BTC-ECHO
Bitcoin & Blockchain Pioneers

Monerujo


Cake Wallet

Monero-Adresse an: TelegramGruppe t.me/MoneroStuttgart

BTC-ECHO
Bitcoin & Blockchain Pioneers

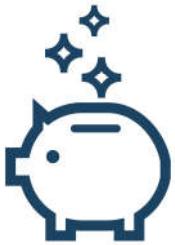
www.btc-echo.de

- **Tägliche Nachrichten** über Bitcoin und Blockchain-Technologie
- **BTC-ECHO Podcast** - Wöchentlicher Podcast
- **BTC-ECHO Newsletter** – Email Newsletter mit selektierten Artikeln
- **Kryptokompass** – monatlicher Investorenbrief
- **Social Media Posts** (Twitter, Instagram & Facebook)
- **Discord-Kanal**

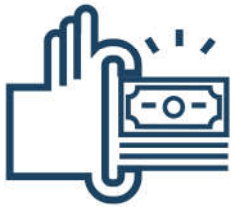
BTC-ECHO
Bitcoin & Blockchain Pioneers

Was ist eigentlich gutes Geld?

6 Eigenschaften von „gutem Geld“



Haltbar

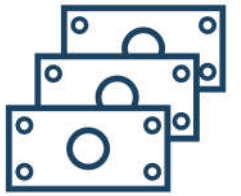


Übertragbar

Teilbar

Selten

Erkennbar

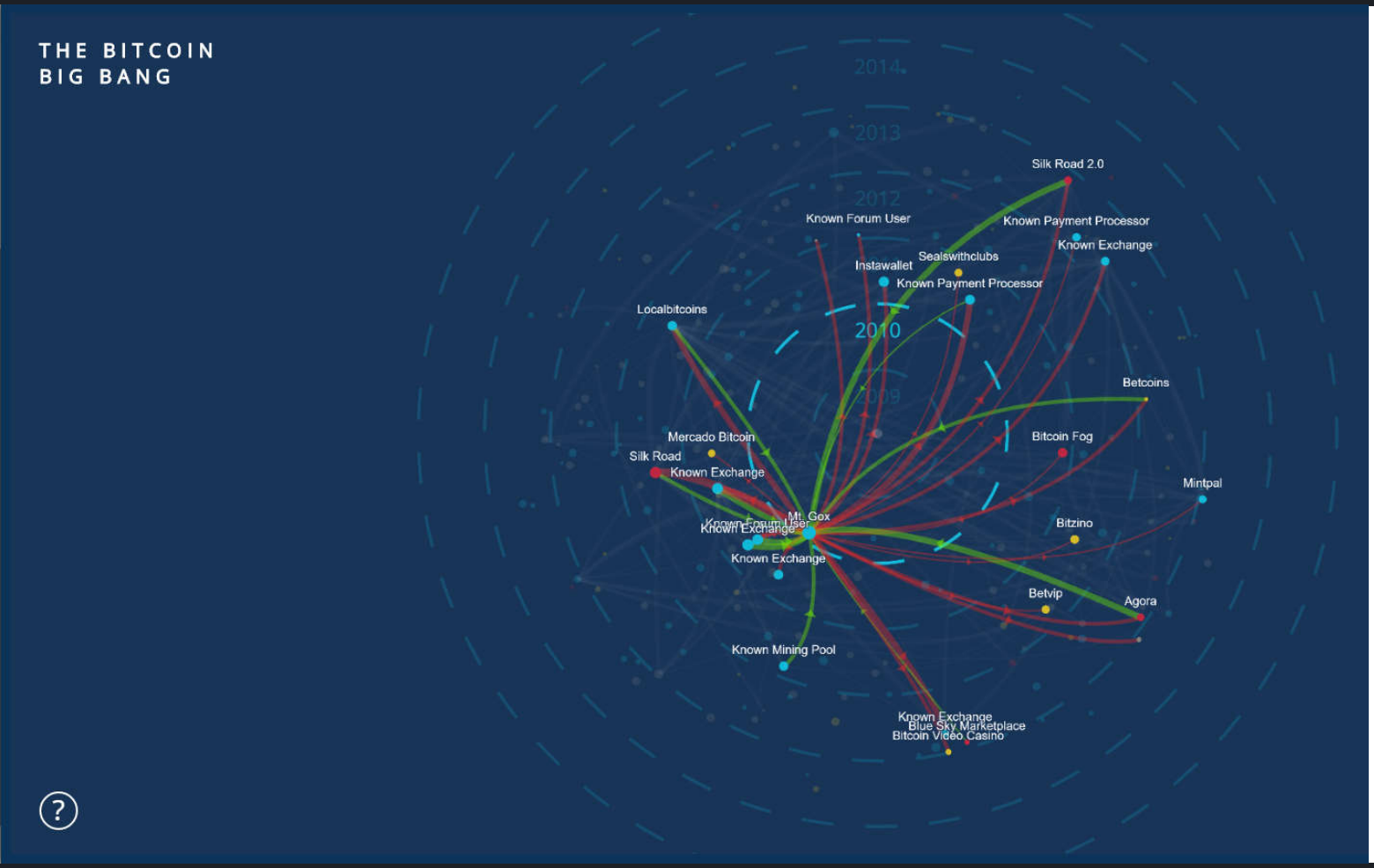


Fungibel

Bitcoin ist nicht privat, sondern transparent.

- Alle Transaktionen sind für immer in der Blockchain festgehalten
- Die Blockchain lässt sich analysieren und Schlüsse auf Identitäten können gezogen werden
- Bitcoins lassen sich voneinander unterscheiden

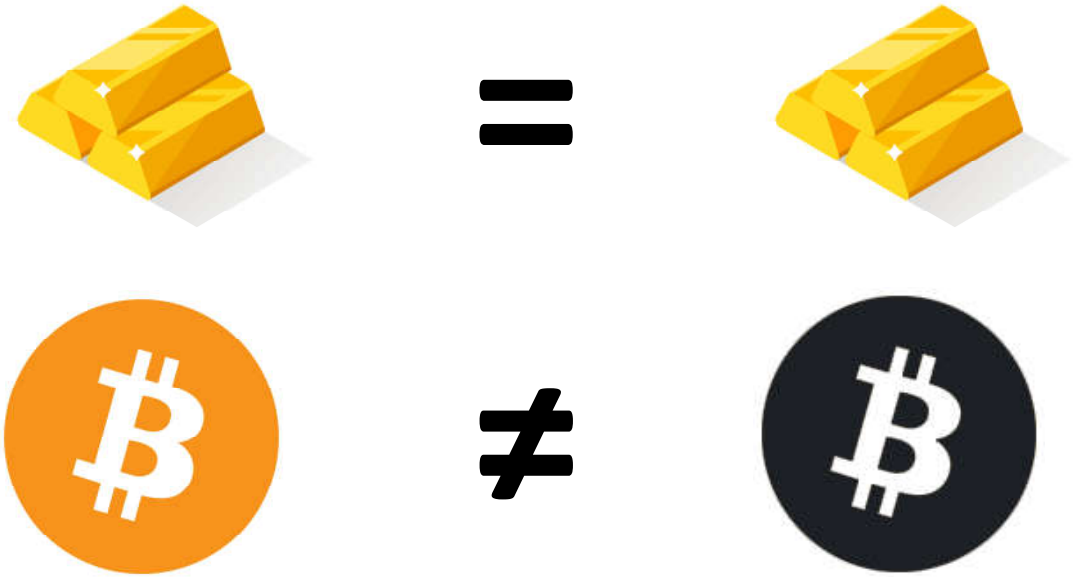
Bitcoin löste das Problem des Double-Spend,
ist allerdings **nicht fungibel**!



