UNIVERSITY of NICOSIA

Session 3

# The Basics of Cryptocurrencies: Cryptography, Transactions and Mining

MSc in Digital Currency

# Session 3: The Basics of Cryptocurrencies

## Cryptography, Transactions and Mining

We are about to step into the more technical aspects of Bitcoin. They are crucial in understanding the foundations of Bitcoin and how its network operates.

For students without a technical background, familiarization with several new concepts will be required. But, we guarantee it will be a very rewarding experience in the long term!

**Objectives**

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

# Session 1: Agenda

1. A Brief History of Bitcoin/Crypto
2. Basics of Bitcoin Cryptography
3. Transactions and the Blockchain
4. Mining
5. Core Development and Improvement Proposals
6. Conclusions
7. Further Reading

# 1. A Brief History of Bitcoin/Crypto

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2008 | |
|---|---|
| 18 August | The domain name Bitcoin.org was registered, owned by Satoshi Nakamoto and Martti Malmi. Eventually, Satoshi gave ownership of the domain to additional people, separate from the Bitcoin developers, to spread responsibility and prevent any one individual from gaining control of the Bitcoin project. |
| 15 September | Lehman Brothers filed for Chapter 11 Bankruptcy protection. This remains the largest bankruptcy filing in U.S. history, triggering a lack of trust towards the banking system. |
| 31 October | Satoshi Nakamoto publishes the Bitcoin whitepaper, which first introduced the foundation of Bitcoin and blockchains. |
| 9 November | Bitcoin Project registered at sourceforge.net |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2009 | |
|---|---|
| 3 January | A headline from *The Times*, "Chancellor on Brink of Second Bailout for Banks," was quoted by Satoshi Nakamoto in the genesis (first) block on the Bitcoin blockchain. Suggesting the initiation of the Bitcoin project was a response to woes in the financial system. |
| 3 January | The genesis block, the first block of the Bitcoin network, is mined. The block reward is 50 BTC. |
| 9 January | First Bitcoin client (bitcoind v0.1) was released. |
| 12 January | First Bitcoin transaction: Satoshi Nakamoto sends 10 BTC (40 BTC in change) to Hal Finney. The transaction was included in block 170. (see slide 50) |
| 30 December | First difficulty adjustment, rising from 1 to 1.18 at block 32256. |

Source: https://en.bitcoin.it/wiki/2009

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2010 | |
|---|---|
| 17 March | Trading opens on the first bitcoin exchange site (Bitcoin Market). |
| 22 May | Known as 'Pizza Day': Laszlo Hanyecz paid 10,000 bitcoin for two delivered pizzas in Jacksonville, Florida. The transaction's value at the time was $8, given $0.0008 USD (price of bitcoin) x 10,000 BTC. At current prices, it is now worth hundreds of millions of dollars. |
| 18 July | OpenGL GPU hash farm established by ArtForz; GPU (Graphic Processing Unit) mining begins. |
| 15 August | A vulnerability (CVE-2010-5139) in Bitcoin was exploited which lead to the generation of 184 billion additional bitcoin in block 74638. This was a major problem, considering one of Bitcoin's essential properties is the fixed supply of coins (approximately 21 million). The bug was quickly detected and a patched client (invalidating the transaction) was released within five hours, which achieved majority consensus in the network by block 74691. |
| 27 November | Pooled mining becomes available with Bitcoin.cz, now known as Slush Pool (mining pools will be discussed in Section 4 of this session). |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2011 | |
|---|---|
| 9 February | Bitcoin reached parity with the U.S. dollar for the first time (1 USD = 1 BTC) on Mt. Gox. |
| 5 May | Bitcoin's difficulty passed 1 TH/s (1 trillion hashes/sec) for the first time. |
| 11 June | First and largest publicly reported theft of bitcoin at the time; 25,000 BTC with a value of $375,000 USD. |
| 19 August | The first Bitcoin Conference and World Expo held in New York City. |

| 2012 | |
|---|---|
| 27 September | Bitcoin Foundation announced. |
| 28 November | First Bitcoin Halving Day observed, where the block reward halved from 50 to 25 BTC with block 210,000. Since the genesis block in 2009, 10.5 million bitcoin had been mined, which was roughly 56% of the total supply. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2013 | |
|---|---|
| 11 March | A chain fork occurred due to some incompatibility between v0.8.0 and pre-0.8.0 clients. |
| 28 March | Total bitcoin market capitalization exceeded $1 billion USD for the first time. |
| 30 May | Bitcoin mining difficulty passed 100 TH/s (100 trillion hashes / second). |
| 21 November | University of Nicosia becomes the world's first university to accept bitcoin for tuition. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2014 | |
|---|---|
| 7 February | The Tokyo-based bitcoin exchange Mt. Gox halts withdrawals. Later in the month, it was discovered that about 850,000 BTC (750,000 of which belonged to customers) had been stolen. The case highlighted the risks of storing funds with a custodial exchange. |
| 2 April | University of Nicosia launched the world's first Master's Degree in Digital Currency. |
| 14 September | University of Nicosia issued its certificates on the Bitcoin blockchain. |
| 31 October | Bitcoin mining difficulty passed 300 TH/s (300 trillion hashes per second). |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2015 | |
|---|---|
| 4 February | Alleged Silk Road operator Ross Ulbricht is convicted on all counts. In March, two law enforcement agents who led the investigation are charged with wire fraud, money laundering, and other offenses. Ulbricht is sentenced in May to double-life imprisonment plus forty years without parole. The murder-for-hire charge was dismissed with prejudice. |
| 8 August | The "BitLicense" came into effect for New York State, after being proposed in July 2014. It defines and regulates 'virtual currency business activity.' |
| 22 October | The Court of Justice of the European Union issued its first ever ruling on bitcoin, stating that it was indeed a currency and a means of payment, not a commodity or an asset (as some argued). Bitcoin was also exempt from VAT. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2016 | |
|---|---|
| 14 January | Joseph Poon and Thaddeus Dryja publish the Lightning Network whitepaper. |
| 4 April | OpenBazaar, the first decentralized marketplace, was released with bitcoin as a payment method. |
| 2 May | Craig Wright fraudulently claimed to be the creator of Bitcoin by reusing an old signature from an early block that Satoshi Nakamoto reportedly mined. |
| 9 July | The second bitcoin halving occurred, reducing the block reward from 25 to 12.5 bitcoin per block. Since the genesis block in 2009, 16.4 million bitcoin had been mined, which was roughly 78% of the total supply. |
| 3 August | Bitfinex, the largest bitcoin exchange by volume, was hacked with 119,756 BTC stolen. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2017 | |
|---|---|
| 1 January | The bitcoin price broke over $1,000 USD for the first time since 2014. |
| 1 April | Japan categorized bitcoin as legal currency, after disputes between regulators and exchanges. |
| 1 August | The Segregated Witness (SegWit) soft fork was activated on Bitcoin after a months-long scaling debate. A portion of the network created a hard fork, dubbed Bitcoin Cash. |
| 29 September | Japan officially recognized 11 companies as Bitcoin exchanges. |
| 31 October | CME Group announced the launch of Bitcoin futures. |
| 7 December | Bitcoin price reached new all-time-high of $19,783 USD. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2018 | |
|---|---|
| 6 February | Bitcoin price dropped 60% to around $7000 USD, initiating its downward slope for the year. |
| 5 March | The U.S. Marshals auctioned off 2,170 BTC, worth circa $25 M, seized in connection with federal, criminal, and civic cases. |
| 15 March | Lightning Labs releases the first Lightning mainnet beta client. |
| 21 March | Twitter CEO Jack Dorsey says Bitcoin will overtake the US Dollar to become the world's primary currency in ten years or less. |
| 27 September | Blockstream's Liquid sidechain for Bitcoin goes live. |
| 31 October | Bitcoin's whitepaper turns 10 years old. The CoinJoin wallet Wasabi launches. |
| 26 November | Ohio becomes the first U.S. state to accept tax payments converted from bitcoin via BitPay, after many other states including Arizona, Georgia, and Illinois previously scrapped such plans. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2019 | |
|---|---|
| 4 February | Canadian crypto exchange QuadrigaCX cannot repay most of $190 million in client holdings after founder Gerald Cotten, the only person who supposedly had access to private keys, unexpectedly died. |
| 19 February | Block.co was established by University of Nicosia to issue blockchain verifiable certificates. |
| 8 May | Hackers stole $41 million worth of bitcoin from the Binance exchange. |
| 28 August | Satoshi Labs implements Shamir Secret Sharing in their Trezor hardware wallet (SLIP-0039). |
| 23 September | Bakkt launches futures contracts. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2020 | |
|---|---|
| 13 January | Suredbits and Crypto Garage announce work on specification for discreet log contracts (DLCs). Chris Stewart and Nicolas Dorier made Bitcoin's first-ever DLC bet on the outcome of the U.S. presidential election. |
| 19 January | Drafts of the Taproot / Schnorr proposals (#340, #341, and #342) are published. Pieter Wuille had written to the mailing list about adding Schnorr signatures back in July 2018. In October 2020, the code was merged into Bitcoin Core. |
| 4 March | A draft Lightning Watchtower protocol specification is published. |
| 11 May | The third bitcoin halving occurred, reducing the block reward from 12.5 to 6.25 bitcoin. |
| 25 May | A design proposal for CoinSwap is published by JoinMarket developer Chris Belcher. |
| 31 December | Bitcoin price reached new all-time-high above $29,000. |

