Bachelor thesis
Computer Science

Radboud University

Why do we need/want cryptocurrency

Author:
Tom Nijholt
S4432037

First supervisor/assessor:
Prof. Lejla Batina
lejla@cs.ru.nl

Second supervisor:
Paulus Meessen
pmeessen@cs.ru.nl

Second assessor:
title, name
e-mail adress

May 31, 2018

Abstract

The abstract of your thesis is a brief description of the research hypothesis, scientific context, motivation, and results. The preferred size of an abstract is one paragraph (*"alinea"*) or one page of text.

Contents

Chapter 1

Introduction

The introduction of your bachelor thesis introduces the research area, the research hypothesis, and the scientific contributions of your work. A good narrative structure is the one suggested by Simon Peyton Jones [6]:

- describe the problem / research question
- motivate why this problem must be solved
- demonstrate that a (new) solution is needed
- explain the intuition behind your solution
- motivate why / how your solution solves the problem (this is technical)
- explain how it compares with related work

Chapter 2

Preliminaries

2.1 Hashes

Hashes are outputs of hash functions. Hash functions are functions that create an output of fixed length that is unique to an input of arbitrary length. Cryptographic hash functions are a subgroup of hash functions which have the following security related properties:

- Pre-image resistance: Given a hash it is infeasible to find an input that results in the hash.
- Second pre-image resistance: Given an input it is infeasible to find another input such that they both result in the same hash.
- Collision resistance: It is infeasible to find two inputs which result in the same hash.

2.1.1 Example

$SHA256$(lorem ipsum dolor sit amet consectetur adipiscing elit) $\rightarrow$
$25217898FFAD2F0788F94385871161BCA4F362FCDA39B8664A1D162A5AC66425$

A small change in the input causes a significantly different output, making it impossible to link the inputs to each other.

$SHA256$(lorem ipsum dolor sit amet consectetur adipiscing elit.) $\rightarrow$
$869FC986CC40487D0D4DAA9A33D0F1576503D0FEFA744A41E1B34AD2FCDF73D2$

There is no inverse function and hashing the output does not result in the input.

$SHA256(25217898FFAD2F0788F94385871161BCA4F362FCDA39B8664A1D162A5AC66425) \rightarrow$
$2D7EEA5EE19D5BB42EDE44E2C9B76404E59BC58152B7F8F9AA94BFEA8FC2244C$

It is unpredictable what the output of the hash function will be. Thus, in order to find an output that is below a certain value one has to try different inputs until they find an input that is below the value.

2.2 ElGamal

2.3 DSA

DSA stands for digital signature algorithm.[1] It is a method which allows verification whether some data is indeed signed by some party. A digital signature algorithm consists of two main components: signature generation and signature verification. For signature generation a hash is created from some data or message. This is then combined with a private key through a signature generation function outputting a signature. The signature verification component consists of creating a hash of the data or message and then using this hash with the signature and corresponding public key as input in a signature verification function. The signature verification function then outputs whether the claimed signer has indeed signed the data.

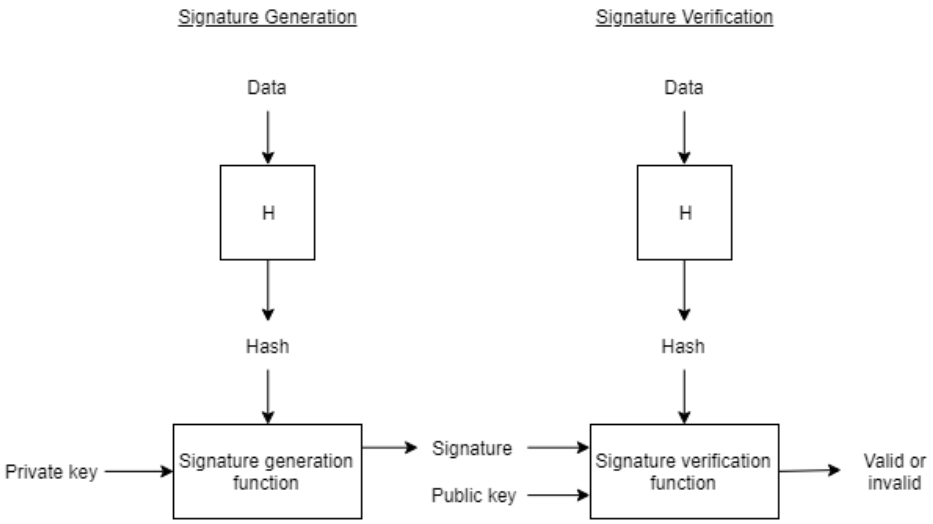

Figure 2.1: General DSA algorithm as described in[2].

