Disclaimer

Die nachfolgende Präsentation wurde am 17.05.2018 an der Universität Passau gehalten. Bilder wurden entfernt und durch rote Platzhalter ersetzt. Die Folien wurden nach besten Wissen und Gewissen erstellt, sind jedoch nur als Teil der Präsentation zu sehen und halten weder Anspruch auf Vollständigkeit noch Fehlerfreiheit.

Cryptocurrencies and Smart Contracts

Tobias Hilbig
tobias.hilbig@siemens.com

Universität Passau

TOC

Introduction

- Wer ist das und warum steht der da vorne?
- Warum gibt es diesen Talk?
- Was erwartet mich?
- Wer kennt CCs? Wer besitzt welche?
- Disclaimer
  - Besitz von Cryptowährungen, ua. Bitcoin
  - Keinerlei formale Qualifikation

What I think I look like explaining crypto VS what I actually look like

Blockchain

Overview

- Replizierte Datenbank (weltweit, viele 1000 Nodes)
- Append only
- Trustless
- CIA: Vertraulichkeit, Integrität und Verfügbarkeit
- Keine Verschlüsselung!
- BTC Whitepaper 31.10.2008
- BTC Netzwerk 03.01.2009

Blockchain

Bitcoin Whitepaper

WHITEPAPER

Blockchain

Topologie

MESH NETWORK

Blockchain

Chaining and Orphans

BLOCK CHAIN

Blockchain

Bitcoin as mining example

- PoW: Proof of Work
- As of 24.04.2018: More energy consumption than Switzerland 0,3% of the world, 66TWh/a, 900kW or 270€/TX
- 30 EH/s as of 15.05.18, 10^{18} = Trillionen
- 50 BTC / 10 min, aktuell 12,5 BTC, Ende ~2130
- 1 BTC = ~7191 EUR Stand 11.05.18 -> 100k$ / Block
- ~18/21 Mio Coins bisher
- CPU, single user mining
- GPU, pooled mining
- FPGAs then ASICs and all pooled
- mostly in China (cheap energy)
- GPU shortage in 2016/17

MINING FARM 1

MINING FARM 2

Bitcoin

Overview

- Währungssystem
- Kleinste Einheit Satoshi, 8 Nachkommastellen
- Eigenschaften
  - Fälschungssicher
  - Keine trusted 3rd party
  - Dezentralisiert
  - Irreversibel
  - Zensurfrei
  - Pseudonym

DE 9556 0320 8002 0000 0000 –> Max Musterman
1QFKsjKMz4tVR3NP19Hc1f6axxxxxxxxxx –> ???

Bitcoin

Supply

BITCOIN SUPPLY

BITCOIN BLOCKCHAIN SIZE

Bitcoin

Notable Events

- 03.01.2009: Here it all began
- 22.03.2010: 2 Pizzas for 10.000 BTCs
- 17.07.2010: Mt. Gox established
- 18.07.2010: GPU Mining
- 2011: Start of DMNs
- *09.02.2011: $ Parity*
- 28.11.2012: 1st Halving (25 BTC)
- 28.02.2014: Mt. Gox bankruptcy, 800k BTC stolen, 450M$
- 09.07.2016: 2nd Halving (12.5 BTC)
- 01.08.2017: Bitcoin Cash Hardfork

Bitcoin

Altcoins

- Open Source -> Copycoins or "Shitcoins"
- `https://coinmarketcap.com/` lists about 1600 Coins
- Marketcap bei 400Mrd$, davon 150 Mrd BTC
- First Gen: Digital Money
  - Classic: Bitcoin, Bitcoin Cash, Litecoin
  - Privacy: Zerocash, Monero
  - Other: Counterparty
- Second Gen: Smart Contract Platforms
  - Main Player: Ethereum
  - "Identity" Platforms
  - Stablecoins, "Metacoins" as Combicoin, Triaconta
- Third Gen: *Upcoming* New Concepts
  - lightweight (browser / phone) but secure as POW
  - IOT, Micropayments
  - fast and DAG based?

Technical background

Bitcoin - Elements

- Asymetrische Crypto & Hashing: $sha256 : \{0,1\}^* \rightarrow \{0,1\}^{256}$
- Public Keys as pseudonyms (their hashes)
- Hash Pointer (TX and Blocks)
- Coin creation by miners, difficulty adjustment $\rightarrow$ 10 min
- Coin ownership allows spending
- Gossip protocol
- Blockchain as public, append only, database
- Fairness is rewarded by the system $\rightarrow$ Greediness?
- Consensus emerges by itself
  - even in case of delays, mistrust, cheating users

Technical background

Bitcoin - Blocks

- Header contains information:
  - version
  - prevHash
  - merkleTreeRoot
  - timestamp
  - difficulty
  - *nonce*
- Miners collect, validate and arrange tx into a merkle tree
  - Fast verification of txs
  - Verification without knowing other tx
  - Part of the header $\rightarrow$ tx set proof for subsequent blocks

Technical background

Bitcoin - Block detail

MERKLE TREE

Technical background

Bitcoin - Genesis Block

GENESIS BLOCK

Technical background

Bitcoin - Transaction chaining

- Identity = pubkey: Anybody can create some
- Transactions are signed by the senders inputs (keys)
- Transactions (their outputs) deposit money to pubkeys