# A Brief History of Bitcoin/Crypto

## Major events in the history of Bitcoin

| 2021 | |
|---|---|
| 14 January | Bitcoin Core v0.21 with the Schnorr / Taproot code is released. In June, it is locked in for scheduled activation on mainnet in November. |
| 15 April | Bitcoin's price reached a new all-time-high above $63,000. |
| 16 May | Following a crackdown on "energy-intensive enterprises" in the China, Bitcoin's hash rate dropped more than 40%, but began recovering in July. |
| 30 May | Ed Carpenter Racing (ECR) team member Rinus VeeKay drove the No. 21 Bitcoin Chevrolet in the annual Indianapolis 500, finishing in 8th place. |
| 7 Sept | The nation of El Salvador adopted Bitcoin as legal tender alongside USD. |

# 2. Basics of Bitcoin Cryptography

# 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" consensus algorithm)
- A decentralized transaction verification system (transaction script) (From "Mastering Bitcoin" Andreas Antonopoulos, 2014)

**As such, it relies heavily on cryptographic technologies, such as:**

- Hash functions (i.e. SHA-256 and RIPEMD-160)
- Public Key Cryptography (i.e. ECDSA – the Elliptic Curve Digital Signature Algorithm)

# Basics of Bitcoin Cryptography

## Bitcoin and Cryptography

A transaction is a record that informs the network of a transfer of funds or value from one owner to another.

- Think of a transaction as a single line on a page in a notebook.
- Think of a block as the page in that notebook.
- And think of the blockchain as being equivalent to the entire notebook.
- All the users are able to read, write, and get updated on what is written in this notebook.

Ownership of bitcoin is established through the relationship between public keys and the digital signatures produced from the corresponding private keys.

# Basics of Bitcoin Cryptography

## Bitcoin and Cryptography

### Digital Keys

A mathematically-related public-private key pair, created using the Elliptic Curve Digital Signature Algorithm (ECDSA).

1. **Private key (Privkey)**

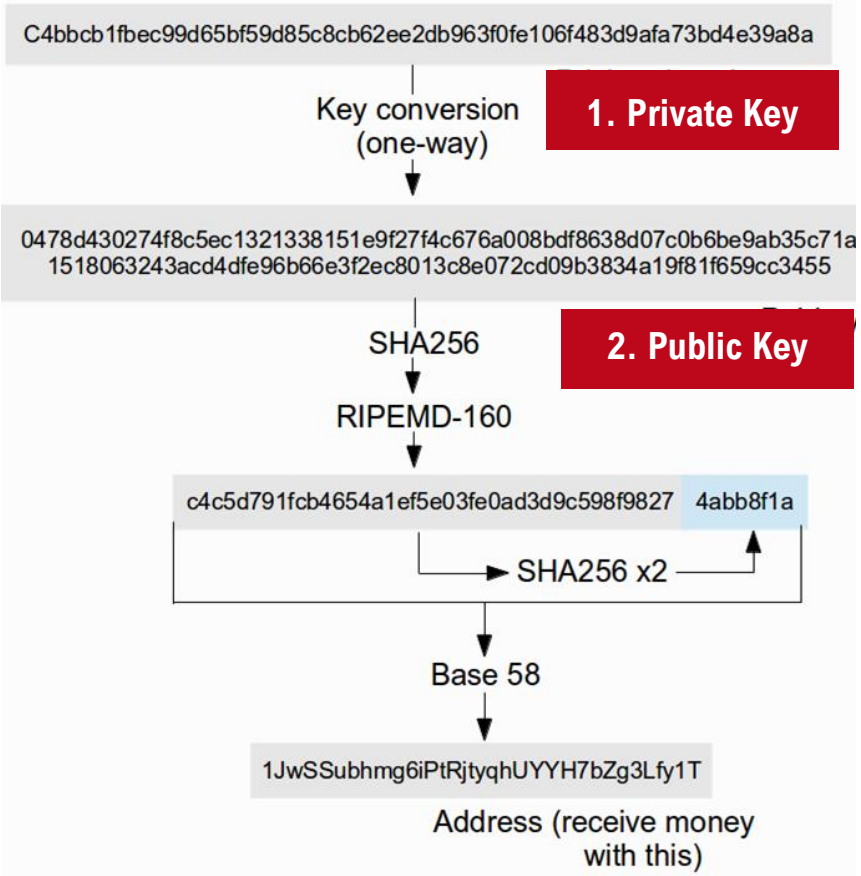
   is essentially a randomly generated number that should be kept secret. It is used to generate digital signatures and confirm ownership, authorizing the spending of bitcoin.

2. **Public key (Pubkey)**

   is generated from the private key using the elliptic curve multiplication process. When spending and receiving, the public key is represented by a bitcoin address.

"Think of the public key as similar to a bank account number and the private key as similar to the secret PIN, or signature on a check, that provides control over the account."

