openHPI Course: Blockchain – Revealing the Myth

Bitcoin (6): Paying with Bitcoins

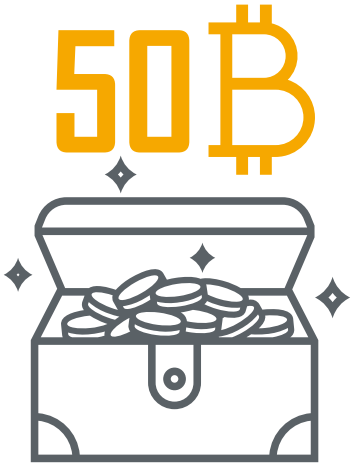
Prof. Dr. Christoph Meinel

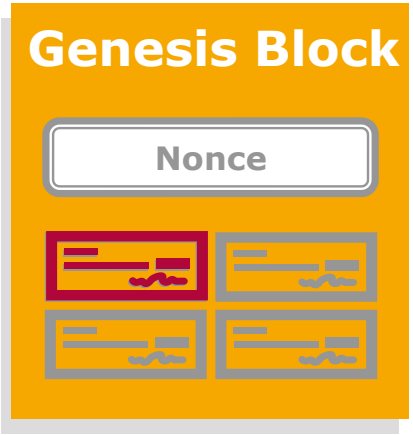
Tatiana Gayvoronskaya

Hasso Plattner Institute
University of Potsdam, Germany

Genesis Block – Mining the First Bitcoins

- As we have already learned, **new coins** enter the system through **coinbase transactions**
- It means that the **first coins** came from the **coinbase transaction of the first block**, also known as **genesis block**
- Let us have a closer look at this transaction





Coinbase Transaction

- The **block creation reward** in form of **newly mined bitcoins** started at **50 bitcoins** and is being halved every **210,000 blocks** – approximately once every four years (today it is 6.25 bitcoins)
- Thus, the **first coinbase** transaction from **block 0** consisted of **50 bitcoins** (BTC) and no transactions fee
- This was created on **03 January 2009**
- If each **new block** is created every **10 minutes**, then the **last bitcoin** will be mined around the **year 2140**
- The block 0, **genesis block**, like numerous subsequent blocks consisted of **only one transaction**, the **coinbase transaction**

Block 0

Block 0

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	669,524
Timestamp	2009-01-03 20:15
Height	0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes
Nonce	2,083,236,893
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

Source: blockchain.com

Coinbase Transaction
Block 0

- Let's take a closer look at **block** number **0**
- Here you can see the **first ever mined** bitcoins
- These were addressed to a **Public Key Hash of Satoshi Nakamoto** and until today **never been spent**/used
- Imagine **you are the owner** of these bitcoins. So, you once generated a key pair in 2009 and gave the hash of your public key (*1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa*) to Satoshi

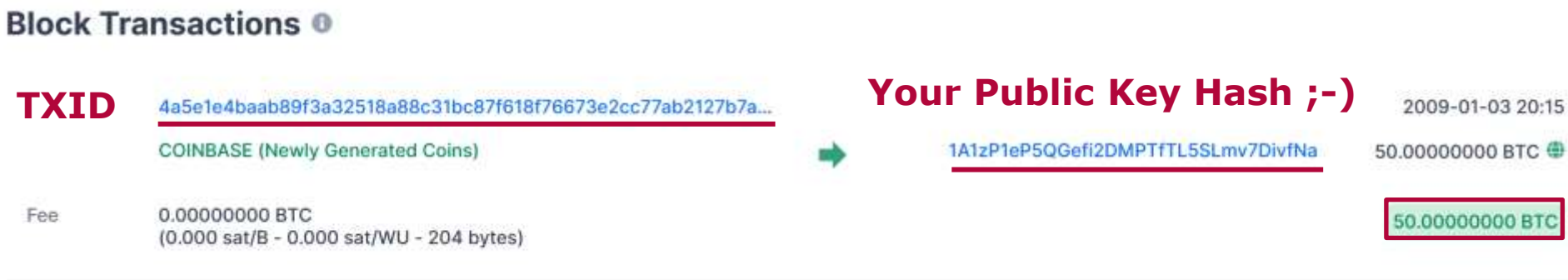
Unspent

Public Key Hash from Satoshi Nakamoto

Source: blockchain.com

Coinbase Transaction
Block 0

- This would mean that you own 50 Bitcoins, which look like this:
  4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
- Correct, this is a **hash of the first transaction**, also called **transaction ID** (TXID)
- Now you can create a **new transaction** and transfer these 50 bitcoins by adding the **public key hash of the new recipient** and signing the transaction with your **private key**



