Cryptography and Computer Security

Cryptocurrencies

Anton Schwericke

19-Jan-18

Abstract

There has been a lot of money flowing toward cryptocurrencies. And the money brought attention with and is also the reason why I choose this topic.

New Cryptocurrencies are invented every day. But all of them trace back to the same concept introduced 2008 in the paper “Bitcoin: A Peer-to-Peer Electronic Cash System” and shared under the still mysterious pseudonym Satoshi Nakamoto.

In my paper I will first give a user guide on how to use cryptocurrencies. Then the main part of this paper, will be to explain the technique going on behind the scene if you transfer bitcoins. And later I will do some computations on the main attack against cryptocurrencies and claim that bitcoin became an investment instead of a currency with the last hype.

Inhalt

I. Bitcoin ... 3
A. How bitcoin works for the user ... 3
1. Some reasons to use cryptocurrencies ... 3
2. Some reasons against cryptocurrencies ... 3
3. History ... 3
4. How to use cryptocurrencies ... 5
5. Wallet ... 5
6. Your first bitcoins ... 5
7. Transaction ... 5
8. Pseudo anonymity ... 5
9. Acceptance ... 6
10. Dark Net ... 6
11. Mining ... 6
B. Technique behind bitcoins ... 7
1. The problem cryptocurrencies must solve ... 7
2. Proof of Work ... 7
3. Block Chain ... 8
4. Block ... 8
5. Transaction ... 9
6. Digital Signatures ... 10
7. Mining ... 11
C. Majority Attack ... 12
D. Weaknesses ... 14
1. Security issues ... 14
2. Tracing Coin history ... 14
3. The last bitcoin ... 14
4. 2400 Transactions per Block ... 14
5. Energy Consuption ... 15
II. Altcoins ... 15
III. Attachments ... 16
A. Eliptic Curve Digital Signature Algorithm Scheme ... 16
B. SHA-256 ... 17
with help of the Merkle-Damgård Construction ... 17
IV. Sources ... 18

1 Bitcoin

This paper will explain how Bitcoin works, representative for all cryptocurrencies. This is because Bitcoin is not just only the first and most popular decentralized cryptocurrency to date but these other cryptocurrencies, called Altcoins, work with the same structure of Signatures, Block Chains and Mining. See more about their advantages in Altcoins.

Note that all numbers in this document are updated at 19.01.2018 and could have changed until your reading.

1.1 How bitcoin works for the user

1.1.1 Some reasons to use cryptocurrencies

- Easy access to everyone with internet
- Quick, cheap and worldwide transfers, (not for bitcoin) in comparison to SEPA/SWIFT
- Private, no bank or government can track your money
- No chargebacks, like with credit cards that the sender takes his money back
- No Identity stealing like with credit cards
- No government, bank or company can freeze your account

1.1.2 Some reasons against cryptocurrencies

- Difficult to understand and lack of knowledge, lets fix that
- Not widely accepted
- Uncertainty of the value
- Money is lost if you lose your wallet password phrase, which is your access to your private key
- No way to reverse money

1.1.3 History

Bitcoin´s (also known by its ticker BTC) software is based on a mysterious paper named “Bitcoin: A Peer Electronic Cash System”. It was published in 2008 under the pseudonym Satoshi Nakamoto, which real identity or identities are still unknown, and shared in a cryptography mailing list as "a system for electronic transactions without relying on trust”. In January 2009 the network launched with a first open source bitcoin client and the first 50 Bitcoins created by Satoshi Nakamoto.

One estimates that Nakamoto earned more than a million bitcoins in the first year, before disappearing from any contribution to bitcoin and handed over to Gaven Andresen, the leader of the Bitcoin Foundation, the anarchic community of bitcoin.

The first values for bitcoin were negotiated in the forum of this community. For example there was an indirect transaction of 10,000 bitcoins, around 100million € today, for two delivered Pizza.

The only major security gap was exploited in 2010, in one transaction 184 billion bitcoins were created in one transaction which was possible because transactions didn’t need to be properly verified before becoming valid. Within hours, the transaction was spotted and erased, the bug was fixed, and the network forked to an updated version of the bitcoin protocol. That means the majority of users and miners started to do their computations with a different code. Another successful attack nowadays could be handled in the same way but would cause a major value drop.

The further story of bitcoin is basically one of the prices going steadily up and more and more venders accepting it. Where it´s notable to know that Bitcoins don’t represent anything in the real

world. They only have value because people are willing to trade goods and services for it and believe others would do the same. Hence the numbers in our computer have value because we believe they do. Like every other Fiat-currency like $ and € too.

The peak bitcoin value had on the 15.12.17 with an exchange rate of 17,900$. This made Bitcoins so popular that bitcoin lost it´s function as a currency. In many ways Bitcoin did function as a currency before December 2017. One person can send another some amount of the currency in exchange for goods or services. But with the high transaction fees of around 10€ per transaction and heavy price volatility, Bitcoin changed from a currency to an investment product.

The only certain thing about the future is that around 2140 the last bitcoin will be mined. Because this was the process which is creating inflation, see New Bitcoins, there will be a deflation, because people will still lose bitcoins because of hardware crashes and insufficient backups. Additionally the transfer fees will raise even more at that point because the computer creating security need to be paid.

1.1.4 How to use cryptocurrencies

Like a credit card is easy to use but the bank system is difficult. Also cryptocurrencies have easy interfaces, while the underlying system fills a paper.

1.1.5 Wallet

Before starting, you have to download a so-called wallet, similar to a bank account, which is the program that will on one site provide all the security (generate private, public address and signatures), on the other side give a graphical interface to make it easy for users to send and receive crypto coins. My personal choice is Coinomi, which saves not only Bitcoins but numerous Altcoins as well.