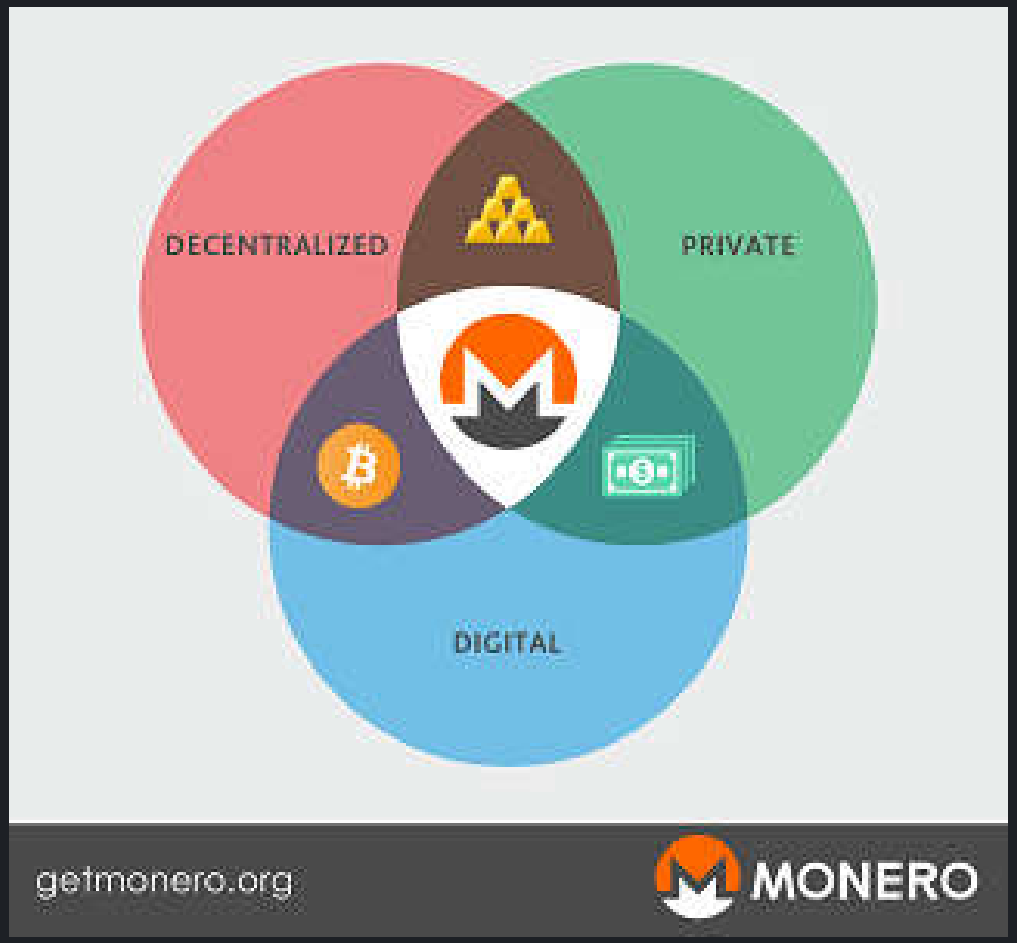
Öffentlich sind:

- Der Betrag einer Transaktion
- Die Herkunft der Bitcoin
- Wohin die Bitcoins gehen

Was ist Fungibilität?



BTC-ECHO
Bitcoin & Blockchain Pioneers



1 XMR = 1 XMR

Monero hat eine merkwürdige Geschichte.