**A Bitcoin Transaction**



# Basics of Bitcoin Cryptography

## Bitcoin and Cryptography

### 3. Bitcoin Address

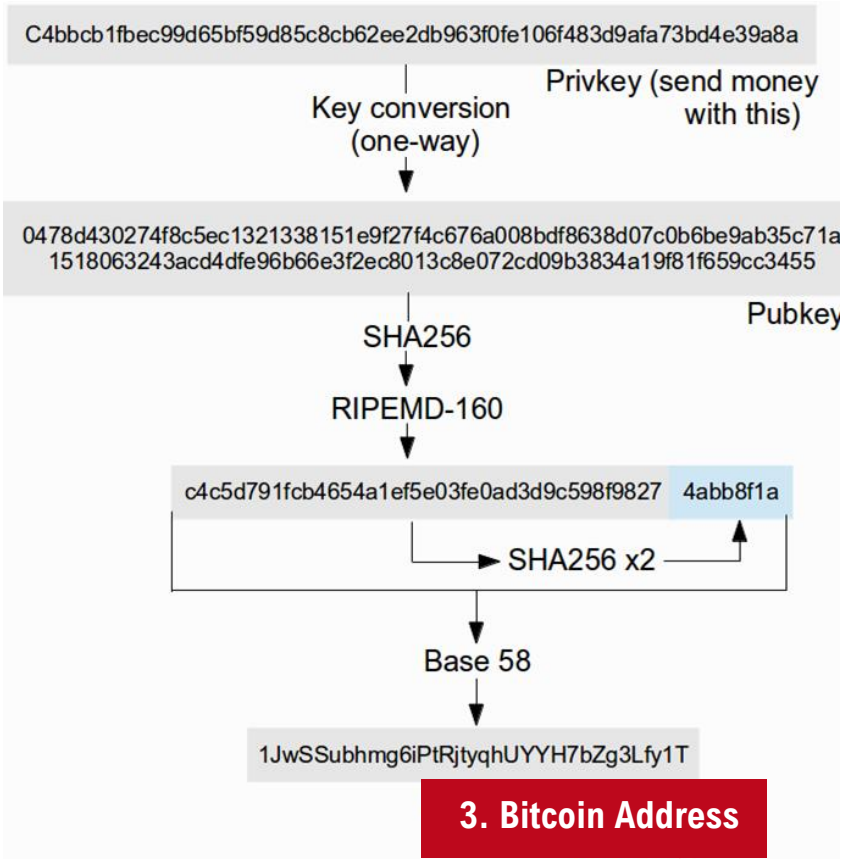
An address is a unique identifier for the destination of a bitcoin payment, generated from and corresponding to a public key or script.

It is usually generated by applying the SHA-256 and RIPEMD-160 cryptographic hash functions (explained on slide 36), in series, on the public key.

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

### Fun fact:

There are 52 characters in the alphabet, if we include all upper and lower-case letters. There are also 10 numbers (0 through 9). To avoid confusion and copying errors, Satoshi removed 4 commonly mistaken characters from the address generation process: uppercase letter 'O' and number '0,' uppercase letter 'I' and lowercase letter 'l.'



# Basics of Bitcoin Cryptography

## 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 digest. Look at the table on the next slide for useful examples.
- Any accidental or intentional modification of the input data (such as rearranging characters) will completely change the hash output, as previously explained in Week 2. See under 'Digest.'

Fun fact: The first hash algorithm was presented by IBM senior engineer Hans Peter Luhn in 1958.

# Basics of Bitcoin Cryptography

## Bitcoin and Cryptography

"Cryptographic hash functions are used extensively in bitcoin: in bitcoin addresses, in script addresses, and in the mining Proof-of-Work algorithm."

- 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 by always referencing the hash of the previous block. Cryptographic hash functions are generally used to:
  - verify block integrity, and
  - establish the chronological order of the blockchain
- SHA-256 is alsopart of proof-of-work (PoW) in Bitcoin mining, discussed later in this session.

Source: Mastering Bitcoin

# Basics of Bitcoin Cryptography

## Hash Functions

**Key Takeaways:**

- The same input always generates the same hash using the same hashing algorithm.
- A slight change in the input will generate an entirely different hash output.
- Different inputs should never generate the same hash. This is referred to as a "hash collision."
- Because hash functions are very difficult to reverse-engineer, it is nearly impossible to derive the input value from its hash output. This is useful for commitment schemes, i.e. sharing a hidden value that can be authentically revealed later.

| Input | Hashing algorithm: SHA-1 |
|---|---|
| Fox | dfcd3454bbea788a751a696c24d97009ca992d17 |
| fox | ff0f0a8b656f0b44c26933acd2e367b6c1211290 |
| fox1 | fcb9f413aa14b3fbec3c29d53dcf880994282874 |

# Basics of Bitcoin Cryptography

## Hash Functions

- Bitcoin uses the SHA-256 hash function. The hash output is 256 bits (32 bytes) long, as 1 byte = 8 bits.
- A SHA-256 hash is usually presented as a string of 64 hexadecimal characters. Each one of the 32 bytes is represented by 2 hexadecimal characters.

For example, the word “Bitcoin” produces the SHA-256 hash shown below (generated using the sha256sum Linux command).

- You can compare various hash generators here: https://8gwifi.org/MessageDigest.jsp
- For example, compare hashing "Bitcoin" using SHA-256 versus SHA-1.

**“Bitcoin” hashed using sha256sum**

```
# sha256sum
Bitcoin
b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4
```

# Basics of Bitcoin Cryptography

## Public Key Cryptography

Public key / two-key cryptography can be used for asymmetric encryption of information. However, in Bitcoin, all transaction information is publicly visible to everyone in the network, and transactions are not encrypted. Bitcoin does utilize digital signatures (another use case) to authenticate transactions in the network.

**In Public Key Cryptography, two types of keys are used:**

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

*Technically, the address is public, and the public key it is derived from is not exposed until bitcoin is spent.

# Basics of Bitcoin Cryptography

## Public Key Cryptography

When encrypting a message, the sender encrypts the message **M** using the recipient's public key to produce encrypted message **C**

The recipient decrypts the encrypted message **C** using their private key to see the original message **M**

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

**Asymmetric Encryption**

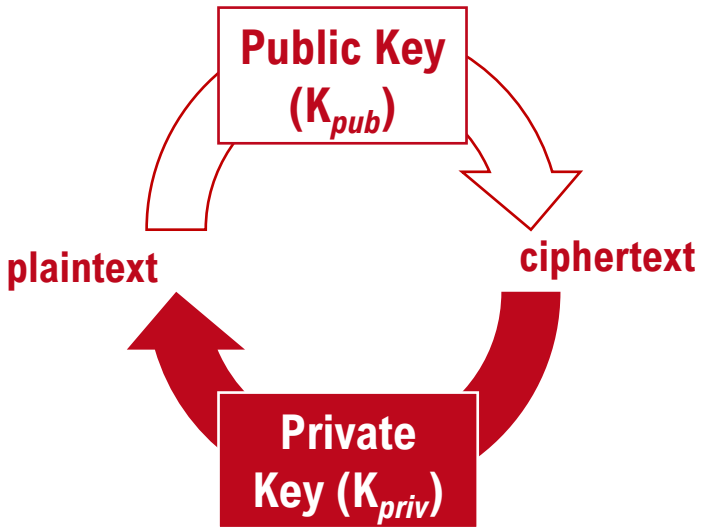
If the same key was used for both the encryption and decryption stages, then the relationship would be symmetric.

However, there is an asymmetric mathematical relationship between the public and private keys because:

- 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.

$$C = encrypt(M, K_{pub})$$

$$M = decrypt(C, K_{priv})$$



# Basics of Bitcoin Cryptography

## Public Key Cryptography

Encryption is not really used in Bitcoin. Instead, public key cryptography is utilized for producing digital signatures with **ECDSA (Elliptic Curve Digital Signature Algorithm)**, specifically the secp256k1 curve, to authorise and validate transactions.

- A private key is kept secret by the owner, and is used to sign a transaction hash which authorises the spending of coins it controls.
- The public key, which is visible to everyone after coins have been spent, can be used to verify that the corresponding private key produced the digital signature that authorised the transaction.

As of January 2021, Bitcoin Core release v0.21 included support for the **Schnorr** digital signature algorithm; after months of testing and debate on methods, the soft fork was locked-in for activation on mainnet sometime this coming November. (For in-depth details, see Bitcoin OpTech's weekly "preparing for Taproot" series.)

("Taproot: Privacy Preserving Switchable Scripting" was originally proposed by core developer Gregory Maxwell in January 2018.)

$$\mathbf{C} = \text{encrypt}(M, \mathbf{K}_{pub})$$

$$\mathbf{M} = \text{decrypt}(C, \mathbf{K}_{priv})$$

The Schnorr digital signature algorithm was designed by German cryptographer Claus-Peter Schnorr. His 1991 patent expired in February 2010.

# Basics of Bitcoin Cryptography

## Digital Signatures

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

### Signing Transaction T

1. Create transaction **T**
2. Select subset **M** of transaction **T** ( for example the transaction identifier, transaction instructions, etc.)
3. Compute hash **H** of **M**: **H** = sha256(**M**)
4. Compute a signature **S** using the output of this hash function $\mathbf{F_{hash}(M)}$ with the sender's private key, where $F_{sig}$ is the signature algorithm:
   $\mathbf{S} = F_{sig}(F_{hash}(\mathbf{M}), \mathbf{K_{priv}})$
5. Send the signature **S** and the public key $\mathbf{K_{pub}}$ along with the transaction **T** to Bitcoin miners.

# Basics of Bitcoin Cryptography

## Digital Signatures

- "Verification is the inverse of the signature generation function, using the R, S values and the public key to calculate a value P, which is a point on the elliptic curve." (Mastering Bitcoin)
- To verify a transaction received with the signature and public key $\mathbf{K_{pub}}$ , a receiver will:

**Verifying Transaction T**

Compute: $P = S^{-1} * F_{hash}(\mathbf{M}) * G + S^{-1} * R * \mathbf{K_{pub}}$

Where

R and S are the signature values

$K_{pub}$ is the public key

M is the transaction data that was signed

G is the elliptic curve generator point

- "If the x coordinate of the calculated point *P* is equal to *R*, then the verifier can conclude that the signature is valid. Note that in verifying the signature, the private key is neither known nor revealed."

# Basics of Bitcoin Cryptography

## Digital Signatures

**In Summary:**

- Each transaction associates an amount of bitcoin with a bitcoin address, which is usually produced from a hash of the owner's public key.
- When bitcoin are sent to someone, the transaction records the transfer of bitcoin from the current owner's Bitcoin address to the new owner's Bitcoin address, authorised by a valid digital signature.
- When this transaction is broadcast to the Bitcoin network, every peer knows that the new owner of these bitcoin is the owner of the receiving Bitcoin address.
- The complete history of transactions is kept by every (full client) peer in the Bitcoin network, so anyone can verify who is the current owner of any amount of bitcoin, without knowing their private keys.

# Basics of Bitcoin Cryptography

## Digital Signatures

In most cases, both the Public and Private keys are stored in a Bitcoin wallet.

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

A Bitcoin wallet, like a credit card, does not contain any bitcoin, but only the Private-Public key pairs, which are used as mechanisms 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**

**DO NOT SEND MONEY TO THESE ADDRESSES!**

# 3. Transactions and the Blockchain

# Transactions and the Blockchain

## From Digital Signatures to Bitcoin

- We've seen how digital signatures are a crucial part of systems of digital currency.
- For other use cases, such as transferring a digital title of ownership without a central authority, we need a ledger that records these changes in a way that cannot be refuted or altered by malicious actors.
- We will now look at how digital signatures and hash functions are used in the Bitcoin protocol to form the blockchain.

# Transactions and the Blockchain

## P2P Network and Ownership

- Bitcoin is run over a peer-to-peer (P2P) network of computers.
- Any computer connected in the network is called a node.
- Anyone can download and install the free open-source Bitcoin software to become a node.
- All nodes are treated equally, and no single node is trusted. The system assumes that the majority of nodes (if mining nodes, then hash power) will be honest nodes, i.e. not relay false or malformed transactions and blocks. However, "in response to such behavior, a node might choose to discourage (mark its misbehavior and perhaps disconnect in favor of new peers), disconnect, or ban the peer."
- Full nodes are responsible for verifying and maintaining all records of ownership according to consensus rules. Mining nodes also process transactions and append new blocks to the blockchain, in exchange for a reward. Pruned nodes verify transactions and blocks but do not store a complete copy of the blockchain.
- Users possess digital keys that control ownerhsip of bitcoin recorded in a public ledger (the blockchain).
- The public ledger records transfers of ownership for a quantity of bitcoin from one owner to another. (Note: Transactions can also be 'self-transfers,' that is, between sets of addresses and/or keys controlled by the same person.)

# Transactions and the Blockchain

## 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 sequence:

**Generating a Bitcoin Address**

```
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)
```

# Transactions and the Blockchain

## Addresses

A Bitcoin address is computed from the user's Public key:

- The **keyHash** is produced by applying the SHA-256 and RIPEMD-160 hash functions, in series, on the Public Key (2).
- **Data** is a concatenation of **keyHash** and an address **version** number.
- The **dataHash** (3) is produced by applying the SHA-256 algorithm twice on the Data.
- However, only the first 4 bytes of the **dataHash** are used as a **checksum** (4).
- The bitcoin **address** (5) is a concatenation of **Data** and **checksum** encoded in Base58 encoding.
- **Base58Encode** is a function that encodes binary as text using the Base58 encoding.