1.1.6 Your first bitcoins

To get your first bitcoins, the fastest is to get them from some friends or Bitcoin meetings in town.

If you are fine with waiting for 5days and paying from your bank account and losing some anonymity by that https://coinbase.com is a good option.

If you want to safe your anonymity you can send cash or even gift cards to https://paxful.com/

1.1.7 Transaction

Simply enter the receiver public address and amount or scan the receivers QR-Code.

Then you will have to enter the transfer fee. This is voluntary, but because in the bitcoin system there are only around 2400 transfers per minute proceeded, you indeed must pay high fees, like 10€ per transaction. https://bitcoinfees.info/ shows you how much you will have to pay currently. The amount is going down a little in the night and at weekends.

Control everything again because no transaction can be reversed, and the money is lost if you use an invalid receiver address. If everything is correct click broadcasting.

Your Wallet will add your signature and a transaction number and broadcast your transaction to the community.

From the receiver perspective you should always create a new wallet, that means a new receiver address for every incoming transaction. Then you must wait a bit after the transaction has been confirmed. Recommendations are to wait for 6 confirmations or an hour until exchanging the good traded. The number of confirmations is visible in your wallet. This waiting secures you from the Majority Attack. The currently most powerful attacker would have a success chance of 0,1%, if he is the sender and tries to fool you in this specific transaction.

Note that unconfirmed transactions do not expire. That means if you pay no transaction fee the transaction can be stuck in the system for a few weeks with currently 160.000 unconfirmed transactions.

1.1.8 Pseudo anonymity

One reason for bitcoin's popularity is the anonymity of its users. Because every user has a list of all transaction ever done, to stay anonymous, you have to prevent associations of your bitcoin public addresses with your real identity by:

1. buying your first bitcoins anonymous, for example with cash at https://paxful.com/
2. encrypting your online activity with TOR every time you log into your wallet
3. making it impossible to link your transactions together to a user profile, which could be linked with you: Generate a new public key for every incoming transaction by opening a new

wallet for each one. It is possible use these coins and prove ownership in the future. (link these transaction as yours, because you can sign each of them with their specific private keys)

1.1.9 Acceptance

A lot of venders accept them look for the sign:

The biggest internet currency so you can buy a lot in the web like:

Microsoft, Reddit and The Pirate Bay

Slowly also offline products are available:

Subway, Dell Computers, Expedia, Gift Cards

Pizzaforcoins.com to order Dominos Pizza

Precious metals

http://www.coinabul.com

Convert to other currencies

http://MtGox.com

The acceptance of other cryptocurrencies is not so well yet.

1.1.10 Dark Net

The Darknet Markets or Crypto Markets are virtual black markets which are not accessible from the open internet but with the hidden service of TOR and I2P. The best known was named Silk Road. The most traded goods are illegal drugs, digital goods like premium accounts or e-books. Some also trade fake money, documents, credit card details and weapons. Every payment here is done by cryptocurrencies because they provide anonymity. Besides of Bitcoins more and more Monero is used because it provides more anonymity.

1.1.11 Mining

Unfortunately, mining bitcoins on a normal CPU costs more money in form of electricity than the expected reward is. That is why CPU mining is not any longer possible. But you can buy special devices starting from 500€ to mine or use your graphic cards. These special devices are ASICs and are specially designed to try out inputs for hash functions efficient but only that. You can find a good beginner guide at online. But keep in mind, it will need at least a year until you have your investments back.

1.2 Technique behind bitcoins

1.2.1 The problem cryptocurrencies must solve

The target of cryptocurrencies is to supply the internet with a currency. But there are many problems to solve. In the real world, if you spend a spend a dollar, it´s easy to verify the transaction. You will hold the dollar in your hand, you will feel it, you can even smell it. A digital dollar on the other hand has one big problem, it can be copied. Hence it can be send to more people then you. As a receiver you want to ensure that you are now the only owner of this dollar.

In the past this problem was solved by a centralized ledger. An account book organized by the bank or any other authority everybody must trust, because they are able to manipulate it. But in the internet no such trustful authority exists and, therefore, the brilliant idea is to give the ledger to every user, so they can verify transactions themselves. Which leads to the central task of cryptocurrencies: How to ensure every user is having the same ledger? How to get decentralized consensus?

1.2.2 Proof of Work

The Idea to solve this problem: Everybody believes the version of the ledger which is has the most computational work done on it. We say it is confirmed the most, or it has the most secure proof of work.

The genial twist in it is that not only everybody is believing the same ledger because only one version is confirmed the most often, but also it needs a big part of all computational power in one hand to make this person fake the correct version.

To create this Proof of Work the hash function SHA-256 is used. To see how it works in detail consider my attachments SHA-256. The two important things about hash functions are firstly that the image, the so-called hash, is easy computable but changes completely unpredictable for just slightly changes in the input. And secondly that inverting it is infeasible. Indeed, it is so hard, that if you want to find the input for SHA-256, which gives you a desired output, there are not much better ways than to guess. (There is no cold hard proof for that, but nobody could yet figure a way. In fact, a lot our modern security like https rely on this)

The Proof of Work is now to find a special number and attach it to the ledger, so that if you take the hash of the last part of the ledger together with this number as the input for SHA-256, the output begins with let´s say 30 zeros.

(This number of zeros is changed in reality every 2016 blocks (difficulty) or every week to ensure that in average one such input is found every 10min, which than creates a new block, see Block Chain)

Because the chance to find the correct input to create 30 zeros in the first try is $1/2^{30}$ in average one must try out $2^{30} \approx 1.000.000.000$ inputs to find a fitting input.

There are a lot of computers in the world working exactly on this, to try out numbers for the bitcoin system. They are called Miners. Read more in Mining.

The point of a proof of work is that this proof of work depend totally on the ledger, if you would change just one single number in the ledger, SHA-256 would give a totally different outcome and the proof of work would be passé.

