UNIVERSITY of NICOSIA

MSc in Digital Currency

DFIN-511: Introduction to Digital Currencies

Session 3
Basics of Cryptocurrencies: Cryptography, transactions and mining

DFIN-511: Introduction to Digital Currencies

UNIVERSITY of NICOSIA

Objectives of Session 3

- Go through major events in the history of Bitcoin
- Understand how Bitcoin and cryptography are related
- Gain a first idea of how Bitcoin transactions work
- Get introduced to Bitcoin mining

We are about to step into the more technical aspects of Bitcoin, as they are crucial in understanding how this system is enabled and how the Bitcoin network operates.

For the non-technical people, familiarization with several new concepts will be required, but we guarantee it will be a very rewarding experience in the long term!

Agenda

1. A brief history of Bitcoin
2. Basics of Bitcoin Cryptography
3. Transactions and the blockchain
4. Mining
5. Conclusions
6. Further Reading

1. A Brief History of Bitcoin

A brief history of Bitcoin/Crypto

2008

- The bitcoin.org domain name is registered
- Satoshi Nakamoto's original Bitcoin paper is published
- The Bitcoin Project is registered at sourceforge.net

2009

- The Genesis block is established on January 3rd at 18:15:05 GMT
- The first Bitcoin client (*bitcoind* v0.1) is released
- The first Bitcoin transaction is performed in block 170, from Satoshi Nakamoto to Hal Finney
- The first difficulty increase occurs on December 30th, from 1.00 to 1.18289953 in block 32256

2010

- The first Bitcoin currency exchange site (Bitcoin Market) is established
- OpenGL GPU hash farm is established by ArtForz and GPU mining begins
- A vulnerability in Bitcoin is exploited to generate 184 billion bitcoins – the bug is quickly fixed
- Pooled mining begins (discussed later in this session)

A brief history of Bitcoin/Crypto

2011

- Bitcoin reaches parity with the US dollar for the first time (1 USD = 1 BTC)
- Bitcoin generation difficulty passes 1 million for the first time in June 2011
- The first Bitcoin Conference and World Expo is held in New York City

2012

- The Bitcoin Foundation is established in September 2012
- The First Bitcoin Halving Day is observed on November 28th, with block 210000 having a block reward of 25 BTC. The next scheduled Halving Day will be observed in 2016, when block reward halves to 12.5 BTC in block 420000.

2013

- A hard fork of reference client v0.8.0 occurs; network updates within a few hours
- The total Bitcoin market capitalization exceeds US $1 billion
- University of Nicosia becomes the world's first university to accept bitcoins for tuition
- Bitcoin mining difficulty passes 1 billion in December 2013

2014

- Bitcoin mining difficulty passes 35 billion
- University of Nicosia launches the world's first Master's Degree in Digital Currency

A brief history of Bitcoin/Crypto

2015

- NASDAQ announces blockchain-based platform “NASDAQ LINQ” for private securities issuance
- New York State releases “BitLicense”, which outlines the rules Blockchain startups should follow within the state
- Bitcoin is exempt from VAT, according to rules imposed by the European Court of Justice

2016

- OpenBazaar is released in April as the first decentralized marketplace accepting Bitcoin as a payment method
- Craig Wright fraudulently claimed to be Satoshi Nakamoto by displaying a private key signing, attempting to present it as Satoshi’s keys
- In July 9, 2016, the second halving occurred as the block reward was reduced to 12.5 bitcoins per block
- The largest Bitcoin exchange by volume to date, Bitfinex, was hacked and 119,756 bitcoins were stolen

2017

- Bitcoin broke the $1000 mark in early January 2017, for the first time since 2014
- Japan categorized bitcoin as legal tender, after long disputes between regulators and crypto exchanges
- A Bitcoin code split initiated Bitcoin Cash in August 1st, with the aim to support blocks of up to 8MB
- CME Group announced the launch of Bitcoin futures in late October 2017.

A brief history of Bitcoin/Crypto

2018

- Facebook, Google and Twitter ban crypto advertisements to protect investors from ICO scams. Ban was then lift
- More than 80% of the total Bitcoin supply has been mined by January 2018.
- US Securities and Exchange Commission says crypto exchanges must register with agency as exchanges
- SegWit implementation allowed Bitcoin fees to fall at the lowest median level since 2011
- In November, Ohio became the first US state to allow taxes to be paid in Bitcoin
- In November, a hard-fork chain split of Bitcoin Cash occurred between two rival concepts, Bitcoin ABC and Bitcoin SV

2019

What to expect? Let us know in the forums!

2. Basics of Bitcoin Cryptography

Bitcoin and Cryptography

- **Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem, including:**
  - A decentralized peer-to-peer network (enabled by **the Bitcoin protocol**)
  - A public transaction ledger (**the blockchain**)
  - A decentralized mathematical and deterministic currency issuance mechanism (distributed **mining** and the **"Proof-of-Work"** concept)
  - A decentralized transaction verification system (transaction **script**)

(From "Mastering Bitcoin")

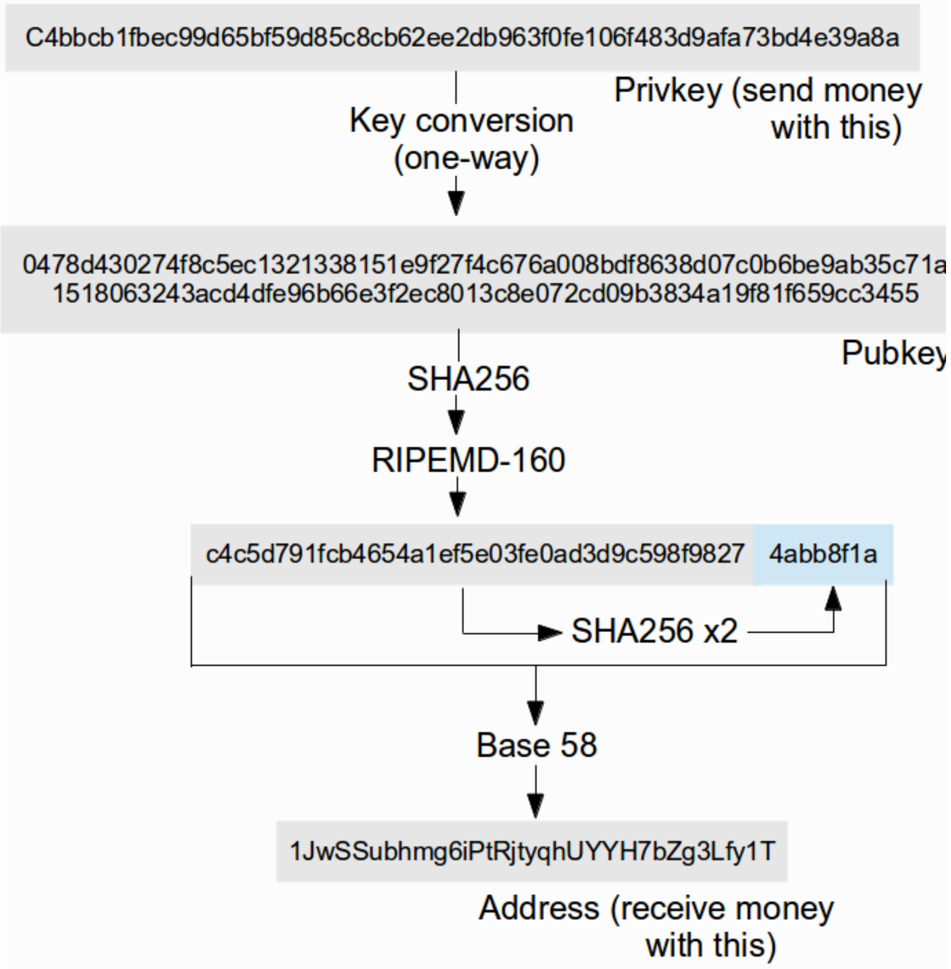
- **The Bitcoin system is based on decentralized trust, thus it heavily relies on cryptographic technologies, such as:**
  - Cryptographic hash functions (i.e. SHA-256 and RIPEMD-160)
  - Public Key Cryptography (i.e. ECDSA – the Elliptic Curve Digital Signature Algorithm)

