universität innsbruck

VIRTCRIME

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Einführung in Kryptowährungen

VIRTCRIME Kryptowährungs-Forensik-Training

Rainer Böhme

Herzlich Willkommen

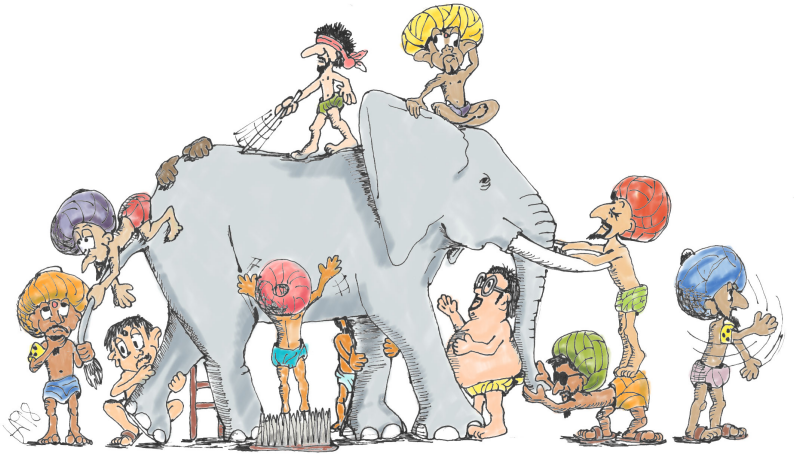
Kurzvorstellung

- Ich beschäftige mich mit digitaler Forensik seit 2004 und mit Bitcoin seit 2011.
- Meine MitarbeiterInnen und ich schulen Polizisten seit 2013 zu Blockchain-Forensik.

Ziele dieses Training

- Vermittlung von Inhalt, aber nicht ausschließlich im Frontal-Unterricht . . .
- Erfahrungsaustausch
- Raum für Fragen und Diskussionen
- Vertrauensaufbau
- Feedback für uns

Bitcoin ist . . .

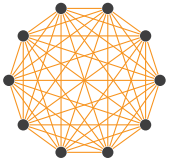


Urs Arnet, Nutzung mit freundlicher Genehmigung

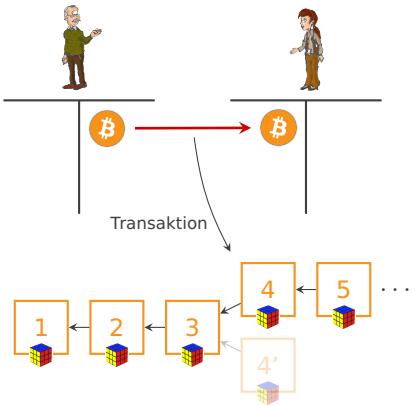
Gliederung

1. **Grundbegriffe und Einordnung der Technik**
2. Transaktionslogik bei Bitcoin
3. Grundtechniken der Bitcoin-Forensik