- Das Cryptonote Paper von Nicolas van Saberhagen
- Bytecoin als erste Implementierung (aber mit 80 % Pre-mine)
- Bitmonero als fairer Launch des Bytecoin Codes am 18.4.2014
- Monero als Fork von Bitmonero durch 7 Stewards am 23.4.2014
- In 2016 standardmäßig Ringgröße
- In 2017 standardmäßig RingCT
- In 2018 standardmäßig Bulletproofs

Die 7 Monero Stewards

- Ricardo „fluffypony“ Spagni
- Francisco „ArticMine“ Cabanas
- binaryFate
- othe
- smooth
- luigi1111
- NoodleDoodle

Weitere Contributor

- Über **400 verschiedene Code Contributer** haben bereits mitgemacht
- 49 aktive Entwickler
- Community Management mit **Workgroups**
- **Monero Research Lab** (MRL) mit 2 Vollzeit Mathematikern

→Alle Contributor arbeiten ehrenamtlich oder durch das **Forum Funding System**

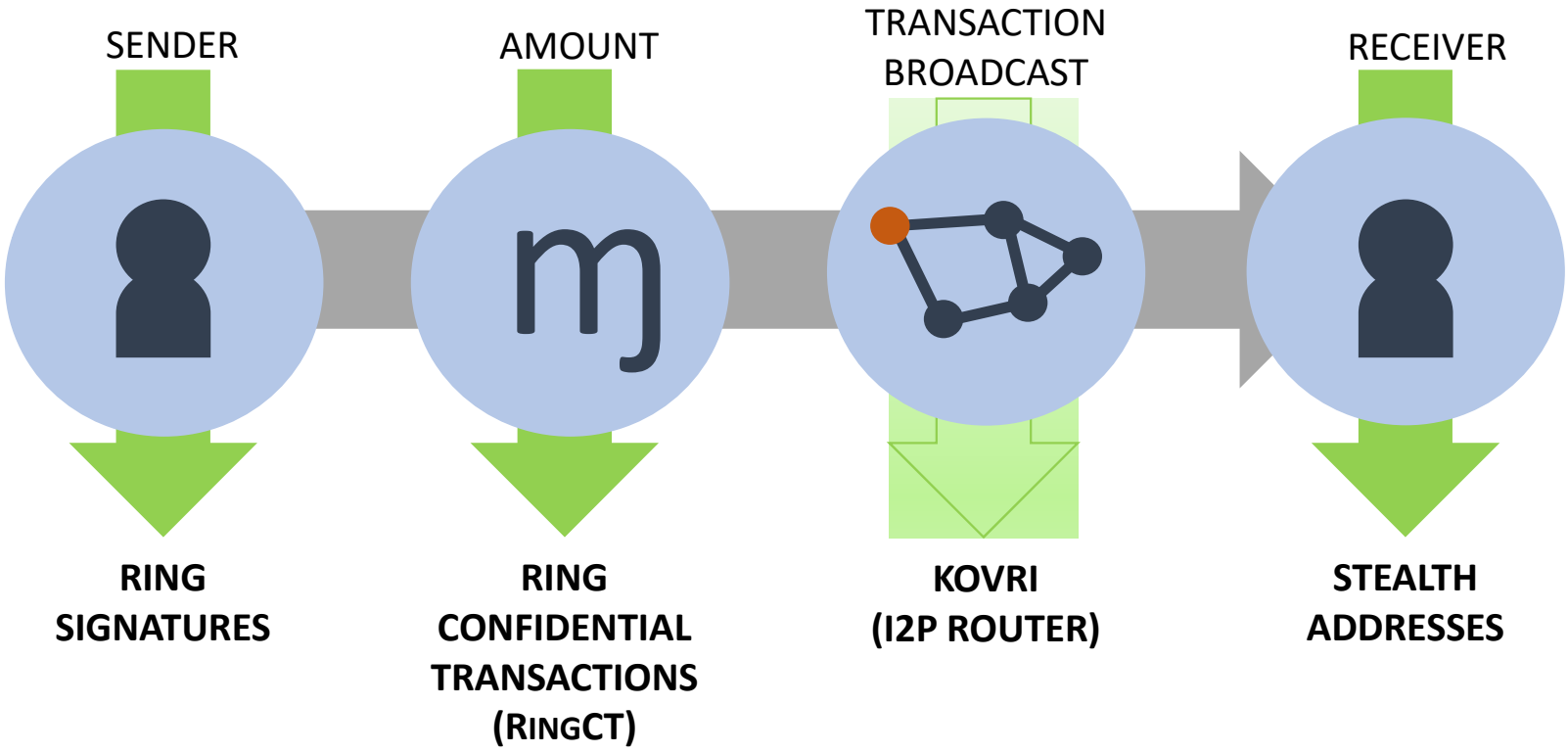
BTC-ECHO
Bitcoin & Blockchain Pioneers

Wie funktioniert Monero?

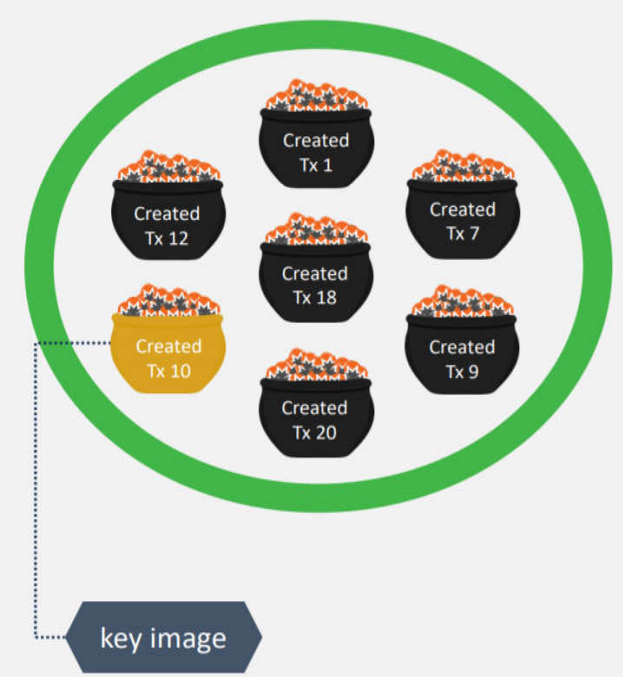
Monero (XMR) im Überblick

- Monero heißt „Münze“ auf Esperanto
- Dezentrales Open-Source-Projekt
- Proof-of-Work-basierte Blockchain mit CryptoNight
- Blockzeit: **2 Minuten**
- **Dynamische Blockgröße**
- Ab 18,4 Millionen XMR tritt **Tail Emission** ein mit **0,6 XMR per Block**
- Standardmäßige Privatsphäre für alle Transaktionen
- **4 Schlüssel**: Private & Public View Key // Private & Public Spend Key

Monero ist per standardmäßig privat.



Eine Ring Signatur versteckt den wahren Sender einer Transaktion.



