



Prinzipien von Post-Bitcoin Währungen

VIRTcrime Kryptowährungs-Forensik-Training

Patrik Keller

Klassifikation von Post-Bitcoin Währungen

Skalierbarkeit



Funktionalität



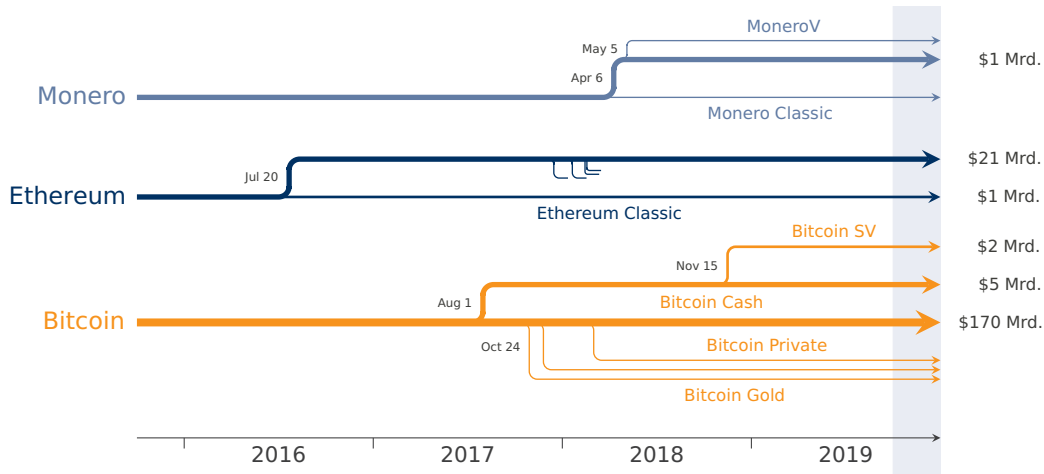
Datenschutz



Gliederung

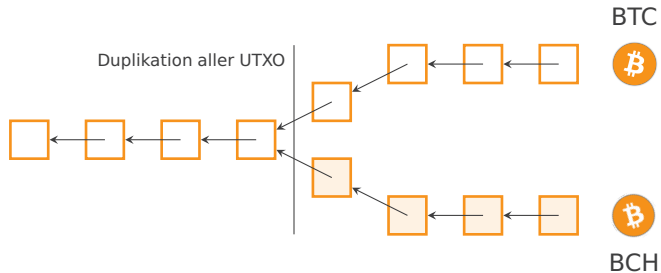
- ① **Forks und Duplizierung von Coins**
- ② „Smart Contracts“ und Tokens
- ③ Techniken für Datenschutz

Zeitleiste ausgewählter Forks



Quelle: coinmarketcap.com | Stand: 5 Nov 2019

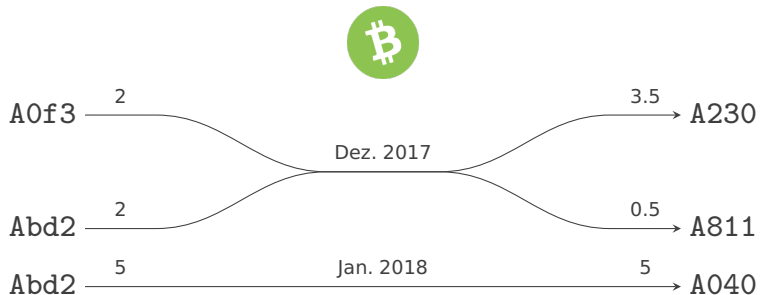
Blockchain-Fork



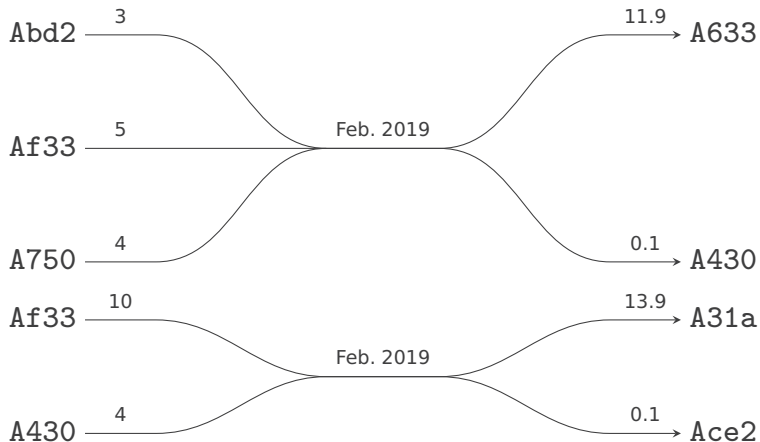
Beispiel



Beispiel (Fortsetzung)



Beispiel (Fortsetzung)



Cross-Chain Address-Clustering

Wenn es Forks gibt, ist das Address-Clustering auf einzelnen Chains nicht vollständig.

Lösung (manuell, umständlich)

Abwechselndes Anwenden der Clustering-Heuristiken auf einzelne Chain und Übertragen der Information

Lösung (effizient automatisiert)

Betrachte einzelnen Transaktionsgraph, der Transaktionen aller Chains enthält.

Umgesetzt als Erweiterung für **BlockSci**.

— **VIRTCRIME D3.2**

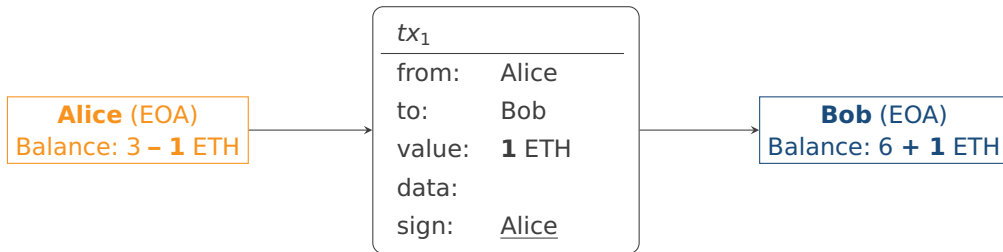
Gliederung

- ① Forks und Duplizierung von Coins
- ② **„Smart Contracts“ und Tokens**
- ③ Techniken für Datenschutz

Ethereum

Account-Modell statt UTXO-Modell

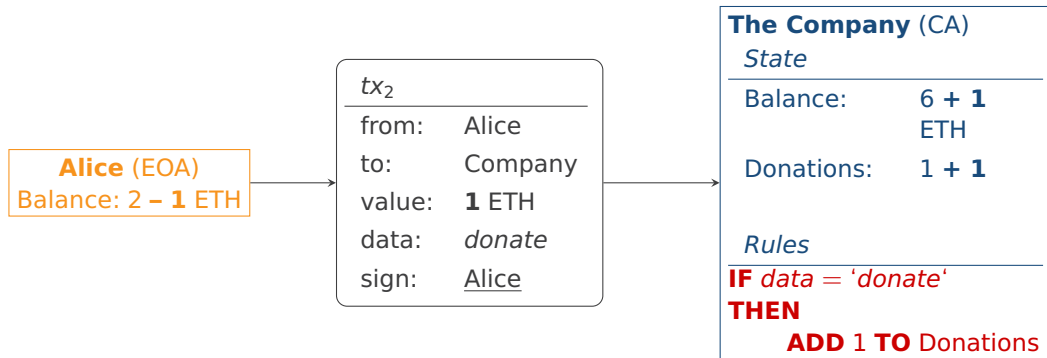
Externally Owned Account (EOA):



Ethereum

Account-Modell + erweiterte Logik + erweiterter Zustandsraum

Code Account (CA) (auch „Smart Contract“):



Code Accounts

- CAs enthalten je ein Programm.
- Aktivierung des Programms durch Transaktion.
- Die Transaktion enthält Eingabe für das Programm.
- Davon abhängig ändert das Programm den Zustand des CA
- oder erstellt weitere Transaktionen.

- Nutzer können nach belieben CAs erstellen.

Was bringt's ?

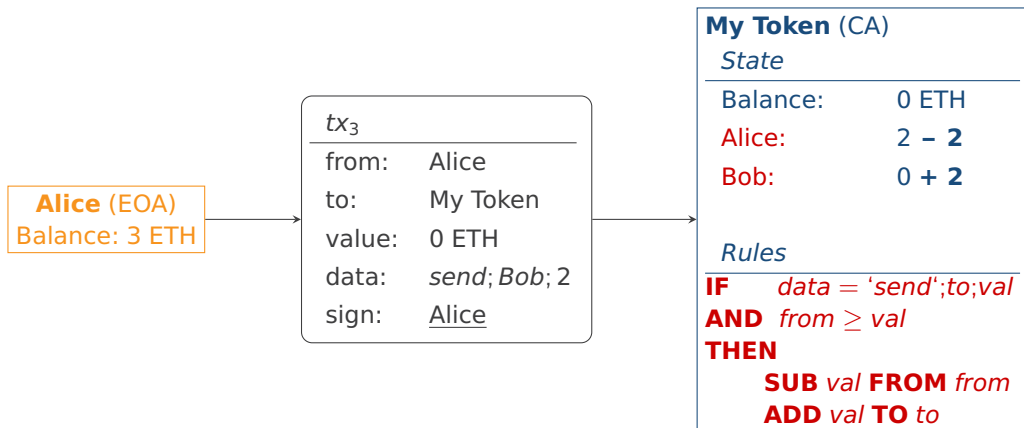
Spekulation, Glücksspiel, Exchanges, Abzocke, Token-Systeme

Token-Systeme

Token: handelbares virtuelles Gut

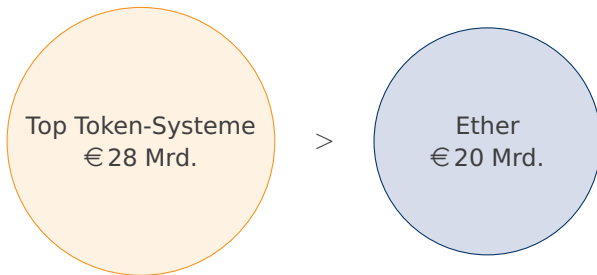
Token-System: Besitz und Transfer eines Tokens verwaltet durch CA

Token-Systeme



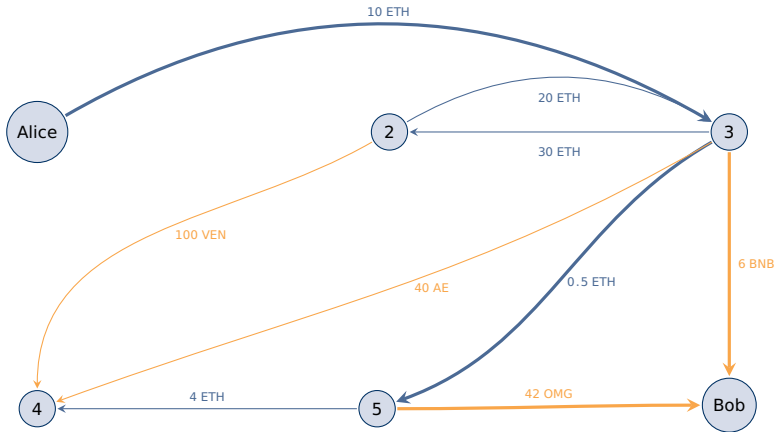
Relevanz von Token-Systemen

Marktkapitalisierung



Quellen: Etherscan, coinmarketcap.com, 9. Oktober 2018

Herausforderung für die Forensik



Erstellung von Token-Systemen

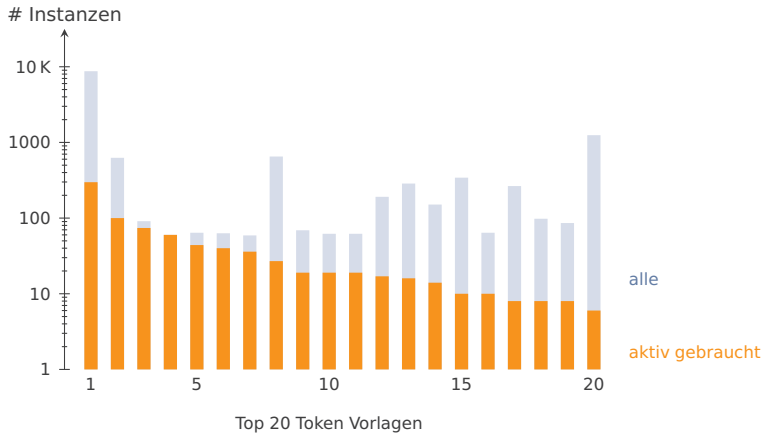
The image is a collage of three screenshots illustrating the creation of a token system on the Ethereum blockchain.

Left Screenshot: A code editor showing Solidity code for a token contract. The code includes a pragma statement for Solidity version 0.4.20, a contract named 'MyToken' with a constructor for initial supply, and a 'transfer' function that updates balances and emits events. The code is partially obscured by a semi-transparent 'The Coin' window.

Middle Screenshot: The Ethereum Wallet interface. It shows the 'SEND' tab with a balance of 4,213.728 ETH. A 'SEND' dialog is open, asking for an amount (0.0 ETH) and a recipient address (0x9b20...435f). The 'SELECT FEE' section shows a fee of 0.00074872 ETH, with a slider between 'CHEAPER' and 'FASTER'.

Right Screenshot: A 'Create contract' dialog box. It shows the contract name 'MyToken' and the gas price '0.004 ether per million gas'. The 'RAW DATA' section displays the transaction hash: 0x00. The dialog prompts the user to 'Enter password to confirm the transaction' and provides 'CANCEL' and 'SEND TRANSACTION' buttons.

Wiederverwendung von Code in Ethereum



Quelle: Fröwis et al. 2019, Daten bis 30. Mai 2018

Herausforderung für die Forensik

Betrachtung von Ether allein gibt unvollständiges Bild.

Herausforderung

Token-Systeme sind technisch vielfältig.

Chance

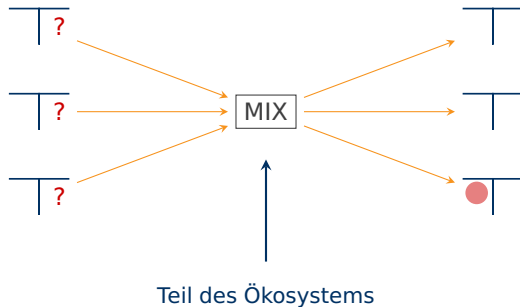
Token-Systeme implementieren oft Standards (ERC-20, ERC-721), welche die Automatisierung ermöglichen, oder sind gar kopiert.

Gliederung

- ① Forks und Duplizierung von Coins
- ② „Smart Contracts“ und Tokens
- ③ **Techniken für Datenschutz**

Anwendung des Mix-Prinzips

Herstellung von Unverkettbarkeit in **Transaktionssystemen**



Erhebliches **Vertrauen** in Mix-Betreiber erforderlich.

Partnersuche für CoinJoins

Join Market	Orders	Size Distribution	Depth	Export orders	GitHub	Getting Started
JoinMarket Orderbook						
364 orders found by 91 counterparties						
Type	Counterparty	Order ID	Fee	Miner Fee Contribution / BTC	Minimum Size / BTC	Maximum Size / BTC
Absolute Fee	J5BNWo4MhLbtAej1	0	0.00000400	0.00000002	0.00002730	0.00863625
Absolute Fee	J58HmZ2eFvZqELwx	5	0.00000400	0.00000002	0.00406800	0.00702015
Absolute Fee	J5E9nx6U7k976mCB	2	0.00000400	0.00000002	0.00844100	0.00863625
Absolute Fee	J5CUynfJ9hYrVWAc	0	0.00000500	0.00000000	0.00100000	13.58535521
Absolute Fee	J58HmZ2eFvZqELwx	22	0.00000539	0.00000060	0.00406800	0.00702015
Absolute Fee	J58HmZ2eFvZqELwx	3	0.00000800	0.00000000	0.00406800	0.00702015
Absolute Fee	J5E9nx6U7k976mCB	20	0.00000800	0.00000000	0.00844100	0.24100000
Absolute Fee	J59Z6KFWtWk4wcjM	6	0.00000800	0.00000000	0.00400000	0.24100000
Absolute Fee	J5Bmy7oT23lrpdVV	0	0.00000889	0.00000065	0.08886283	1.82194683
Absolute Fee	J59pheQXDj7MZzFp	0	0.00000950	0.00000150	0.00100000	0.71455724
Absolute Fee	J58HmZ2eFvZqELwx	1	0.00000950	0.00000150	0.00406800	0.00702015
Absolute Fee	J5E9nx6U7k976mCB	0	0.00000950	0.00000150	0.00844100	0.71455724
Absolute Fee	J58HmZ2eFvZqELwx	21	0.00000997	0.00000000	0.00406800	0.00702015

Quelle: <http://joinmarket.io>, Abruf: 4. Jänner 2017

Bitcoin + JoinMarket

Eingebauter JoinMarket reduziert notwendiges Vertrauen in Intermediär.



Dash

Herausforderung

CoinJoin erschwert Clustering.

Offline Mixing

Ring Signaturen ermöglichen Mixing ohne Interaktion mit Mixing Partnern.



Monero

Herausforderung

Bei korrekter Anwendung ist die Nachverfolgung stark erschwert bis unmöglich.

Transaktionen ohne Referenzen

Zero Knowledge Proofs ermöglichen Transaktionen ohne Referenz auf UTXO.



Zcash

Herausforderung

Theoretisch ist eine optimale Verschleierung möglich.

Chancen für die Forensik

Technisches Versagen

- Unerforschte theoretische Schwachstellen
- Fehlerhafte Implementierung
- Korrekte Anwendung nicht praktikabel
- Korrekte Anwendung teuer
- Schwache Voreinstellungen
- Fehlbedienung

Menschliches Versagen