UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

ORÁCULOS DISTRIBUIDOS EN LA BLOCKCHAIN

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN CIENCIAS MENCIÓN COMPUTACIÓN

MEMORIA PARA OPTAR AL GRADO DE INGENIERO CIVIL EN COMPUTACIÓN

FRANCISCO JAVIER ANDRÉS MONTOTO MONROY

PROFESOR GUÍA:
ALEJANDRO HEVIA

MIEMBROS DE LA COMISIÓN:
INTEGRANTE 1
INTEGRANTE2
INTEGRANTE3

SANTIAGO DE CHILE
MES AÑO

RESUMEN DE LA MEMORIA PARA OPTAR
AL TÍTULO DE
POR: FRANCISCO JAVIER ANDRÉS MONTOTO MONROY
FECHA: MES AÑO
PROF. GUÍA: ALEJANDRO HEVIA

ORÁCULOS DISTRIBUIDOS EN LA BLOCKCHAIN

Este es un resumen muy resumido

Una dedicatoria corta. Por ejemplo, A los creadores de U-Campus

Agradecimientos

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1. Gambling

Gambling is the activity of predicting events and placing a wager on the uncertain outcome of those events, with the intent of winning money or valuable goods. A wager can be put on many different events, in a casino we find randomizing devices as dices, roulette wheels, etc. which are used to get randomize events. In other establishments we can bet on sport events, such as a horse racing, football games, etc. or the minimum temperature in Santiago during this night. Its popularity and the big amounts of money at stake inevitably entails a lot of interest on this activities. Most of the time gambling is heavily regulated and taxed, also it is usual that lotteries are owned by the state.

Internet has been making cheaper to open and operate a casino, even without complying laws from any country. This and the massive internet use, has been moving the gambling industry online[19] [10]. The global Internet gambling market was estimated to be worth US$28.32 billion in 2012 and forecasted to rise to US$49.64 billion by 2017[9]. However, gambling not only takes place in casinos, lotteries or betting sites, it can also involve two or more individuals with no intermediaries. In Chile friends usually bet on their favorites football teams.

Nonetheless all the different ways for placing a bet, all of the mentioned share a common obstacle, participants are required to trust in the other parties to pay if they lose. Even if the bet takes place in a physical casino, where the law can enforce the bet, is not certain the casino will be able to pay after the resolution. We might not be aware of the fact, but every time we place a bet we are implicitly trusting in a third party, either the other player or the bet site. For physical casinos this is usually not a problem, as they are regulated by the law, any misconduct can get the casino to the justice and even get its license revoked. As there is a significant cost on starting a physical casino, them are also encouraged to keep a good reputation, in order to get customers.

Friends usually are trusted people, so trusting them when gambling might not be considered an issue. Also, probably the friendship is at risk if the bet is not paid. Other option is

to get a third friend to get the money until the bet result. Online casinos on the other hand are more problematic, there are many knowns scam schemes, as described by Griffiths[11]. And half of the players at this sites believe the providers are cheating on them[15]. However, some of them are subject of government regulation and many have being in the business for several years, this kind of characteristics could help to indicate an online site is trustworthy.

But, what if you would like to gamble in a event that no gambling site offers nor any friend want to? Probably the internet would be the place to look for somebody willing to gamble on this event. Yet, how could you trust the potential person in order to bet with him?

1.2. Cryptocurrency

Digital currency refers to any currency stored and transferred electronically. A subset of the digital currencies is called virtual currencies: them are usually defined[1] as a « *unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*».

Based on the interaction of the currency with currencies outside the community there are three types of virtual currencies: The ones with almost no interaction with the outside money, this is usually the case of video games, where its currency is only valuable within the game. A second type is where the currency can be purchased directly using other currency. Here, we observe an unidirectional flow. The third type is when the flow is bi directional, the users can sell and buy the currency. A cryptocurrency is a bi directional virtual currency, that uses cryptography for security and anti-counterfeiting measures. Virtual currencies are been historically linked to cryptography, the first known investigations [3] to establish a virtual currency where lead by David Chaum, an American cryptographer. However, despite his and others effort (e-gold[1], Ecash[4], DigiCash, LibertyReserve, among others), virtual currencies never where massively adopted.

By late 2008, using a pseudonym, was released a short whitepaper[17] with yet another virtual currency protocol specification. A few months later, during 2009 its implementation was made available as open source code. The main difference with previous implementations was its lack of a central organization, this new coin was completely decentralized. The software started to being run by some early enthusiasts and Bitcoin gave the step from an idea to an usable coin. The first years was the coins were exchanged for free among the community users. However, at some point the community was big enough and its members started to give value to the coin, then the first exchanges from and to other coins started to take place. Bitcoin transitioned into a bi directional flow virtual coin.

Then the first online exchanges between bitcoin and other currencies started to appear, the coin started to gain traction as people outside the community were able to buy and sell coins. As the money became popular, the idea was taken and a whole generation of cryptocurrencies were born. Today the market capitalization of Bitcoin (this is, the amount of money times its value in USD) is over 25,000,000,000 USD.

[1]https://www.wired.com/2009/06/e-gold/

1.3. Gambling using Cryptocurrencies

With cryptocurrencies getting more and more popular, it was only a matter of time until the first sites started to offer started to offer some games of chance an act as online casinos. Where the only difference with a traditional online casino was the currency on which the bet takes place. However, as any other currency online casino, any player who decided to play here is at the mercy of the casino. If the casino does not want or does not have the means to pay, there is nothing the participant can do and its money is lose. More on online casinos at subsection 1.1. The problems described for online casinos using traditional currencies apply in the same way to the new ones.