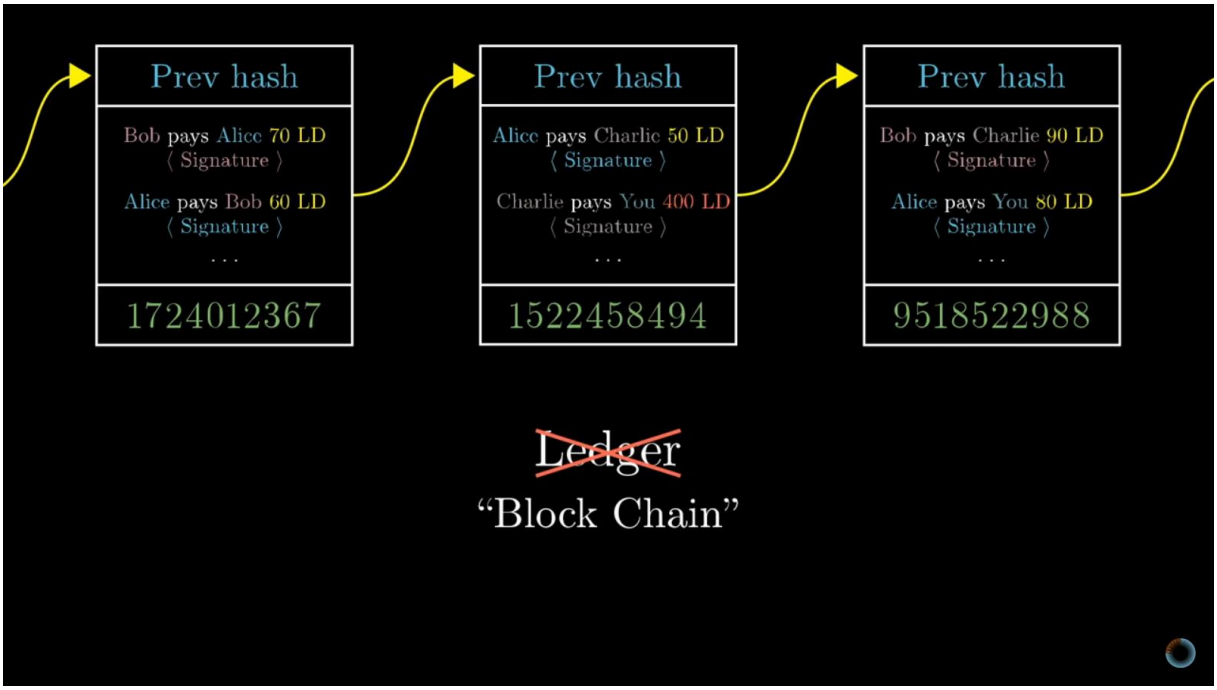
One other point is that it was very hard to find this proof, but verifying it, is easy. You simply compute the SHA-256 hash of the ledger with that special number in the end, and check if it starts with 30 zeros.

1.2.3 Block Chain

All transfers of bitcoins are verified are recorded on a public ledger known as the block chain. You can see the ledger online, for example under https://blockexplorer.com.

The main purpose of the block chain is to fix the order of transactions which is important to prevent double spending.

The Block Chain is quite a natural way to organize the ledger. You part the ledger into blocks and add a new block every time a Miner finds a new Proof of Work. Then the transactions, the miner included in the Block together with the Proof of Work, form a new Block together with one extra transaction. The first thing written in the Block is the hash of the previous block, and all the previous Blocks do, too, so every block contains a hash of the whole Block chain. This is to secure that nobody can change the Blockchain later by adding or deleting some information or changing the order of the blocks.



Now we know the structure of the Block Chain but let us have a closer look at the single Block.

1.2.4 Block

Every time a miner finds a proof of work a new block is created, and broadcasted in the network. By this it getS added to the block chain.

A block consists mainly of:

1. Hash of the previous Block
2. Miners reward transaction
3. Up to 2400 transactions
4. Proof of Work

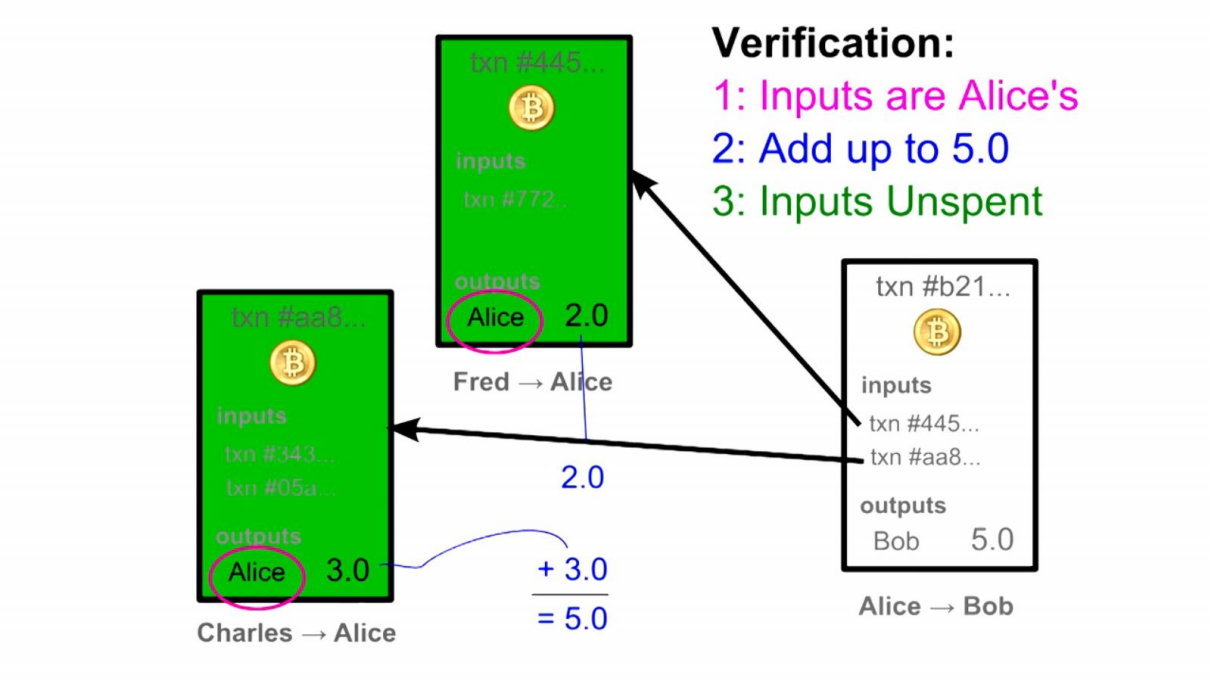
And of some technical data like difficulty (number of 0bits the hash function shall produce), block size, Block version number, Time. More about the miner's reward in New Bitcoins