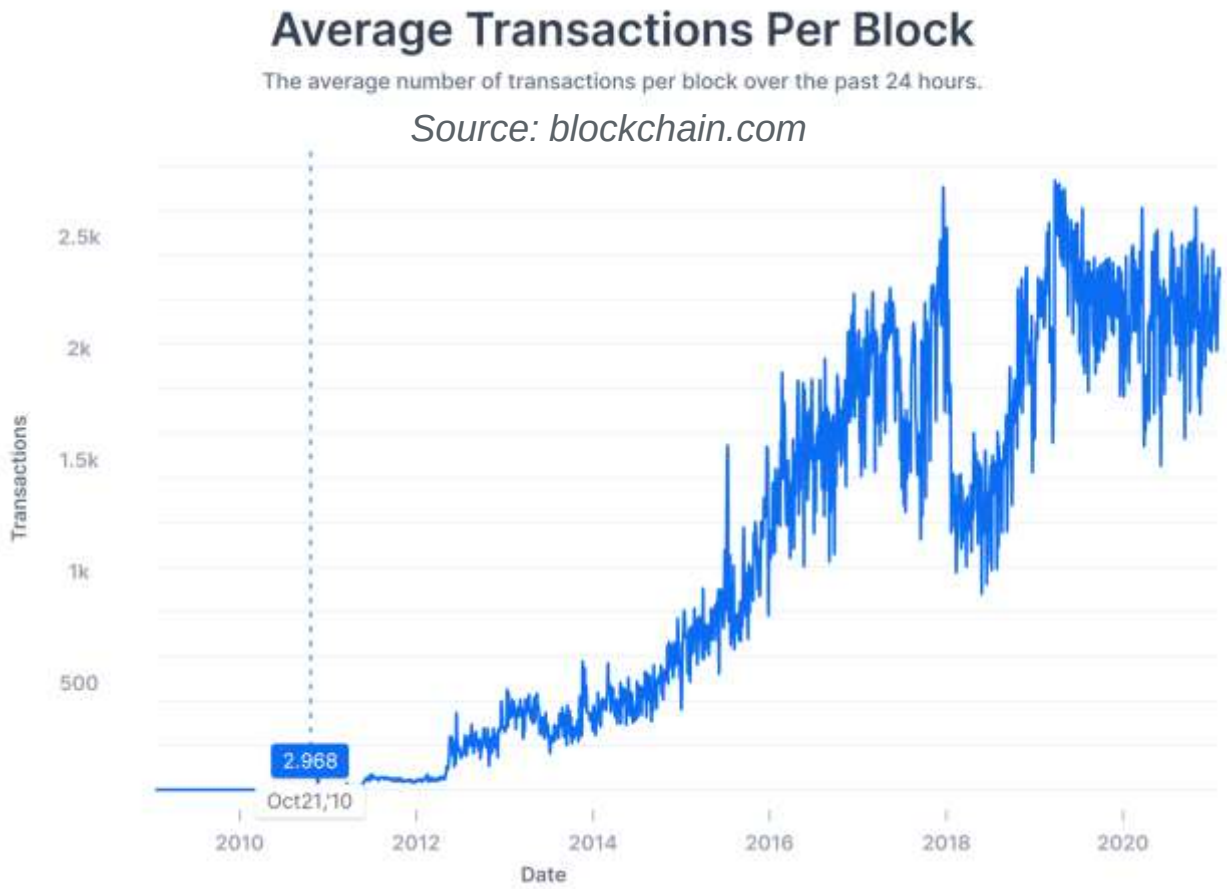
Source: blockchain.com

Definition of a Bitcoin

"We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership." - Satoshi Nakamoto

Average Transactions per Block

Only around November 2010 (**after about 88,900 blocks**) did the number of transactions per block **start to increase continuously**