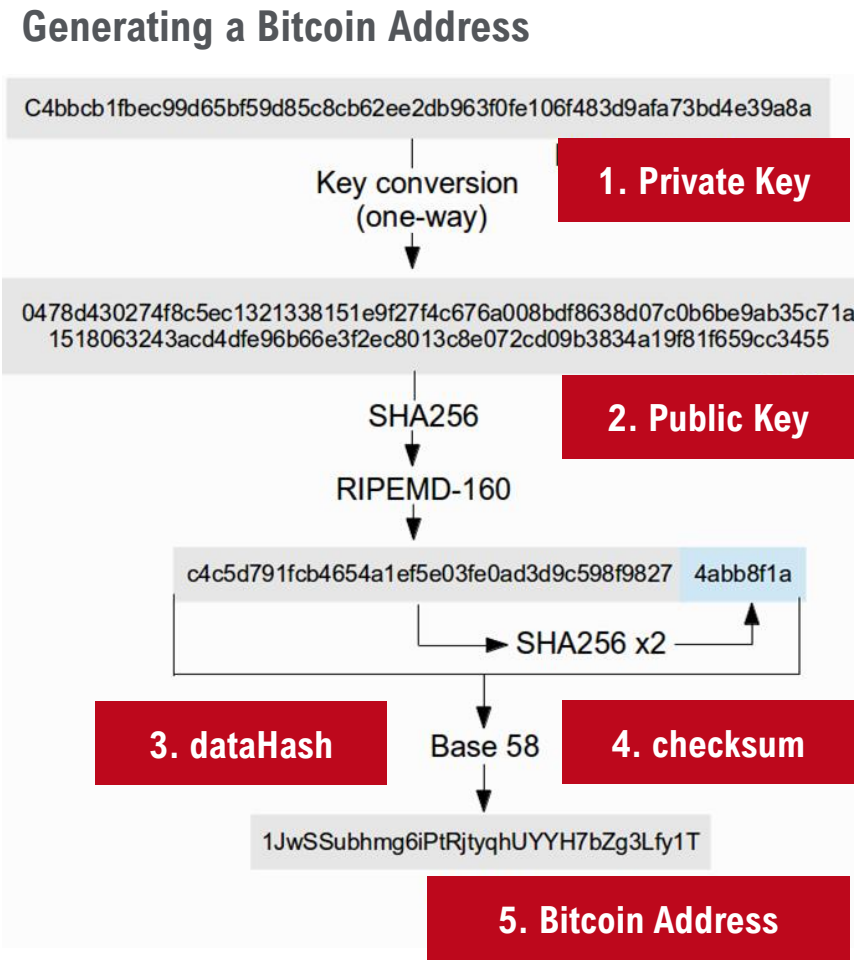



Image Source: www.bitcoinnotbombs.com/wp-content/uploads/2014/01/address.png

# Transactions and the Blockchain

## Transactions

- The Bitcoin network can be used to transfer information about transactions, blocks, peer nodes, and miscellaneous data.
- A Bitcoin transaction tells the network that someone has authorized the transfer of some or all of these bitcoin to another owner (or to themselves, but under a different address / public key identity).

**From 'Mastering Bitcoin':**

- "The new owner can now spend the bitcoin by creating another transaction that authorizes the transfer to another owner, and so on, in a chain of ownership."
- "Each transaction contains one or more 'inputs,' which are like debits against a bitcoin account. On the other side of the transaction, there are one or more 'outputs,' which are like 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, which is a small payment collected by the miner who includes the transaction in the ledger."
- "The transaction also contains proof of ownership for each amount of bitcoin (inputs) whose value is being spent, in the form of a digital signature from the owner, which can be independently validated by anyone" in the Bitcoin network.

# Transactions and the Blockchain

## Transactions Visualized


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

A transaction can have multiple outputs.

A chain of ownership is created.

# Transactions and the Blockchain

## The most common transaction types

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:

**Inputs are debited from the original owner’s Bitcoin address**

**Outputs are credited to the new owner’s Bitcoin address; change is returned to the original owner in a second output.**

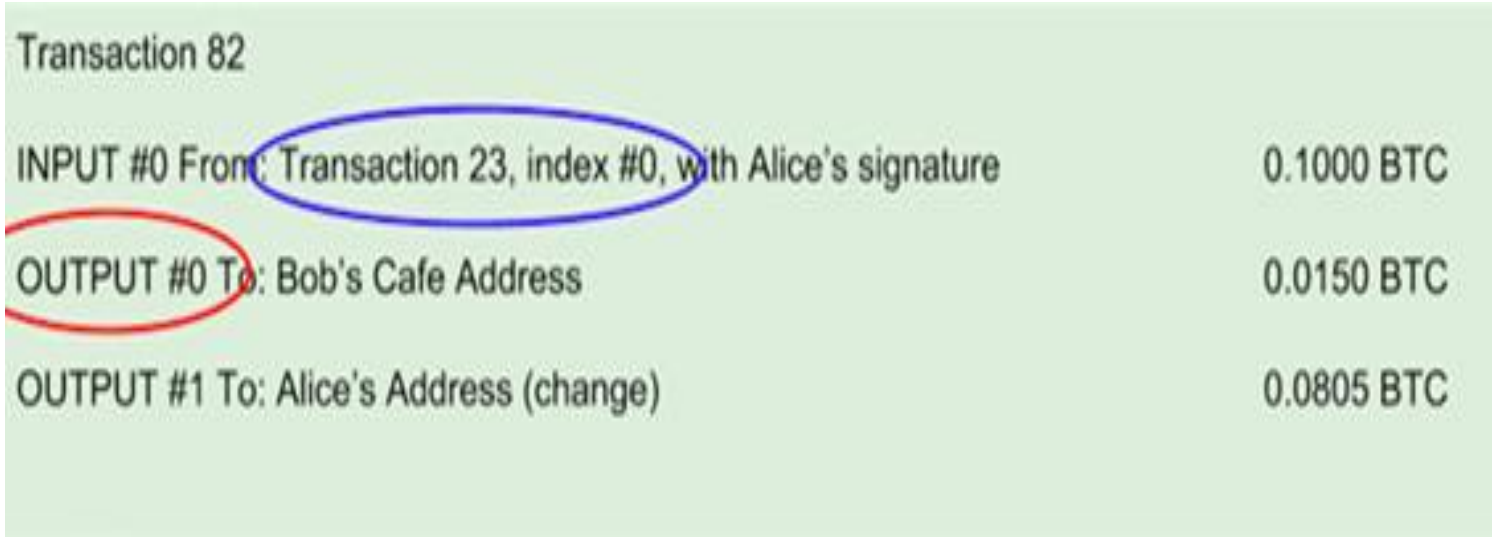
Input # 0
(transaction 1: Sender)

Output # 0
(transaction 1: Recipient)

Output # 1
(transaction 2: Change returned to Sender

# Transactions and the Blockchain

## Transactions Visualized



# Transactions and the Blockchain

## The most common transaction types

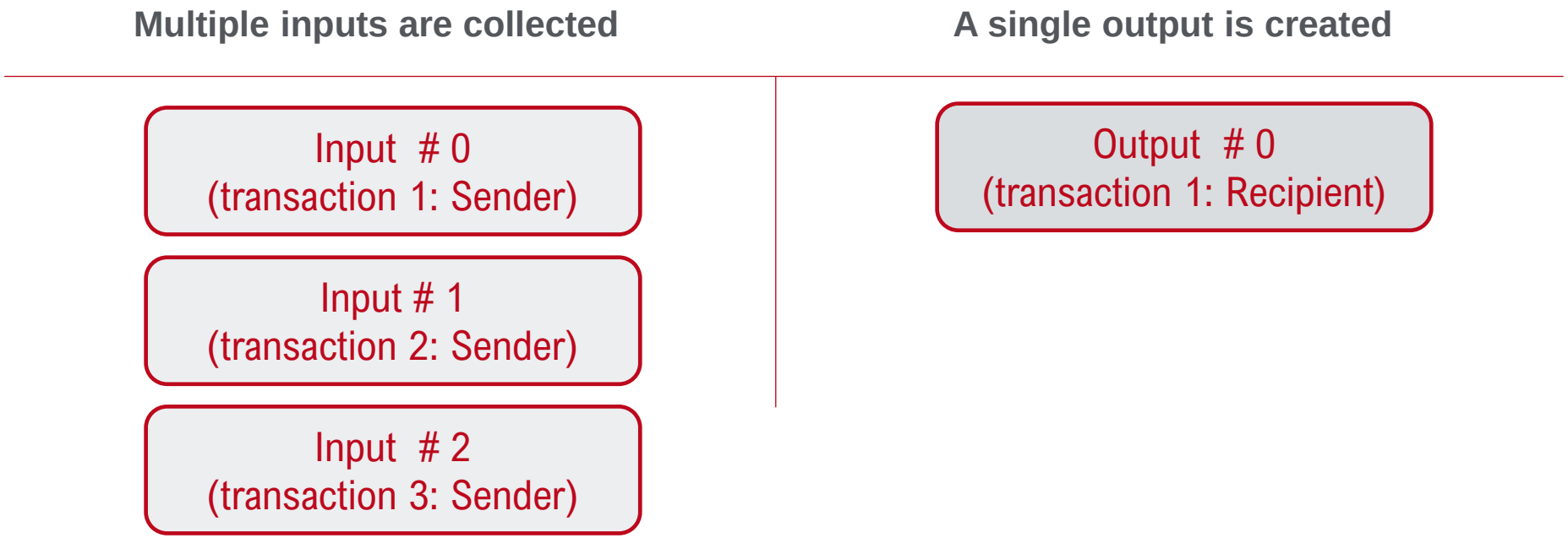
A real example of this type of transaction


- You're welcome to use any "block explorer" to search through the whole blockchain, since all transactions are publicly visible. Here is a list of them: http://bit.ly/blockexplorers
- Pick any transaction, follow it, and see what you can find about the inputs, outputs, and change. Look at how it is connected to previous transactions. We will also ask you to explore some transactions in the weekly quiz, using a blockchain explorer.