Now we know the structure of a Block, let´s have a closer look at a single transaction.

1.2.5 Transaction

Transactions are structured the way they are to ensure nobody spends more money than they have. That needs some tricks because not the balances of the owners are stored in the public ledger but only the transactions.

Instead of balances the ownership of the bitcoins somebody wants to send is guaranteed by linking to other transactions in the blockchain, where the owner received the required number of bitcoins. Here Alice must link as inputs transaction outputs, in which she got at least the amount she wants to pay to Bob. If these outputs sum up to more than Alice wants to pay to Bob, there will be a second output referring to Alice. All the bitcoins that are left over count as transaction fee.



It is useful that all amounts linked in the input of the transaction are used up completely because all the transaction outputs linked to become invalid with this link. To use these bitcoins next time, Alice must refer to her own last transaction where she got money back as one of the outputs.

With this system the validity of each transaction depends on the validity of other transactions. Can one ensure that all of them are valid? When you first download a wallet software it goes through all transaction ever made and checks if they are valid. This needs around a day but it´s necessary because there is no trustful institution in bitcoins.

To verify a transaction one has to check three steps

1. Alice has to provide a valid signature (see Digital Signatures) to proof her ownership for every linked transaction
2. The linked transaction outputs in the input of the specific transaction sum up to more than the output of this transaction
3. Check all transactions in the meantime if they used the transaction. Note that the order of transaction is fixed in the blockchain.

With this system, bitcoins are passed from address to address through a chain of transactions. Each step in the chain can be verified to ensure that bitcoins are being spent validly.

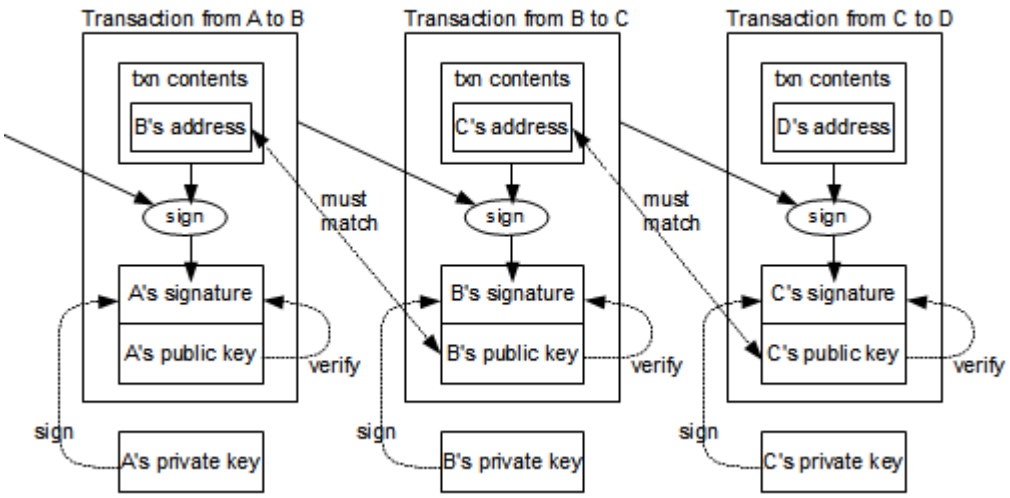
1.2.6 Digital Signatures

Every transaction has a transaction identification number TXID and digital signature of the sender attached, to ensure nobody can spend someone else´s money. The signature makes it impossible that some other person, Bob, can steal Alice money by writing “Alice sends Bob 100€” on the public ledger or by modifying any messages on the ledger. And the transaction ID, which is part of the signed message, ensures that Bob cannot copy the transaction “Alice sends Bob 10€” to the ledger to receive the 10€ several times.

The signature used for bitcoins is the elliptic curve digital signature algorithm, you can find more details on it in the attachment. Eliptic Curve Digital Signature Algorithm Scheme

For Bitcoins every person creating a wallet is creating a private key of length 256. From that the ECDSA creates a 512-bit Public Key and adds 04 as the first bits. Because this 512bit are inconvenient it is hashed down to 160bit by SHA-256 and another, so-called RIPEMD hash. The resulting 20bytes are the bitcoin address which could look like *1P82rBjJMDFSay2RqKx1bydDRVh5QnGkkZ*.

As a matter of fact, nobody checks if the private key you just rendered is already used by somebody else. Therefore if by chance you render the private key somebody else is also using, then you would know his public address because you would have the same, it is simply derived from the private key. Then you can compute his balance because all transactions are listed in the public ledger and you could spend all his money by producing valid signatures. But the chance for this to happen his incredibly small. There are 2^{266} atoms in universe and 2^{256} different private keys in the bitcoin system.



The above diagram gives a simplified view of how transactions are signed and linked together. Consider the middle transaction, transferring bitcoins from address B to address C. The contents of the transaction (including the hash of the previous transaction) are hashed and signed with B's private key. In addition, B's public key is included in the transaction.

Anyone can verify that the transaction is authorized by B, in two stepts: Firstly, B's public key must fit to B's address in the previous transaction, proving the public key is valid. Secondly, B's signature of the transaction can be verified using the B's public key in the transaction.

1.2.7 Mining

In a simple way, what miners are doing is listening for transactions, creating blocks, broadcasting these blocks and getting rewarded with money for doing so. By doing so they make the blockchain longer and the transactions more secure and irreversible.

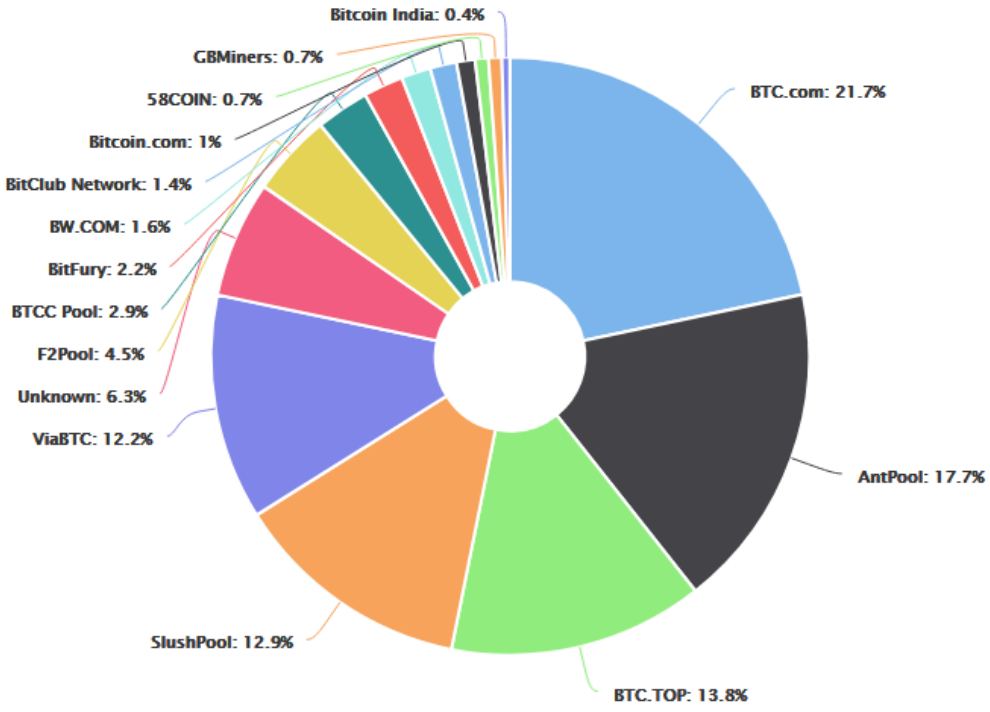
All miners are searching for the right input for the hash function SHA-256 to produce a certain output starting with a certain number of zeros and by that creating a Proof of Work. To see how that creates security read Majority Attack.

The miners also get the transaction fees of all the transactions in their Block. These are voluntary, but Miners are more willing to include the transactions with higher fees in the Block and there are only around 7 transactions per second that are included in the blockchain.

Hence, Mining is called like this, because it requires a lot of work and it introduces new bits of currency in the economy.

1.2.7.1 New Bitcoins

There is a reward, so that people invest money, time and electricity into mining. Once somebody is lucky and finds such an input, he is creating a new block. And can add a special transaction at the top of the block, which does not have to be signed because it does not come from anyone. That is the reward, the miner is getting (currently 12,5 Bitcoins which is around 100.000€). Because the chance to win this much money is very low as a single miner, they group together in mining pools which will share the money. The biggest mining pools concentrate around 20% of the hash rate.



Mining is the only way new bitcoins can be created. Because the amount created is halved every 210.000 Blocks or approximately 4years, the last bitcoin will be mined around the year 2140.

The reason is that halving it all the time is a converging geometric series with limit: the maximum number of bitcoins:

$$\sum_{i=0}^{\infty} 210.000 \times \frac{50}{2^i} = 210.000 \times 50 \times \sum_{i=0}^{\infty} \frac{1}{2^i} = 210.000 \times 50 \times 2 = 21.000.000$$

This decreasing-supply algorithm was chosen because it approximates the rate at which commodities like gold are mined. Users who use their computers to perform calculations to try and discover new blocks are thus called Miners.

1.3 Majority Attack

To come back to our main problem to ensure that everybody uses the same ledger: From the perspective of the user of bitcoins, it can happen that two different conflicting ledgers are broadcasted in the network, this is called a fork. For this there is an easy solution: believe the ledger that is longer, the Blockchain which has more Blocks, because there has been more computational work put into it. If there is a draw wait until one more block is broadcasted, and one chain is longer.

To see why this makes a trustworthy system and to understand at which time a payment is legit, I will show how it would look like to fool someone in this system.

Maybe Eve wants to buy something from Alice and aims on fooling her with a faked block. Namely Eve is broadcasting his transaction of paying 100€ to Alice, but secretly working on a different chain where Eve keeps the money and is only including other transactions in his blocks. When Alice sends the product, Eve wanted to buy from Alice, Eve will broadcast his fork of the blockchain. If it is longer, everybody will believe his version and Alice is unpaid.

To do this Eve would need to find two valid proofs of work faster than all the other miners (one to not include his transaction and one to be longer than the other chain). And this is possible, maybe she is lucky. But Alice is doubting and still waiting for some more blocks to be broadcasted from the miners. Hence Eve needs to find more and more proofs of work faster than the others. And unless she controls more than half of the computational power of the network, at some point she will lose the run, and Alice will be finally paid.