Bitcoin als verteiltes Kontensystem



P2P-Netzwerk

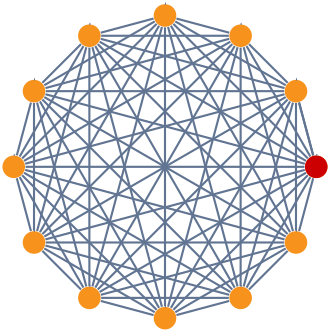


Bitcoin-Blockchain

Nakamoto 2008

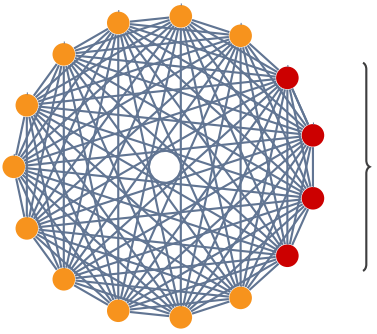
Offene Systeme

mit schwachen Identitäten

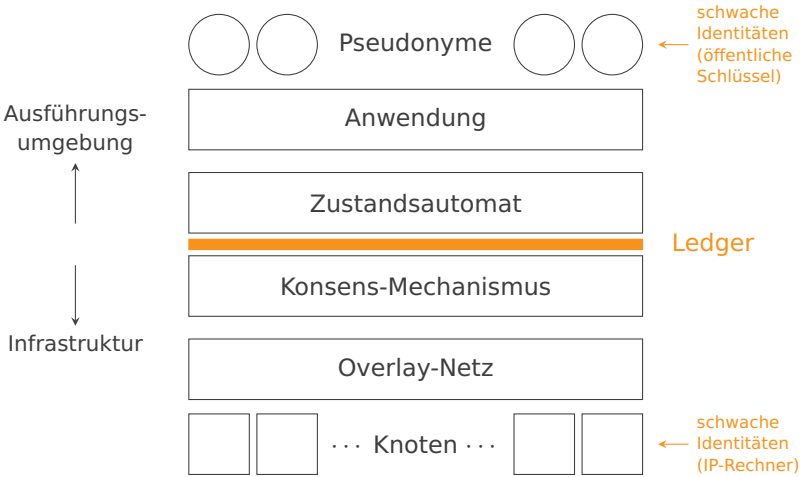


Offene Systeme

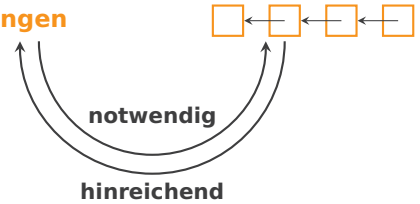
mit schwachen Identitäten



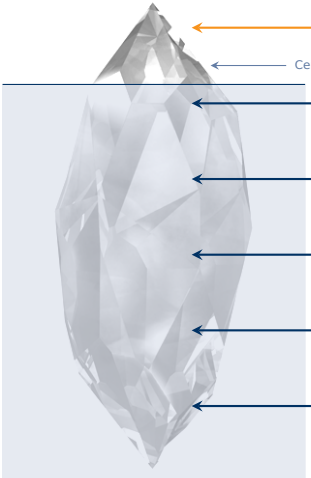
Schichtmodell für Blockchain-Systeme



Die Suche nach Blockchain-Anwendungen



Die Suche nach Blockchain-Anwendungen



Kryptowährungen

Certificate Revocation

Spekulation

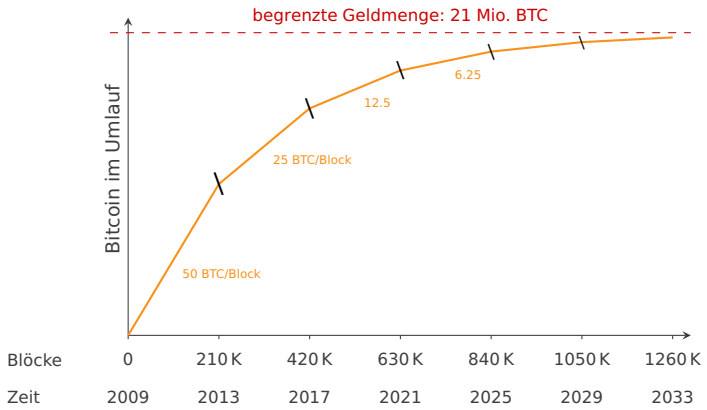
Glücksspiel

anonyme Treuhandkonten

außergesetzliche Wert-„Papiere“

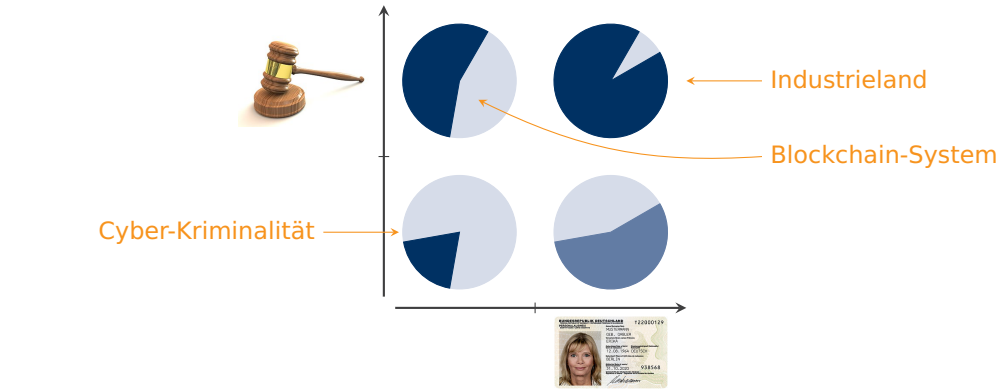
sichere Geldwaschmaschinen

Belohnung beim „Block-Minen“



Wer profitiert von der Blockchain-Technik ?