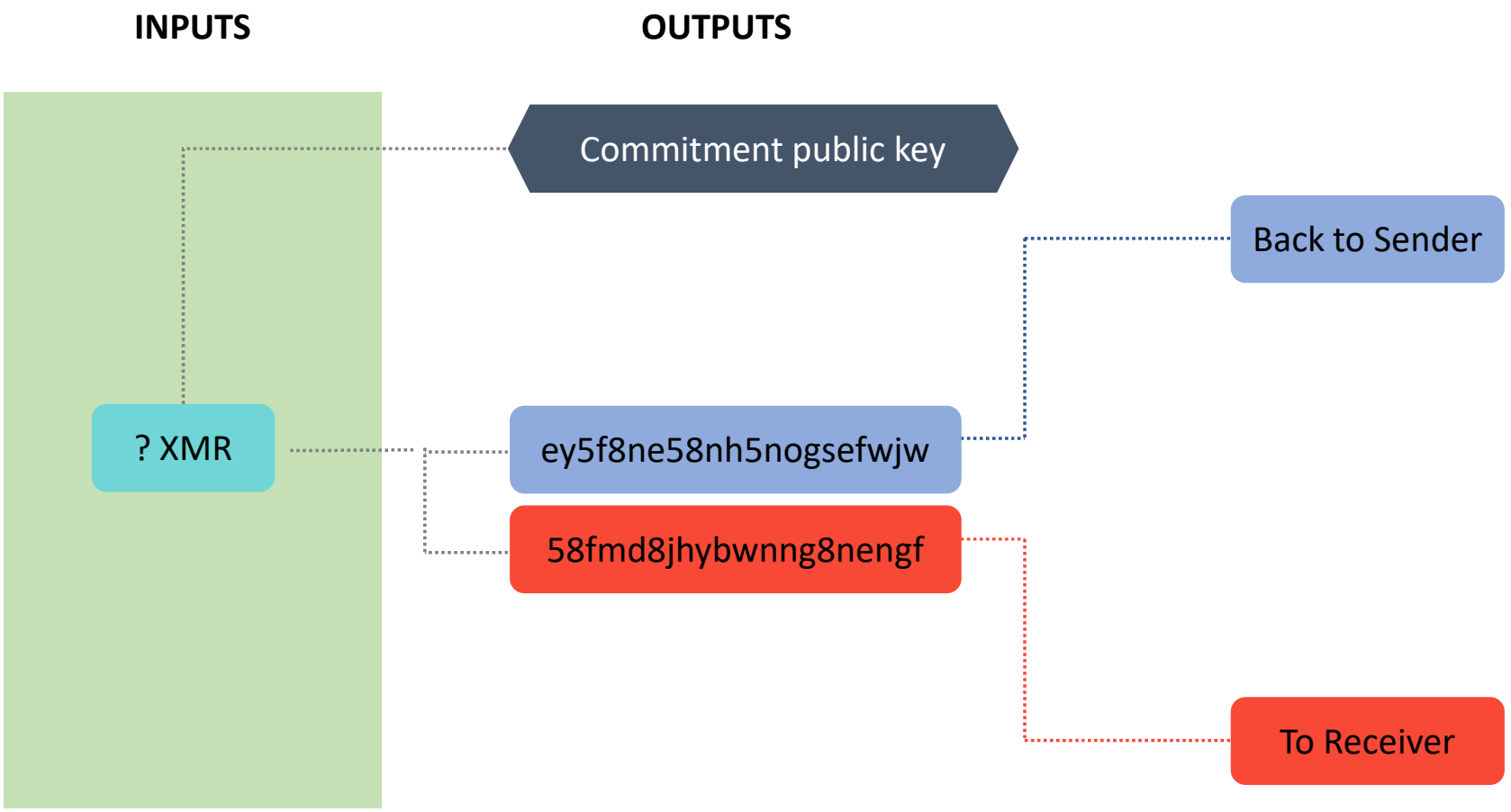
- Ein Sender nimmt sich andere Outputs auf der Blockchain als **Decoys**.
- Jeder Output in der Ring Signatur könnte der wahre Sender sein.
- Das **Key Image** beweist, dass der Output zum ersten mal ausgegeben wird.
- Aktuell hat Monero eine notwendige, feste **Ring Größe von 11**.

Stealth-Adressen verstecken den Empfänger.

- Zufällige One-Time-Adresse **`P = Hs(rA)G + B`**
- Enthält Bob‘s Public View Key und Public Spend Key

Where:
•P -- the final stealth address (one-time output key, the destination where funds will actually be sent);
•Hs* -- a hashing algorithm that returns a scalar (i.e., the hash output is interpreted as an integer and reduced modulo l);
•r -- the new random scalar Alice chose for this transaction;
•A -- Bob's public view key;
•G -- the standard Ed25519 base point;
•B -- Bob's public spend key.