TX CHAINING

Technical background

Bitcoin - Transaction format

TX SOURCE

Technical background

Bitcoin - Transactions cont

TX BLOCKEXPLORER

Technical background

Bitcoin - Scripting System

Default Pay-to-pubkey-hash format:

```
1 scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
2 scriptSig: <sig> <pubKey>
```

Stack processing: (Source: https://en.bitcoin.it/wiki/Script#Script_examples)

Stack	Script	Comment
	<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	scriptSig and scriptPubKey are combined.
<pubkey> <sig>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Constants are added to the stack.
<pubKey> <pubKey> <sig>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is duplicated.
<pubHashA> <pubKey> <sig>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is hashed.
<pubKeyHash> <pubHashA> <pubKey> <sig>	OP_EQUALVERIFY OP_CHECKSIG	Constant added.
<pubkey> <sig>	OP_CHECKSIG	Equality is checked between the top two stack items.
TRUE		Signature check successful, true returned

Technical background

Smart Contracts

- First serious platform: Ethereum
- Contracts deployed on the blockchain
- Arbitrary Code, turing complete language
- 15sec blocktime
- Examples
  - Providing a deposit
  - Escrow (2 out of 3)
  - Kickstarter like funding
  - Inheritance
  - "The DAO" - decentralized & democratic investment fund
    150 Mio$, 14% of all ETH, was hacked shortly after

Technical background

Smart Contracts - Example

Source https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/examples/SimpleSavingsWallet.sol

```
1  pragma solidity ^0.4.21;
2
3  import "../ownership/Heritable.sol";
4
5  contract SimpleSavingsWallet is Heritable {
6
7  event Sent(address indexed payee, uint256 amount, uint256 balance);
8  event Received(address indexed payer, uint256 amount, uint256 balance);
9
10 function SimpleSavingsWallet(uint256 _heartbeatTimeout) Heritable(_heartbeatTimeout) public {}
11
12 function () public payable {
13   emit Received(msg.sender, msg.value, address(this).balance);
14 }
15
16 function sendTo(address payee, uint256 amount) public onlyOwner {
17   require(payee != 0 && payee != address(this));
18   require(amount > 0);
19   payee.transfer(amount);
20   emit Sent(payee, amount, address(this).balance);
21   }
22 }
```

Trading

Wallet

- Desktop: Bitcoin Core, *Electrum*
- Mobil: *Mycelium*
- Offline: Paperwallet, *Electrum + TAILS*
- **Webwallet: Don't to it!**
- Recommendation:
  - KISS
  - Cold Storage nutzen
  - **Backups, Backups, Backups!**
  - **if you dont own the keys you dont own the coin!**

Trading

Platforms

- Kraken, Coinbase, *Cubits*, Bitcoin.de
- Localbitcoins, *Mycelium Local Trader*
- Trading with SEPA, CC, Crypto, Cash
- Crypto -> Crypto at *Poloniex* and *Shapeshift*

Trading

Mycelium (Android)

MYCEZLIUM WALLET

Trading

Sag mir endlich wie ich reich werde!

- Get rich quick, FOMO
- Höchstspekulatives "Investment"
  - völlig neue Anlageklasse
  - Fremdwährungsrisiko
  - Liquiditätsrisiko
  - Keine zentrale Stelle
  - Keine Rechtssicherheit
  - Marktmacht & Manipulation
  - Volatilität
  - Malicious Software
  - Atomarität von TX
  - Past performance predicts future returns!
  - Steuern?
  - Sicherheit der darunter liegenden Kryptografie

Trading

Andererseits...

'Never invest in a business you cannot understand.' Warren Buffett

- Facts
  - Egal wann -> Profit (3m)
  - Sehr hohes Risiko, sehr hoher Ertrag
  - Einfaches Investment, sehr knappes Gut
- Do's
  - Bewährte Strategien anwenden
  - Regelmäßig und kontinuierlich investieren - cost average
  - Feste Beträge investieren und diversifizieren (intern wie extern)
  - 1-2% des Portfolios / ein paar Hunderter?
  - "Spielgeld" investieren, Spaß haben!
- Dont's
  - Daytrading / timing the market
  - FOMO und "Catch the falling knive"
  - All eggs in one basket
  - Use case and application?

Trading

Price history

BITCOIN PRICE

Trading

Price history logarithmic

BITCOIN PRICE LOGARITHMIC

Further Information

Fazit / Meinung

- Völlig neue Technologie, "die Katze ist aus dem Sack"
- "Geld" mit bisher unmöglichen Eigenschaften
- Sehr viel Betrug & Verbrechen
  $\rightarrow$ DNMs, "Hacks", ICOs, wenig rechtliche Handhabe
- Geldfunktion $\rightarrow$ Smart Contracts
- Sehr viel Arbeit nötig für
  - Sicherheit (beweisbar!)
  - Alltagstauglichkeit
  - *Sinnvolle* Anwendungen
  - Regulierung / Rechtssicherheit

Further Information

Links

- Reddit: /r/btc, /r/bitcoin, /r/cryptocurrency, etc
- medium.com
- `https://forum.bitcoin.com/`
- `https://coinmarketcap.com/`
- Sidebar of /r/btc
- Vorlesung System Security im SS
  (Master, anrechenbar im WP Bachelor)

ZITAT LINDNER BITCOIN

Q&A