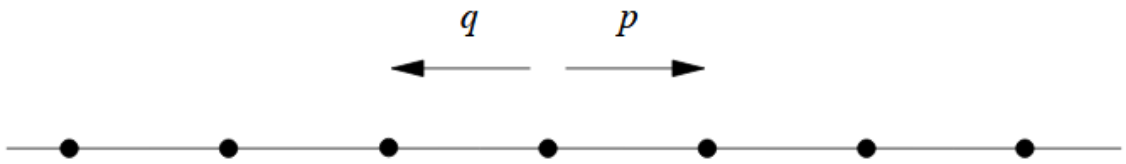
Hence from Alice perspective, it is good to wait for a certain number of blocks after the transaction is included in the blockchain until she considers the transaction confirmed and sends the product. Most venders wait for 6 blocks, also called confirmations. Also, Alice should watch out if there is a fork broadcasted to ensure the community is really 6 blocks in front of the attacker and not only the attacker one behind.

As well Alice should generate a new key pair and gives the public key to the Eve shortly before signing. This prevents Eve from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far ahead. Then executing the attack and having all proof of works prepared.

To make some calculations:

Let us simulate it with Markov chains and especially the simple homogeneous random walk on the integers. But you will break it down, so the reader does not have to understand the concept of Markov chains. The simulation is: at starting time zero we are at the integer zero, $(\mathrm{X}_0) = 0$. For every

$n \in N$ each step we go to left $(\mathrm{X_n}) = (\mathrm{X_{n-1}}) - 1$ with probability $q = P(X_n = y - 1 \mid X_n = y)$("Propability to be at time n in y-1 under the condition to be in y at time n-1") and to the right $(\mathrm{X_n}) = (\mathrm{X_{n-1}}) + 1$ with probability $p = P(X_n = y + 1 \mid X_n = y)$



First we will calculate some probabilities analogue to the gamblers ruin for the Markov Chain $(\mathrm{X_n}) = \#\text{Blocks the attacker is catching up} = \#\text{Blocks the attacker is adding to his chain} - \#\text{Blocks the community is adding to their chain}$

And start with $(\mathrm{X_n}) = 0$, p the propability of the Attacker to find a block, and q the probability of the community to find a block. We want to find out what the probability is to catch up from k blocks behind $\mathrm{P}(\exists n \in N: X_n = \mathrm{k}) = \mathrm{P_k}$ for any time $n \in N$. Because of independence and strong Markov Property $\mathrm{P_k} = \mathrm{P_1^k}$.

And $\mathrm{P_1} = \mathrm{p} * 1 + \mathrm{q}\mathrm{P_2} = \mathrm{p} + \mathrm{P_1^2}$. To deduce solutions set $\mathrm{P_1^2} - \frac{1}{\mathrm{q}}\mathrm{P_1} + \frac{\mathrm{p}}{\mathrm{q}} = 0$ and calculate:

$$\mathrm{x_{1,2}} = \frac{1}{2\mathrm{q}} \pm \sqrt{\frac{1}{4\mathrm{q}^2} - \frac{\mathrm{p}}{\mathrm{q}}} = \frac{1}{2\mathrm{q}} \pm \sqrt{\frac{1-4\mathrm{pq}}{4\mathrm{q}^2}} = \frac{1}{2\mathrm{q}} \pm \sqrt{\frac{(\mathrm{p}+\mathrm{q})^2 - 4\mathrm{pq}}{4\mathrm{q}^2}} + \frac{1}{2\mathrm{q}} \pm \sqrt{\frac{(\mathrm{p}-\mathrm{q})^2}{4\mathrm{q}^2}}$$
$$= \frac{(1 \pm \mathrm{p} - \mathrm{q})}{2\mathrm{q}} = \begin{cases} 1, \text{if } \mathrm{p} \geq \mathrm{q} \\ \frac{\mathrm{p}}{\mathrm{q}}, \text{if } \mathrm{p} < \mathrm{q} \end{cases}$$

Hence $\mathrm{P_k} = \mathrm{P_1^k} = \begin{cases} 1, \text{if } \mathrm{p} \geq \mathrm{q} \\ \frac{\mathrm{p^k}}{\mathrm{q}}, \text{if } \mathrm{p} < \mathrm{q} \end{cases}$

Assuming the community needs the average expected time to find new blocks, the amount of blocks the attacker is finding in the same time is Poisson distributed with expectation $\alpha = k * \frac{p}{q}$.

Then the probability for the attacker still to catch up if the community has already found k blocks to make the attack successful is the sum over all the possible progresses of the attacker (Poisson densities) multiplied with the chance still to catch up

$$\sum_{i=0}^{\infty} \frac{\alpha^i * e^{-\alpha}}{i!} * \begin{cases} 1, \text{if } \mathrm{k} \geq \mathrm{i} \\ \frac{\mathrm{p^{k-i}}}{\mathrm{q}}, \text{if } \mathrm{k} < \mathrm{i} \end{cases} = 1 - \sum_{i=0}^{k} \frac{\alpha^i * e^{-\alpha}}{i!} (1 - \frac{\mathrm{p^{k-i}}}{\mathrm{q}})$$

To give some examples for the percentage of the hash rate of the biggest mining pools p=0,2 with k confirmations there we get these probabilities that an attack would still work

K=0	K=1	K=2	K=3	K=6	K=10
100%	42,4%	20,3%	10,2%	1,43%	0,11%

One does not have to be anxious now. In most of the transaction nobody tries to attack. And the biggest mining pools restricted their own size, to prevent people mistrusting them. These big mining pools are living from the value of bitcoins being up. Hence the last thing they want is a successful attack, which would cause a major drop of value, because of users losing their trust.

If we look at it from a different perspective of how big k must be for some p to have the chance an attack works to be smaller then 0,1% which is widely seen as secure:

p=0,1	P=0,2	P=0,3	P=0,4	P=0,45
5	11	24	89	340

This attack is called Majority attack because if P≥0,5 the attacker can just fool everybody, no waiting for confirmation can secure the transfer anymore. But still it would be hard for the attacker to reverse transactions from the far past.

Hint: This calculation is not exact. The Miner pools have an extra advantage: They know which inputs for the hash the other pool members already tried out which single miner do not. That results in the problem that my simulation would need to be more complex because when the attacker finds a block, the community is not starting from the scratch on finding their block because they are working on a different chain. In specially they already tried out some inputs they can exclude and search so more efficient at the others. This would destroy independency and ruin my first calculation for the Markov chain.

1.4 Weaknesses

Bitcoins have a lot of weaknesses. Unfortunately, nobody can solve them, because there is no admin for bitcoins, I mean this is the crucial part about cryptocurrencies. Therefore, the only way to clean out some weaknesses is buy letting more than 50% of the Miners start to work with a different protocol. Even much more percent need to stand behind an idea to prevent that there will be a hard fork, so one group of users using one and the other another version. Like it happened for the split in Bitcoin and Bitcoin Cash.

1.4.1 Security issues

Vulnerable for Sybil and Denial of Service attack.

In the Sybil attack the attacker would float the peer to peer network with nodes, so it would be likely that victim of a majority attack does not listen the real broadcasted blocks anymore and believes the slow calculated fake blocks.

In a Denial of Service attack the attacker would send loads of data to a node to make him busy and hence not listening to other broadcasts anymore, to then apply the majority attack.

1.4.2 Tracing Coin history

The public Blockchain can be used to connect identities to addresses

1.4.3 The last bitcoin

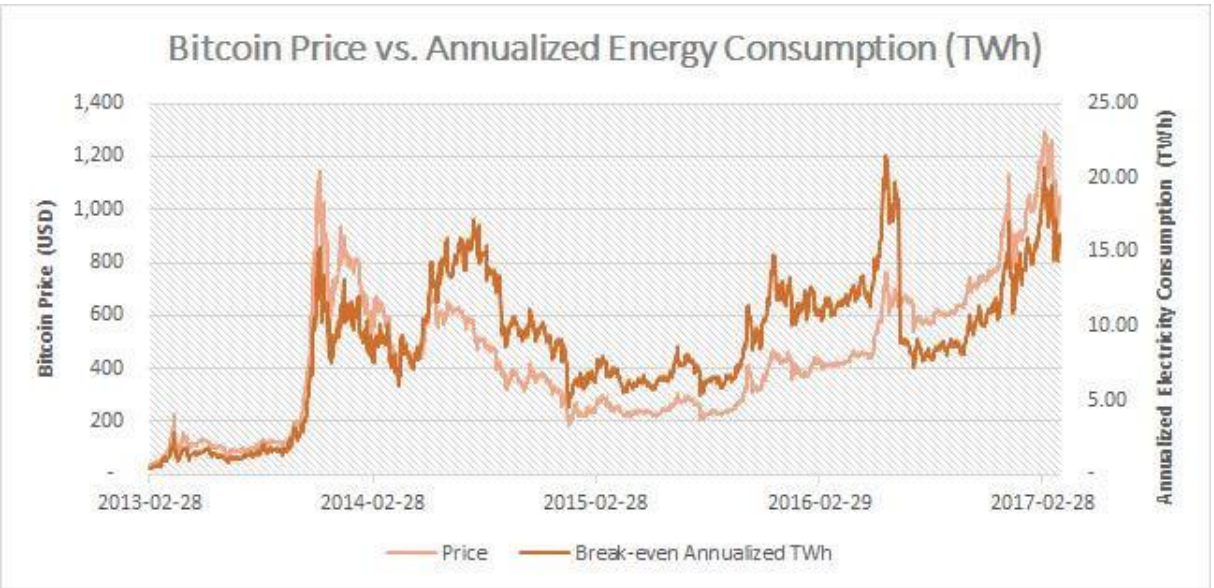
When the last bitcoin is mined, there will be a deflation, because every day bitcoins get lost because of invalid public keys, and loss of private keys.

1.4.4 2400 Transactions per Block

Due to a technical barrier the Block size is ≤ 1MB. That results in a maximum of 2400 transactions per Block. Because the protocol changes how many zeros a proof of work needs to have in average a Block every 10min. In the moment it´s 73 bits of zeros. That makes only approximately 7 transactions per second possible, which is far to less for the popularity of Bitcoin. That's why 160.000 transaction are waiting.

And it´s the reason why the transaction fees are around 10€ per transaction. Which makes normal payments with bitcoins not lucrative, but only usable for speculations on the value.

1.4.5 Energy Consuption



Mining is a market. Because the price went up high, mining became more lucrative and higher payments for electricity possible. This huge amount of currently 32 TWh per year is three times the annual consumption of Slovenia. This power is not needed to secure the network but simply a financial decision of more people to invest in mining. And it has no greater purpose because the proof of work is to try out random hash inputs.

But all these disadvantages are repaired in other cryptocurrencies, called Altcoins.