Anzahl möglicher Allokationen in Abhängigkeit der Entwicklung von Institutionen



Bildnachweis: Bundesrepublik Deutschland, CC-BY-2.0 Chris Potter

Spielarten der Kryptocoin-Kriminalität

Kryptocoin-spezifischer Betrug

- Erspähen von privaten Schlüsseln (oder Berechnung aus Zwischenergebnissen)
- Double-Spending: Nutzung temporärer Informationsasymmetrien
- Double-Receiving: Vortäuschen nicht ausgeführter Transaktionen
- Mining auf fremden Rechnern

Geldwäsche

- Verschleierung von Zahlungsströmen in Kryptocoins
- Eröffnung von Konten bei Bitcoin-Intermediären unter falscher Identität

„Tatmittel Kryptocoins“

- Handel mit illegalen Gütern und Dienstleistungen
- Erpressung; individuell und automatisiert
- Anlagebetrug, betrügerische Intermediäre

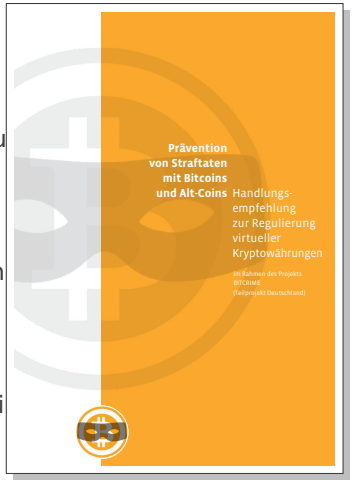
Relevante Forschungsprojekte

BITCRIME, 2014–2017, DE+AT
Strafverfolgung und Prävention durch Regu
https://www.bitcrime.de

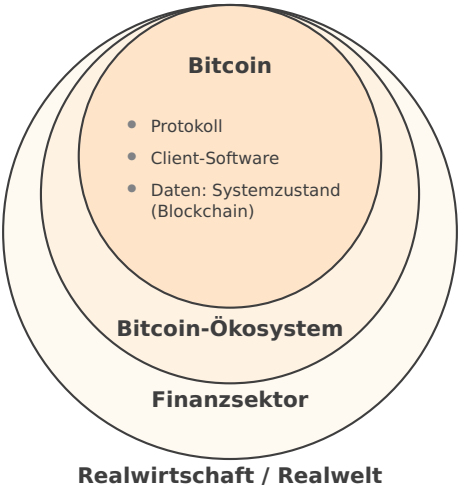
TITANIUM, 2017–2020, EU
Strafverfolgung EU-weit, haupts. Bitcoin un
https://www.titanium-project.eu

VIRTCRIME, 2018–2019, AT
Technologie für Strafverfolgung, Post-Bitcoi
http://virtcrime-project.info

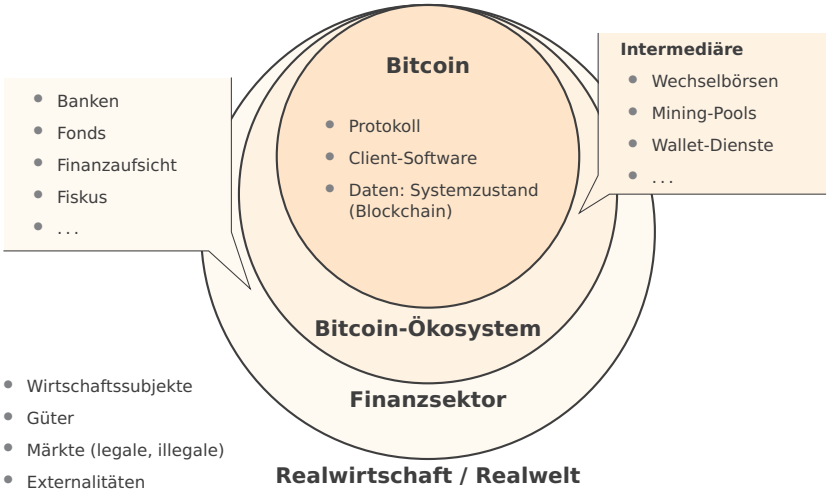
ECRIME, 2014–2017, EU
Messung wirtschaftlicher Schäden durch Cyber-Kriminalität allgemein