After some time, people started to see some potential on cryptocurrencies to solve some of the trust issues related to gamble. In 2014 Andrychowicz et al. proposed a two party randomized gambling protocol. Players are not required to trust each other in order to gamble, so even if the loser does not behave correctly the honest player, can get its prize. The protocol is not a representation of a casino game, but effectively allows player to gamble on a random event. Also in 2014, a group of Bitcoin enthusiasts started Orisi[2], a distributed oracles system for cryptocurrency contracts. Orisi allows users to access data of the outside world from the blockchain, by using a distributed set of oracles. So instead of trusting in one instance to provide the data, the trust is placed in the majority of several different oracles. More recently, on early 2017, Winsome[3] was released. Advertised as a «*Provably Fair / Trustless Casino*», Winsome is an online casino where wager are placed in a public smart contract posted in the Ethereum's blockchain. So the contract, defining the game, is enforced by the Ethereum protocol. As May 2017, they do offer two casino games, blackjack and `Rouleth`, an online roulette.

Motivated to provide an option to gamble over real world events with untrusted peers. This work proposes a protocol to define the destination of an initial wage between the two player. The decision is taken by a set of oracles, which are being paid also inside the protocol to behave correctly.

1.4. Objectives

Design and implement a distributed protocol where real world observations can be used as blockchain transaction inputs.

1.4.1. Specific Objectives

1. Provide a protocol to make possible to gamble with untrusted peers over real world events.

[2]http://orisi.org
[3]https://www.winsome.io

2. Provide the correct economic incentives to the protocol participants to behave correctly, so everyone incentives are aligned.
3. Implement a proof of concept of the designed protocol.
4. Debate of implications and other applications for the designed protocol.

1.5. Methodology

The main phases of this work will be the following:

1. Extensive review of existing proposal and implementations to solve the proposed problem or similar ones. As cryptocurrencies are a recent investigation field, this review must cover literature as well as community gathering places, such as forums and specialized blogs, magazines, etc..
2. Analysis of current solutions to the problem and similar ones.
3. Design and implementation of a protocol to solve the problem. Implementation is considered very important as the current rate of change of cryptocurrencies is considerably fast, validating the protocol within a real implementation is critical.
4. Analysis of the economic incentives of the protocol participants, to ensure protocol viability.

1.6. The Protocol

The main idea behind this work is to eliminate the more single points of trust we can when performing bets. Traditional currencies are produced and controlled at Government's will, so the first decision was to use a currency without a single controller, we chose Bitcoin mainly for two reasons. It is the first and one of the most stable currencies out there, changes are made much slower than other currencies, the market back this claim by making bitcoin the Cryptocurrency with by far the biggest market capitalization. And second, the network supporting bitcoin is much bigger than the ones for other cryptocurrencies. This makes much harder to attack and take control of the currency.

There are two mains phases in the protocol, where the first one is optional and can be replaced at players will:

1.6.1. Oracle's selection

Bitcoin (like most of the cryptocurrencies) includes a scripting language able to control money transferences, well defined and with its execution enforced by the complete bitcoin network. The challenge is to bring data from outside the bitcoin data and reason about it. Our protocol relies on several paid "oracles" to bring this data. As the oracles' output will

be used to decide who is the bet's winner, it is a crucial step to avoid a player getting itself or compromised oracles to decide the bet winner. We say this phase is optional as it might be the case both players trust already in a set of oracles.

1. The first step is to compile a list of available oracles, we use as decentralized database for this list the blockchain. Everyone willing to be an oracle can send a transaction to register into the blockchain.
2. The players negotiate some parameters, as the number of oracles to use and the threshold to decide the winner.
3. In order to decide which oracles to use, the oracles need to pick a subset of the available oracles, they do this by running a distributed coin tossing protocol. With this, they can be sure the compiled list is a random subset of the full list. If the list is big enough, the chance of one user controlling the oracles gets smaller. As it would be too expensive to control almost all the oracles in the list.

1.6.2. Bet resolution

This is phase starts after both players agree the bet with and the oracles to be used on it.

1. The players send a transaction to the blockchain with the bet description, including the IDs of the oracles they want to decide the winner. We call this transaction "Bet promise",as the players commit to the bet by placing it. The wage is also on it. The other purpose of this transaction is to invite the oracles to participate in the bet, we make its ID public so they can identify itself and inscribe to participate as oracles.
2. The oracles will see the transaction inviting them to participate in the bet, they will evaluate it and, if they are interested. They will reply with a transaction containing a reference to the "Bet promise" transacation and a small deposit as commitment that they will participate in the process.
3. When the players see the answer from the expected number of oracles, they will send the "Bet" transaction with funds of the bet and the oracles' reward. If not enough oracles reply to the call, a second invitation can be send to a different set of oracles to fill the available spots.
4. As soon as the bet event takes place, oracles are able to collect its payment from the Bet transaction. This payment gets available by making public, -voting- by the winner. After the threshold number of oracles collect its payment, the winner player is able to collect its prize, its private key and the oracle votes are required to get it.
5. After a second timeout, players can take the deposit from the oracles that did not participate in the bet resolution.