Standard DSA signatures consist of a tuple (r, s) where:
x =the private key,
y = the public key, where $y = g^x \mod p$,
k = an unique secret number,
p, q = generated primes,
g = generator of a subgroup of order q in the multiplicative group of $GF(p)$,

[1] `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf`

such that $1 < g < p$,
H = a hash function
$r = (g^k \mod p) \mod q$
z =the leftmost $min(N$,outlen) bits of $H(M)$
$s = (k^{-1}(z + xr)) \mod q$

2.4 Blind signature scheme

Blind signatures were introduced by David Chaum.[1] They are digital signatures wherein a message is blinded, hiding its contents, before it is signed. Blind signatures can be conceptualized in a voting system as follows:

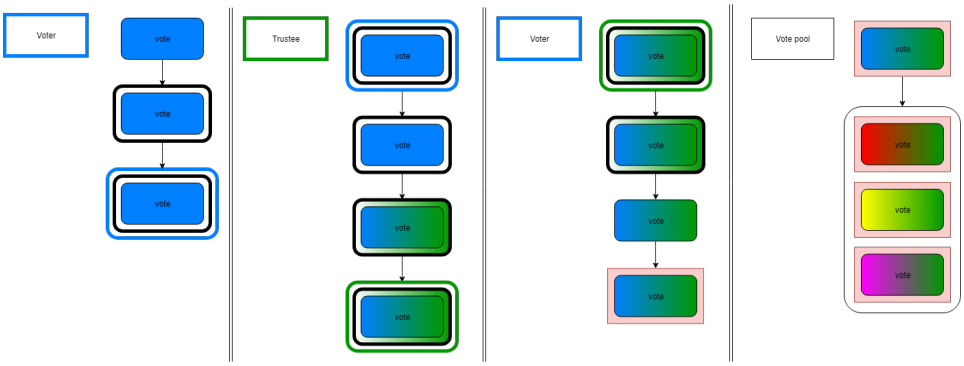

Figure 2.2: An overview of the blind signature scheme. Blue-filled boxes are ballots which contain the vote of the voter. Green-filled boxes are ballots that are signed by the trustee. A green and blue-filled box is a vote of a voter with a signature of the trustee.

A voter writes a vote on a ballot, puts this in a carbon lined envelope, puts this envelope in a new envelope with their own return address on it and finally sends it to a trustee. The trustee checks the return address, unpacks the outer envelope, signs the carbon lined envelope (and with it the ballot), encases the carbon lined envelope in a new envelope and sends it back to the return address. The voter opens the envelopes and puts the signed ballot in a new universal envelope. When the time to vote arrives, the voter sends the universal envelope to the trustee and it is added to the pool of votes. To truly finish this scheme all ballots need to be displayed in public. Then anybody can check the signatures and the legitimacy of the votes. If voters have some identifying aspect on their paper which only they know about they are also able to tell whether their vote is actually on display. Furthermore, this scheme provides unlinkability between the vote and the voter as no party besides the voter has actually seen what is on the ballot.

Chapter 3

Research

In this section we describe the main contributions of this paper. We review the goals of cryptocurrency, whether these are achieved or not, legality, future goals in cryptocurrency, challenges in cryptocurrency.

3.1 Why this subject

Cryptocurrencies are very popular at the moment. Many people don't really *understand* it yet. Which is understandable since it is very *new*. Most cryptocurrencies are really not fully developed yet and have active goals that their developers wish to fulfill. Nevertheless *a lot of money* has been made with cryptocurrencies and financial sectors invest heavily in it. With cryptocurrencies become a larger part of society a couple questions arise:

- What is the purpose of cryptocurrencies?
- Do we want to use cryptocurrencies?
- Should we use cryptocurrencies?
- Why do we not just use the standard banking system?
- Are cryptocurrencies legal?
- Do we want anonymous cryptocurrencies?
- Are we bending to far from the original goal of cryptocurrencies?
- Has the original goal developed into something new?
- Is the only reason for cryptocurrencies financial gain at the moment?

These questions are of interest to me(/seem significant), and I will attempt to provide a substantiated answer.

3.2 Why Cryptocurrencies

In order to find the initial reason for developing cryptocurrencies we need to look back to the first conceiving of a cryptocurrency which started in 1983 in a proposal by David L. Chaum called "Blind signatures for untraceable payments"[1]. In this article David L. Chaum notes that payments are being automated by electronic payment systems and argues his belief that these electronic payment systems can have a large impact on our personal privacy as well as possible crime. He argues that a third party's knowledge about transactions can expose the individual and diminish their privacy. But a system providing too much privacy is also not desirable as it lacks control and security in the form of lack of proof of payment, theft, black payments, tax evasion, and black markets.
He proposes the usage of a new kind of cryptography, which achieves both a certain degree of privacy as well as providing control and security. The scheme that he thereafter proposes is the basic groundwork for the first ever cryptocurrency, ecash.

(Important note: David L. Chaum argues against anonymity!)

3.3 Properties and challenges of currency

In order for something to be a currency it must adhere to the definition of currency. In economics, currency is defined as the system of money that is used in a particular country at a particular time. [1]

The first question is thus whether the assumed currency adheres to the definition of a system of money. The functional definition of money lists money having multiple functions[4]:

- Money is a medium of exchange.
- Money is a standard of value.
- Money is a store of value.

Crypto money must thus be usable as a medium of exchange. You must be able to exchange it for goods or services. One must be confident that when walking into a store in a country of the medium of exchange that the money will be accepted as a method of payment.

A standard of value or unit of account is an agreed upon worth for a transaction in a country's medium of exchange.[2] In the country of the

[1] `https://dictionary.cambridge.org/dictionary/english/currency#dataset-business-english`

[2] `https://www.investopedia.com/terms/s/standard-of-value.asp`

medium of exchange, goods, services and debts are quoted in the amount of money.

Store of value signifies the ability to save money, retrieve it and exchange it later.[4] For example, I can work a day and be compensated in money. I can use the money today but also store it and use it at a later point in time. [3] A good store of value does not fluctuate much.

3.3.1 Applicability of currency definition

Almost all of the functional definitions of money described above are not applicable to any cryptocoins at the moment. This is mostly because no country has adopted a cryptocoins as its official medium of exchange. At the time of writing there is no cryptocoins which completely satisfies the function of medium of exchange. There are a lot of merchants that accept cryptocoins, but since there is no country where you can reasonably expect to be able to pay everything with a certain cryptocurrency this properties is not satisfied by any cryptocoin. Similarly, cryptocoins do not function as a standard value since there is no country that expresses prices of goods, services and debts in cryptocoins. There are however some cryptocoins that do have the function of store of value. Bitcoin is an example of this. You can store bitcoin, retrieve it and exchange it at a later date. It is not a great store of value though, since a good store of value does not fluctuate much and bitcoin fluctuates a lot. Fiat currencies usually have government backing to ensure stability in fluctuation. There is currently only one government backed cryptocurrency which is the Sovereign backed by the Marshall Islands. Alternatives to government backed currencies are oil-backed and gold-backed. Government backing means that the government guarantees the value of the money. In the case of oil and gold-backed currencies it is guaranteed that a certain amount of the currency translates directly to a constant amount of oil or gold.

3.3.2 Adoption

Thus, cryptocurrencies are really not currencies at all according to the definition. However, cryptocurrencies arguably merely need proper adoption by a country. Adoption by a country (and its people) could result in:

- it becoming a medium of exchange, since every store must accept payment in the currency.
- it becoming a standard of value. When everybody in a country uses it, it seems only natural that prices and debts will be valued in it as well, assuming steady value of the currency.

[3] https://www.investopedia.com/terms/s/storeofvalue.asp

- it becoming a store of value. Assuming that the currency will be government backed it will not fluctuate too heavily and value will be guaranteed by the government. US Dollar is however not backed by anything but faith in the value. However since US dollars are legal tender they are backed by all the services and goods available in the US since they can be bought with dollars.

Need more sources or reasoning for above.

This is however open to speculation and more issues related to this may be missed with this general view.

The current definition of currency is very much centred about it being recognised within the boundaries of a country. Cryptocurrencies are however not generally recognised by countries. This likely has to do with the fact that most cryptocurrencies do not originate from countries. Changing "countries" to "a large group of peers" in the traditional definition can cause some cryptocurrencies, at least bitcoin, to be considered a currency.

Is this for all currency? as well for fiat currency? Needs more motivation and source! Alles subkopje van adoptie. Meer structuur. Wat zijn de design goals van geld?

3.3.3 Adoption of a currency

The desired result with implementing a new currency is widespread adoption and recognition. Widespread adoption is a result of merchants and users wanting to use a currency. Below I have identified some properties which are generally considered important for widespread adoption. Most of these principles are applicable to currency in general, but some are specific to cryptocurrencies. It is important to keep in mind that some of these properties need not have perfect solutions but merely be better than the current standard.

- Double spending
- Transaction cost
- Volatility
- Security
- Transaction speed
- Market liquidity and Convertibility
- Auditability
- Anonymity/Pseudonymity

3.3.4 Double spending

Double spending is the problem of the same money being spent twice. With physical money this is the equivalent of spending both a valid 10 euro note and a copy of it. Since digital currency is merely a set bits and bytes it is simple to make a copy of a coin. The original and copy could then both be spent and someone could create money out of other money. To prevent this some protocol should check whether a coin is spent such that a copy cannot be spent again.

3.3.5 Transaction cost

Transaction costs must be lower than the standard or other benefits must be worth the extra costs. Transaction costs are one of the key determinants of net returns. Lower transaction costs mean higher returns. Furthermore lower transactions costs help to achieve optimal allocation of resources. According to research it always pays off to reduce transactions costs unless it diminishes quality of service.[3]

3.3.6 Volatility

Volatility is a statistical measure of the dispersion of returns for a given security or market index.[4] A certain amount of volatility is important for investment companies and foreign currency exchanges since they use volatility to generate profit. However, a currency that has very high volatility is not desirable since you cannot safely use it for storing of value and prices of goods and services may fluctuate heavily. Heavy fluctuation is undesirable since it might mean that one day you can buy a whole bread with your money and the next you canb only buy a slice of bread with the same amount.

3.3.7 Security

It must not be easy to steal money. Consider the case of an easy to steal currency. Nobody would want to hold it since it might just be stolen from them. When money is easily stolen trust in the currency decreases and it cannot be considered a functional store of value.

3.3.8 Transaction speed

Consider the case of transactions taking a long time. One enters a store and buys something, transfers the money but then has to wait a long time for the transaction to complete. It is simply not practical to wait a long time for a

[4] `https://www.investopedia.com/terms/v/volatility.asp`

transaction to complete. Furthermore in stock trading and finance trading it is even more important that transactions are fast since prices change rapidly.

3.3.9 Market liquidity and Convertibility

Market liquidity and convertibility refers to the extent to which a currency can be quickly traded into other assets for stable prices. Liquid markets are generally deeper and smoother while the opposite can leave traders in a hole they cannot get out of.

3.3.10 Auditability

Assets need to be reported to governments and it should be possible for the government to verify them. Be this not the case, fraud would become a major issue. It is furthermore quite likely that if the currency is not easily auditable governments would ban usage.

3.3.11 Anonymity/Pseudonimity/privacy

Most cryptocurrencies advertise a certain degree of anonymity/pseudonimity. This seems like an attractive feature for both citizens and companies. This is also the main aspect that sets it apart from traditional banking systems.

3.4 Ecash

According to David L. Chaum, an ultimate payment system should take care of our personal privacy as well as provide control and security, in order to for example, diminish criminal opportunities [1]. He proposes a payment system with 3 specific properties:

- Third parties, like the bank in a traditional system, are not able to determine payee, time or amount of payments made by an individual.
- The ability to provide proof of payment, or to determine the identity of the payee under exceptional circumstances.
- The ability to stop use of payments media reported stolen.

3.4.1 Specifics and technical: The blind signature ecash system

There are three functions associated with this system.

1. A secret signing function s', known only to the signer, and the corresponding publically known inverse s, such that $s(s'(x)) = x$ and s give no clue about s'.

2. A commuting function c and its inverse c'.

3. A redundancy checking predicate r

Ecash works by having banks cryptographically signing money that is kept on an individuals computer. This is achieved by using the blind signature scheme described above. The blind signature scheme mainly constitutes the creation of the currency. The only differences are that the ballot with a vote is now a random number x such that $r(x)$, the trustee assigns a constant value to this number by signing, and the trustee lowers your bankacount by the constant value every time it signs an envelope with your return address. Spending is done having the payer give the payee a note $s'(x)$ signed by the bank. A payee can then check legitimacy by applying the public key and checking $r(x)$. The payee then sends it to the bank. The bank can then check legitimacy in the same manner and after verifying credit the account of the payee.

3.4.2 Ecash transactions

There are 3 types of transactions in ecash:

- Withdrawals
- Deposits
- Transfers

Two schemes are considered in ecash transactions:

- Online: where validity of coins is verified before accepting a transaction. This is commonly the default scheme and is used in many different protocols designed to implement ecash.
- Offline: where bank involvement is not required during transaction. Validity of coins is determined in another way.

3.4.3 Online scheme

A basic withdrawal works as follows[2]:

Alice		**Bank**
$s \leftarrow rand(n)$		
$s' \leftarrow h(s)$		
	$\xrightarrow{E_{Pk_B}(I_{Alice}, blinded(s'))}$	
		checks balance
		withdraws amount m from Alice
	$\xleftarrow{Sign_{Bank}(blinded(s'))}$	
$C \leftarrow (s, Sign_{Bank}(s'))$		

Alice now has the pair $(s, Sign_{Bank}(s'))$
This pair then represents a coin. Using this in payment along with bank verification goes as follows:

Alice	**Bob**	**Bank**
$\xrightarrow{(s, Sign_{Bank}(s'))}$		
	$\xrightarrow{E_{Pk_B}(s, Sign_{Bank}(s'))}$	
		if $Sign_{Bank}(h(s)) == Sign_{Bank}(s')$
		then X = true else X = false
	$\xleftarrow{X}$	

Depositing is simply sending the coin to the bank along with account information on who to credit.

Bob	**Bank**
$\xrightarrow{E_{Pk_B}(s, I_{Bob}), Sign_{Bank}(s')}$	
	if $Sign_{Bank}(h(s)) == Sign_{Bank}(s')$
	then credit account of Bob

3.4.4 Upgrades and additions

In the years following the release of ecash improvements were made by DigiCash, the developing company led by David Chaum. A solution to the double spending problem was added called the one-show blinding paradigm. This involved a protocol wherein traceability of a coin was provided if there were two signatures for one coin. However this involved having the banks encode trace information into the coins and, in order to enable this protocol, every coin must go through a bank, thus having a trusted third party in the protocol. When a coin is verified by the bank it is added to a database of valid coins.

3.4.5 Usage

Ecash was used in a trial for 3 years in the United States by the Mark Twain bank in Saint Louis, MO, from 1995 to 1998.[5][6] It was dropped because it did not meet profit goals.
In europe it was tried out by more banks. Deutsche Bank, Bank Austria, Sweden's Post AB, Den norske Bank of Norway and Finnish Merita Bank/E-Unet all implemented it. In Australia, St. George Bank and Advance Bank[7] had implemented it as well. Overall the interest in ecash was quite high.

3.4.6 Fall of ecash

In 1998 DigiCash filed for bankruptcy. The exact reasons why are not publicly known. David Chaum has suggested in an interview that the world might not have been ready for it. Electronic commerce was not large enough at the time for instance and the public did not realize the importance of privacy.[8]
Some ex-employees of DigiCash mostly claim fault by management and David Chaum. David Chaum was supposedly not a great manager and caused many projects to never be fully completed. Furthermore he would be paranoid about business deals and had screwed up more than a few deals by being stubborn. [9]

3.5 After ecash

After ecash the cryptographic currency there were some other notable digital currencies that show some insight in how the

[5] `https://chaum.com/ecash/`
[6] `https://www.cnet.com/news/digicash-loses-u-s-toehold/`
[7] `https://chaum.com/ecash/`
[8] http://firstmonday.org/ojs/index.php/fm/article/view/683/593
[9] https://nettime.org/Lists-Archives/nettime-l-9902/msg00036.html

3.5.1 Liberty Dollars

Liberty dollars was a currency invented by Bernard von NotHaus in 1998 that tried to compete with US dollars. They were available in gold and silver coins, gold and silver certificates and electronic currency. Liberty dollars were never recognised as legal tender. Bernard and NORFED, National Organization for the Repeal of the Federal Reserve and the Internal Revenue Code, the company that distributed the currency, were charged with making coins resembling and similar to United States coins in May 2009. In March 2011, Bernard was convicted of this crime. In announcing the verdict the U.S. Attorney said "Attempts to undermine the legitimate currency of this country are simply a unique form of domestic terrorism".[10]

3.5.2 E-gold

E-gold was a gold-backed digital currency that started in 1996 in the United States and continued to operate until 2009 when it ended due to legal issues. The e-gold system allowed users to open an account on a website and buy value denominated in grams of gold or other precious metals. The system processed at its peak about 2 billion dollars in value yearly.[11] According to the US government, users of the system did not have to provide thorough identification and therefore allowed usage of the system for money laundering, child pornography and other illegal acts.[12] The CEO of e-gold, Douglas Jackson, stated however that e-gold provided no anonymity whatsoever as e-gold worked like a book entry mechanism.[13] Following a change of the legal definition of money transmitter in 2006-2008, e-gold and other digital currency companies were prosecuted on the basis of transmitting money without a license. This eventually resulted in the e-gold company and its directors entering into a plea agreement.[14] Transactions were then suspended on the platform and after a Value Access Plan to allow customers of e-gold to retrieve some of their money, e-gold ceased to operate.

[10] https://archives.fbi.gov/archives/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency

[11] https://web.archive.org/web/20061109161419/http://www.e-gold.com/stats.html

[12] https://www.gpo.gov/fdsys/pkg/CHRG-109hhrg31467/html/CHRG-109hhrg31467.htm

[13] https://www.gpo.gov/fdsys/pkg/CHRG-109hhrg31467/html/CHRG-109hhrg31467.htm

[14] http://legalupdate.e-gold.com/2008/07/plea-agreement-as-to-douglas-l-jackson-20080721.html

3.6 Bitcoin

Bitcoin is conceived by Satoshi Nakamoto, a pseudonym for an unknown person or group of people, in 2008. In the bitcoin whitepaper, Satoshi argues in favor of the usage of cryptocurrencies in order to eliminate the trust factor held by banks, allow irreversible transactions, protect against fraud and lowering transaction costs by removing mediation costs.[5] Bitcoin also seems to be the first cryptocurrency to solve the double spending problem in a decentralised manner.

3.7 Motivation for bitcoin

Satoshi Nakamoto has suggested that the economic crisis that started in 2007 was the main motivation for starting to write the code for bitcoin. This is reiterated by the fact that Satoshi has put "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" in the genesis block of the blockchain, the first ever transaction. This refers to a news article in the UK newspaper The Times which indicated that the government had failed to stimulate the economy.

3.7.1 Decentralised

According to satoshi e-currency companies before him failed because they were not decentralised.[15] - hard to prosecute, since there is no company or person to prosecute. - According to satoshi e-currency companies before him failed because they were not decentralised.

3.7.2 Double spending

The main thing that differentiates bitcoin from other e-currencies before it is the way it handles double spending. Traditionally, both in the digital world and the analog world, double spending is solved by introducing a mint, or trusted central authority, to the system. The mint is responsible for checking every transaction for double spending. Coins in these systems are obtained from such a mint and after each transaction coins must be returned to the mint. Only coins that have been obtained from the mint are trusted to not be double spent. This theoretically solves the double spending problem, but makes the whole system depend on these mints. Furthermore, since these coins have to go through the mint after every transaction we have basically added a new trusted party, which we initially so desperately sought to eliminate.
Bitcoin introduces an original solution to this problem. In bitcoin every transaction is publically announced and a majority vote of peers decide on

[15] http://p2pfoundation.ning.com/xn/detail/2003008:Comment:9493

the order of transactions. Thus the majority of peers decides on which transaction was first and deneis the other transaction.

3.7.3 Verifying

As previously mentioned the double spending problem in bitcoin is solved by a majority vote. This is managed by sending every transaction to the nodes in the P2P-network. These nodes then verify and encapsulate this transaction (and others) in a block. Verifying and encapsulating does not take a lot of time and in order to prevent nodes from spamming the network with blocks there is an additional challenge. To proof that time has been spent to verify the transactions a nonce must be added to the block such that the hash of the block starts with a network specified amount of zeros (or be lower than a target value). To find such a nonce is very difficult and requires simply guessing solutions/brute forcing. This challenge is commonly known as the proof of work and exists in multiple modern cryptocurrencies. As a reward for verifying blocks, verifiers(/miners) get a block reward and an optional miner fee included in the transaction by the initiator of the transaction. This is also the main way that the amount of available bitcoin in the network is increased as the block rewards have no previous owners.