Bitcoin im Kontext



Bitcoin im Kontext

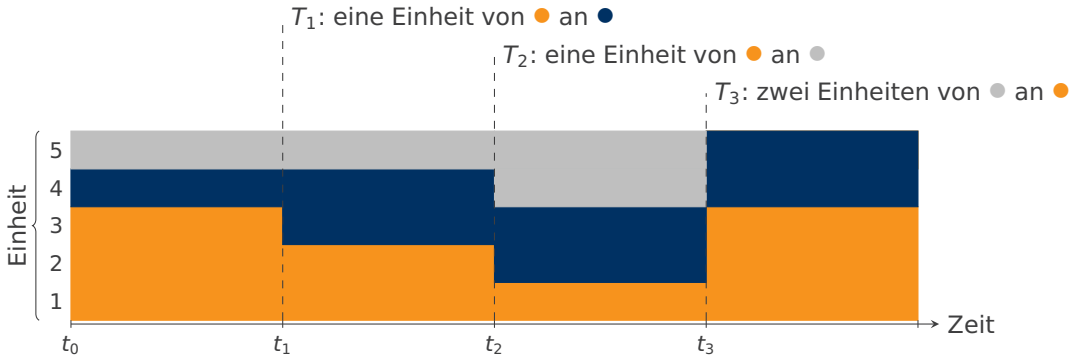


Gliederung

1. Grundbegriffe und Einordnung der Technik
2. **Transaktionslogik bei Bitcoin**
3. Grundtechniken der Bitcoin-Forensik

Verwaltung eines virtuellen Gutes

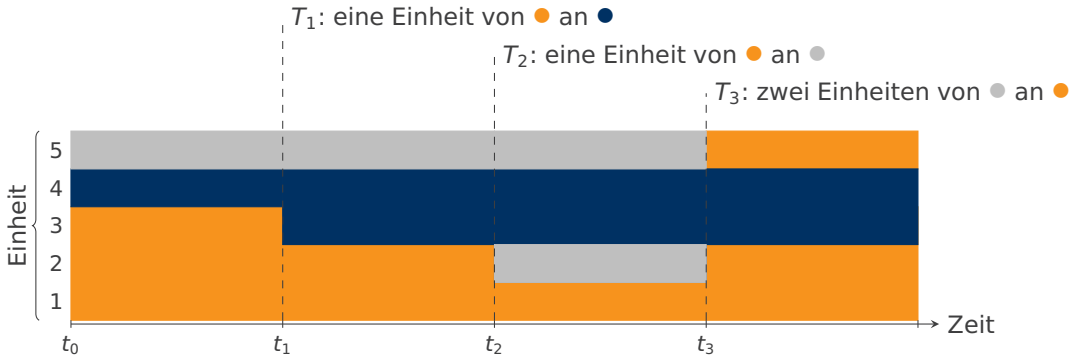
- Differenzkodierung durch Transaktionen
- Einhaltung von Nebenbedingungen
  - 1. Summe aller Konten konstant
  - 2. Kein Konto negativ
- Sichere Aufzeichnung



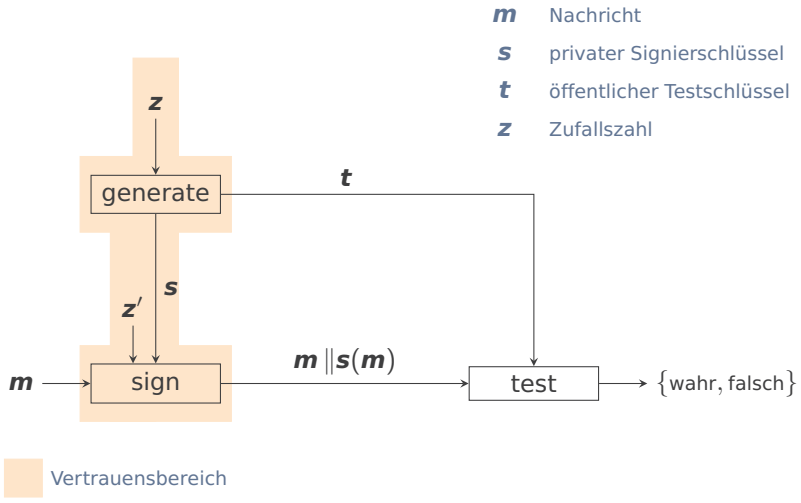
Verwaltung eines virtuellen Gutes

- Differenzkodierung durch Transaktionen
- Einhaltung von Nebenbedingungen
- Sichere Aufzeichnung

Variante ohne Fungibilität



Digitales Signatursystem



Autorisation mit digitalen Signaturen

Idee

- Besitzzuweisende Transaktion enthält Testschlüssel ***t*** (gibt neuer Besitzer bekannt)
- Weitergabe-Transaktion ist nur gültig, wenn sie korrekt digital signiert ist.

$\rightarrow$ Kopplung von Besitz i. S. v. Verfügungsgewalt an Kenntnis von ***s***.

„Öffentliche Schlüssel sind Kontonummern“

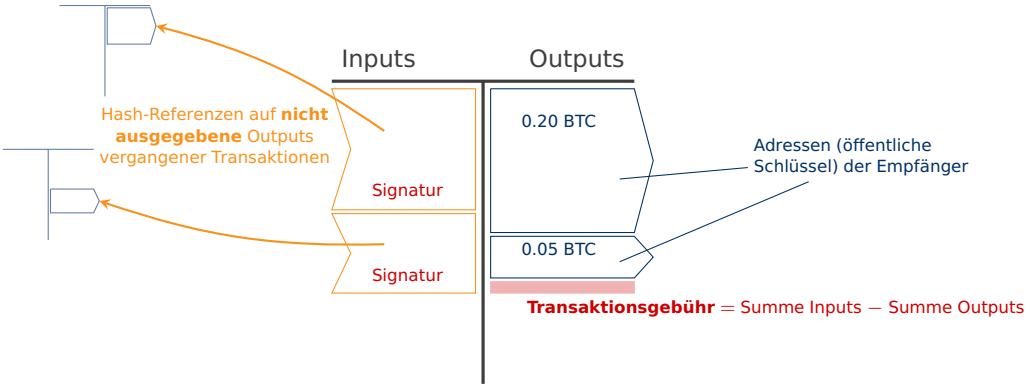
Kodierung bei Bitcoin Statt ***t*** wird ein Commitment zu ***t*** verwendet.
Der Testschlüssel wird erst bei der Weitergabe offengelegt.

Vorteil Geheimnisse mehrfach verwendbar: ***s***(● an ●) gibt nicht ***s*** preis.

Nachteil Transaktionen mit gleichem ***t*** sind verkettbar $\rightarrow$ Ansatz für Forensik

Transaktionskodierung bei Bitcoin

Jede Bitcoin-Transaktion besteht aus einer Liste aus Inputs und einer Liste aus Outputs.



Optional: `nLockTime`-Feld gibt Zeitpunkt in Blockhöhe oder Realzeit an, vor der die Transaktion ungültig ist.

Einfache Formalisierung

Wie verwenden die Notation

$$T_n = \Big(\overbrace{\underbrace{(T_{i,3}, T_{j,1})}_{\text{Input-Liste}}, \underbrace{((0.2, \boldsymbol{t}_{\text{Alice}}), (0.05, \boldsymbol{t}_{\text{Bob}}))}_{\text{Output-Liste}}}^{T'_n}, \underbrace{(\boldsymbol{s}_{\text{Bob}}(T'_n), \boldsymbol{s}_{\text{Bob}}(T'_n))}_{\text{Signaturen}} \Big)$$

mit folgenden Konventionen:

- $T_{i,3}$ ist eine Referenz auf den 3. Output von T_i.
- Der erste Wert jedes Output-Tupels ist der Betrag.
- $\boldsymbol{s}_{\text{Bob}}$ und $\boldsymbol{t}_{\text{Bob}}$ sind Signier- bzw. Testschlüssel unter der Kontrolle von Bob.
- Wenn Bob mehrere Schlüsselpaare hat, schreiben wir z. B.: $\boldsymbol{t}^1_{\text{Bob}}$, $\boldsymbol{t}^2_{\text{Bob}}$, ...

T' kann auf mehrere Arten gebildet werden: `https://bitcoin.org/en/developer-guide#signature-hash-types`

Beispiele

Bob besitzt 1.2 BTC aus dem 1. Output von T_1
0.3 BTC aus dem Wechselgeld (2. Output) von T_2
0.5 BTC aus dem Wechselgeld (4. Output) von T_3

Bob nutzt $\boldsymbol{t}^2_{\text{Bob}}$ als Wechselgeldadresse. Er möchte Alice 1.5 BTC an $\boldsymbol{t}_{\text{Alice}}$ überweisen:

$$T_4 = \left((T_{1,1}, T_{3,4}), \left((1.5, \boldsymbol{t}_{\text{Alice}}), (0.15, \boldsymbol{t}^2_{\text{Bob}})\right), (\boldsymbol{s}_{\text{Bob}}(T'_4), \boldsymbol{s}^2_{\text{Bob}}(T'_4))\right)$$

Alice verschiebt 1.0 BTC zur Sicherheit in ihre eigene *paper wallet* mit Schlüssel $\boldsymbol{t}^2_{\text{Alice}}$:

$$T_5 = \left((T_{4,1}), \left((1.0, \boldsymbol{t}^2_{\text{Alice}}), (0.45, \boldsymbol{t}_{\text{Alice}})\right), (\boldsymbol{s}_{\text{Alice}}(T'_5))\right)$$

Bob möchte sein Wechselgeld konsolidieren. Ist folgende Transaktion gültig?

$$T_6 = \left((T_{2,2}, T_{3,4}), ((0.4, \boldsymbol{t}_{\text{Bob}})), (\boldsymbol{s}^2_{\text{Bob}}(T'_6), \boldsymbol{s}^2_{\text{Bob}}(T'_6))\right)$$

Wallets

Wallets unterstützen Nutzer bei der Verwaltung ihrer privaten Schlüssel. Oft werden viele Schlüsselpaare deterministisch von einem Geheimnis abgeleitet.

Typen von Wallets

- Client-Software, typischerweise mit Passphrase und Backup-Funktionalität
- Spezialhardware (einfacher: vom Netz getrennte Standardrechner – *cold wallet*)
- Nicht-digital: Papier, Gedächtnis (*brain wallet*)

- Cloud-Software, erfordert Vertrauen in Anbieter
- Spezialfall **Verwahrer** (*custodial wallets*): Der Verwahrer besitzt alle Kryptocoins seine Kunden. Endnutzer haben keine Identität auf der Blockchain.