Bitcoin and Cryptography

- In Bitcoin, a **transaction** is a record informing the network of a transfer of bitcoins from one owner to another owner.
  - *You may think of a transaction as the equivalent of a single line in a notebook page*
  - *You may think of a block as the equivalent of a page on that notebook*
  - *You may think of blockchain as the equivalent of the whole notebook*
  - *All the users are able to read, write and get updated on that notebook*

- Ownership of bitcoins is established through digital keys, Bitcoin addresses, and digital signatures.

- **Digital keys** are created and stored offline and consist of a mathematically-related Private-Public key-pair, created using the **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm (**ECDSA**).

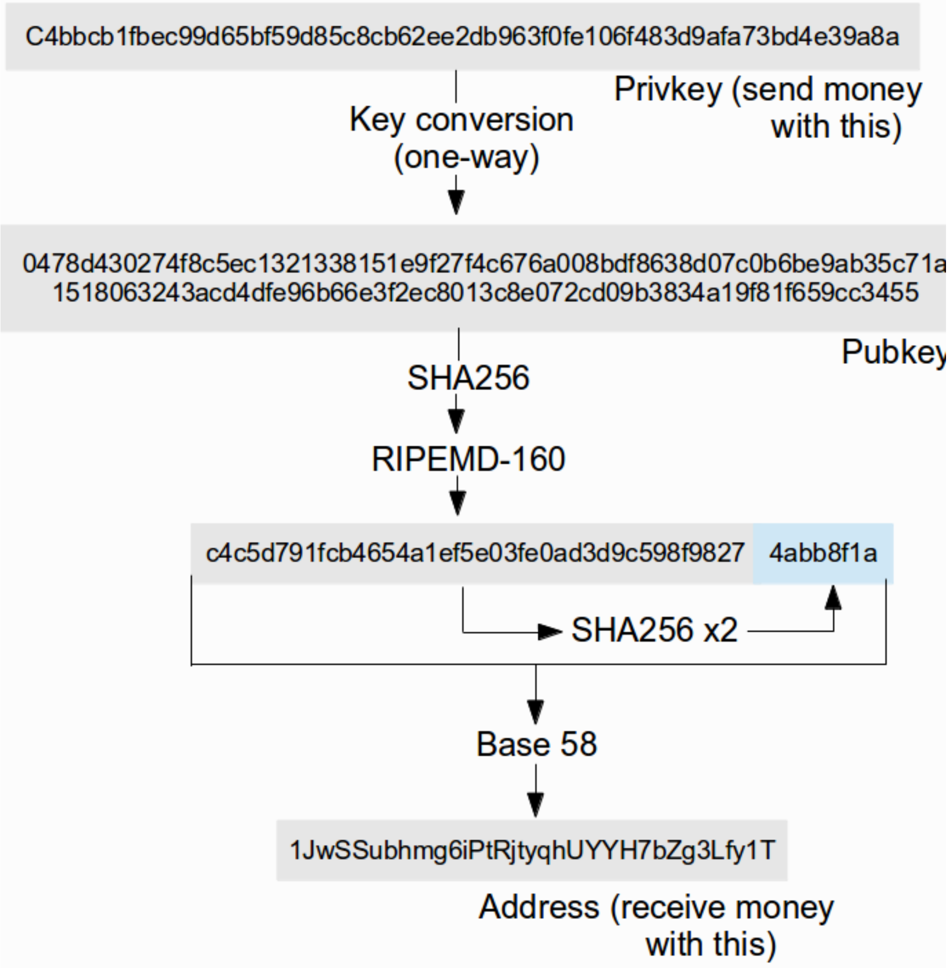


source

Bitcoin and Cryptography

- The **Private key (Privkey)** is initially generated at random, and is kept secret at all times. It is used by the current owner of bitcoins to digitally sign a Bitcoin transaction, when he authorizes the transfer to the new owner. A transaction's **digital signature** confirms ownership, and can be used to verify that the transaction is authentic.

- The **Public key (Pubkey)** is generated from the Private Key using a one-way cryptographic hash function. It is used by the new owner to validate a transaction's digital signature.



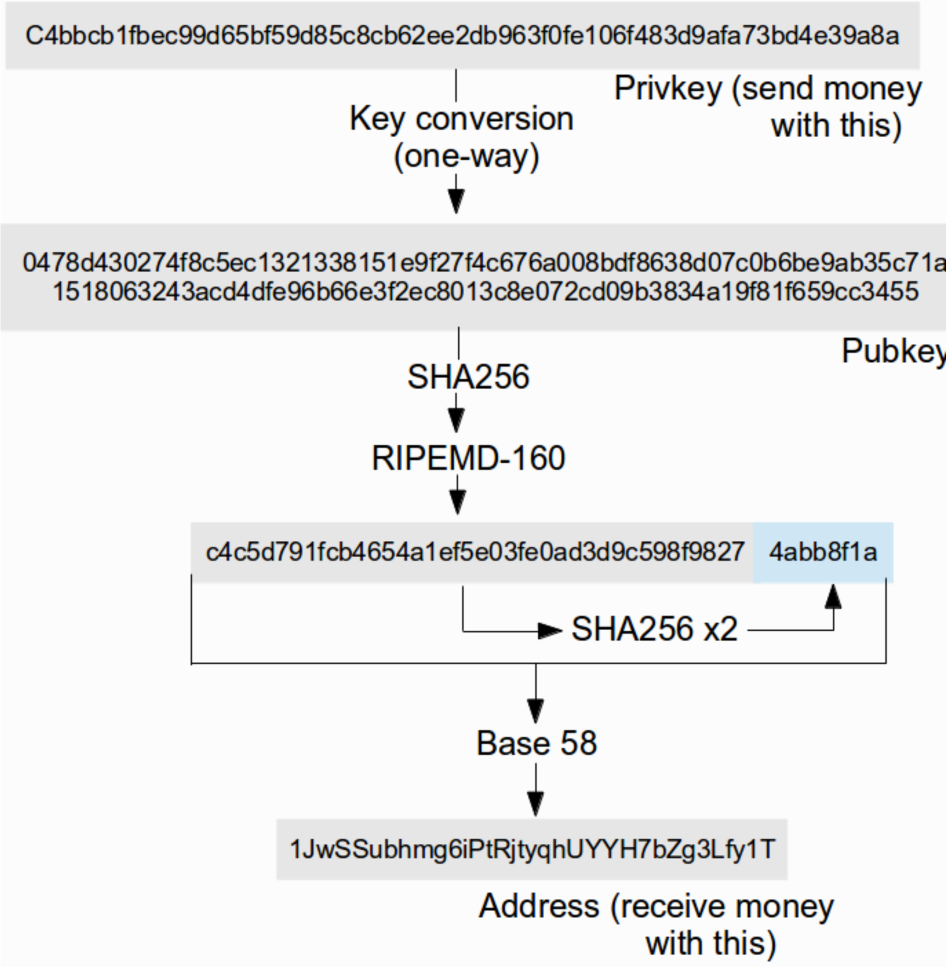
source

Bitcoin and Cryptography

- A **Bitcoin address**, which is a participant's unique identifier on the Bitcoin network, is usually generated by applying the SHA-256 and RIPEMD-160 cryptographic hash functions (discussed later), in series, on the Public key.

- Finally, Bitcoin addresses are encoded using Base58 encoding, which represents an address in a human-readable form of 58 alphanumeric characters.

Fun fact: While there are 62 characters if we take all small and capital letters and numbers, Satoshi wanted to avoid confusion in Bitcoin addresses over commonly mistaken characters, so he removed 4 of them: O0lI – which is which ?!?



source

Bitcoin and Cryptography

- When transactions are broadcasted over the network, the SHA-256 hash function is used to verify data integrity (i.e. to establish that data was not corrupted or modified during transmission).

- All Bitcoin transactions are stored in blocks, which are linked (or "chained") together in sequence to form the blockchain. Cryptographic hash functions are generally used to:
  - verify block integrity, and
  - establish the chronological order of the blockchain

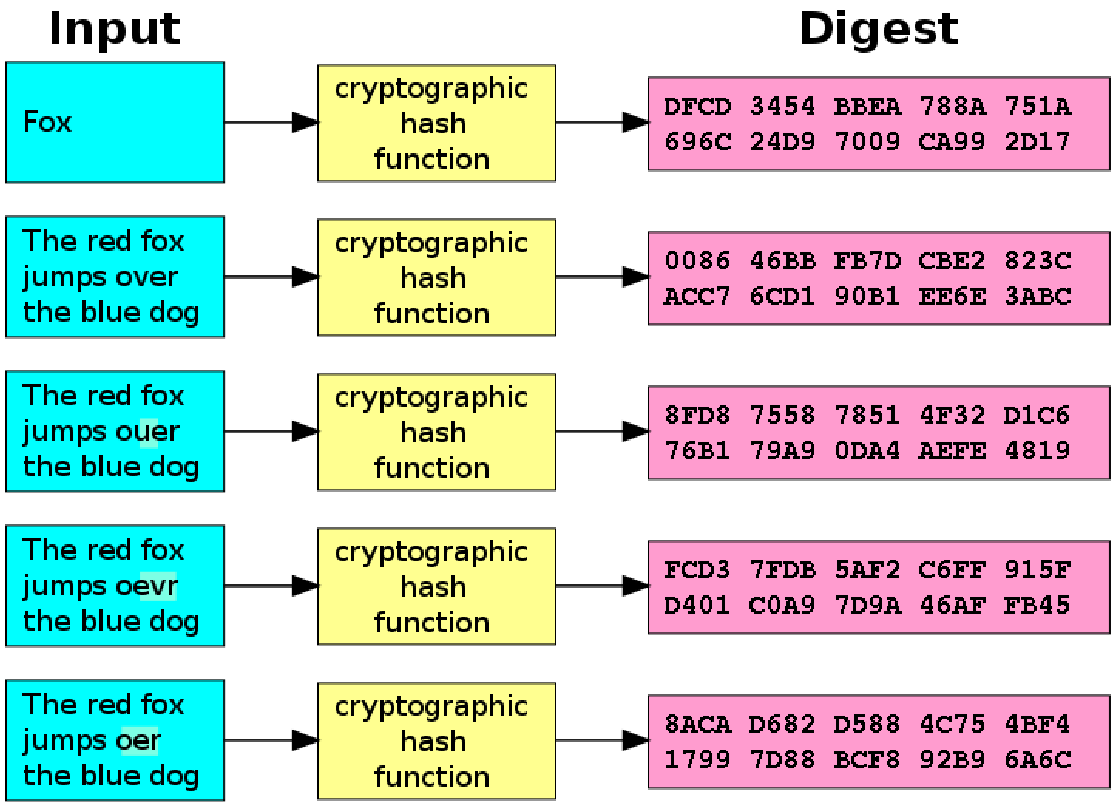
- Furthermore, hash functions are used as part of the ***Proof-of-Work (PoW)*** *algorithm*, which is a prominent part of the Bitcoin mining algorithm (discussed later in this session).

The following pages will explain the *basics* of cryptographic hash functions and public key cryptography, as used by Bitcoin.

Hash functions

- A cryptographic **hash function** is a mathematical function commonly used to verify the integrity of data, by transforming identical data to a unique, representative, fixed-size code. See the diagram for better understanding.

- Any accidental or intentional modification to the data (such as rearrange of letters) will completely change the hash code as displayed under *Digest*



Source

Hash functions

- Bitcoin uses the SHA-256 hash function, where the hash code is 256 bits (or 32 bytes) long

- The SHA-256 hash is usually presented as a string of 64 hexadecimal characters (i.e. each one of the 32 bytes is represented by 2 hexadecimal characters)

For example, the word "*Bitcoin*" produces the SHA-256 hash shown in the screenshot below (generated using the *sha256sum* Linux command).

```
# sha256sum
Bitcoin
b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4
```

Public Key Cryptography

- In Bitcoin, all transaction information is publicly visible to everyone in the network, and transactions are not encrypted. However, Bitcoin heavily relies on digital signatures (one of the main uses of Public Key Cryptography) to verify transactions in the network.

- In Public Key Cryptography, two keys are used:

  - K_{priv} the **Private key** which must be always kept secret by the owner, and
  - K_{pub} the **Public key** which is visible by everyone

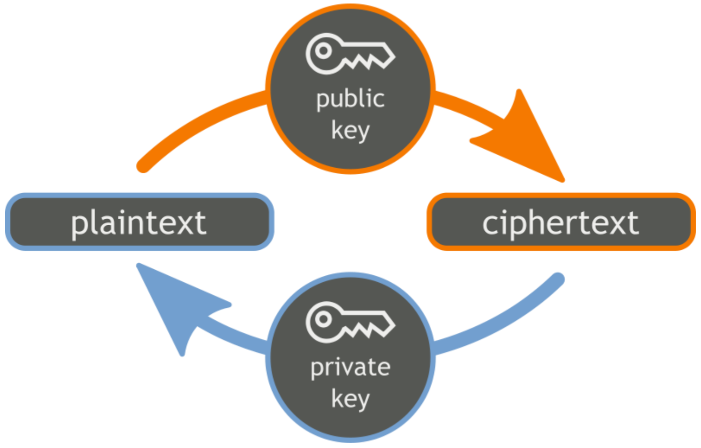
- Encryption = Turning a readable plaintext into cyphertext
- Decryption= Turning cyphertext into readable plaintext

Public Key Cryptography

- The sender encrypts the message **M** using the recipient's *public key*: C = encrypt(M, K_{pub})
- The recipient decrypts the encrypted message **C** using his own *private key*: M = decrypt(C, K_{priv})

Where: **C** is the result of encryption (also known as "ciphertext"), and **M** is the unencrypted/ decrypted message (also known as "plaintext").

- If the same key was used in Bitcoin for both encryption and decryption stages, then the relationship would be symmetric
- There is an ***asymmetric*** mathematical relationship between the public and private keys:
  - The public key can be easily derived from the private key
  - The private key is nearly impossible (or computationally infeasible) to derive from the public key



Source: Wikimedia Commons

Public Key Cryptography

- The public and private keys can also be swapped (i.e. are interchangeable):

For example, if one encrypts a message **<u>M</u>** with his private key: C = encrypt(M, $\mathbf{K}_{priv}$),

then this message can be decrypted using the corresponding public key: M = decrypt(C, $\mathbf{K}_{pub}$)

These two keys are mathematically linked through the asymmetric scheme of public key cryptography

- The above property is used by Bitcoin for digital signing, using **ECDSA (Elliptic Curve Digital Signature Algorithm)** to implement transaction ownership verification:
  - The private key is kept secret by the owner, and is used to sign a plaintext message
  - The public key (which is visible to everyone) can be used to verify the validity of the plaintext message's digital signature
  - If the plaintext message is long, the corresponding ciphertext might be long as well. Thus, a hash function is applied on the plaintext message first, and the result is used to produce the digital signature, instead.

Digital Signatures

- Digital signatures are used to create valid transactions by signing them.
- To make a Bitcoin payment, a Bitcoin transaction **T** is constructed. A subset **M** of the information in transaction **T**, is signed as follows:

1. Create transaction T

2. Select subset M of transaction T (e.g. Transaction identifier, transaction instructions, etc.)

3. Compute hash H of M:
   H = sha256(M)

4. Compute a signature S by encrypting hash H with the sender's private key:
   S = encrypt(H, $\mathbf{K}_{priv}$)

5. Send the signature S and the public key $\mathbf{K}_{pub}$ along with the transaction T to Bitcoin miners.

Digital Signatures

- To verify a transaction T received with signature S and public key K_{pub} , a receiver will:

1. Select subset M of the information in transaction T

2. Compute hash H of M: H = sha256(M)

3. Decrypt signature S with the public key K_{pub}:

   H' = decrypt(S, K_{pub})

4. Compare H and H'. If they match, then the signature is valid and the transaction is valid

Digital Signatures

- In summary:
  - Each transaction associates an amount of bitcoins with a bitcoin address, which is usually produced from a hash of the owner's public key
  - When bitcoins are sent to someone, the transaction records the transfer of bitcoins from the current owner’s Bitcoin address to the new owner's Bitcoin address, and includes a valid transaction signature
  - When this transaction is broadcast to the Bitcoin network, every peer knows that the new owner of these bitcoins is the owner of the receiving Bitcoin address
  - The current owner’s signature verifies for everyone that the transaction is authentic
  - The complete history of transactions is kept by every peer in the Bitcoin network, so anyone can verify who is the current owner of any particular amount of bitcoins

Digital Signatures

Both the Public and Private keys are stored in a Bitcoin wallet.

```
>getaddressesbyaccount ""
[
"1aavsnddTKS3fWFiW83t9vwqHCZYrpFAd"
]
>dumpprivkey 1aavsnddTKS3fWFiW83t9vwqHCZYrpFAd
L3nzYUMrpMua59tqgnR7Gk37nvr5458auGzXRWQnUWY5fuZCu6ab
```

A Bitcoin wallet, similarly to a credit card, does not contain any bitcoins, but only the Private-Public key-pairs as mechanisms that allow you to access your funds. The output above was produced by the bitcoin Core daemon and reveals the Private key:

L3nzYUMrpMua59tqgnR7Gk37nvr5458auGzXRWQnUWY5fuZCu6ab

which is used to derive its corresponding Public key, and then the Bitcoin address:

1aavsnddTKS3fWFiW83t9vwqHCZYrpFAd

Some more of the core features will be covered in Session 5 (Bitcoin in practice - part 2)

3. Transactions and the Blockchain

From Digital Signatures to Bitcoin

- We saw how Digital Signatures, a crucial part of many systems involving digital transactions, can be used to convey private information using Public Key Cryptography

- When we need to transfer a digital title of ownership without a central authority, we need a ledger that records these changes in ownership, so that these changes cannot be refuted or altered by malicious activity

- Next, **we will see how Digital Signatures and hash functions are used to form the blockchain** of the Bitcoin protocol, i.e. its distributed ledger of transactions.

P2P Network and Ownership

- Bitcoin is run over a peer-to-peer (P2P) network of computers, called **nodes**
- Nodes are responsible for processing transactions and maintaining all records of ownership
- Anyone can download the free open-source Bitcoin software and become a node
- All nodes are treated equally, and **no single node is trusted**. However, **the system is based on the assumption that the majority of computing power (i.e. at least 51%) will come from honest nodes**
- Ownership records are replicated on every node
- Bitcoin users possess digital keys that allow control over bitcoins recorded in a public ledger *(the blockchain)*
- The public ledger records transactions transferring ownership of a quantity of bitcoins from one owner to the another, like a double-entry bookkeeping ledger

Addresses

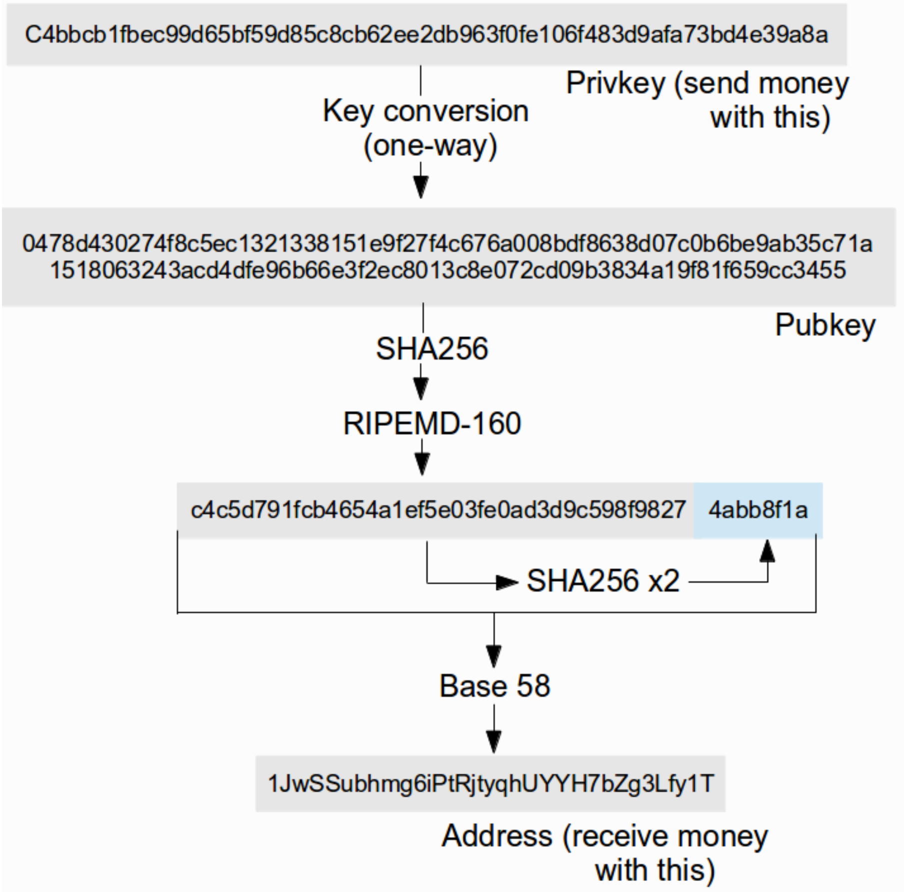
- Transactions in the blockchain do not record the public keys or recipients, but instead use an abstraction called a "Bitcoin address" to record the beneficiary of each amount, allowing for greater flexibility
- To create a Bitcoin address, the Bitcoin client software first generates an ECDSA Public-Private key-pair from a random number
- The Bitcoin address is then generated by applying the following algorithm, in order:

```
version  = (1 byte version number)
keyHash  = RIPEMD-160(SHA-256(publicKey))
data     = version + keyHash
dataHash = SHA-256(SHA-256(data))
checksum = (first 4 bytes of dataHash)
address  = Base58Encode(data + checksum)
```

Addresses

As noted earlier, a Bitcoin address is a computation based on the user's Public key:

- The ***keyHash*** is produced by applying the SHA-256 and RIPEMD-160 hash functions, in series, on the *Pubkey*
- ***Data*** is a concatenation of **keyHash** and an *address* ***version*** *number*
- The ***dataHash*** is produced by applying the SHA-256 algorithm twice on ***Data***
- However, only the first 4 bytes of the ***dataHash*** are used as a **checksum**
- The bitcoin ***address*** is a concatenation of ***Data*** and ***checksum*** encoded in Base58 encoding.
- ***Base58Encode*** is a function that encodes binary as text using the Base58 encoding.



source

Transactions

- A Bitcoin **transaction** tells the network that the owner of a number of bitcoins has authorized the transfer of some of these bitcoins to another owner
- The new owner can now spend these bitcoins by creating another transaction that authorizes transfer to another owner, and so on, in a chain of ownership
- Transactions are like lines in a double-entry bookkeeping ledger. Each transaction contains one or more **inputs**, which are debits against a Bitcoin account
- On the other side of the transaction, there are one or more **outputs**, which are credits added to a Bitcoin account
- The inputs and outputs (debits and credits) do not necessarily add up to the same amount. Instead, outputs add up to slightly less than inputs and the difference represents an implied **transaction fee**, a small payment collected by the miner who includes the transaction in the ledger
- The transaction contains proof of ownership for an amount of bitcoins (inputs) whose value is transferred, in the form of a digital signature from the owner, that can be independently validated by anyone in the Bitcoin network

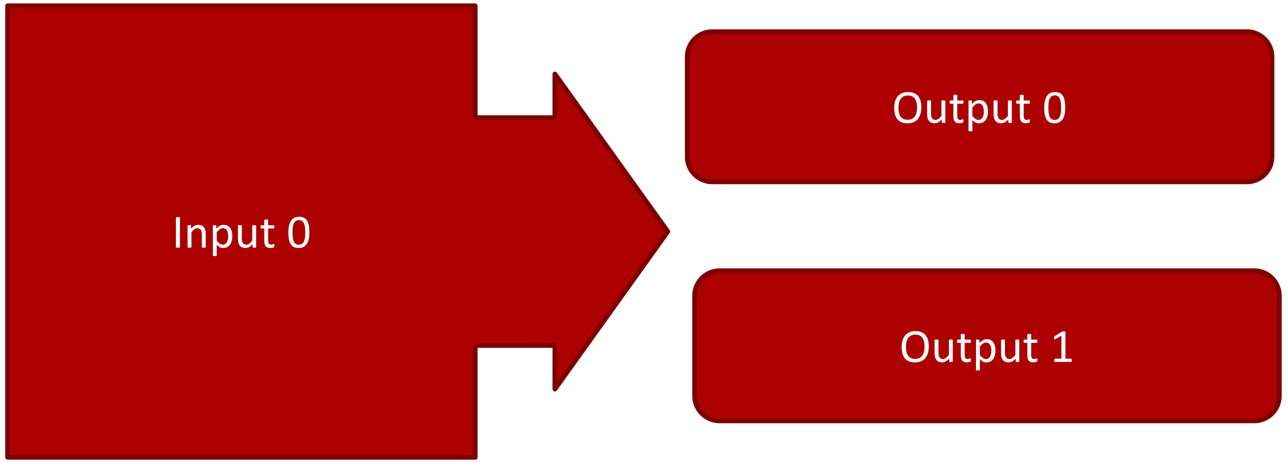
Transactions

We can see that outputs of one transaction are inputs for the next transaction

(From "Mastering Bitcoin")

Transactions

- The most common form of transaction is a simple payment from one Bitcoin address to another, which often includes some “change” to be returned to the original owner. This type of transaction has one input and two outputs and is shown below:



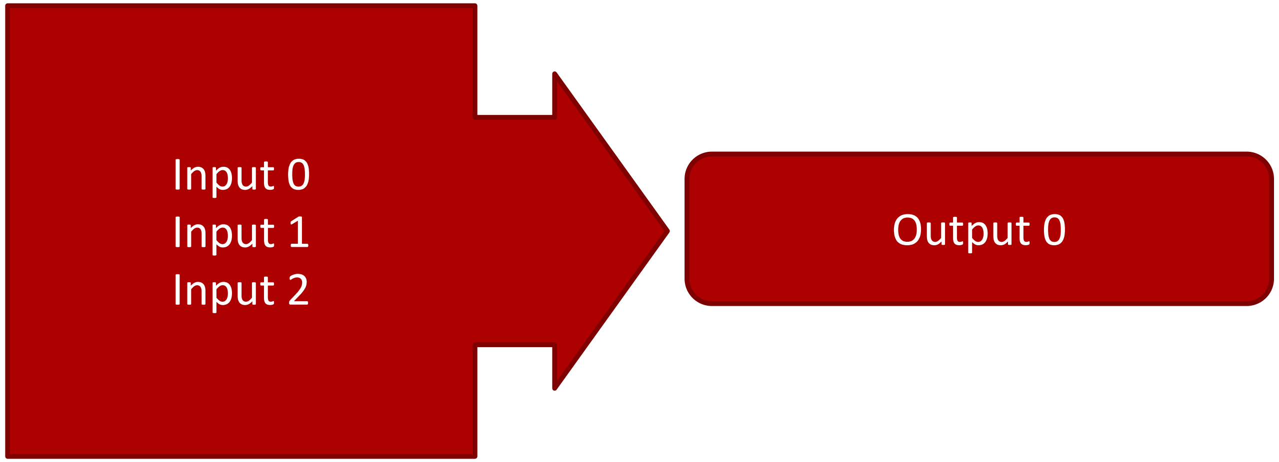
Transactions

- Real example of this type of transaction:

- You're welcome to use any "block explorer" to search through the whole blockchain, since all transactions are publicly visible. Here's list you can choose from : http://bit.ly/blockexplorers
- Pick one and follow any transaction in there, and see what you can find about the inputs, outpus, change and how it's connected with previous ones

Transactions

- Another common form of transaction is a transaction that aggregates several inputs into a single output. This represents the real-world equivalent of exchanging a pile of coins and currency notes for a single larger note. Transactions like these are sometimes generated by wallet applications to cleanup lots of smaller amounts that were received as change for payments.



Transactions

- Real example of this type of transaction:

a2d7f24a020d2c1c4d1abaec07a4ae8d7fa04a9ec9e1d0230834efd9d48ffccf 2014-01-14 00:36:37

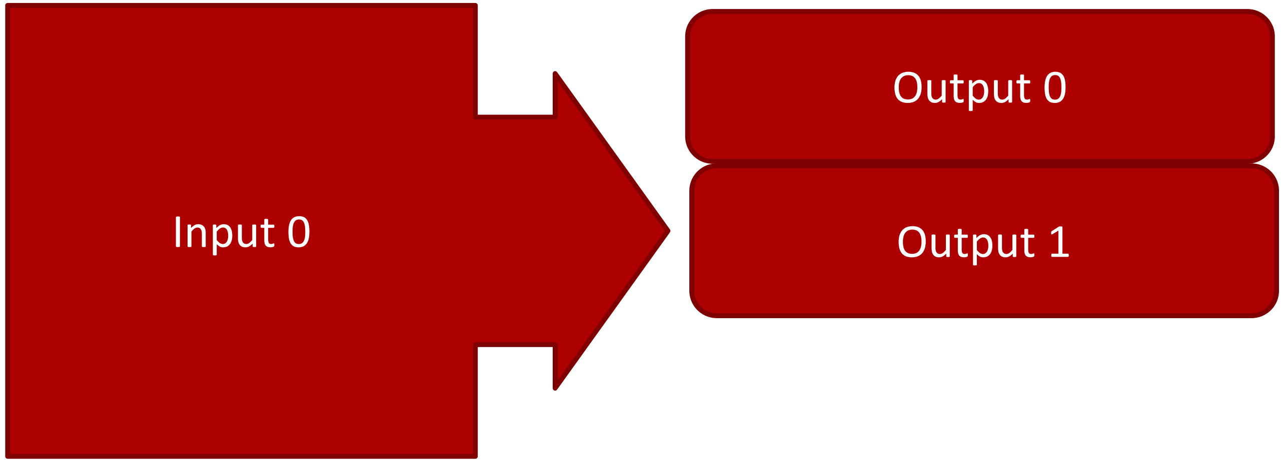
1CXyk23Sy3pnVz8G9EN95HbHzpT9WXXhaB
1HbRuiWGBayVsCcz4goYFypHNUR7huAPbr
1P4mBUEUaZnDpREZD8Tk8BAFMKPnPpP97S
1CdoNnxx3A6QvMqJuuy9ER5MW7MiVjovFH
19BPriDhWRpmPaMVEja42tbgACjXHAbBYA
1FVC7eFrTQiBPUg7jv9AJF3oc4wDvud3GK
1MHAfAXefHKxbjEQWWTajmNSb2wqSXAoTA
18KTTPULXw5NTQQj3b6HrfAMRz6Jh4YQ8f
1QCV36hs1yuYJNSzjkxfwfiW7NhdYGJp3D
19wpPopMDWySLeMhP8LVA71GtUDzPN668x

→ 114RkSMy4q2deixQStcru7pbQFU9hwczEH 16.47174935 BTC

16.47174935 BTC

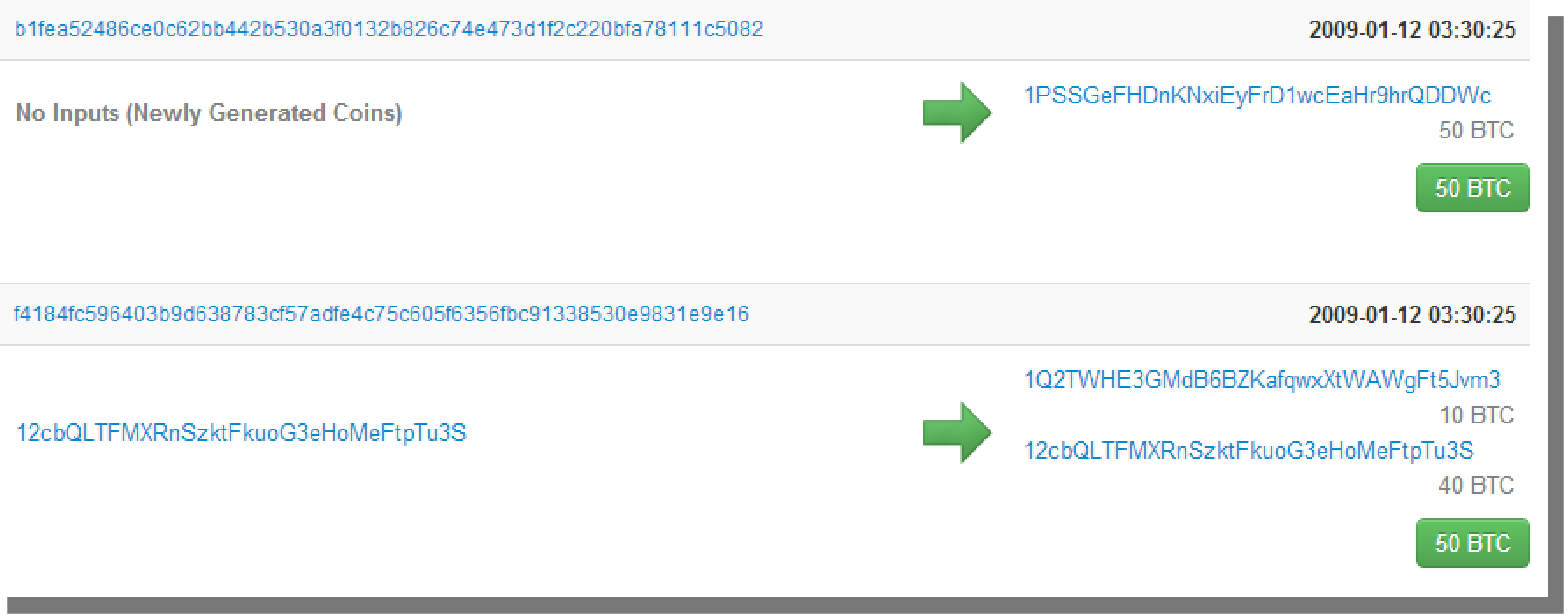
Transactions

- Finally, another transaction form that is often observed in the Bitcoin ledger is a transaction that distributes one input to multiple outputs representing multiple recipients. This type of transaction is sometimes used by commercial entities to distribute funds, such as when processing payroll payments to multiple employees.



First Transaction Ever

- Below is the first transaction ever performed between Satoshi and Hal Finney. We can also see the coinbase transaction that rewarded that block’s discovery with 50BTC without having any inputs. The transaction was for 10 BTC so 40 BTC are returned as change.

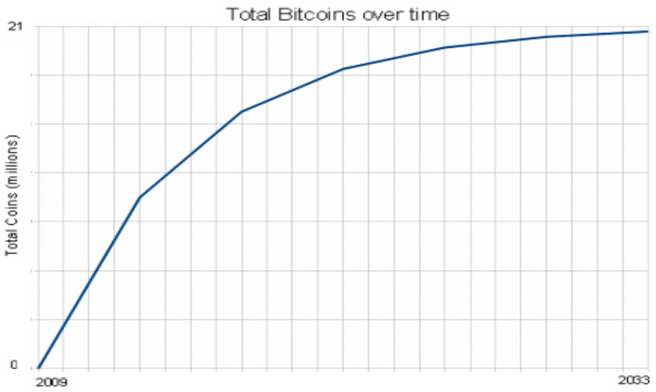


4. Mining

Mining

- The Bitcoin system of trust is based on computation. **Transactions** are bundled into **blocks**, which require an enormous amount of computation to “prove” (or “confirm”), but only a small amount of computation to verify as “proven”, in a process called **mining**

- **Mining creates new bitcoins in each block**, almost like a central bank printing new money. The amount of bitcoins to be created is fixed and diminishes with time (see Session 2)
- **Mining creates trust** by ensuring that transactions are confirmed only when enough computational power was devoted to the block that contains them. More blocks mean more computation, which means more trust.



Bitcoin production over time

Mining algorithm

- Mining consists of the following steps, which are performed in a continuous loop:
  - **Bundling transactions** that were broadcast on the peer-to-peer network into a **block**. Each miner can arbitrarily decide which transactions to include in their block
  - **Verifying** that all **transactions** in the block are **valid**
  - **Selecting the most recent block** on the longest path in the blockchain and **inserting a hash of its header into the new block**
  - **Trying to solve the Proof of Work (PoW) problem for the new block** and simultaneously watching for new blocks coming from other nodes

- If a solution is found to the Proof of Work problem, the new block is added to the local blockchain and broadcast to the peer-to-peer network

Proof of Work

- Miners search for acceptable blocks using the following procedure, performed in a loop:
  - Increment (add 1 to) an arbitrary number in the block header called a **nonce**
  - Take the hash of the resulting block header
  - Check if the hash of the block header, when expressed as a number, is less than a predetermined target value
- If the hash of the block header is not less than the target value, the block will be rejected by the network. Finding a block that has a sufficiently small hash value is the PoW problem.
- **Mining performance, therefore, is measured in hashes/sec**. Currently the performance of miners is measured in GH/s (billions of hashes per second) or TH/s (trillions of hashes per second)

H/ s = Hashes per second	1,000 H/ s = 1 KH/ s
KH/ s = Kilo Hashes per second	1,000 KH/ s = 1 MH/ s
MH/ s = Mega Hashes per second	1,000 MH/ s = 1 GH/ s
GH/ s = Giga Hashes per second	1,000 GH/ s = 1 TH/ s
TH/ s = Tera Hashes per second	1,000 TH/ s = 1 PH/ s
PH/ s = Peta Hashes per second	

Mining Difficulty

- Bitcoin nodes that mine, actively regulate the rate of creation of new blocks
- As more miners join, the rate of block creation will go up. As the rate of block creation goes up, the **mining difficulty** rises to compensate, which pushes the rate of block creation back down
- **The creation of new blocks must take an average of 10 minutes**
  (Ten minutes was specifically chosen by Satoshi Nakamoto as a tradeoff between fast confirmation time and the amount of work wasted due to chain splits and orphan blocks. Read more about this here)
- The regulation is done by periodically adjusting the hash target value for blocks
- Every 2,016 blocks (which ideally spans every 2 weeks, with each block taking 10 minutes to confirm) Bitcoin nodes calculate a new difficulty accordingly, based on the time it took to mine the last 2,016 blocks
- In December 2018, Bitcoin's mining difficulty saw its second largest drop in history, with a 15% adjustment.