3.7.4 Contents of a block

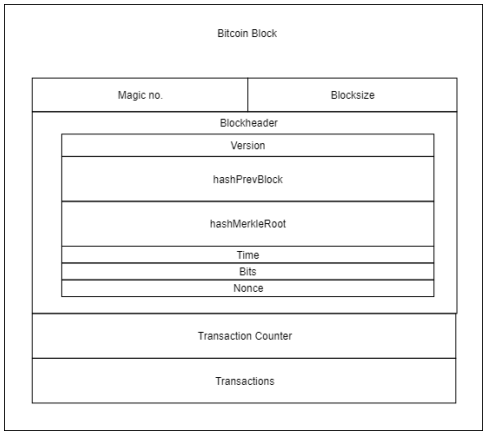

Figure 3.1: Contents of a bitcoin block.

A block consists of the following components

- Magic No. : Identifier for the type of data.
- Blocksize : Size of the block.
- Blockheader : Consisting of 6 additional data entries.

- Transaction Counter : The amount of transactions this block contains.
- Transactions : The transaction details.

The contents of the blockheader are then as follows:

- Version : Block version number.
- hashPrevBlock : The hash of the previous block in the blockchain.
- hashMerkleRoot : The hash of a binary Merkle root tree. This is a tree where the leaves are hashes of the transactions included in the block and nodes are hashes of children. The root then signifies the entire tree.
- Time : a UNIX timestamp, added as an additional source of variation in the block and making it more difficult for an adversary to manipulate the block chain.
- Bits : The target value that the hash resulting from the block generation must result below for the block to be accepted as valid and entered in the chain.
- Nonce : a initially empty field which can be incremented in order to find a hash which would be valid.

3.7.5 Blockchain

The blockchain is a chain of blocks attached to each other by including the hash of the previous block in their own block. This linking is a part of the security. By linking these blocks to each other it becomes difficult for attackers to disrupt a chain. Because of POW and the blockhain a double spend attack where a chain of multiple blocks is quickly added to the chain becomes impossible, since the hash of the first block in the attack chain is dependent on the current header block. If an attacker tries to create an attack chain of multiple blocks he/she will have to do the POW at least twice and in the mean time the entire network will continue and likely change the header block causing the first block of the attacker chain to invalidate. Theoretically an attack like this could still work but it involves astronomical odds(insert odds).

3.7.6 Balance of an account

There is no official place where the current balance of accounts is saved. The balance of an account is simply determined by going through all the transactions an user has been involved in and then calculating the sum of the coins obtained and spent in these transactions.

3.7.7 Identity

3.7.8 Bitcoin transactions

Performing a transaction consists of building a transaction and then sending it to the p2p network for verification. After it is verified, added to a block and subsequently added to the blockchain the receiver can obtain the currency using the private key only known to them.

A transaction consists of the following data

- Version no. : Version number of the transaction.
- In-counter : Number of inputs
- list of inputs : A list of inputs. These inputs are outputs of previous transaction.
- Out-counter : Number of outputs
- list of outputs : A list of outputs. These outputs consist of instructions on how to redeem the coins.
- lock_time : allows for a change of mind after signing. This field shows a time when the transaction can be added to a block. If another transaction with an input identical to one of the inputs of this transaction and a lower lock_time is added before the lock_time of this transaction then this transaction will become invalid.

3.7.9 Receiving Bitcoin

Once a transaction is sent, verified and in the blockchain it is already somewhat in the hands of the receiver. The output part of the transaction can be seen as a locked global box of which the receiver has the only key. When an output of a transaction is not reused in a new transaction it is considered an unspent output. In the future, when the receiver intends to use the funds described in the output field they supply in the input to the new transaction their signature and public key and then miners can verify ownership of the coins. This property allows for the storing of value as described as one of the components of a currency.

3.7.10 Popularity of Bitcoin

3.7.11 Temporary Notes

- public - write only - order matters - decentralised.
  - Honest nodes must collectively control more CPU power,
- POW and its invention : Hashcash - Blockchain: Transaction ordering

—— Transaction chain: History of ownership

- decentralised(was ecash first?-¿mint system not truly decentralised)
- blockchain branching and how it can result in double spending. Branches can occur because of differences in time of arrival. This is solved when a branch is extended by one, at the moment one branch becomes longer than the others, the longest branch will be considered more important(as more work has been done). But if there is a branch in the chain it is possible that two of the branches spend the same coin and as such double spending is possible if the last addition to a branched chain is considered valid. For this reason it is wise to consider only blocks further back in the chain as confirmed.
- cost of sending money
- mining pools and how they may invalidate the double spending security

3.8 Purpose today

And how does it compare to the purposes S. Nakamoto and D. Chaum envisioned. Cryptocurrencies are not widely adopted yet. D. Chaum and S. Nakamoto envisioned these cryptocurrencies as ideal payment systems eventually replacing the standard banking system that we still use today. Chaum mainly wanted privacy while Nakamoto wants privacy as well as eliminate the third party aspect.