- Software in Form eines „Smart Contracts“ z. B. für Mehr-Augen-Prinzip oder Vertretungsvollmachten → gewerbsmäßige Nutzung, jedoch fehleranfällig

→ Beherrschung der Wallet-Varianten essentiell für Forensik und Beschlagnahmungen

Gliederung

1. Grundbegriffe und Einordnung der Technik
2. Transaktionslogik bei Bitcoin
3. **Grundtechniken der Bitcoin-Forensik**

Datenschutz in Blockchain-Systemen

Fundamentaler Konflikt zwischen:

- Öffentlichkeit der Blockchain-Daten, erforderlich für die dezentrale Verifikation, und
- Persönlichkeitsrechten der Nutzer, denn Informationen in (Finanz-)Transaktionen lassen Rückschlüsse auf Gewohnheiten und Lebensumstände zu.

Erhoffte Milderung:

- Pseudonyme sind nicht unmittelbar natürlichen Personen zuordenbar.

Trotzdem sind Blockchain-Daten als **personenbeziehbar** anzusehen, denn:

- Personenbezug kann oft durch **Verknüpfung mit weiteren Daten** (z. B. in der Hand von Intermediären wie Wechselbörsen, P2P-Datenpakete) hergestellt werden.
- Die Unveränderbarkeit der Blockchain erhöht die Wahrscheinlichkeit, dass dies in der Zukunft geschieht.

Böhme, R., Pesch, P. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. *Datenschutz und Datensicherheit*, 41, 8 (2017), 473–481.

Ansätze zur Deanonymisierung von Bitcoin-Nutzern

Pseudonyme	Know your customer (KYC)
Blockchain	Clustering-Heuristiken
Overlay-Netz	Echtzeitüberwachung Aktive Angriffe auf Clients

Zusammenführung von Bitcoin-Adressen zu Entitäten

Bekannte Heuristiken um Adressen in Entitäten (d.h. vermuteten Parteien) zu clustern:

1. Multiple-Input-Heuristik

- **Annahme** Wenn Inputs aus mehreren Adressen stammen, werden diese von der gleichen Partei kontrolliert.

$$T_3 = \big((T_{1,1}, T_{2,1}), ((1.0, \boldsymbol{t}_{\text{Casino}})), (\boldsymbol{s}_{\text{Pseudonym A}}(T'_3), \boldsymbol{s}_{\text{Pseudonym B}}(T'_3))\big)$$

2. Wechselgeld-Heuristik

- **Annahme** Die Wechselgeldadresse gehört zur Wallet des Senders.

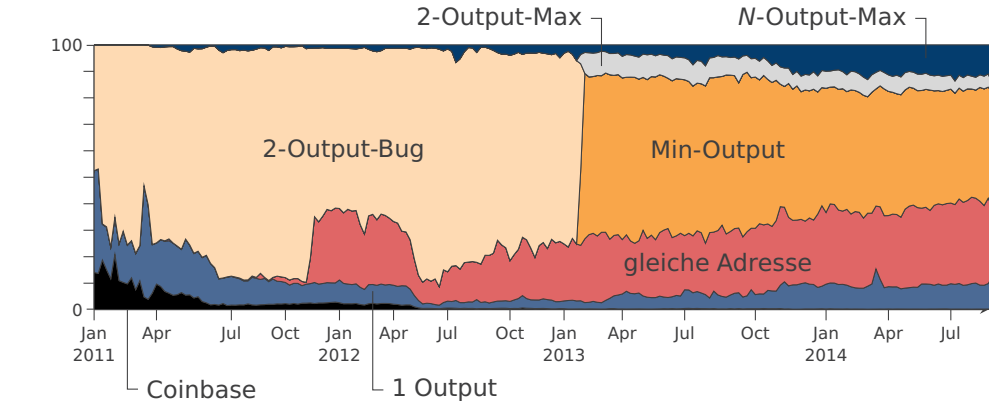
$$T_4 = \big((T_{3,1}), ((0.9, \boldsymbol{t}_{\text{Gewinner}}), (0.05, \boldsymbol{t}_{\text{Pseudonym C}})), (\boldsymbol{s}_{\text{Casino}}(T'_4))\big)$$

- Bitcoin-Clients verschleiern das Wechselgeld durch Randomisierung der Outputs.

Meiklejohn, S. et al. A Fistful of Bitcoins: Characterizing Payments among Men with No Names. *CACM*, 59 (4), 2016, 86–93.

