Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption
Payments

Bank A

Transfer

Bank B

Pay Alice $10
Account ID: 12345678
Sort Code: 20-20-30

Account ID: 12345678
Sort Code: 20-20-30

Pay Alice 10 BTC
From Account ID: a5437da8
To Account ID: 85539d81

Miners agree on a consensus

Blockchain

Bob has 100 BTC
Bob pays Alice 10 BTC
History

- Bitcoin was created in 2009 by someone known as Satoshi Nakamoto.
- Does not require the support of a central government or organisation to regulate it, nor a broker to manage payments.
- The Bitcoin currency is instead created when users *mine* for it, using their computers to perform complex calculations through special software.
- Bitcoin (BTC) divisible to the 8th decimal place.
- BTC can be split into 100,000,000 units.
- 0.00000001 bitcoin is one Satoshi.
History

• Bitcoin designed to limit the number of bitcoins that can ever be created.

• Each transaction then has a reward, and the reward reduces over time, which should reduce the supply of the coins.

• In 2016, the reward for a successful mining process was reduced from 25 BTC to 12.5 BTC. This reward will continue to reduce until the currency is forked (and where new parameters are used), or when we reach a saturation level.

• Others: Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, Steem, KiloCoin and Augur.
## Genesis Record

<table>
<thead>
<tr>
<th><strong>Summary</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>0 (Main chain)</td>
</tr>
<tr>
<td>Hash</td>
<td>0000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f</td>
</tr>
<tr>
<td>Previous Block</td>
<td>000000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>Next Blocks</td>
<td>000000000839a8e6886ab5951d78f411475428afc90947ee320161bbf18eb6048</td>
</tr>
<tr>
<td>Time</td>
<td>2009-01-03 18:15:05</td>
</tr>
<tr>
<td>Difficulty</td>
<td>1</td>
</tr>
<tr>
<td>Bits</td>
<td>486604799</td>
</tr>
<tr>
<td>Number Of Transactions</td>
<td>1</td>
</tr>
<tr>
<td>Output Total</td>
<td>50 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>0 BTC</td>
</tr>
<tr>
<td>Size</td>
<td>0.285 KB</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Merkle Root</td>
<td>4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b</td>
</tr>
<tr>
<td>Nonce</td>
<td>2083236893</td>
</tr>
<tr>
<td>Block Reward</td>
<td>50 BTC</td>
</tr>
<tr>
<td><strong>Transaction Fees</strong></td>
<td></td>
</tr>
</tbody>
</table>

No Inputs (Newly Generated Coins) 50 BTC

1A1zP1eP5QGefi... (Genesis of Bitcoin) 50 BTC

2009-01-03 18:15:05
Big accounts

**Bitcoin Address** Addresses are identifiers which you use to send bitcoins to another person.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>3D2oetdNuZUqQHPJmcmDDHVtqykYNvSfk9r</td>
</tr>
<tr>
<td>Hash</td>
<td>7c6775e20e3e938d2d7e9d79ac310108ba501ddc</td>
</tr>
<tr>
<td>Tools</td>
<td>Related Tags - Unspent Outputs</td>
</tr>
</tbody>
</table>

No. Transactions: 3493
Total: 1,210,471.32658275 BTC
Final Balance: 180,773.05403806 BTC

**Bitcoin Address** Addresses are identifiers which you use to send bitcoins to another person.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>3EDzR4QKeGjyCZWXMFFk1AGqi8gHNQ798sF</td>
</tr>
<tr>
<td>Hash</td>
<td>897d25262f68b8a8d4e2af2ab082ce058a69d1</td>
</tr>
<tr>
<td>Tools</td>
<td>Related Tags - Unspent Outputs</td>
</tr>
</tbody>
</table>

No. Transactions: 1
Total Received: 2,034.668943 BTC
Final Balance: 2,034.668943 BTC