# Transactions and the Blockchain

## The most common transaction types

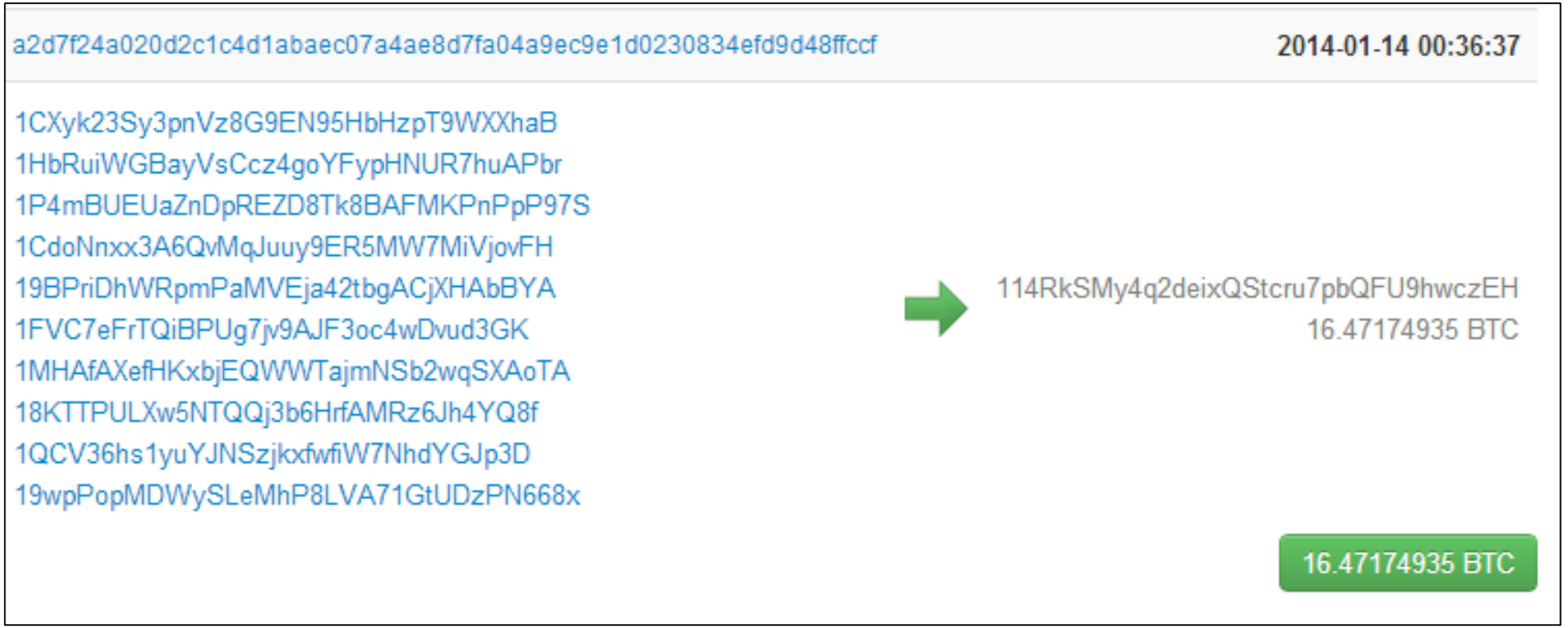
Another common form of transaction is a transaction that aggregates several inputs (3 in the example) into a single output. This represents the real-world equivalent of exchanging a pile of coins and currency notes for a single larger note. Transactions like these are sometimes generated by wallet applications to clean up lots of smaller amounts that were received as change.



# Transactions and the Blockchain

## The most common transaction types

A real example of this type of transaction:



# Transactions and the Blockchain

## The most common transaction types

Another transaction form often observed in the Bitcoin ledger distributes one input to multiple outputs, which may or may not represent multiple independent recipients. This type of transaction is sometimes used by commercial entities, such as when processing payroll to employees.

| **A single input** | **Multiple outputs are credited to new owner's Bitcoin addresses.** |
|---|---|
| Input # 0<br>(transaction 1: Sender) | Output # 0<br>(transaction 1 : Recipient 1)<br><br>Output # 1<br>(transaction 2 : Recipient 2 |

# Transactions and the Blockchain

## The most common transaction types

A real example of this type of transaction:

| | | | | | |
|---|---|---|---|---|---|
| Hash | 21bed779f4f3a396b2a346c2df16abc0e6a081658d0683f397115f14... | | | | 2020-02-05 01:02 |
| | 17A16QmavnUfCW11DAApiJxp7ARnxN5pGX | 0.67494458 BTC | → | 36JLK9gDTD4w2JQHDVnfbHEYmdZ7XuKmq9 | 0.00686725 BTC |
| | | | | 1GnvUXzvWGnqWjnpyvqsauxUAQDsNBza9e | 0.03205449 BTC |
| | | | | 1QKj5HMqKieEiWBFW3yKAshqHAGCXTtjX7 | 0.03227507 BTC |
| | | | | 1MyNHavqezVAQ1GMG36dMMt7LyogqKZT75 | 0.44950000 BTC |
| | | | | 17A16QmavnUfCW11DAApiJxp7ARnxN5pGX | 0.15324777 BTC |
| Fee | 0.00100000 BTC<br>(280.112 sat/B - 70.028 sat/WU - 357 bytes) | | | | 0.67394458 BTC |

# Transactions and the Blockchain

## The most common transaction types

Another transaction form often observed in the Bitcoin ledger is a coinbase transaction that has no input (represents newly generated coins) and one output (block miner).

| No input (newly generated coins) | Output credited to miner's Bitcoin addresses. |
| --- | --- |
| No input (newly generated coins) | Output # 0 (transaction 1 : Miner) |

# Transactions and the Blockchain

## The most common transaction types

Below are two coinbase transactions: one with just the block reward (50 BTC), and one with the block reward (12.5 BTC) plus transaction fees.