The payment of the oracle's is not the only cost of this protocol. There is a not insignificant number of transactions in the protocol, as there is a fee by each transaction in the Blockchain, this makes the protocol more expensive. This is a problem for small bets, the presented protocols is prohibitively expensive for bet of just a few dollars. At least with the current fee costs of bitcoin.

Chapter 2

Preliminaries

2.1. Hash

Hash is an overload word and it is usually used for a few different things:

2.1.1. Hash Function

Is a function able to map data from arbitraty size to data of a fixed size. The range has only elements of a fixed size, so it's bounded by all the elements of that size. If we represent the data in a binary base, the range is bounded by 2^n where n is the size in bits of the output. The domain of the function is unbounded, so by the *Pigeonhole Principle:*

$$\exists \mathrm{i}, j \mid f(\mathrm{i}) = f(j), \mathrm{i} \neq j \tag{2.1}$$

We call this a collision, and for most uses of a Hash function are unwanted.

Hash functions are used for many things: File comparison, instead of comparing files bit to bit, the image of a Hash Function can be compared instead; Hash-Tables, this allows quick lookups for the elements; Find similar records, by using a Hash Function that produces similar images for similar pre-images, etc..

2.1.2. Image of a Hash Function

If not stated otherwise, will use the word "Hash" to denote the image of some data using a Hash Function.

2.1.3. Cryptographic Hash Function

This refers to a special class of Hash Functions the Cryptography has defined to be suitable for its use on cryptographic applications. The main property this functions are designed to is to be "one way" functions, this means its infeasible[1] to invert.

In an ideal cryptographic function, the most efficient way to find one of the preimages is a brute-force search[2]. We call this property *preimage-resistance*. It is also important for this ideal function to be *collision resistance*, this means it is infeasible to find any two distinct inputs x, x' with the same image, i.e., such that $h(x) = h(x')$.

When using this ideal function producing a (second) preimage requires 2^n operations, and producing a collision requires at least $2^{n/2}$ operations[**preneel1993analysis**].

2.2. Bitcoin

Bitcoin is the first fully distributed cryptocurrency made publicly available, it was proposed in 2008 by Satoshi Nakamoto (a pseudonym) [17]. The same author shared as open source code a implementation of the protocol in January 2009. And the protocol has being running since then.

Nevertheless, Bitcoin is not the first idea of electronic cash. The idea of electronic cash has been present within the cryptographic community since at least 1983, when Chaum [3] proposed a system for anonymous payments. And the attempts kept going for other three decades, hundreds of paper have been published with improvements of e-cash schemes[2]. So, why is Bitcoin so popular and achieved the notority that three decades of academic research on the field could not achieve?

Barber et al.[2] suggest a few key points to explain why was Bitcoin the first electronic currency to take off.

1. No central point of trust. Bitcoin is a fully distributed system, there are no trusted entities in the system. The only asumption is that the majority of the network participants are honests. Every previous proposal had a central trusted entity for critical tasks, as preventing double spending and coin issuance.
2. Predictable money supply. The money supply is minted at a defined and transparent rate, defined from the begining of the protocol.
3. Transaction irreversibility. Bitcoin transactions quickly become irreversible. This is a big difference with credit cards, where chargebacks has been using largely to commit frauds.

[1] We say something is computational infeasible when even it is computable, it will require far too many resources to do it.

[2] Also known as exhaustive search, it consists of enumerating all the potential solutions and to check which of them satisfies the predicate

...	
Num Inputs	Num Outputs
$Input_0$	$Output_0$
$Input_{...}$	$Output_{...}$
$Input_{n-1}$	$Output_{m-1}$

Figure 2.1: Simplified Transaction

Bitcoin has not stopped to gain massive popularity and attention from the press. Mainly because its market capitalization (over USD 36 000 000 000), and some illegal activities it has been using to as ransom to retrieve victim's data encrypted for malicious software, or as exchange medium in one of the most famous online black market, closed in 2013 by the FBI.

The main technical advance in Bitcoin is its database, the `blockchain`[7][18]. The blockchain is a distributed database formed by an always growing list of blocks, where each block contains the data to be stored, a timestamp and a link to a previous block. Its fully distributed nature allows bitcoin to lack a central authority.

2.2.1. Transaction

Bitcoin works with accounts where coins can be stored. Accounts are identified with an address, a 25-byte value, usually encoded in the bitcoin's own encode format of base 58, resulting in a string of 25-33 characters. This address is public, and required to send bitcoins. It represents a hash of a public key. Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA)[3] to ensure the owner of an address is the only one able to spend its content.

A transaction is the only way to move bitcoins from one account to other one, it is basically a list of accounts where to get the money from and a list of accounts where the money is going to, a simplified view in the figure 2.1.

There is only one exception to this rule, the miner that builds each block is allow to send money to his account from nowhere, this is called the generation transaction and its amount is defined in the protocol. This is the only way bitcoins are generated.

A transaction input spends a previous transaction output, so it links to the previous transaction (by its hash) and to one of its outputs. Plus, in order to ve valid must have a signature from the address of the output being spent. This implies that the money from an account must be spent in the same amount the money was received. If an output of $\$10 BTC$ is received, when trying to spend it, the same amount must be spent. If willing to spend just a portion, a second output is created and send to the same account.

[3]ECDSA is a digital signature algorithm using Elliptic Curve Cryptography. It is an asymmetric scheme, with a private and public key. In bitcoin transactions are secured with a private key signature and validated using the public one.

