Public, Private keys
Crypto Wallets
Exchanges

Georgi Mitev FMI Sofia University

Public and Private keys

- What is Private key
  - 256-bit number, which can be represented one of several ways.
  - 256 bits in hexadecimal is 32 bytes, or 64 characters in the range 0-9 or A-F
  - Bitcoin uses Elliptic Curve Digital Signature Algorithm or ECDSA wikipedia link
  - Signature – hash of the transaction to be signed + private key
- What is Public key (Public address)
  - Number that can be generated from the private key
  - 256bit long - Final hash Public address (160bit)long

Public BTC Address

- Public key

Creating address is created by hashing the public key with SHA-256, then hash that with RIPEMD-160 (this is probably where the “160” comes from in “hash 160 address”;

Hashing functions used:

SHA-256 (successor of MD5) – hash function using 32bit words

RIPEMD-160 - https://en.wikipedia.org/wiki/RIPEMD

Examing Transaction

Inputs

HEX | ASM

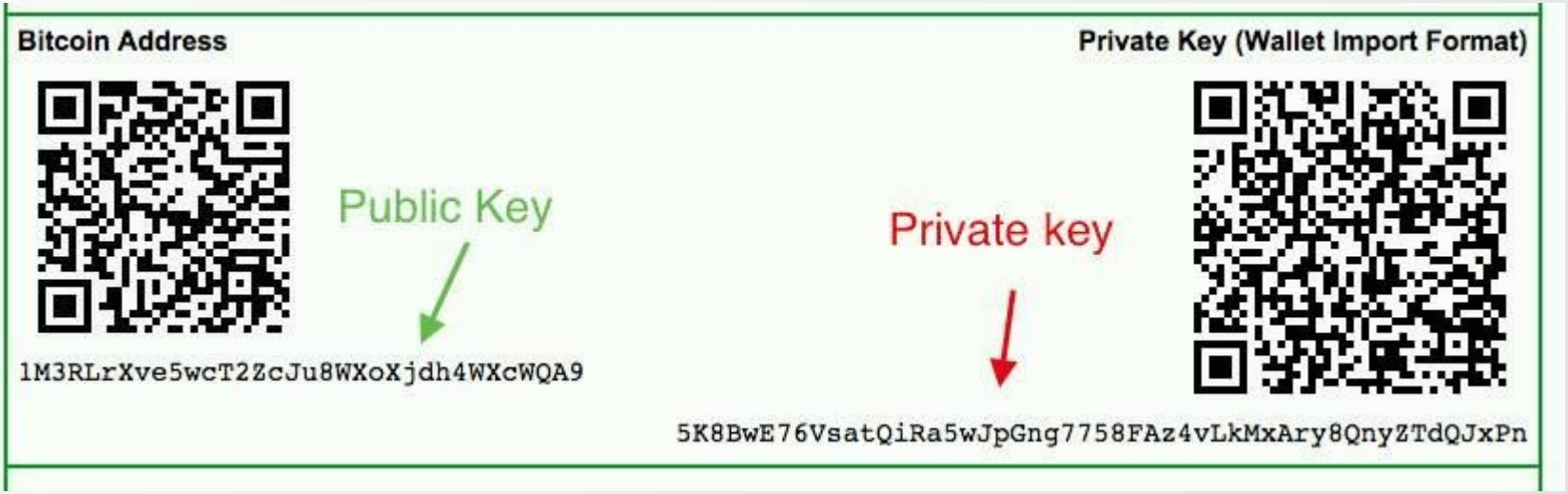
Index	0	Details	Output
Address	1GqpaRRvdX8HpqRUzg42v5GMPEoFDXV27Q	Value	1684.00000000 BTC
Pkscript	OP_DUP OP_HASH160 adc5914b705df9bc45cd6561de89a514b7901f00 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab59aa63d02201fe27c3e6374dd3a5425a577d9ca6ad8ff079800175ef9a44475bc98bcef21cf01 023b027d54ce8b6c730e0d5833f73aec6a5bae4efe04f57d2864a6a7df2af56e46		
Witness	N/A		

Link to transaction

Outputs

Index	0	Details	Spent
Address	17rfobSZ8Dj61c8sanhzzR76ADMjWYYpCP	Value	5.93100000 BTC
Pkscript	OP_DUP OP_HASH160 4b358739fc7984b8101278988beba0cc00867adc OP_EQUALVERIFY OP_CHECKSIG		

BTC Public/Private key



Creating BTC Private key

- Everyone can create BTC private key – even with web based tools
  - https://www.bitaddress.org/

https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.html

Public and Private keys

- Why we should protect/secure out private key
- Example BTC private key, Ethereum private key

- How secure are private keys?
- Can QuantComputers brake the encryption
  - Andreas Antanopoulus - https://www.youtube.com/watch?v=wlzJyp3Qm7s

Different type of wallet

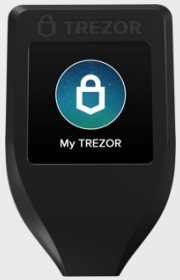
- Paper wallet
- Software wallet (Metamask, Exodus)
- Web-based (MyEtherWallet)
- Hardware wallet (cold wallet) – Ledger (Nano S), Trezor

- Friendly advices
  - Don’t use web wallets (DNS spoofing, javascript snippets)
  - Don’t use printer for paper wallets
  - Use Android / IOS wallets carefully