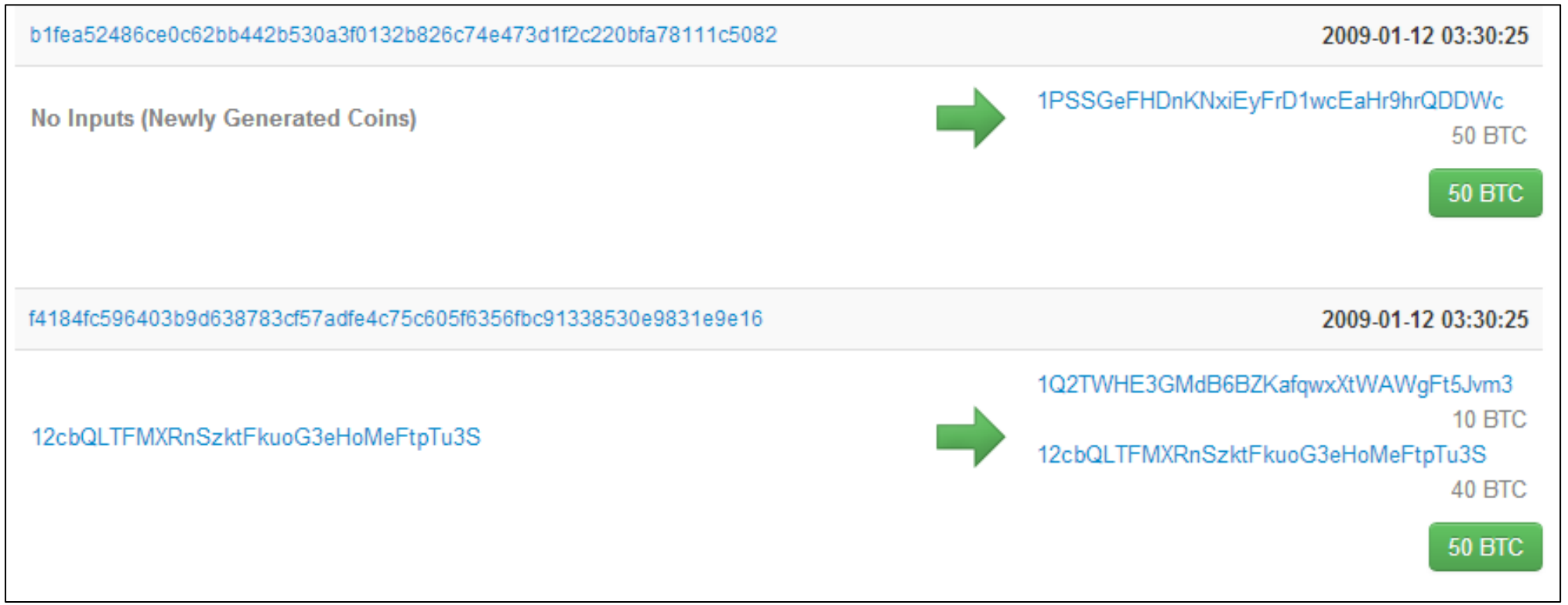
| | | | | |
|---|---|---|---|---|
| Hash | 8c14f0db3df150123e6f3dbbf30f8b955a8249b62ac1d1ff16284aefa... | | | 2010-12-29 13:57 |
| | COINBASE (Newly Generated Coins) | → | 1HWqMzw1jfpXb3xyuUZ4uWXY4tqL2cW47J | 50.00000000 BTC |
| Fee | 0.00000000 BTC<br>(0.000 sat/B - 0.000 sat/WU - 135 bytes) | | | 50.00000000 BTC |

| | | | | |
|---|---|---|---|---|
| Hash | 1cc3849ec1b91aecc24cf40f675b3cdc9c002ed2c008c1de621bd2c... | | | 2020-02-05 01:40 |
| | COINBASE (Newly Generated Coins) | → | 39m5Wvn9ZqyhYmCYpsyHuGMt5YYw4Vmh1Z | 12.85909023 BTC |
| | | | OP_RETURN | 0.00000000 BTC |
| | | | OP_RETURN | 0.00000000 BTC |
| Fee | 0.00000000 BTC<br>(0.000 sat/B - 0.000 sat/WU - 296 bytes) | | | 12.85909023 BTC |

# Transactions and the Blockchain

## First Transaction Ever

Below is the first bitcoin transaction ever performed, between Satoshi and Hal Finney. Satoshi sent 10 BTC, with 40 BTC returned as change. We can also see the coinbase transaction for the block it was included in, with no inputs and a block reward of 50 BTC.



# 4. Mining

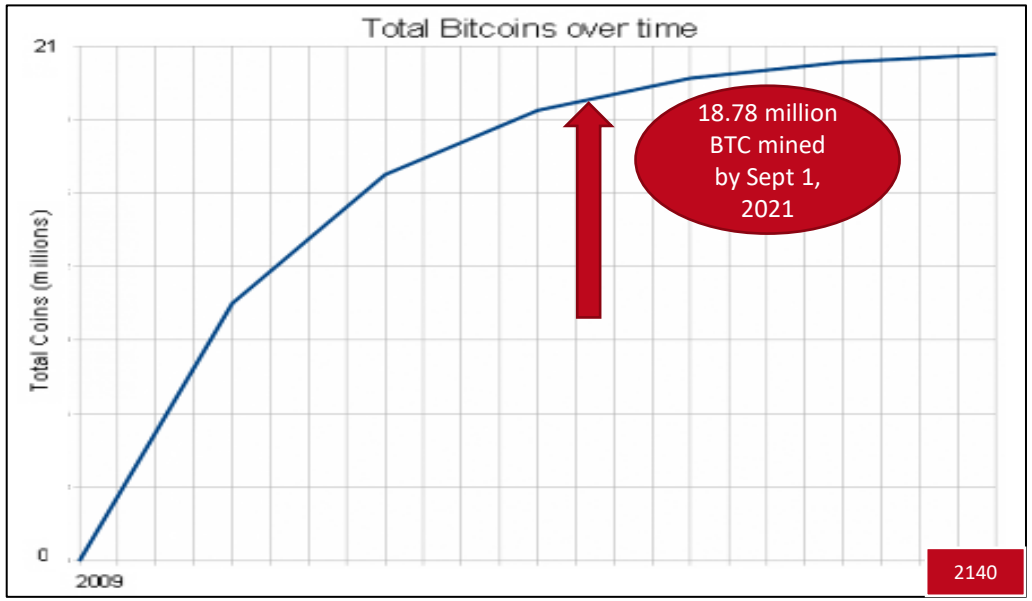
# Mining

## 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 bitcoin in each block, almost like a central bank printing new money. The amount of bitcoin 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

## 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, though they usually select transactions with the highest fee per byte.
- **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 their local copy of the blockchain and broadcast to the peer-to-peer network.

# Mining

## 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 the computation of hashes / second.
- 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

## Mining Difficulty

- Mining nodes actively regulate the rate of new blocks.
- As more miners (or, rather, hashpower) join, the rate of block creation will go up. As the rate of block creation goes up, the mining difficulty rises to compensate. More inefficient mining hardware will leave the network, which will let block time go down again
- The creation of new blocks should 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 here.)
- The regulation is done by adjusting the hash target value 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.
- While most adjustments are small, there have been a few major downward adjustments in the hash rate in Bitcoin's history: -15% in December 2018, -31% in September 2019, and -40% between May and July 2021. It has since recovered to 2020 levels.

# Mining

## 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 for each successfully mined block.
- The issuance schedule is embedded in the Bitcoin protocol.
  - Currently the block reward is 6.25 BTC (since May 11th 2020).
  - The block reward halves every 210,000 blocks (i.e. approximately every 4 years).
  - The next Bitcoin halving will occur around May 2024 and the reward will decrease to 3.125 BTC.
  - The reward will be removed when the asymptotic limit of 21 million bitcoin is reached, in the year 2140. After that point, transaction processing will be rewarded solely through transaction fees.
- In addition to the block reward, miners are awarded the transaction fees paid by Bitcoin users.
- See this short article by Andreas Vlachos which examines whether mining profitability will be impacted over time by the halving of block rewards and Bitcoin price.