2.2.2. Blockchain

It works as the bitcoin's ledger, it keeps record of all transactions and coin generation that had ever taken place in the protocol. It is completely distributed and public, anybody can participate in the protocol and get a copy of it. This makes simple to prevent double spending and be sure the received coins are valid, as anybody can examine where each coin came from.

As any other distributed system, the blockchain must resolve the consesus problem [8]. Get all the participants to agree on the data. This is a fundamental problem to any distributed system. In the the blockchain anybody with an internet connection can be part of the protocol, so solving this problem is quite challenging. Some authors argue the blockchain is the first practical solution to the Byzantine Consensus problem [16] [20].

Proof of work is the algorithm used by the bitcoin blockchain to seek consensus. Each entity trying to add data to the database must prove it has done some required work. This algotithms was designed originally to fight the email spam, by requiring the sender of an email to prove a small work was done in order to send the email[6]. It works by using a hard to calculate, but easy to check function. This way the receiver or the mail server can easily check if the sender did the required work, however this work was much harder. The difficulty of a work is defined by the amount of computational power required to get it done.

The atomical piece in the blockchain is the block. Each valid block carries transactions of the protocol and a proof of work. So every entity trying to get a valid block into the database need to collect transactions and solve the puzzle to get a valid proof of work for its block. This process is called mining, therefore the entities trying to get a valid block are called miners. A block is linked to the previous one, as show by the figure 2.5. Once block is produced, all the others miners need to delete the transactions added by the block from the one they are building and update the link to the new last block. And they start to mine a new block. By design a block must be produced every 10 minutes, so the work required to mine a block is a ajusted periodically to met this goal.

The proof of work consists in building a block with a hash under a threshold value, so the miners should reorder and change the block until the hash fulfill the requirement. There is not a known algorithm to do this in a better way than brute force, so the only method to get a hash that mets the criteria is to try with different block configurations, there are also some bytes of nonce, a timestamp and transactions to be changes to get different hashes.

The structure of a Bitcoin block is show in the figure 2.2, the fields with the gray background represents the block header, the data hashed to get the block's hash. The transactions are indirectly hashed in the Merkle Root[4].

As expected in a protocol with many participants, there are times were more than one block is generated with the same parent (figure 2.6), this is call a fork. In order to achieve

[4]A `Merkle Tree` is a tree in which each non leaf node is labeled with the hash of its children's labels. In the block each transaction is mapped into a tree leaf. So the root of this tree hashes all the transactions

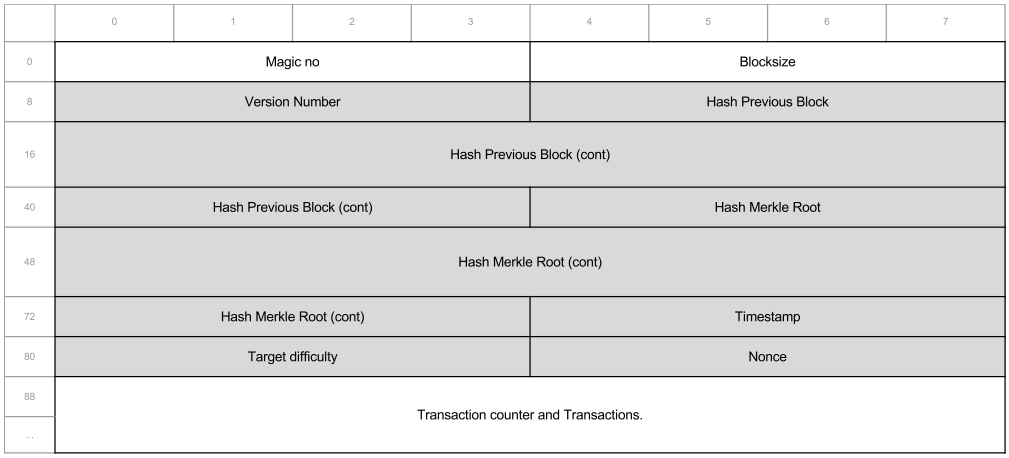

Figure 2.2: Block Structure

consensus, the protocol determines that the chain with more work[5] on it is the active chain. So when a fork happen there are two active chains, while having a non unique active chain miners will try to mine in any of the candidates with the same work. A block mined on one of the branches will decide which is the active one because it adds more work to the chain. However the situation that originated the fork can repeat itself and prevent to have one consensus branch, this is very unlikely[**decker2013information**] to happen during a long time.

2.2.3. Script

When sending money, there is a little more than we saw at section 2.2.1. In an input (figure 2.3 there is more than a signature, and at each output (figure 2.4) also more than an address.

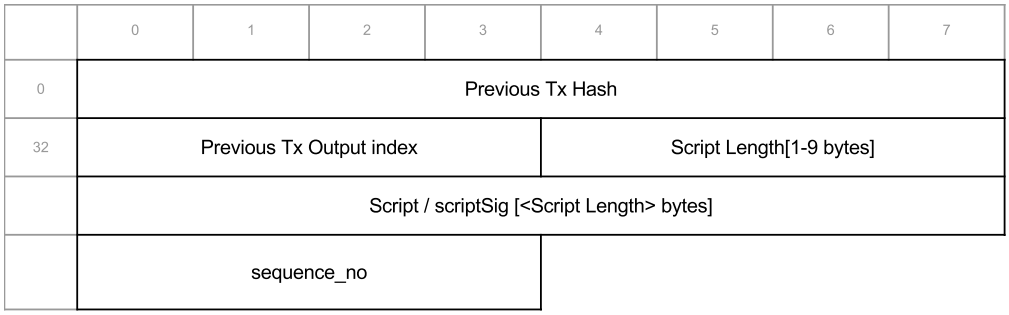

Figure 2.3: Wire format of an Input.