3.8.1 Privacy

3.9 Mixnets

3.10 Comparison to standard banking system

Discuss extra possibilities that one offers over the other. Also compare to physical cash. Keep in mind that both systems are not ideal, but that slight advantages in one mechanism over the other can result in significant changes in the world.
Pros for bank

- Possible to charge back
- Easy government oversight
- Legal framework
- Easier to use
- Reversible payments

- Not able to just lose
- Constant transaction time
- Regulation

Pros for crypto

- Decentralised
- Private through (anonymisation)/pseudonymisation
- Less points of failure
- Irreversible payments
- Transparency, public ledger
- Inflation is unlikely due to limited amount of coins(bitcoin)
- Portability
- You hold your own money
- Untraceability (in some cases)
- Lower transaction costs (generally, bitcoin has 0 at the moment)
- Global currency
- Less fraud since security is hard to fake (stolen coins from exchanges? Mt. Gox)
- Possible to incorporate software/scripts into transactions
- Available for everybody

Crypto cons

- Lost coins are lost forever
- Public doesn't understand it yet. It is complicated
- Untraceability (in some cases)
- Fluctuations
- Inconsistent transaction time : depends on network traffic and lately average transaction time is 45 minutes
- Cryptocurrency is not anonymous and the ledger may provide information you do not want others to have.

- Offers criminal opportunities
- Hacked exchanges
- Energy consumption
- Uncertainty

3.11 Anonymous cryptocurrencies

Pseudonymous to anonymous. Mixers: currencies that use it. Comparison to Tor. Have we achieved true anonymity. How future proof must the anonymity be? multiple years?

- Zcash
- Monero

3.12 Legality of cryptocurrencies

"Nakamoto had good reason to hide: people who experiment with currency tend to end up in trouble. In 1998, a Hawaiian resident named Bernard von NotHaus began fabricating silver and gold coins that he dubbed Liberty Dollars. Nine years later, the U.S. government charged NotHaus with "conspiracy against the United States." He was found guilty and is awaiting sentencing. "It is a violation of federal law for individuals . . . to create private coin or currency systems to compete with the official coinage and currency of the United States," the F.B.I. announced at the end of the trial."

3.13 Financial interest

3.14 Future of cryptocurrencies

- fluctuation
- cheaper than traditional methods? Will mining fees be less than
- Inevitability of cryptocurrencies(is it inevitable?)
- What happens if it replaces the traditional system? Can it replace the traditional system? Is it more an additional type of currency instead of replacing the existing currency system?
- Proof of stake
- forcing mining pools to split efforts

3.14.1 Fluctuations in value

3.15 Conclusions/Discussion

Chapter 4

Related Work

In this chapter you demonstrate that you are sufficiently aware of the state-of-art knowledge of the problem domain that you have investigated as well as demonstrating that you have found a *new* solution / approach / method.

Chapter 5

Conclusions

In this chapter you present all conclusions that can be drawn from the preceding chapters. It should not introduce new experiments, theories, investigations, etc.: these should have been written down earlier in the thesis. Therefore, conclusions can be brief and to the point.

Bibliography

[1] David L. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology*, pages 199–203. Springer, Boston, MA, USA, 1983.

[2] Issa Traoré Isabelle Simplot-Ryl and Patricia Everaere. Distributed architectures for electronic cash schemes: A survey. *The International Journal of Parallel, Emergent andDistributed Systems*, 24:3, 2009. `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.372.1343&rep=rep1&type=pdf`.

[3] Adam Koronowski. Does it always pay off to reduce transaction costs? *Journal of Business and Economics*, 1:1, 2010. `http://www.academicstar.us/UploadFile/Picture/2013-10/2013101211128835.pdf`.

[4] N. Gregory Mankiw. *Macroeconomics (6th ed.)*. New York: Worth Publishers, 2007.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. `https://bitcoin.org/bitcoin.pdf`.

[6] Simon Peyton Jones. How to write a good research paper, 2004. Presentation at Technical University of Vienna, `http://research.microsoft.com/en-us/um/people/simonpj/papers/giving-a-talk/writing-a-paper-slides.pdf`.

Appendix A

Appendix

Write one or more appendices to cover additional material that is required to support your hypothesis, conclusions, experiments, measurements, etc. that would otherwise clutter the presentation of your research.