→ **Nur Bob kann die Stealth-Adresse als seine eigene erkennen**

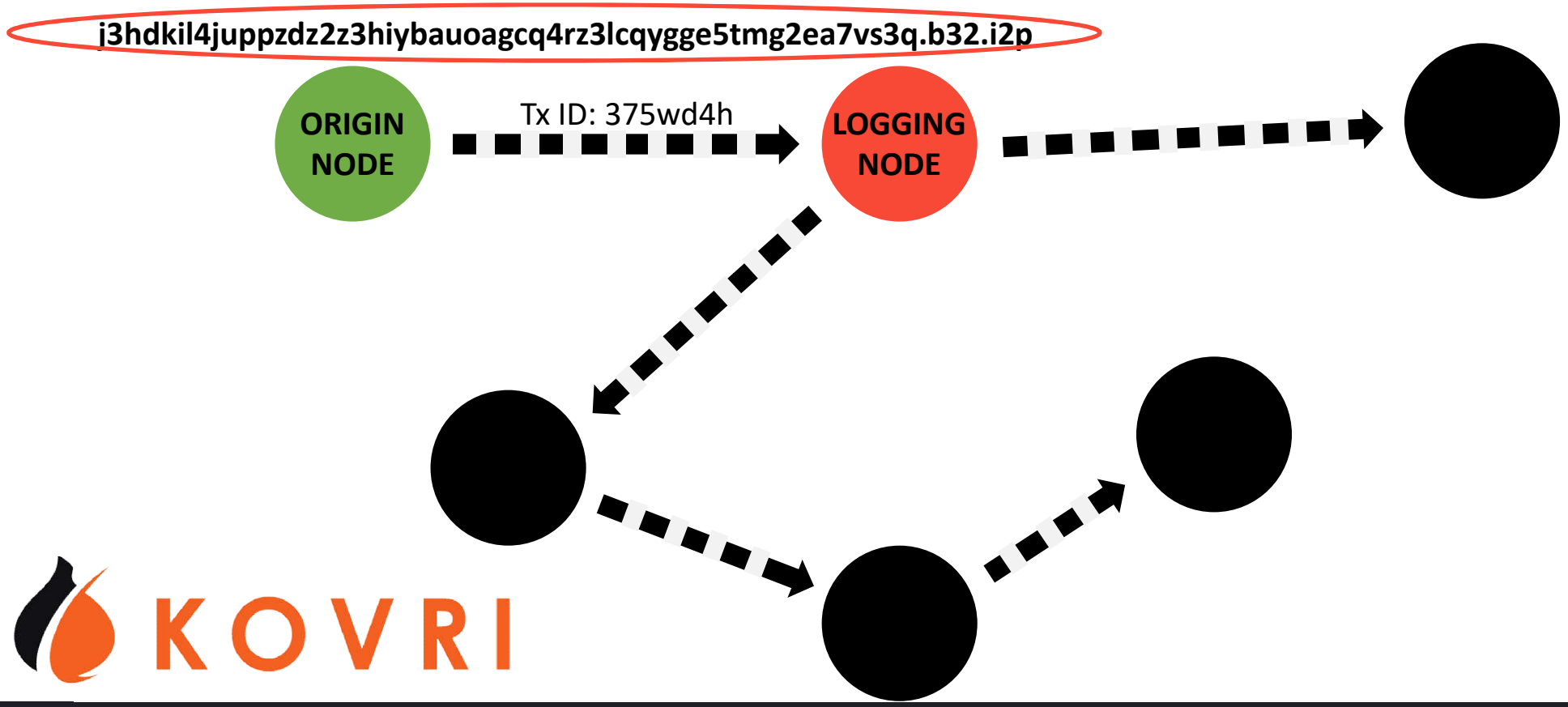

INPUTS
OUTPUTS
Commitment public key
Back to Sender
? XMR
ey5f8ne58nh5nogsefwjw
58fmd8jhybwnng8nengf
To Receiver

RingCT verstecken die Beträge einer Transaktion.