Block 88,900

- Let's take a closer look at **block** number **88,900**
- It looks like an **ownership register**
- As we see in all transactions except coinbase transaction, **certain amounts of bitcoins** are overwritten from **one owner to another**

Hash	eb94648f3026b32fab56b7289dec19d91323282c3046b07c1bd828...			2010-11-01 03:10
1	COINBASE (Newly Generated Coins)		1C6j6iYFUZhjhRn5zSfzWXXzR67kCGV59v	50.00000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 135 bytes)			50.00000000 BTC

Hash	289a8814a94e1abee23ed0efb8f18a01b21317c6c2bcac40b40a705...			2010-11-01 03:10
2	16iN2ndr6bdSFUmZtiUWW4cq65fh2e5urA	495.80000000 BTC	14dw2L2mE8Hk66CmgH5Smgg5KU2VYyJhAJ 15JKQaSHNSiqKdApyDFAVTzhaN6GKGApu5	0.05000000 BTC 495.75000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 259 bytes)			495.80000000 BTC

Hash	d74d4d07aed3225b98ccb4ca77ca22cf6fad5078e5db52e9ff5d2af...			2010-11-01 03:10
3	1BjpZqmfaTbooGV2bcxZxMXtQur2j92Er	50.00000000 BTC	1nHBbVFepCvvuVcVp9NVpRJgSH4ycjNxP	50.00000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 157 bytes)			50.00000000 BTC

Bitcoins
Combining and Splitting Value

Let's take the last example. Imagine **you want to pay for a coffee with your Bitcoins**

- You currently have **50 Bitcoins from Satoshi**, and according to the current exchange rate it is **1,894,100 dollars**
- To allow value to be split and combined, transactions contain multiple **inputs** and **outputs**
- Normally there will be either a **single input** from a larger previous transaction or **multiple inputs combining smaller amounts**, and **at most two outputs**: one for the payment, and one returning the change, if any, back to the sender
- If this difference is not **transferred back** to the sender, then this is considered a **transaction fee** that is added to the incentive value of the block containing the transaction

Bitcoins
Combining and Splitting Value

- So, your transaction would look like this:

Input	Output
	1
Your 50 BTC - 4a5e1e4baab89f3a325…	Number of bitcoins to spend - 0.00005…
Your Signature - 304402204e45e1693…	Public Key Hash of Coffee shop - 12cb…
	2
	Number of bitcoins to spend back – 49.9…
	Your Public Key Hash - 1A1zP1eP5QG…
TXID: ea44e9727	169199015755…

- In that case, if we have **multiple outputs**, the **hash of the transaction** will not be enough for us to continue using the bitcoins sent back to us. For this, we need an **output index** that points to the output in which we sent the 49.9 bitcoins back to us

Bitcoins
UTXO – Unspent Transaction Output

- If you have **already spent** your 49.99 bitcoins (used the hash of the sample transaction and the index of your output in the input of a new transaction)
- The coffee shop has still **not used** their 0.00005 bitcoins
- Therefore, the 0.00005 bitcoins **can still be spent**, one calls this an **unspent transaction output – UTXO**

Input	Output
Your 50 BTC - 4a5e1e4baab89f3a325…	1 Number of bitcoins to spend - 0.00005…
Your Signature - 304402204e45e1693…	Public Key Hash of Coffee shop - 12cb…
	2 Number of bitcoins to spend back – 49.9…
	Your Public Key Hash - 1A1zP1eP5QG…
TXID: ea44e9727	169199015755…

Bitcoins
UTXO – Valid Transaction

- A **transaction (UTXO)** is considered **valid** if it has been included in a block that already has at least **five successor blocks**
- This number was determined based on the **assumption** that potential attackers **do not have enough computing power** – or want to expend it – to recalculate six blocks

Bitcoin Transactions

Summary

- An electronic **coin is a chain of digital signatures**
- Only the **UTXO's** counts as "**valid**/existing" **bitcoins** that can be used for further transactions (after 5 blocks)
- It is important, above all, that the users sufficiently **protect their private key**. Because the one who has the private key is allowed to trade with the values bound to it, more specifically to the Public Key Hash address. Comparable to physical currency