Request Payment
Donation Button

**Transaction Details**

- 3QkDqh68n4wY9wUCm5AT4ggbHbRRyPt3d3W
- 1LAGKBi34p9h434WgQjHls3RNUgARKW8Cbo
- 1G4NHvqWvHfG1ZmV5U2WLaUqGOG6P0qjKBNx
- 3MY7rJk4KXYYHgOuJ7yOzL115qWg
- 37KtYmCNe8WmzhzBRRStBzElSzH642qB
- 1FQidwv878iG5DlUL21ZxnnYoqoGAqH
- 3H3eWUURUzFtVwVryGyFvS9PnJZwVn
- 3uHCtJEJHyp0TJiXkWQauJxuMF6sczBn

13,083 32396362 BTC

17-11-14 08:03:03
Genesis Record

Summary
Address: 3EDzR4QKeGJyCZWXMF1kAQi8gHNQ798sF
Hash: 897d252f268b8a8d4e2ad52ab082ce0f5869d1
Tools: Related Tags - Unspent Outputs

Transactions
No. Transactions: 1
Total Received: 2,034.668943 BTC
Final Balance: 2,034.668943 BTC

Transactions (Oldest First)

Buy Bitcoin, Ethereum, Ripple and 13 other coins via Instant Bank Transfer with no registration required.

Buy Now with GBP

67079f670818b0e44ed70399bdcd4664a8595fb8f90/8538b7821c7ac889b8e8

3HomPY371CsvvjaCZj7fXf1TcSQ82HuG

3EDzR4QKeGJyCZWXMF1kAQi8gHNQ798sF

2,034.668943 BTC

1 Confirmation

12,601,546.94 USD
2017-11-13 19:10:37
Bitcoin transactions
Bitcoin trading volume
Bitcoin value
Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption
Bitcoin Wallet and Addresses

512-bit Public Key (Elliptic Curve DSA)

04774c929d61c6c17b290383e4cea29babc782d7df11e2d7ad40cf4dbddf1ce23c2047ea7bb8bef2c4b60d62cda7f7cc644385ff16bfd070461a6ec9fd9058cda6e

Wif Private key
5JQdwmJiEAEb3VxRN9oNAokCq7gGST1JZcGycD4fxRxT2Z1FkiA

Base-58
4dff94c127874ed988bd2846cfbf34632bb522e0c3e3d70e1a9bd9d5adf5abc

256-bit Private key

Bob’s Wallet

Public Key ID
1GqdnsdQfMXWjEEdpkhqcL9DhU9aNqRHUH
Private key:
4c0333a50b7724c71b89df148d83f64d49d896e21701007eeb8cada52744aca2

Public key:
0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Wif: 5JPmDetQXXvc5aT5efyrq7BxHbH4135owRzq9DD7n2eWQCta5MN

Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

Signed:
4830450220264c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e9ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b676407ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97
Bitcoin transaction

Transaction ID
IN:
Previous hash: f5d8ee39..0b9a6
<Signature> + <Public Key> (Alice)

OUT:
Amount: 3
Pubkeysign: OP_DUP OP_HASH160 [BobID]
OP_EQUALVERIFY OP_CHECKSIG

Alice creates transaction
Bob sends his public key

Alice’s private key
1FJGlqicf3sxQH4gw4V7adPiQ13vmrQrWf

1GqdnsdQfMXwJEEdpkhqCL9DhU9aNHUH

Miner
Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption
Mining process

Block 1  Hash 1  Block 2  Hash 2  Block N  Hash N

Transaction N1  Transaction N2  Transaction N3

Miner  Miner  Miner

Hash 1 scope  Hash 2 scope
Successful miners

- AntPool: 17.7%
- SlushPool: 11.9%
- ViaBTC: 11.7%
- BitFury: 6%
- BTC.TOP: 10.3%
- BTC.com: 10.3%
- BTCC Pool: 6.2%
- Bixin: 4.1%
- F2Pool: 5.5%
- BitClub Network: 3.3%
- 1Hash: 3.1%
- BW.COM: 2.4%
- 58COIN: 1.7%
- GBMiners: 1.7%
- Bitcoin.com: 1.2%
- Unknown: 1.2%
- Waterhole: 0.2%
- Bitcoin India: 0.2%
- BitMinter: 0.2%
- ConnectBTC: 0.2%
Mining Processes