2 Altcoins

There are 1373 Altcoins, alternative coins, out there, new are coming up every day. They use the same system as bitcoin with just slide adjustments and they have different advantages and disadvantages but solve a lot of problems bitcoin has. On the other hand they haven´t reached the same acceptance yet. There are for example:

Iota – No Transaction Fees, Transactions/Block are not limited

Monero – encrypts the public ledger to increase anonymity

Riecoins – use as Proof of Work the scientific interesting verifying Hardy-Littlewood k-tuple

Gridcoin – some computer power is linked to BOINC (Berkely Open Infrastructure for Network Computing to find e.g. Neutron stars, better Whether Predictions and fold Proteins to cure illnesses)

3 Attachments

3.1 Eliptic Curve Digital Signature Algorithm Scheme

Agreed on before:

p Prime, the finite group Z_p

a,b ∈ Z_p for the Curve=$\{(x,y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\}$

a generator of the curve P and its order n>256

Secred Key d $\epsilon_{\{1,\dots,n-1\}}$ randomly

Public Key Q=d*P

Alice signs a message m

k $\epsilon_{\{1,\dots,n-1\}}$ randomly but for every signature newly

r= $x_1 \, mod \, n$ for (x_1, y_1)=kQ

s=k^{-1}(SHA-256(m)+rd) mod n

signature = (r,s) if r≠0≠s otherwise repeat with different k

Bob verifies

w=$s^{-1} \, mod$ n

(x_1, y_1)=SHA-256(m)× w×P + r×w×Q

If r= $x_1 \, mod \, n$ the signature is valid, otherwise not

Bitcoin uses the elliptic function with hexadecimal numbers

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

a = 0, b = 7

G compressed = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

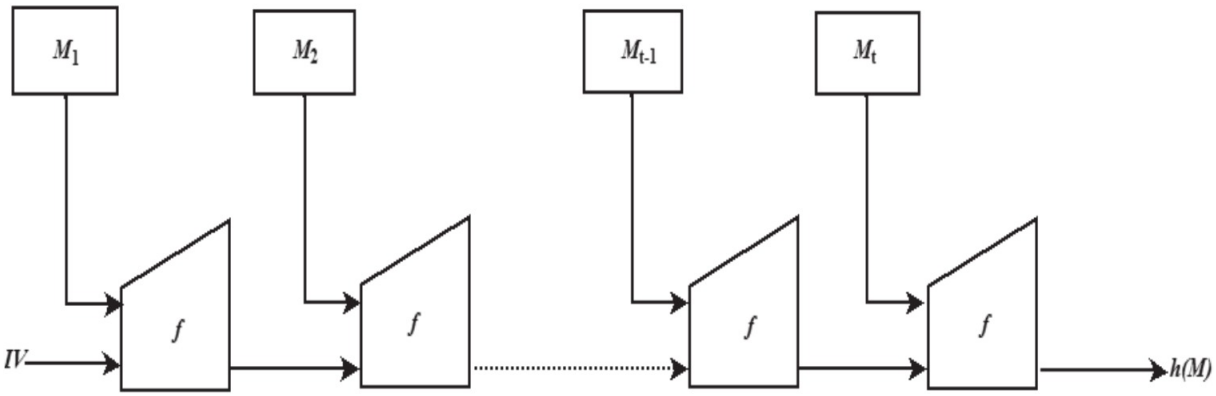
3.2 SHA-256

with help of the Merkle-Damgård Construction

This construction relies on a cryptographic compression function $f: \{0,1\}^{64} x \{0,1\}^{8} \rightarrow \{0,1\}^{8}$ which is hard to invert. In SHA-265 it is

```
for i from 0 to 63
        S1 := (e rightrotate 6) xor (e rightrotate 11) xor (e rightrotate
        25)
        ch := (e and f) xor ((not e) and g)
        temp1 := h + S1 + ch
        S0 := (a rightrotate 2) xor (a rightrotate 13) xor (a rightrotate
        22)
        maj := (a and b) xor (a and c) xor (b and c)
        temp2 := S0 + maj

        h := g
        g := f
        f := e
        e := d + temp1
        d := c
        c := b
        b := a
        a := temp1 + temp2
```



To get the hash output *h(M)* of a message M, the message is first padded to a multiple of 64 bit and then chaining the compression function f that means:

$H_0 = Initialisation\ vector =$ `( h0 := 0x6a09e667; h1 := 0xbb67ae85; h2 := 0x3c6ef372; h3 := 0xa54ff53a; h4 := 0x510e527f; h5 := 0x9b05688c; h6 := 0x1f83d9ab; h7 := 0x5be0cd19 )`

$H_i = f(M_i, H_{i-1})$ `for` $i \in \{1, \dots, 8\}$

$H(M) = H_8$

These are the main parts of SHA-256, if you want to go deeper visit see the original paper https://csrc.nist.gov/publications/detail/fips/180/4/final

4 Sources

Content

The original Bitcoin Paper: https://bitcoin.org/bitcoin.pdf

BitcoinWiki: https://en.bitcoin.it/wiki/How_bitcoin_works

Wikipedia: https://de.wikipedia.org/wiki/Elliptic_Curve_DSA

https://en.wikipedia.org/wiki/SHA-2

https://de.wikipedia.org/wiki/Darknet-Markt

CuriousInventor https://www.youtube.com/watch?v=Lx9zgZCMqXE&feature=youtu.be

Others: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

https://www.huffingtonpost.com/ameer-rosic-/7-incredible-benefits-of-_1_b_13160110.html

http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

Content and pictures

Merkle-Damgård Construction Method and Alternatives: A Review (published 12 2017)
https://jios.foi.hr/index.php/jios/article/view/1070/787

3Blue1Brown: https://www.youtube.com/watch?v=bBC-nXj3Ng4

Pictures

https://www.shutterstock.com/image-vector/vector-bitcoin-logo-icon-cloud-shield-412115728

https://bitstickers.net/shop/bitcoin-accepted-sticker-inside-window-158x57mm/

https://en.bitcoin.it/wiki/Confirmation

https://charts.bitcoin.com/chart/price

https://www.youtube.com/watch?v=Lx9zgZCMqXE&feature=youtu.be

http://www2.math.uu.se/~sea/kurser/stokprocmn1/slumpvandring_eng.pdf