# Mining

## Solo Mining

- Solo miners user their own computer (or specialized mining hardware) to search for blocks. Solo miners will only get paid if they independently solve / find a block.
    - As of September 2019, the Bitcoin hash rate was over 90,000,000 TH/s.
    - As of September 2020, the Bitcoin hash rate was close to 140,000,000 TH/s.
    - As of February 2021, the Bitcoin hash rate is over 150,000,000 TH/s.
    - As of the end of August 2021, the Bitcoin hash rate was over 129,000,000 TH/s. Between May and July, the hash rate dropped from a high of 180,000,000 TH/s to about 85,000,000 TH/s, following a crackdown on mining in China.
- For the average person, solo mining is not ideal, as it is highly competitive and may require significant investment. However, here is a recent exploration of the viability of at-home mining (U.S.-focused).

# Mining

## Pool Mining

- Pool mining is the main mining method used in Bitcoin today. Each miner contributes their individual hash power towards solving proof-of-work as a group, "like a lottery pool allows several participants to share their efforts and rewards." (Mastering Bitcoin)
- When a block is found, the mining pools wallet receives the payment and then distributes the reward to each individual pool miner.
- Distribution of the reward is based on their personal contribution of hash power. If a pool miner contributed half of the pool's hash power, then they would receive half of the reward.
- For an exploration of the pros and cons of decentralized mining pools, see this thread:

> "Pools help these smaller miners by enabling them to accumulate BTC off-chain (in their pool accounts) so that they can receive larger but less frequent payouts that are more cost effective. Direct coinbase payouts for garage miners don't scale." (**Braiins**)

# Mining

## Mining Pools

Most mining 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/getblocktemplate request (more about basic commands in Week 5).
- Each miner tries to solve the Proof-of-Work problem for the block, by incrementing the nonce and hashing the block header.
  - Each time a nonce is changed, the result is a different hash value. To win the block, the result must be below the difficulty target with enough leading 0s.
- Whenever a miner finds a hash value below an easier target, they submit it 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, in case a new block was discovered.

# Mining

## Pool Mining

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 shares, it counts every share between each block and then calculates the payments based on each person's proportional amount.

# Mining

## 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.

# Mining

## Other Consensus Mechanisms

- Several other consensus mechanisms have emerged since Bitcoin's creation, approaching distributed consensus differently.
- Most notable examples are:
  - Byzantine Fault Tolerant (BFT)
  - Proof-of-Stake (POS)
  - Delegated Proof-of-Stake (dPOS)
  - Proof-of-Burn
  - Proof-of-Importance
  - And more…
- These consensus protocols have been / are being explored through alternative cryptocurrencies (or "altcoins"). Ethereum was expected to switch to Proof-of-Stake in 2019, but those protocol changes remain under development, to be implemented with ETH 2.0.
- We will explore some of these other consensus protocols during a later session.

# 5. Core Development & Improvement Proposals

# Core Development and Improvement Proposals

## Bitcoin Core

Since Satoshi released Bitcoin v0.1 in January 2009, under the MIT free software license, hundreds of developers from around the world have contributed to the daemon and reference client, not to mention alternative clients.

Contributors who participate in / manage core software development are referred to collectively as "**Bitcoin Core**." Discussions and releases are often published through the open 'bitcoin-dev' mailing list. Most of them do so as volunteers; some are sponsored by their employers or through grants from businesses in the industry. Recently, funding has become more distributed through initiatives like GitHub Sponsors, Human Rights Foundation (HRF) Bitcoin Development Fund, the Bitcoin Donation Portal, and Open Sats.

The "janitorial role" of maintainers (currently led by Wladimir van der Laan), as in other open-source software projects, is to "balance reactive tasks (community interactions) with proactive ones" such as writing and reviewing code. (Eghbal, 2020)

A weekly code review club of important concepts and pull-requests is organised here.

**You will learn more about the Bitcoin Core reference implementation during Session 4.**

# Core Development and Improvement Proposals

## Bitcoin Improvement Proposals

Since 2011, changes to / around Bitcoin (outside of maintenance tasks) are introduced and organised through a process called Bitcoin Improvement Proposals or "BIPs." Ideas are first formulated and vetted organically via IRC, mailing lists, forums, and social media etc. before being submitted as a draft. "Once a BIP has been accepted, the reference implementation must be completed. When the reference implementation is complete and accepted by the community, the status will be changed to 'Final'." (BIP0001)

In practice, if a BIP concerns changes that do not require network consensus, wallets may adopt a standard while it is still in the drafting stage or even 'discouraged' for implementation.

- Example 1: BIP144 defined the Segregated Witness (SegWit) soft-fork consensus change, a transaction malleability fix and scaling solution, which was activated on mainnet in 2017.
- Example 2: BIP47, despite still being in the 'Draft' stage, is already actively being used in the 'PayNyms' feature implemented by Samourai Wallet.

# Core Development and Improvement Proposals

## Ethereum Core

While Ethereum does not have a reference implementation, there is still a "core" team:

"Ethereum core developers hold a meeting known as the All Core Devs meeting regularly, typically every two weeks. Any Ethereum core researcher or developer, i.e., someone working on the core Ethereum protocol or an Ethereum client, is invited to join these calls and as of publication they typically attract 20-30 attendees.

The agenda for a call is published ahead of time and anyone may propose an addition or a change to the meeting agenda in the following Github repository:

https://github.com/ethereum/pm"

- from ***Mastering Ethereum*** by Andreas M. Antonopoulos & Gavin Wood

## Ethereum Improvement Proposals

Similar in concept and formatting to BIPs, Ethereum Improvement Proposals were introduced shortly after the launch of Ethereum in 2015.

# Session 3: The Basics of Cryptocurrencies

## 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 (the entire network is spread across all of its participants).
  - Secure (as long as 50% or more of the nodes are honest).
  - Reliable (transaction ledgers are replicated by all network nodes).
  - Peer-to-peer: transactions can be made from one party to another without the need for an intermediary or central authority.
  - Open: anyone can join or leave the network, can validate transactions or mine new coins.
  - Public: all transactions recorded in the Bitcoin network are publicly verifiable and available to all the operators in the network.

# Session 3: The Basics of Cryptocurrencies

## Conclusions (continued)

- Permissionless: no need for credentials, IDs or authorization to join the network.
- Borderless: the network operates freely across geographical boundaries, and can be accessed from practically anywhere.
- Censorship resistant: there is no central authority or government which can stop the transfer of funds from one peer to another.
- Neutral: the Bitcoin network is agnostic to who, what, when, where, or why you are sending and receiving bitcoin.
- Bitcoin generation is self-regulated, based on mathematical algorithms and game theoretical models.

# Session 3: The Basics of Cryptocurrencies

## Further Reading

**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**

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

**How Bitcoin transactions work**

http://visual.ly/bitcoin-infographic

**Bitcoin Mining Power Hits New High**

https://www.coindesk.com/bitcoin-mining-power-hits-new-high-as-half-a-million-new-asics-go-online

https://www.coindesk.com/bitcoin-mining-difficulty-record-20-trillion-january-2021

# Session 3: The Basics of Cryptocurrencies

## Further Reading

**How Bitcoin Works Under the Hood**

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

**Bitcoin Mining Pools**

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

**Inputs and Outputs – Bitcoin "change" Explained**

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

**ASIC Mining**

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

https://www.asicminervalue.com/

# Session 3: The Basics of Cryptocurrencies

## Further Reading

**Comparison of mining pools and hardware**

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

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

**Mining calculators**

https://www.cryptocompare.com/mining/calculator/btc?HashingPower=1&HashingUnit=TH%2Fs&PowerConsumption=1500&CostPerkWh=0&MiningPoolFee=1

UNIVERSITY of NICOSIA

# Questions?

Contact Us:

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