- Hash
  - 000000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
- Previous Block
  - 00000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c
### Blocks

#### Block #475370

<table>
<thead>
<tr>
<th>Summary</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Of Transactions</td>
<td>1937</td>
</tr>
<tr>
<td>Output Total</td>
<td>10,443.01703436 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>555.96160374 BTC</td>
</tr>
<tr>
<td>Transaction Fees</td>
<td>0.87013657 BTC</td>
</tr>
<tr>
<td>Height</td>
<td>475370 (Main Chain)</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2017-07-11 21:44:58</td>
</tr>
<tr>
<td>Received Time</td>
<td>2017-07-11 21:44:58</td>
</tr>
<tr>
<td>Relayed By</td>
<td>AntPool</td>
</tr>
<tr>
<td>Difficulty</td>
<td>708,659,466,230.33</td>
</tr>
<tr>
<td>Bits</td>
<td>402754864</td>
</tr>
<tr>
<td>Size</td>
<td>998.17 KB</td>
</tr>
<tr>
<td>Version</td>
<td>0x20000000</td>
</tr>
<tr>
<td>Nonce</td>
<td>1203121562</td>
</tr>
<tr>
<td>Block Reward</td>
<td>12.5 BTC</td>
</tr>
</tbody>
</table>

| Hash            | 0000000000000000000000000d99e57b83834a2d1f4387a93d08661b9c3a5f498bdc55 |
| Previous Block  | 000000000000000000000000012138e05f0779765277a9d2ab7e4a2a70882790af88a0c |
| Next Block(s)   | 000000000000000000000000010e3117695c04d65d31cfa8489b7d579dce2112c5a2daae |
| Merkle Root     | 140d91abab9501d50ace079ba12c80125f48c2b5e7d9da885ea3ee8ea767e82          |
Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption
History

• Ethereum was created by Vitalik Buterin in 2015 and which built on the Bitcoin/Blockchain concept by included the concept of smart contracts.

• After a hack, in 2016, the Ethereum currency split into two: Ethereum (ETH) and Ethereum Classic (ETC).
Ethereum setup

Gas: One Keccak256 cryptographic hash takes 30 gas, plus 6 more gas for every 256 bits of data.
Gas

- Within Ethereum applications we define the concept of *gas*. This is basically the unit that is used to measure the amount of work that is required to perform a single Keccak-256 hash, and where 30 gas are consumed for a single hash and 6 more gas for each 256 bits of data hashed. In this way there is a motivation to keep contracts small, as they will be less costly.
Gas

• Gas thus provides a way to define the fee that miners receive in performing operations on the blockchain.

• This differs from Bitcoin which only charges for the number of kiloBytes in a transaction. When it comes to the actual payment of the transaction fees, there is a payment of ether to the miners who create the blocks.
Gas

- Ethereum transactions thus have a fee associated with them. If the fee is too low, then the miners will not process the transaction.
- When gas is consumed it is paid to the miner, and cannot be recovered back.
- If the transaction fee is set too high, there are likely to be many eager miners who are keen to profit from the high fee, and your transaction is likely to be prioritized.
• Overall, though, miners only charge for the work they have done, and they will return back any excess gas which they have not used. A miner can decide whether it needs to change the use of gas according to the price of gas varying. This overcomes the changes in transaction fees that happen in Bitcoin.
Gas

In Ethereum, just like Bitcoin, there is a block limit, so you'll end up paying more if you overspill into another block (which means you should be efficient with your code and data).

The gas price per transaction aims to overcome denial of service and infinite loops, and where 0.00001 Ether or 1 Gas is used to execute a line of code. If there is not enough Ether, no transaction will be performed. It also aims to make code designers efficient and not use waste bandwidth and CPU utilization.
Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption
Smart Contract

Blockchain

Smart contract

Bob

Enact smart contract between Bob and Alice

Alice
pragma solidity ^0.4.0;

contract test2 {
    uint a;

    function test2() {
        a = 1;
    }

    function val() returns (uint) {
        return a;
    }
}

contract test3 is test2 {
    uint b = a++;

    function show() returns (uint) {
        return b;
    }
}
Compile with Solidity
Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption