notoriously insecure and dual-factor authentication generally relies on sending a code over SMS or a third-party service. A solution to this problem could be the Blockchain. By distributing a ledger among all members of the network, Blockchain authentication eliminates someone from maliciously altering the ledger. Every time a "transaction" or block of data is added to the chain a majority of the network must verify its validity. This guarantees the integrity of the ledger. These principles could be applied to transition everything from the electoral process, to state identification cards, to dual-factor authentication and turned into a secure, fast, reliable, and readily available service.

2.3.2. The future of BLOCKCHAIN

The explosive growth of Bitcoin in 2017 promoted the reliability and benefits of the underlying technology used by cyber currency, the Blockchain. In 2017, Blockchain became the second most popular search word on Gartner's website, and distributed ledger technology will continue to gain significance across many industries. According to Gartner, the business value-add of Blockchain will grow to slightly more than 176$ billion by 2025, and then it will exceed 3.1$ trillion by 2030.
The BLOCKCHAIN technology will reshape our day to day life in many fields such as:

- **Banks**
  Blockchain will be adopted by central banks and cryptographically secured currencies will become widely used.

- **Industries**
  Blockchain technology will make the world even smaller as it increases the speed and efficiency of transactional activity.
- **Governments**
  The future of finance in many nations could be dominated by bitcoin and cryptocurrencies.
- **Crime**
  A new Blockchain startup has claimed its software could help track down criminals faster and cheaper than ever.
- **Blockchain meets the Internet of Things**
  According to the report of IDC (international data corporation), by the year of 2019, 20% of all IoT deployments will have basic levels of Blockchain services enabled.

3. EXPECTED RESULTS

We expect the system to be a convenient and safe tool that will allow users to gamble without fear of publishing their personal information. We also expect that the system will supply a simple and convenient and web-based interface that every that every web site manager can create and delete games easily. It will allow the manager to create certain conditions such as: adding new contracts, place the minimum and maximum bet amount and how much money a gambler will win. We expect the system to be a tool that will also allow the manager to withdraw relevant statistical data about previous games.
We wish that our system will be accessible from any electronic device, anonymously so the gamblers wont risk their own identity. We plan to achieve this goal by using MetaMask plug-in. adding to that, we hope that our site will be as user-friendly as possible, that it can provide any gambler with all the information it needs for each smart contract to give the gambler a sense of maximum transparency. Furthermore, the system can be improved and modified so in the future any gambling platform will be able to use our idea in order to improve their own website that probably using the old payment method.

4. SOFTWARE ENGINEERING DOCUMENTS

4.1. Use Case

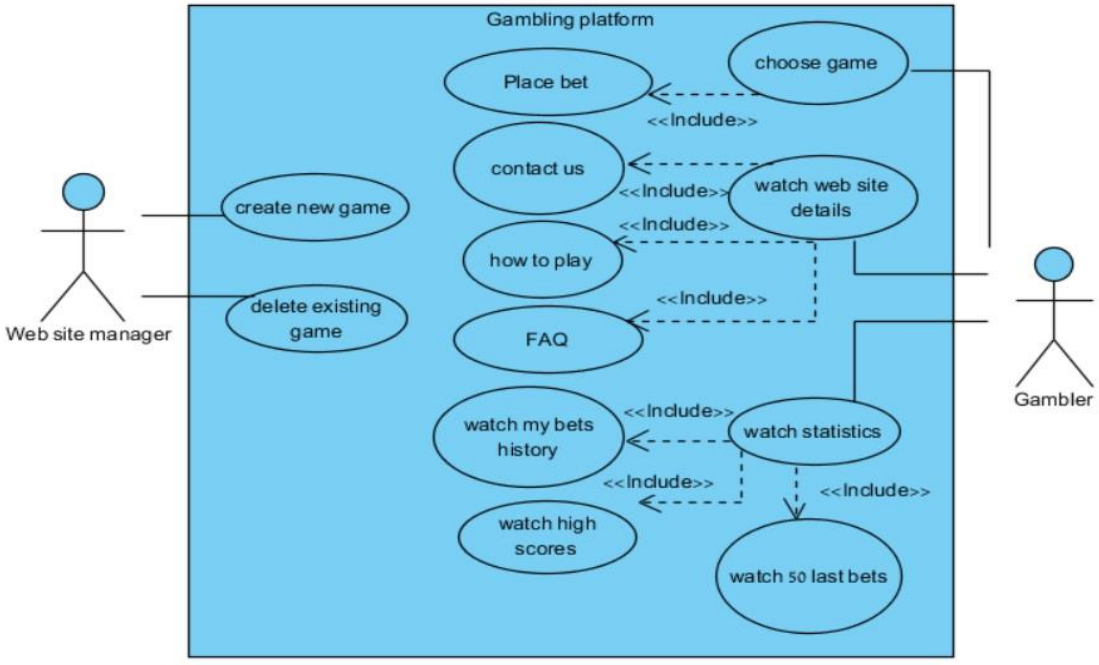

Fig.8: Use Case Diagram

Use case 1: place bet

Goal: placing a bet and creating a new smart contract.
Preconditions: gambler need to be connected to "MetaMask"
Possible user errors: There is not enough balance in the wallet.
Limitations: maximum or minimum bet.
Pseudo code Flow:

Actor	System
1) Press "place bet" button next to the relevant game	2) open a new page of placing a bet
3) enter the addresses of the game wallet and the gambler wallet then enter bet amount and press "place bet"	4) show a massage "placing a bet of (amount) press ok to confirm"
5) press "ok"	6) shows a massage "bet sent"
	7) add bet to the BLOCKCHAIN

Use case 2: Check statistics

Goal: enable the gambler to see all the information about last bets and wins.
Preconditions: there are statistics to show.
Possible user errors: none.
Limitations: In case there is no statistics the table will be blank.
Pseudo code Flow:

Actor	System
	1) shows all the statistics options
2) choose the desired option	3) shows the relevant statistics

Use case 3: watch website details

Goal: enable the gambler to see all the information about the website.
Preconditions: none.
Possible user errors: none.
Limitations: none.
Pseudo code Flow:

Actor	System
	1) shows all the details options
2) choose the desired option	3) shows the relevant details

Use case 4: Create new game

Goal: Create a new game
Preconditions: there is a valid smart contract.
Possible user errors: Enter wrong values in the fields.
Limitations: maximum bet should be higher than minimum bet.
Pseudo code Flow:

Actor	System
1) Enter the following: game address, maximum and minimum bet, multiplier and wining number.	
2) press "create new game"	3) system add new game to the website

Use case 5: delete game

Goal: delete an existing game from the website
Preconditions: there is at least one open game in the website.
Possible user errors: none.
Limitations: none.
Pseudo code Flow:

Actor	System
1) press "delete game"	2) system deletes game from the website

4.2. Class Diagram

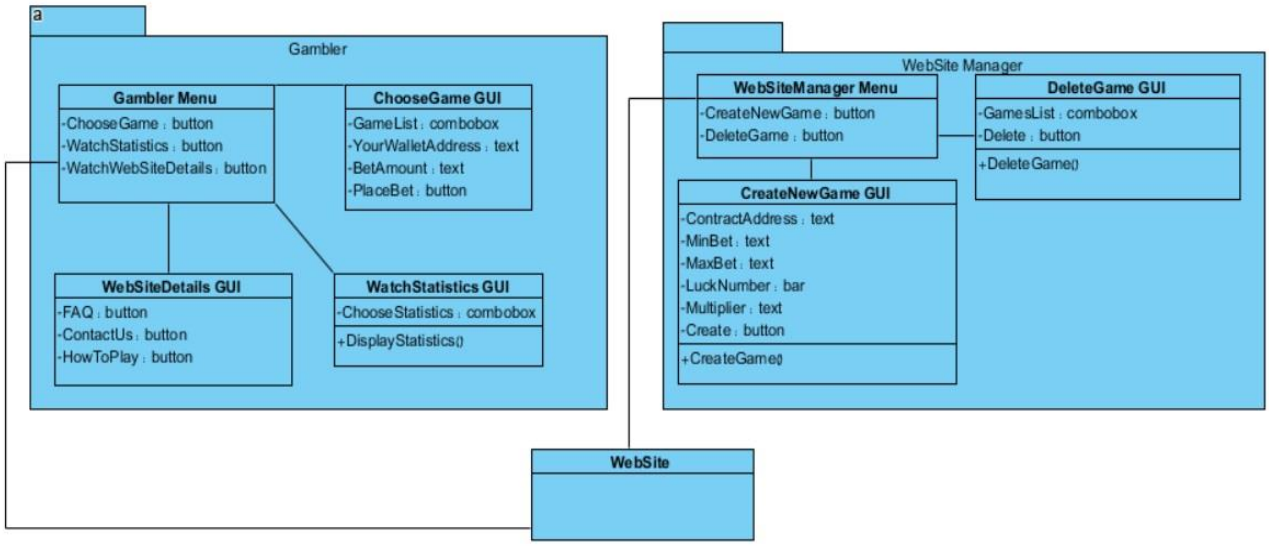

Fig.9: Class Diagram

4.3. GUI

Main Window

Fig.10: Main Window GUI

The main window of our site will allow the user to perform all the actions that can be performed in the game system. We decided to call our BLOCKCHAIN based website "I AM Gambling".
We will give a short explanation about this page:

1. In this window the user can get help with the header button.
2. In order to play, the user must choose a game from the offered games, then he press "Place Bet", it will bring him to a new window with the relevant game.
3. A user can choose to watch one of the statistics that are listed at the bottom of the page, each statistic will change the data in the table:
    a. Player wallet: displays the player who participated in the game.
    b. Roll: the number the player rolled.
    c. Target: indicates which game the player participated in.
    d. Bet amount: how much money the player invested.
    e. Winning amount: Displays the total amount that the participant will earn or lose

Place bet

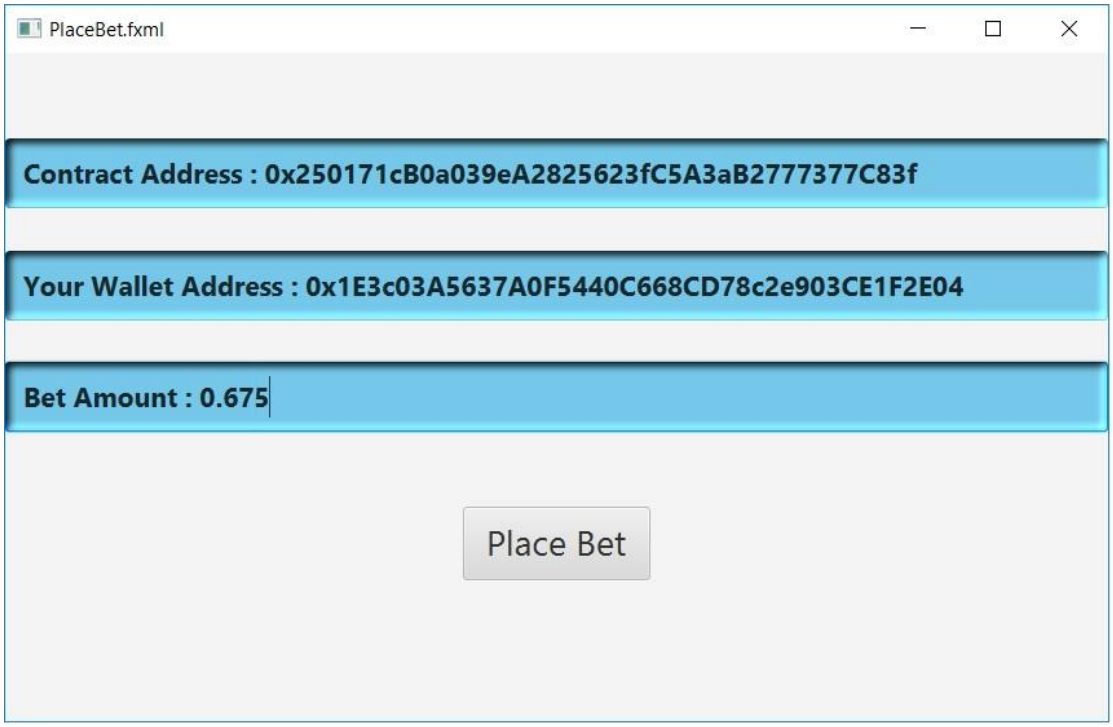

Fig.11: Place bet GUI

After selecting the right game, in order to finish the bet, the player must fill in the right information:

1. Contract address: this will be filled automatically according to the game the player chose.
2. Your wallet address: the player MetaMask wallet address, every player that wish to play must have a MetaMask plugin installed in his browser, a short explanation about that will be given on the FAQ page.
3. Bet amount: how much the player wants to bet.
4. When the player filled all the fields he may press the "Place bet" button in order to process the bet.

Administrator Main Window

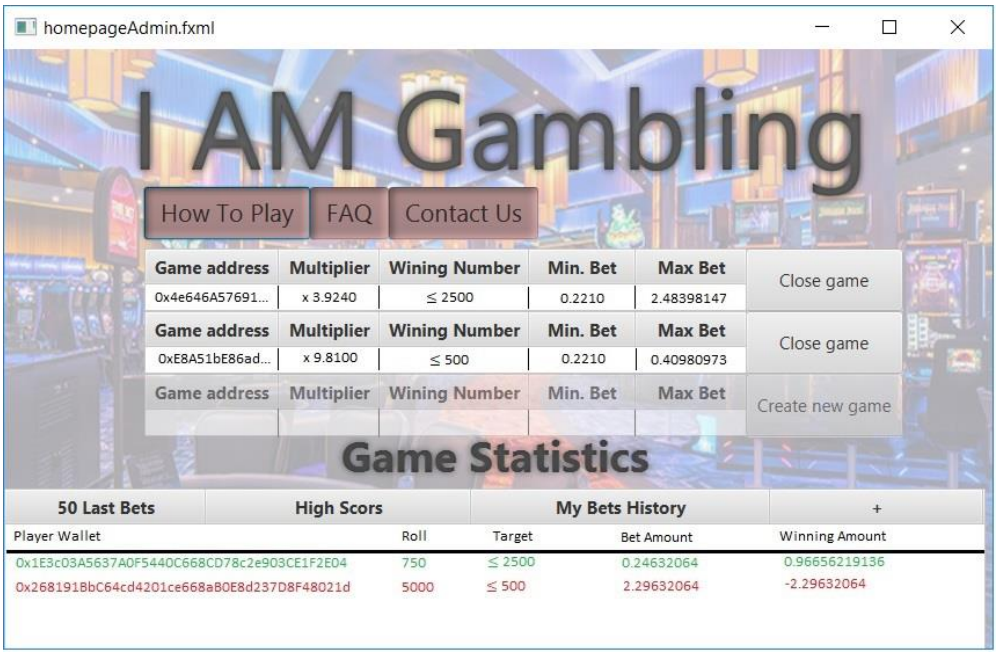

Fig.12: Administrator Main Page

Compared to the gambler main window, this window will provide the admin of the website with the ability of editing things in our website.
We will explain two very important actions on this page:

1. "Close game", the admin has the option to close an open game, in order to do so he need to go to the right row and press the "Close game" button.
2. Also, the admin has the option to open a new game, it's important to explain that when we say "open a new game", we mean that the admin will place the smart contract link, which he had created in advance, in the website. There are few things to talk about:
   a. Game Address: means the smart contract address, this address will be provided upon creating of a new contract.
   b. Multiplier: will tell the gambler how much money he can make by playing this game.
   c. Winning Number: tells the user which number he needs to get in order to win.
   d. Min. Bet – minimum bet amount.
   e. Max bet – maximum bet amount, note that max bet should be higher than min bet.

The rest of the editing options are just a regular website editing, such as: changing texts, buttons/tables locations etc.

Smart Contract Creation

Fig.13: Smart contract creation environment

We won't explain about this page too much because this environment can be found online, it was just important for us to show how a smart contract can be created and where the relevant information to open a new game can be taken from.

How to play

We made a very simple page with very clear instructions about how to play on our website

Fig.14: How to play page

FAQ –frequently asked questions

This page is just an example of a page with some common questions and answers that every player must ask before he wants to play on our website.

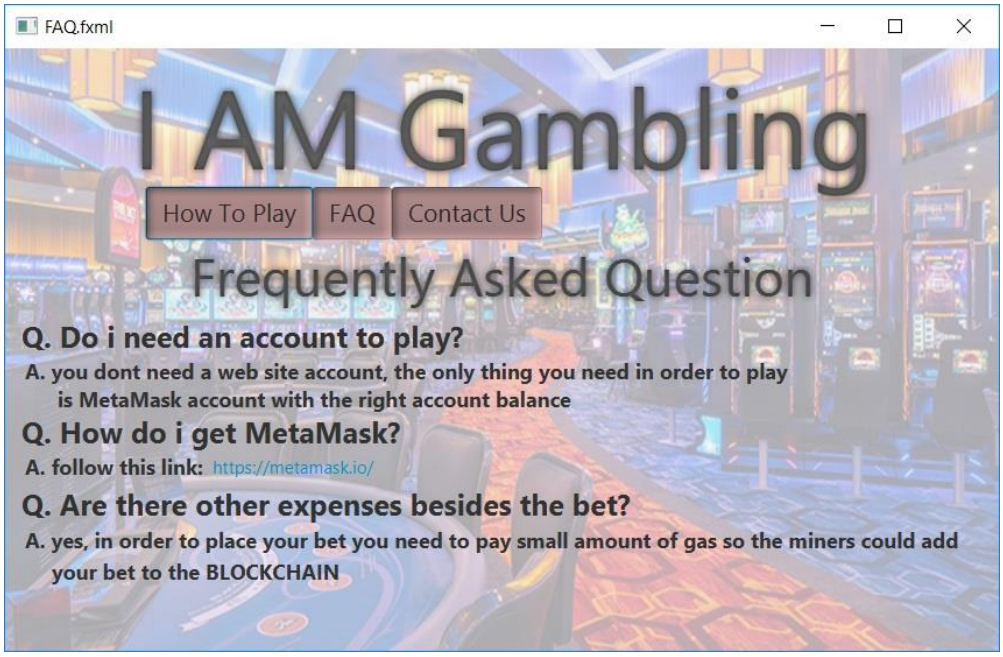

Fig.15: FAQ page GUI

Contact us

Some players may ask themselves, who manages this site? How can I contact him in case of problems? Just for this purpose this page was created.

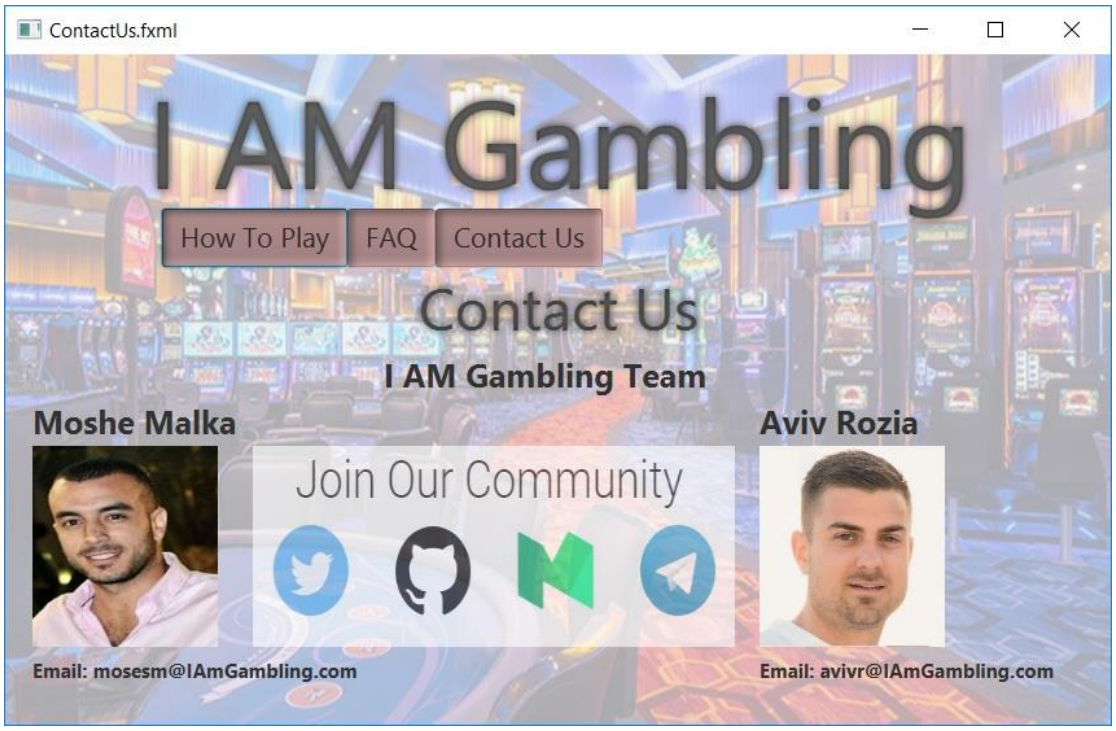

Fig.16: Contact us page GUI

4.4 Program Structure

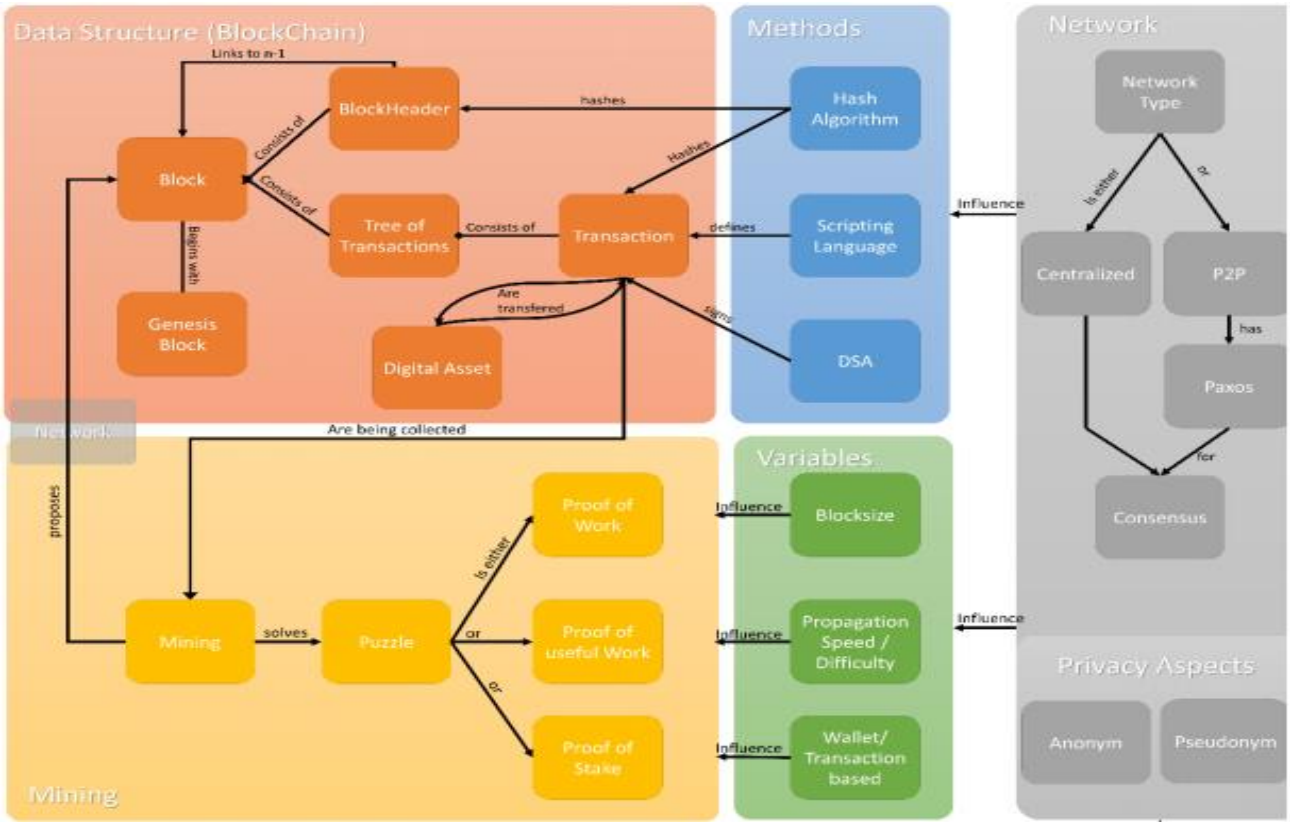

Fig.17: The Blockchain architecture

As you can see, we did not invent the wheel, in our project we are using a platform that already exists. The vast majority has already been explained in the book, but we will elaborate on major issues that have not yet been mentioned in the book.

Transactions:

Transactions are the things that give a BLOCKCHAIN purpose. They are the smallest building blocks of a BLOCKCHAIN system.
Transactions generally consist of a recipient address, a sender address, and a value. This is not too different from a standard transaction that you would find on a credit card statement.
A BLOCKCHAIN is a shared, decentralized, distributed state machine. This means that all nodes (users of the BLOCKCHAIN system) independently hold their own copy of the BLOCKCHAIN, and the current known "state" is calculated by processing each transaction in order as it appears in the BLOCKCHAIN.
Transactions are bundled and delivered to each node in the form of a block. As new transactions are distributed throughout the network, they are independently verified and "processed" by each node.

Blocks:

Blocks are created by miners (discussed in more detail below).
Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.
Blocks contain some metadata:

- Index – the block number
- previous block header hash - the reference to the previous block.
- Merkle root hash - a cryptographic hash of all of the transactions included in this block.
- Timestamp - the time that this block was created.
- Data – the data in this block (the transactions)
- nonce ("number used once") - a random value that the creator of the block used in order to hash the block.

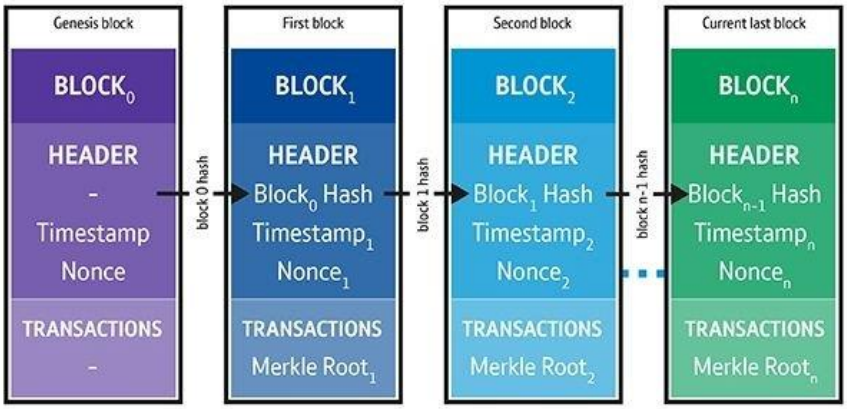

Fig.18: Block structure

Within the context of a BLOCKCHAIN, there are a few different types of blocks.

- Most blocks simply extend the current main BLOCKCHAIN. These are called "main branch blocks".
- Some blocks reference a parent block that is not at the current BLOCKCHAIN tip. These blocks are called "side branch blocks".

- Some blocks reference a parent block that is not known to the node processing the block. These are called "orphan blocks."

The "main" branch of the BLOCKCHAIN is the one that has had the most work done on it. As new blocks are appended to the BLOCKCHAIN, it becomes increasingly difficult to "overwrite" existing blocks because the most valid chain is the one that has had the most work done on it.

Mining:

Mining is the process of putting in real-world work (in the form of electricity) to create a valid block that will be accepted by the rest of the network.
Miners validate new transactions and record them on the global ledger (blockchain). On average, a block (the structure containing transactions) is mined every 10 minutes. Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm. The solution found is called the *Proof-Of-Work*. This proof proves that a miner did spend a lot of time and resources to solve the problem. When a block is 'solved', the transactions contained are considered *confirmed*, and the contract can be proceeded.

Hashing:

Hashing functions have a few properties that make them desirable for creating proof of work (POW):

- Hashing means taking an input string of any length and giving out an output of a fixed length.
- Due to the high number of bits, the probability of collisions is close to 0.
- No matter how big or small your input is, the output will always have a fixed 256-bits length.
- Ethereum uses KECCAK-256 hash function

Due to hashing, editing even a single bit of the block header will result in a different hash. Therefore, changing the nonce will create a new hash value to cross-check with the current difficulty rules. This process must be done over and over for each new potential block, until a valid hash is found.

INPUT	HASH
Hi	639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Fig.19: Hash examples

4.5. Testing

User window

Test ID	Description	Expected result	Actual results	comment
Successful bet	User enters the wallets addresses and bet amount. User press "place bet"	System checks the contract address. System checks the user address. System checks the bet amount. System saves the new contract in the Blockchain.		Bet submitted successfully

		System shows a massage "Bet submitted successfully"		
Wallet address does not exist	User entered a wallet address that does not exist. User press "place bet"	System checks the fields and detects a mistake in the address field. System shows a massage "wrong address was entered"		
Bet not in range	User entered bet amount that was not in range. User press "place bet"	System checks the fields and detects a mistake in the bet amount. System shows a massage " Bet not in range "		
Succeed to show statistics	User press on one of the statistics	System shows the information about statistics		Succeed
Failed to show statistics	User press on one of the statistics	System shows a massage "failed to show statistics "		Failed
Succeed to show site's information.	User press on one of the site's information button	System shows the information about the site		Succeed
Failed to show site's information.	User press on one of the site's information button	System shows a massage "failed to show information "		Failed

Table.1: User Window Tests

Administrator window

Test ID	Description	Expected result	Actual results	comment
Creating a game successfully	User enters the following: Game address, multiplier, wining number, min bet, max bet. User press "create new game"	System checks the Game address. System shows a massage "game successfully created"		game successfully created
Close game successfully	User press "close game"	"game successfully deleted"		Game successfully deleted
Game address does not exist	User entered a game address that does not exist. User press "create new game"	System checks the fields and detects a mistake in the address field. System shows a massage "wrong address was entered"		

Table.2: Administrator Window Tests

5. REFERANCES

Articles:

[1] Satoshi Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, [Online]. https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin *"A next generation smart contract & decentralized application platform"*, [Online]. https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] Medium – *"Legality of Gambling on the Blockchain"*, [Online]. https://medium.com/edgefund/legality-of-gambling-on-the-blockchain-26599785700f.

[4*] "How Blockchain can Solve Problems for Online Gambling Sites"* [Online]. https://www.btcmanager.com/blockchain-can-solve-problems-online-gambling-sites/

[5] Ethereum BLOCKCHAIN APP PLATFORM, [Online]. https://www.ethereum.org/

[6] *"BLOCKCHAIN Architecture"*, [online]. https://www.ibm.com/cloud/garage/architectures/blockchainArchitecture/reference-architecture/

[7] Aleksandr Bulkin, *"Explaining BLOCKCHAIN"*, [Online]. https://www.keepingstock.net/explaining-BLOCKCHAIN-how-proof-of-work-enables-trustless-consensus-2abed27f0845

[8] Nick Szabo, *"Smart Contracts: Building Blocks for Digital Markets"*, [online]. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[9] Metaphilisophy LLC and John Wiley & Sons Ltd, *"Toward a philosophy of Blockchain: a symposium"*, [online]. https://www.researchgate.net/publication/320303954_Toward_a_Philosophy_of_Blockchain_A_Symposium_Introduction_INTRODUCTION