Mining Reward

- Solving the Proof of Work problem requires a lot of computing power and that power costs money. To encourage participants to invest their resources in mining, Bitcoin provides a reward in each successfully mined block (**plus the transaction fees** of the transactions contained in the new block)

- When a block is discovered, the discoverer will award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network
  - Currently this bounty is 12.5 bitcoins
  - Based on Bitcoin's algorithm, this bounty halves every 210,000 blocks (i.e. approximately every 4 years)
  - Eventually, the reward will be removed entirely when the limit of 21 million bitcoins is reached asymptotically, by the year 2140
  - After that, transaction processing will be rewarded solely by transaction fees

- As mentioned in the first bullet, the miner is awarded in addition the fees paid by Bitcoin users sending transactions

Solo Mining

- **Solo mining** is when you use your computer (or specialized mining hardware) to search for blocks. In this case, you are getting paid only when you personally find a block, receiving the full amount of the reward, plus any transaction fees
- This type of mining was efficient only when the mining difficulty was low enough to expect to find new blocks relatively often
- Today (February 2018), the hashrate of the Bitcoin network is over 20,000,000 TH/s (!!). In order to mine one block per day, your mining rig should perform with the speed of:
  - 20,000,000 TH / 24 Hours / 6 Blocks per Hour = 833,327.2 TH/s ≈ 833 PH/s
- In this case, you are getting paid only when you personally find a block, receiving the full amount of it, plus any transaction fees

Pool Mining

- **Mining pools** collect all of the hashing from miners and basically run them off of one account
- When a block is found, the mining pool's wallet is the one that gets the payment, and then the payments are split and distributed into each miner's site account based on their personal contribution towards finding the block
- For example, if a miner contributed half of the pool's shares into finding the new block, they would get half of the block reward

Mining pools

- Most pools work using the following algorithm:
  - The pool server prepares a block with the coinbase transaction pointing to the pool's address
  - Miners in the pool contact the pool server and make a getwork request to get the block to work on
  - Each miner tries to solve the Proof of Work problem for the block, by incrementing the nonce and hashing the block header
  - Whenever a miner finds a hash value that is below the easier target, it submits the solution to the server for a share
  - The mining server verifies submitted shares and tracks how many each miner has
  - When a miner finds a solution to the Proof of Work problem, the server pays out the reward in proportion to the number of shares each miner earned since the last payout
  - Miners periodically contact the pool server for updates on what to work on, in case a new block was discovered

Pool Mining - Rewards

- Mining pools use different distribution schemes, the most popular of which are:

  - **PPS (Pay Per Share):** Each miner gets paid a guaranteed amount for every share they submit. Pools that use this method often employ custom pool difficulties as well, rather than allowing for variable difficulties. This makes the calculations a lot easier and ensures every miner is fairly treated

  - **PPLNS (Pay Per Last Number of Shares):** Each miner gets paid based on the last x number of shares after a block is found. For example, if it is set to pay at 5,000 shares and a miner has contributed 2,500 of the last 5,000, this miner would get half of the block's payment

  - **Proportional:** Each miner gets paid based on the proportion of shares since the last block. This is a lot like PPLNS, but instead of only counting n shares, it counts every share between each block and then calculates the payments based on each person's proportional amount

Mining Hardware

- **CPU mining**: Initially, Satoshi's Bitcoin client software did mining on a user's PC (i.e. CPU mining), but now CPUs have been eclipsed by more efficient mining hardware.

- **GPU mining**: GPUs (i.e. Graphics Processing Units on Graphics cards) are designed for doing lots of mathematical calculations in parallel and are orders of magnitude faster than CPUs

- **FPGA (Field Programmable Gate Arrays):** An intermediate step between a fast processor and a dedicated ASIC, FPGAs were used until ASICs emerged and dominated Bitcoin mining

- **ASIC mining:** ASICs (Application-Specific Integrated Circuits) are custom built for a particular application and are thus orders of magnitude faster than GPUs, which are general-purpose. In Bitcoin, these chips are customized to only perform SHA-256 hashing.

- Today, ASIC mining is the only economically efficient mining technique.

Other Consensus Mechanisms

- Several consensus mechanisms have evolved with the aim to approach distributed consensus on various ways
- Most notable examples are:
  - Proof-of-Stake
  - Delegated Proof-of-Stake
  - Proof-of-Burn
  - Proof-of-Importance
  - And more…
- Cryptocurrencies with a significant market share such as Peercoin, NEM, NXT rely on some of these consensus protocols. Ethereum is also expected to switch to Proof-of-Stake algorithm in 2019 to address scaling issues
- We will explore all these consensus protocols during a later session

5. Conclusions

Conclusions

- The Bitcoin protocol relies on the following cryptographic techniques:
  - Hash functions (i.e. SHA-256, RIPEMD-160)
  - Digital signatures (i.e. using ECDSA, and specifically the Secp256k1 curve)

- The Bitcoin network is:
  - Distributed (i.e. it does not have any central points of trust/failure)
  - Secure (as long as more than 50% of nodes are trustworthy)
  - Reliable (transaction ledgers are massively replicated by all network nodes)

- Bitcoin generation is self-regulated and based on a mathematical algorithm

Some Further Reading (1/2)

Bitcoin Wiki

https://en.bitcoin.it/

Mastering Bitcoin, Andreas Antonopoulos
https://www.amazon.com/Mastering-Bitcoin-Unlocking-Digital-Cryptocurrencies/dp/1449374042

Mastering Bitcoin (2nd edition), Andreas Antonopoulos
https://bitcoinbook.info/

Hashcash - a denial of service counter-measure , Adam Back, 2002.

http://www.hashcash.org/papers/hashcash.pdf
(Introduces the Proof-of-Work concept)

How Bitcoin transactions work

http://visual.ly/bitcoin-infographic

Some Further Reading (2/2)

How Bitcoin Works Under the Hood

https://www.youtube.com/watch?v=Lx9zgZCMqXE

Bitcoin Mining Pools

https://www.bitcoinmining.com/bitcoin-mining-pools/

Ethereum's Proof of Stake Casper Testnet Nears Launch

https://www.trustnodes.com/2017/11/28/ethereums-proof-stake-casper-testnet-nears-launch

Ethereum Mining

https://www.coindesk.com/information/ethereum-mining-works

Inputs and Outputs – Bitcoin "change" Explained

https://99bitcoins.com/inputs-outputs-bitcoin-change-explained/

ASIC Mining

https://www.buybitcoinworldwide.com/mining/hardware/

UNIVERSITY *of* NICOSIA

Questions?

Contact us:

Twitter: @mscdigital
Course Support: digitalcurrency@unic.ac.cy
IT & Live Session support: dl.it@unic.ac.cy