- Problem: Öffentliche Beträge erlauben Transaktionen zuzuordnen
- Kryptographischer Beweis, dass **Inputs = Outputs**
- Keine neuen Coins können generiert werden
- **Seit Mitte 2017 standardmäßig** bei allen Transaktionen (außer Coinbase)
- Range Proof verbrauchte viel Speicherplatz → **Bulletproofs**
- Bulletproofs **seit Oktober 2018 standardmäßig**

Soon™

- **Kovri** für die Verschleierung des Netzwerks
- Second Layer Scaling Solution (**Lightning Network**)
- **Tari** als merge-mined Sidechain für digital Assets


j3hdkil4juppzdz2z3hiybauoagcq4rz3lcqygge5tmg2ea7vs3q.b32.i2p
ORIGIN NODE
Tx ID: 375wd4h
LOGGING NODE
KOVRI

BTC-ECHO
Bitcoin & Blockchain Pioneers

GetMonero.org
t.me/MoneroStuttgart

BTC-ECHO
Bitcoin & Blockchain Pioneers

Wie sieht die Transaktion auf der Blockchain aus?

Local Monero und BISQ

- **LocalMonero.co** – Pendant zu LocalBitcoins, aber mit Sitz in Hong Kong

- **BISQ.network** – DEX für den Kauf/Verkauf von Kryptos
  - Bald XMR als Fiat-Paar?

Vergleich mit anderen Privacy Coins

Private	✓	✗	✗	✗	✗
Untraceable	✓	✗	?	✗	✗
Secure	✓	✓	✓	✓	✓
Fungible	✓	✗	✗	✗	✗
Decentralized	✓	✗	✗	✓	✓

Privatsphäre in Zcash

Fully-shielded

- Sending from one z-address to another z-address
- Sender, receiver, and amount hidden with zero-knowledge proofs
- <0.5% of transactions in the past month
- These theoretically provide greater untraceability than Monero

Partially-shielded

- Sending from one z-address to a t-address or vice versa
- Sender OR receiver hidden
- Amount visible
- <10% of transactions in the past month

X Transparent

- Sending from one t-address to another t-address
- Sender, receiver, and amount visible, just like Bitcoin
- >90% of transactions in the past month

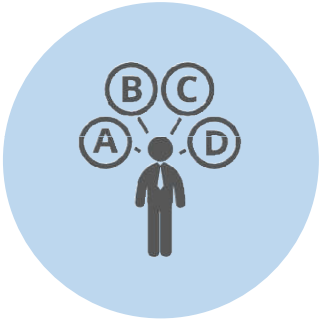
BTC-ECHO
Bitcoin & Blockchain Pioneers

Regulatorische Aspekte

Regulatorische Aspekte (Transparenz mit View Key)

Transparency

A view key is used to reveal all transactions for a Monero account, or just the key for a single transaction



Selected Parties

View keys can be given to selected parties, or can be made public

Charities

By publishing their view key, charities can invite easy public oversight

Parents

Children can be given their own accounts, and parents can monitor their spending

Monero ist anonymes Geld im Internet.

- Sender, Empfänger und Betrag sind verschleiert.
- Bald ist auch der Netzwerkverkehr verschleiert.
- Transaktionen können nicht zensiert werden.
- Die Geldmenge kann nicht willkürlich angehoben werden.
- Staaten können diese Technologie nicht abschalten.

Mehr Monero Ressourcen:

- **Offizielle Website**: https://getmonero.org
- **GitHub**: https://github.com/monero-project/monero
- **Reddit**: https://reddit.com/r/monero
- **StackExchange**: https://monero.stackexchange.com
- **Podcasts**: https://moneromumble.de
- **Telegram Gruppen**: @MoneroGer // @Monero // @Bitmonero

Vielen Dank für Eure Aufmerksamkeit!

https://de.linkedin.com/in/alextroos

https://btc-echo.de/author/alexander-roos

@AlexAnarcho

alexander.roos@btc-echo.de