Hardware wallet

Ledger Nano X / Ledger Nano S
https://www.ledger.com/

Trezor One / Trezor Model T
https://trezor.io/start/



Hardware / cold wallet

- Software / hardware wallets usually use seed words
- Private keys are hidden from the user
- Usually many addresses are used to create obfucation
  - This means with one cold walltet you can have many addresses for deposit
  - For example one device Ledger Nano S uses around 50 addresses for BTC deposit

Using mnemonic seed words

Exchanges

- Centralized Exchanges
  - Private keys are stored on the exchange
  - Kraken, Binance, Coinbase, Bittrex

- Decentralized exchanges
  - Private keys are only shared with the exchange – not stored there
  - Waves, 1inch.exchange, IDEX (trading ether tokens)
  - Uniswap - https://app.uniswap.org/#/swap
  - https://etherscan.io/stat/dextracker

Centralized exchanges

- Well established UI – good user experience
- Big exchanges have good liquidity

- Hackable – trust issues
- User's private keys stays on the exchange
- Centralized :/

Decentralized Exchanges

- Private keys stays with the user
- Low taxes
- Decentralized :)

- Hard to use, not popular
- Low to none customer support
- Lack of liquidity (solved with Uniswap)

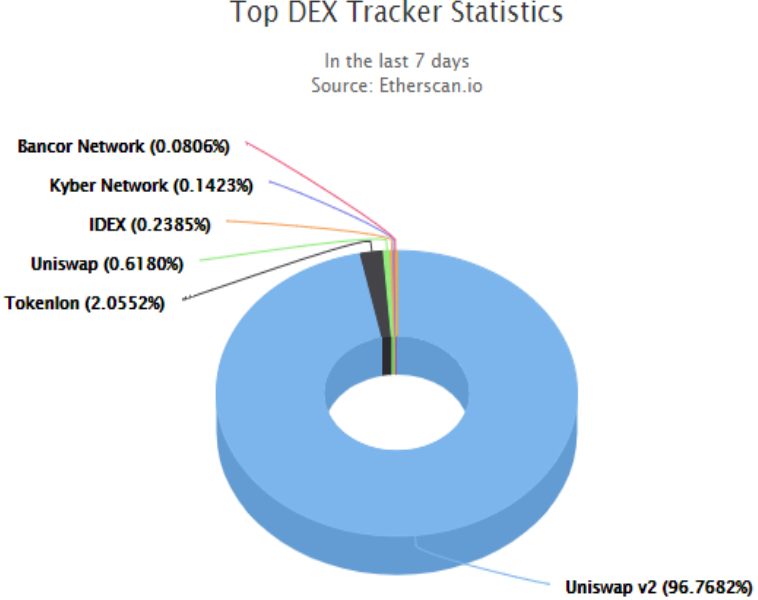
History of decentralized Exchanges

In 2016, Vitalik Buterin proposed a decentralized exchange that would employ an on-chain automated market marker with certain unique characteristics. Two years later, Uniswap was born. On November 2, 2018, Uniswap launched at Devcon 4 and was publicly announced and deployed to the Ethereum mainnet.

Uniswap v2

Uniswap is a simple smart contract interface for exchanging ERC20 tokens. It has an innovative model for pooling liquidity reserves and serves as an open-source frontend interface for traders and liquidity providers. A mechanism called the “Constant Product Market Maker” is used for determining exchange rate and price slippage as well as eliminating the need for an order-book.

- Why do we pay attention for Uniswap?
- How can Decentralized Exchange has Liquidity
  - Liquidity providers



https://etherscan.io/stat/dextracker

First ‹ Page 1 of 1 › Last

Rank	Decentralize Exchange (DEX)	Total Transactions	Percentage
1	Uniswap v2	817,240	96.7682%
2	Tokenlon	17,357	2.0552%
3	Uniswap	5,219	0.6180%
4	IDEX	2,014	0.2385%
5	Kyber Network	1,202	0.1423%
6	Bancor Network	681	0.0806%
7	Ether Delta	370	0.0438%

More concepts of a blockchain

- Block difficulty chart - https://etherscan.io/chart/difficulty
- Network Hash Rate - https://etherscan.io/chart/hashrate
- BTC Difficulty - https://bitinfocharts.com/comparison/bitcoin-difficulty.html
- Block reward
  - BTC Block reward https://bitcoinvisuals.com/chain-block-reward

Concept of mining

- Mining – PoW consensus
  - Solo mining, Pools
  - https://www.etherchain.org/charts/topMiners
  - https://www.blockchain.com/bg/pools
- Coin distribution must be decentralized
  - Pre-mine concept
  - Bitcoin Genesis block #1 (Timestamp 2009-01-03 18:15:05)

Sources

- **Block explorers**
  - https://chain.so/ - BTC + BTC Forks (LTC, Dash, Zcash)
  - https://www.blockchain.com/explorer
  - https://etherscan.io
  - https://kovan.etherscan.io/ Explorer for test network

- https://en.bitcoin.it/wiki
- https://learnmeabitcoin.com/beginners/blocks

- Andreas Antonopoulus – Bitcoin origins
  - https://bit.ly/2PltdU0

- Introduction to Bitcoin
  - https://bit.ly/2dnNDxC

Thank you!

Questions ?