Bestimmung der Wechselgeldadresse

Die Grafik zeigt den Erfolgsanteil (in %) von sieben Heuristiken im Zeitverlauf

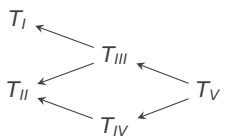


Möser, M., Böhme, R. Unveröffentlichte Analyse zur Schätzung des Netto-Transaktionsvolumens, 2014.

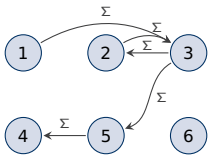
Graphische Blockchain-Analyse

Darstellungsvarianten zur Verfolgung von Zahlungsströmen in Bitcoin

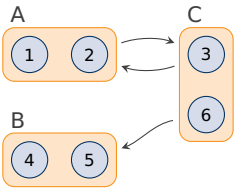
Transaktionsgraph



Adressgraph



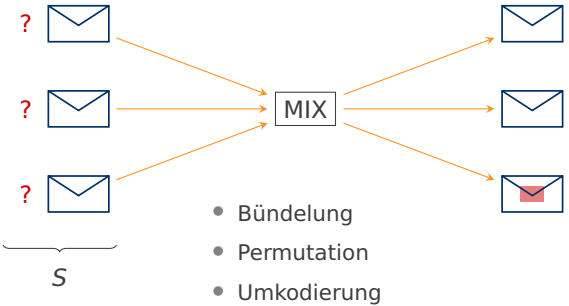
Entitätengraph



Angelehnt an: Abb. 6 aus Tschorsch, F. und Scheuermann, B. Bitcoin und Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys und Tutorials*, 18, 3 (2016), 2084–2123.

Das Mix-Prinzip

Herstellung von **Unverkettbarkeit** in Kommunikationssystemen

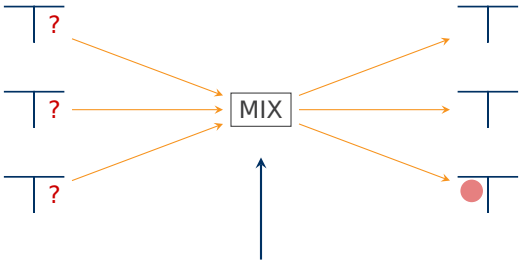


Die Kardinalität der **Anonymitätsmenge** $|S|$ ist eine einfache Datenschutzmetrik.

Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *CACM*, 24 (2), 1981, pp. 84–88.

Anwendung des Mix-Prinzips

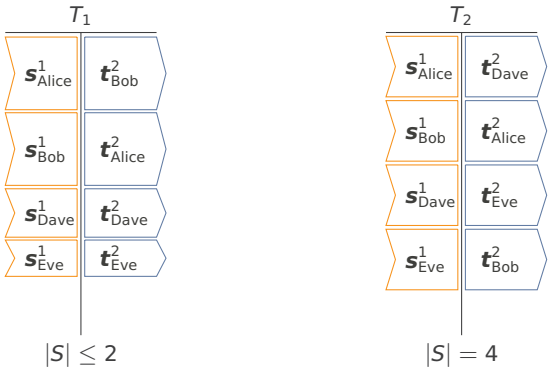
Herstellung von Unverkettbarkeit in **Transaktionssystemen**



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

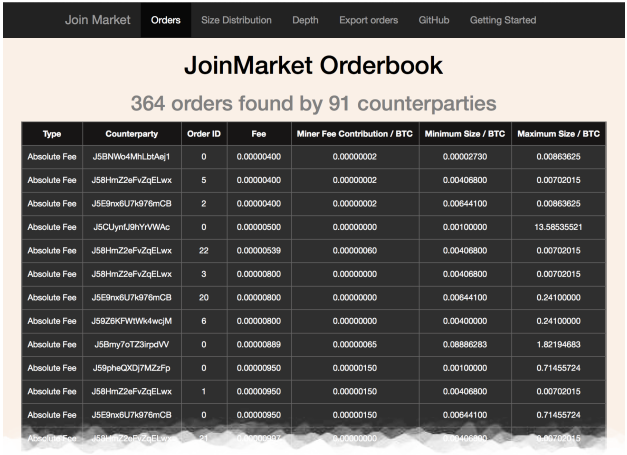
CoinJoin

Prinzip (unter Vernachlässigung von Transaktionsgebühren)



Maxwell, G. *CoinJoin: Bitcoin Privacy for the Real World*, 2013.

Partnersuche für CoinJoins



Join Market | Orders | Size Distribution | Depth | Export orders | GitHub | Getting Started

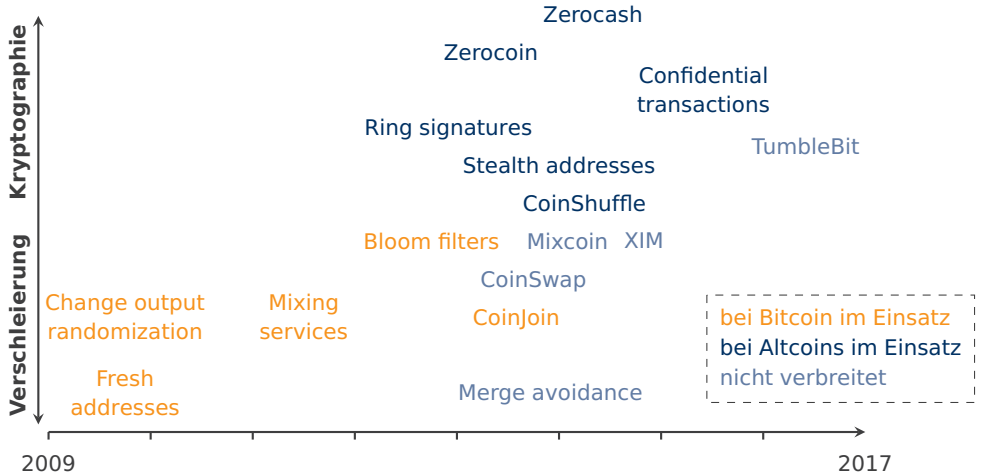
JoinMarket Orderbook

364 orders found by 91 counterparties

Type	Counterparty	Order ID	Fee	Miner Fee Contribution / BTC	Minimum Size / BTC	Maximum Size / BTC
Absolute Fee	J5BNWo4MhLbtAaj1	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	0.00644100	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	0.00644100	0.24100000
Absolute Fee	J59Z6KFWtWk4wcjM	6	0.00000800	0.00000000	0.00400000	0.24100000
Absolute Fee	J5Bmy7oTZ3irpdVV	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	0.00644100	0.71455724

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

Datenschutztechniken in Blockchain-Systemen



Narayanan, A., Möser, M., *Obfuscation in Bitcoin: Techniques and Politics*, 2017.

UTXO-Modell versus Kontenmodell

Jargon: TX = Transaction, TXO = Transaction Output, UTXO = Unspent TXO

UTXO-Modell

- „Rechnet in Transaktionen“, Münzanalogie
- Benötigt Wechselgeld
- Outputs gliedern Transaktionen in kleinere, fest definierte Einheiten.
- Client-Datenhaltung optimiert zur Bestimmung der Neuheit von Outputs, jedoch keine Salden
- Wert ergibt sich aus Rückverfolgbarkeit jeder Einheit zur Coinbase-Transaktion.
- Nicht fungibel

Bei Bitcoin im Einsatz.

Kontenmodell

- „Rechnet in Konten“, Giralgeldanalogie
- Kein Wechselgeld nötig
- Transaktionen ähneln Nachrichten mit Empfängern und Parametern.
- Client schreibt Systemzustand fort und prüft Salden.
- Zähler zur Bestimmung der Neuheit.
- Wert ergibt sich aus Korrektheit aller Zustandsübergänge.
- Fungibilität möglich

Bei Ethereum im Einsatz.

Literatur

Abramova, S. und Böhme, R. Perceived Benefit und Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study. In Proceedings of the Thirty Seventh International Conference on Information Systems (ICIS). Dublin, Ireland, 2016.

Anderson, R., Barton, C., Böhme, R., et al. Measuring the Changing Cost of Cybercrime. In Workshop on the Economics of Information Security (WEIS). Harvard University, Cambridge, MA, 2019.

Böhme, R., Christin, N., Edelman, B., und Moore, T. Bitcoin: Economics, Technology, und Governance. *Journal of Economic Perspectives*, 29, 2 (2015), 213–238.

Böhme, R., Grzywotz, J., Pesch, P., Rückert, C., und Safferling, C. Prävention von Straftaten mit Bitcoins und Alt-Coins: Handlungsempfehlung zur Regulierung virtueller Kryptowährungen. BITCRIME-Projekt, 2017.

Böhme, R. und Pesch, P. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. *Datenschutz und Datensicherheit*, 41, 8 (2017), 473–481.

Möser, M. und Böhme, R. The Price of Anonymity: Empirical Evidence from a Market for Bitcoin Anonymization. *Journal of Cybersecurity*, 3, 2 (2017), 127–135.

Möser, M., Böhme, R., und Breuker, D. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. In APWG eCrime Researchers Summit (ECRIME). San Francisco, CA, 2013, pp. 1–14.

Pesch, P. und Böhme, R. Datenschutz trotz öffentlicher Blockchain? Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten. *Datenschutz und Datensicherheit*, 41, 2 (2017), 93–98.

Riek, M. und Böhme, R. The Costs of Consumer-facing Cybercrime: An Empirical Exploration of Measurement Issues und Estimates. *Journal of Cybersecurity*, 4, 1 (2018).