An output does not send money to a given address, but defines how the money can be spent. Currently there are two formats in use. The most used is called “Pay To Public Key Hash” (P2PKH)[6]. And “Pay To Script Hash” (P2SH).

[5]The amount of work in a chain is the sum of the difficulty of every block on it.

[6]The key hash is the address of an account

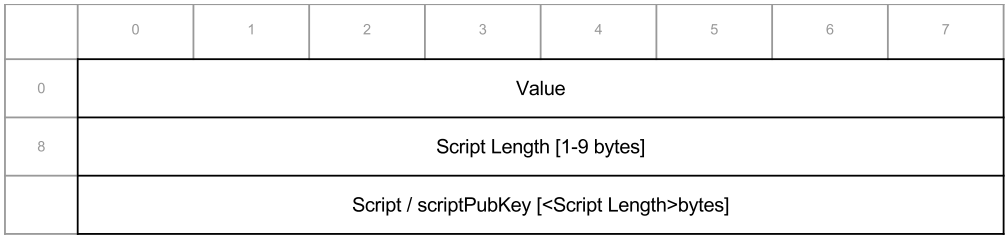

Figure 2.4: Wire format of an Output.

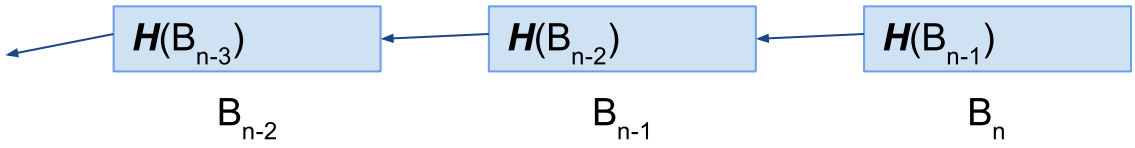

Figure 2.5: Blocks linked to each other in the blockchain.

As the figure 2.4 shows, the output have a script on its wire representation, this script is written in a small stack based language. It is read from left to right and it is purposefully not Turing-complete. The script is evaluated using the scriptSig as input. If the transaction willing to spend this output provides a valid[7] scriptSig, the output is available to be spend. This is how a P2PKH script looks like:

Listing 2.1: P2PKH script.

```
OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

It receives two values as input: <pubKeyHash> and <sig>. And the execution looks like:

The chain structure gives a chronological order to the transactions in the protocol, so it makes clear to check if a transaction is valid. Any participant willing to probe the validity of the tramsaction needs to check the block where the output being spend is stored up to the current block and see if the money was already spent in a different transaction.

[7] A script is considered valid if after its execution the value in the top of the stack is True.

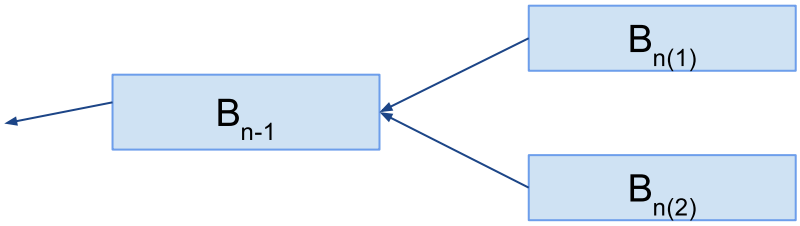

Figure 2.6: A fork in the blockchain.

Table 2.1: Script evaluation to check a P2PKH transaction.

Stack	**Script**
Constants from scriptSig are copied to the stack.	
<pubKey> <sig>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
OP_DUP copies the top element from the stack.	
<pubKey> <pubKey> <sig>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
The hash of the top element is calculated.	
H(<pubKey>) <pubKey> <sig>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
The destination address is moved to the stack.	
<pubKeyHash> H(<pubKey>) <pubKey> <sig>	OP_EQUALVERIFY OP_CHECKSIG
The destination address is compared with the Hash of the Public Key (PK) provided by the sig Script. This check the provided Public Key is the one from the intended receiver.	
<pubKey> <sig>	OP_CHECKSIG
Using the already verified PK, the script checks the transaction was signed using the corresponding Private Key. This step secures the transaction from tampering an proves it was sent by the private Key controller.	
True	

2.3. Previous Work

2.3.1. Distributed oracles

Orisi

Orisi[14] is a distributed system for bitcoin smart contracts that relies in multiple oracles to bring information from outside of the blockchain. It allows its users to transfer money from one address to another when a condition is met.

Both players agree on 7 oracles to be used to decide the transfer, usually chosen from "The Oracle List", a curated list with oracles. But could also be chosen from any other place the players want. Then, a multisignature address is generated to store the money while the bet takes place. A multisignature address is defined by `m` addresses and a required number `n` (`n` $<$ `m`) of them to sign. A valid signature for a multisignature address is generated by using at least `n` out of the `m` addresses defining it.

The multisignature address generated will store the money until the oracles decide where the transaction goes. To avoid the oracles sending the money to themselves the multisignature transaction include the address of the receiver, so we want a $1 + (n \text{ of } m)$, where the extra signature is from the receiver. As this kind of transaction is not considered standard [8], Orisi uses a bigest multisignature address, where instead of using n out of m oracles, it adds more receiver keys. Requiring $m + 1$ signatures of $2m$ - $n + 1$. With this configuration the oracles are not able to move the money by themselves, and at least one signature from the receiver is required.

2.3.2. Trustless distributed casino

Winsome.io

In may 2016 Rouleth[12] was launched as a distributed application on the ethereum network. Offering its players a "provably-fair", real money roulette. Later, in early 2017, also using the ethereum network "BlockJack" was launched, the first playable blackjack game on the Ethereum mainnet.

Winsome.io is the instance where these games are enclosed, it offers unique advantages over traditional casinos (physical and virtual), like trusless, and complete control over the funds the entire time while playing. It does work in a distributed fashion using smart contracts, publicly availables for everyone's scrutiny.

Winsome.io provides its users trustless gambling over random events, by using the ethereum

[8] Non standard is recognized as a valid transaction by everyone, however by the time this article was written only about the 5% of the mining power will not process it. Including this transaction in the blockchain will take on average much more time than a standard one.

network as backend. It have been quite successful, it is one of the most popular descentralized applications on the Ethereum Network.

2.3.3. Secured data feeds

Oraclize

Oraclize[13] provides an interface for using data fetched from a web site in the ethereum blockchain, it works with arbitrary URLs or queries in certain web services, as "Wolfram Alpha" [9]. It provides an Authenticity Proof of the data gathered, so the user can check the data provided by the interface was generated by the source and have not been tampered.

Town Crier

Town Crier[21] is an authenticated data feed system for the ethereum blockchain, as oraclize it works as a bridge between web feeds, and the blockchain. It uses an Intel technology called "Software Guard Extensions"[5], than provide some execution guarantees of the software executed by hardware protected areas. This protects the execution of the data feed even with the the host OS, BIOS or any other piece of the machine compromised.

[9]Wolfram Alpha is a knowledge engine, able to answer queries rather than provide links to data sources, as a search engine does.

Chapter 3

Primero

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Definición 3.1 (ver) *Definición definitiva*

$$\frac{\mathrm{d}}{\mathrm{d}x}\int_a^x f(y)\mathrm{d}y = f(x).$$

Chapter 4

Segundo

Quisque facilisis auctor sapien. Pellentesque gravida hendrerit lectus. Mauris rutrum sodales sapien. Fusce hendrerit sem vel lorem. Integer pellentesque massa vel augue. Integer elit tortor, feugiat quis, sagittis et, ornare non, lacus. Vestibulum posuere pellentesque eros. Quisque venenatis ipsum dictum nulla. Aliquam quis quam non metus eleifend interdum. Nam eget sapien ac mauris malesuada adipiscing. Etiam eleifend neque sed quam. Nulla facilisi. Proin a ligula. Sed id dui eu nibh egestas tincidunt. Suspendisse arcu.

Maecenas dui. Aliquam volutpat auctor lorem. Cras placerat est vitae lectus. Curabitur massa lectus, rutrum euismod, dignissim ut, dapibus a, odio. Ut eros erat, vulputate ut, interdum non, porta eu, erat. Cras fermentum, felis in porta congue, velit leo facilisis odio, vitae consectetuer lorem quam vitae orci. Sed ultrices, pede eu placerat auctor, ante ligula rutrum tellus, vel posuere nibh lacus nec nibh. Maecenas laoreet dolor at enim. Donec molestie dolor nec metus. Vestibulum libero. Sed quis erat. Sed tristique. Duis pede leo, fermentum quis, consectetuer eget, vulputate sit amet, erat.

Donec vitae velit. Suspendisse porta fermentum mauris. Ut vel nunc non mauris pharetra varius. Duis consequat libero quis urna. Maecenas at ante. Vivamus varius, wisi sed egestas tristique, odio wisi luctus nulla, lobortis dictum dolor ligula in lacus. Vivamus aliquam, urna sed interdum porttitor, metus orci interdum odio, sit amet euismod lectus felis et leo. Praesent ac wisi. Nam suscipit vestibulum sem. Praesent eu ipsum vitae pede cursus venenatis. Duis sed odio. Vestibulum eleifend. Nulla ut massa. Proin rutrum mattis sapien. Curabitur dictum gravida ante.

Phasellus placerat vulputate quam. Maecenas at tellus. Pellentesque neque diam, dignissim ac, venenatis vitae, consequat ut, lacus. Nam nibh. Vestibulum fringilla arcu mollis arcu. Sed et turpis. Donec sem tellus, volutpat et, varius eu, commodo sed, lectus. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Quisque enim arcu, suscipit nec, tempus at, imperdiet vel, metus. Morbi volutpat purus at erat. Donec dignissim, sem id semper tempus, nibh massa eleifend turpis, sed pellentesque wisi purus sed libero. Nullam lobortis tortor vel risus. Pellentesque consequat nulla eu tellus. Donec velit. Aliquam fermentum, wisi ac rhoncus iaculis, tellus nunc malesuada orci, quis volutpat dui magna id mi. Nunc vel ante. Duis vitae lacus. Cras nec ipsum.

Morbi nunc. Aliquam consectetuer varius nulla. Phasellus eros. Cras dapibus porttitor risus. Maecenas ultrices mi sed diam. Praesent gravida velit at elit vehicula porttitor. Phasellus nisl mi, sagittis ac, pulvinar id, gravida sit amet, erat. Vestibulum est. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Curabitur id sem elementum leo rutrum hendrerit. Ut at mi. Donec tincidunt faucibus massa. Sed turpis quam, sollicitudin a, hendrerit eget, pretium ut, nisl. Duis hendrerit ligula. Nunc pulvinar congue urna.

Nunc velit. Nullam elit sapien, eleifend eu, commodo nec, semper sit amet, elit. Nulla lectus risus, condimentum ut, laoreet eget, viverra nec, odio. Proin lobortis. Curabitur dictum arcu vel wisi. Cras id nulla venenatis tortor congue ultrices. Pellentesque eget pede. Sed eleifend sagittis elit. Nam sed tellus sit amet lectus ullamcorper tristique. Mauris enim sem, tristique eu, accumsan at, scelerisque vulputate, neque. Quisque lacus. Donec et ipsum sit amet elit nonummy aliquet. Sed viverra nisl at sem. Nam diam. Mauris ut dolor. Curabitur ornare tortor cursus velit.

Morbi tincidunt posuere arcu. Cras venenatis est vitae dolor. Vivamus scelerisque semper mi. Donec ipsum arcu, consequat scelerisque, viverra id, dictum at, metus. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut pede sem, tempus ut, porttitor bibendum, molestie eu, elit. Suspendisse potenti. Sed id lectus sit amet purus faucibus vehicula. Praesent sed sem non dui pharetra interdum. Nam viverra ultrices magna.

Aenean laoreet aliquam orci. Nunc interdum elementum urna. Quisque erat. Nullam tempor neque. Maecenas velit nibh, scelerisque a, consequat ut, viverra in, enim. Duis magna. Donec odio neque, tristique et, tincidunt eu, rhoncus ac, nunc. Mauris malesuada malesuada elit. Etiam lacus mauris, pretium vel, blandit in, ultricies id, libero. Phasellus bibendum erat ut diam. In congue imperdiet lectus.

Aenean scelerisque. Fusce pretium porttitor lorem. In hac habitasse platea dictumst. Nulla sit amet nisl at sapien egestas pretium. Nunc non tellus. Vivamus aliquet. Nam adipiscing euismod dolor. Aliquam erat volutpat. Nulla ut ipsum. Quisque tincidunt auctor augue. Nunc imperdiet ipsum eget elit. Aliquam quam leo, consectetuer non, ornare sit amet, tristique quis, felis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque interdum quam sit amet mi. Pellentesque mauris dui, dictum a, adipiscing ac, fermentum sit amet, lorem.

Ut quis wisi. Praesent quis massa. Vivamus egestas risus eget lacus. Nunc tincidunt, risus quis bibendum facilisis, lorem purus rutrum neque, nec porta tortor urna quis orci. Aenean aliquet, libero semper volutpat luctus, pede erat lacinia augue, quis rutrum sem ipsum sit amet pede. Vestibulum aliquet, nibh sed iaculis sagittis, odio dolor blandit augue, eget mollis urna tellus id tellus. Aenean aliquet aliquam nunc. Nulla ultricies justo eget orci. Phasellus tristique fermentum leo. Sed massa metus, sagittis ut, semper ut, pharetra vel, erat. Aliquam quam turpis, egestas vel, elementum in, egestas sit amet, lorem. Duis convallis, wisi sit amet mollis molestie, libero mauris porta dui, vitae aliquam arcu turpis ac sem. Aliquam aliquet dapibus metus.

Vivamus commodo eros eleifend dui. Vestibulum in leo eu erat tristique mattis. Cras at elit. Cras pellentesque. Nullam id lacus sit amet libero aliquet hendrerit. Proin placerat, mi non elementum laoreet, eros elit tincidunt magna, a rhoncus sem arcu id odio. Nulla

eget leo a leo egestas facilisis. Curabitur quis velit. Phasellus aliquam, tortor nec ornare rhoncus, purus urna posuere velit, et commodo risus tellus quis tellus. Vivamus leo turpis, tempus sit amet, tristique vitae, laoreet quis, odio. Proin scelerisque bibendum ipsum. Etiam nisl. Praesent vel dolor. Pellentesque vel magna. Curabitur urna. Vivamus congue urna in velit. Etiam ullamcorper elementum dui. Praesent non urna. Sed placerat quam non mi. Pellentesque diam magna, ultricies eget, ultrices placerat, adipiscing rutrum, sem.

Conclusión

Mauris ac ipsum. Duis ultrices erat ac felis. Donec dignissim luctus orci. Fusce pede odio, feugiat sit amet, aliquam eu, viverra eleifend, ipsum. Fusce arcu massa, posuere id, nonummy eu, pulvinar ut, wisi. Sed dui. Vestibulum nunc nisl, rutrum quis, pharetra eget, congue sed, dui. Donec justo neque, euismod eget, nonummy adipiscing, iaculis eu, leo. Duis lectus. Morbi pellentesque nonummy dui.

Aenean sem dolor, fermentum nec, gravida hendrerit, mattis eget, felis. Nullam non diam vitae mi lacinia consectetuer. Fusce non massa eget quam luctus posuere. Aenean vulputate velit. Quisque et dolor. Donec ipsum tortor, rutrum quis, mollis eu, mollis a, pede. Donec nulla. Duis molestie. Duis lobortis commodo purus. Pellentesque vel quam. Ut congue congue risus. Sed ligula. Aenean dictum pede vitae felis. Donec sit amet nibh. Maecenas eu orci. Quisque gravida quam sed massa.

Nunc euismod, mauris luctus adipiscing pellentesque, augue ligula pellentesque lectus, vitae posuere purus velit a pede. Phasellus leo mi, egestas imperdiet, blandit non, sollicitudin pharetra, enim. Nullam faucibus tellus non enim. Sed egestas nunc eu eros. Nunc euismod venenatis urna. Phasellus ullamcorper. Vivamus varius est ac lorem. In id pede eleifend nibh consectetuer faucibus. Phasellus accumsan euismod elit. Etiam vitae elit. Integer imperdiet nibh. Morbi imperdiet orci euismod mi.

Figure 4.1: Logo de la Facultad

Donec tincidunt tempor metus. Aenean egestas cursus nulla. Fusce ac metus at enim viverra lacinia. Vestibulum in magna non eros varius suscipit. Nullam cursus nibh. Mauris neque. In nunc quam, convallis vitae, posuere in, consequat sed, wisi. Phasellus bibendum consectetuer massa. Curabitur quis urna. Pellentesque a justo.

In sit amet dui eget lacus rutrum accumsan. Phasellus ac metus sed massa varius auctor. Curabitur velit elit, pellentesque eget, molestie nec, congue at, pede. Maecenas quis tellus non lorem vulputate ornare. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Etiam magna arcu, vulputate egestas, aliquet ut, facilisis ut, nisl.

Donec vulputate wisi ac dolor. Aliquam feugiat nibh id tellus. Morbi eget massa sit amet purus accumsan dictum. Aenean a lorem. Fusce semper porta sapien.

Campo 1	Campo 2
Valor 1	Valor2

Table 4.1: Tabla 1

Curabitur sit amet libero eget enim eleifend lacinia. Vivamus sagittis volutpat dui. Suspendisse potenti. Morbi a nibh eu augue fermentum posuere. Curabitur elit augue, porta quis, congue aliquam, rutrum non, massa. Integer mattis mollis ipsum. Sed tellus enim, mattis id, feugiat sed, eleifend in, elit. Phasellus non purus sed elit viverra rhoncus. Vestibulum id tellus vel sem imperdiet congue. Aenean in arcu. Nullam urna justo, imperdiet eget, volutpat vitae, semper eu, quam. Sed turpis dui, porttitor ut, egestas ac, condimentum non, wisi. Fusce iaculis turpis eget dui. Quisque pulvinar est pellentesque leo. Ut nulla elit, mattis vel, scelerisque vel, blandit ut, justo. Nulla feugiat risus in erat.

Bibliography

[1] Europen Central Bank. Virtual Currency Schemes. 2012. URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (visited on 01/03/2017).

[2] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. Bitter to better—how to make bitcoin a better currency. In *International conference on financial cryptography and data security*. Springer, 2012, pages 399–414.

[3] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*. Springer, 1983, pages 199–203.

[4] David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In *Proceedings on advances in cryptology*. Springer-Verlag New York, Inc., 1990, pages 319–327.

[5] Victor Costan and Srinivas Devadas. Intel sgx explained. *Iacr cryptology eprint archive*, 2016:86, 2016.

[6] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Annual international cryptology conference*. Springer, 1992, pages 139–147.

[7] Liam Edwards-Playne. The invention of the blockchain. 2013. URL: https://medium.com/@liamzebedee/the-invention-of-the-blockchain-fe25be0caebc (visited on 05/24/2017).

[8] Michael J Fischer. The consensus problem in unreliable distributed systems (a brief survey). In *International conference on fundamentals of computation theory*. Springer, 1983, pages 127–140.

[9] Sally M Gainsbury, Alex Russell, Robert Wood, Nerilee Hing, and Alex Blaszczynski. How risky is internet gambling? a comparison of subgroups of internet gamblers based on problem gambling status. *New media & society*, 17(6):861–879, 2015.

[10] Mark Griffiths and Andrew Barnes. Internet gambling: an online empirical study among student gamblers. *International journal of mental health and addiction*, 6(2):194–204, 2008.

[11] MD Griffiths. Crime and gambling: a brief overview of gambling fraud on the internet. *Internet journal of criminology*, 2010.

[12] Hrishikesh Huilgolkar.

[13] John Ferlito John Ferlito Robert Lord. Oraclize docs. 2016. URL: http://docs.oraclize.it/ (visited on 07/09/2017).

[14] Tomasz Kolinko and the Orisi team. Orisi white paper. 2014. URL: https://github.com/orisi/wiki/wiki/Orisi-White-Paper.

[15] John L McMullan and Aunshul Rege. Online crime and internet gambling. *Journal of gambling issues*:54–85, 2010.

[16] Andrew Miller and Joseph J LaViola Jr. Anonymous byzantine consensus from moderately-hard puzzles: a model for bitcoin, 2014.
[17] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system. 2008.
[18] John Naughton. Is blockchain the most important it invention or our age? 2016. URL: https://www.theguardian.com/commentisfree/2016/jan/24/blockchain-bitcoin-technology-most-important-tech-invention-of-our-age-sir-mark-walport (visited on 05/24/2017).
[19] Bhiru Shelat and Florian N Egger. What makes people trust online gambling sites? In *Chi'02 extended abstracts on human factors in computing systems*. ACM, 2002, pages 852–853.
[20] Felix Sun and Peitong Duan. Solving byzantine problems in synchronized systems using bitcoin, 2014.
[21] Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. Town crier: an authenticated data feed for smart contracts. In *Proceedings of the 2016 acm sigsac conference on computer and communications security*. ACM, 2016, pages 270–282.