Anonymität von Bitcoin Transaktionen

Analyse von Bitcoin Mixern

Westfälische
Wilhelms-Universität
Münster

Malte Möser

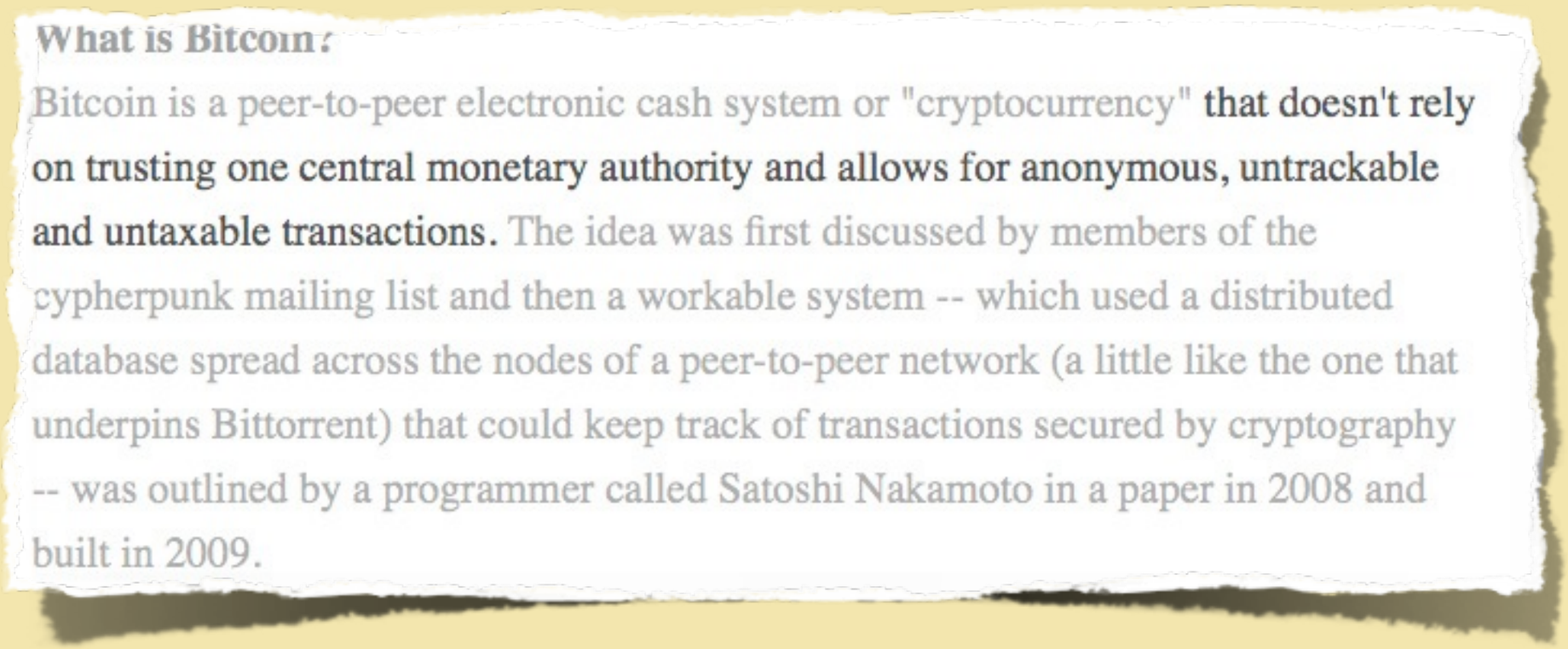
MBC'13 Münster Bitcoin Conference

AGENDA

1. Wie anonym ist Bitcoin?
2. Bitcoin Grundlagen
3. Bitcoin Mixer
4. Analyse
5. Fazit

1 WIE ANONYM IST BITCOIN?

https://twitter.com/wikileaks/status/80774521350668288



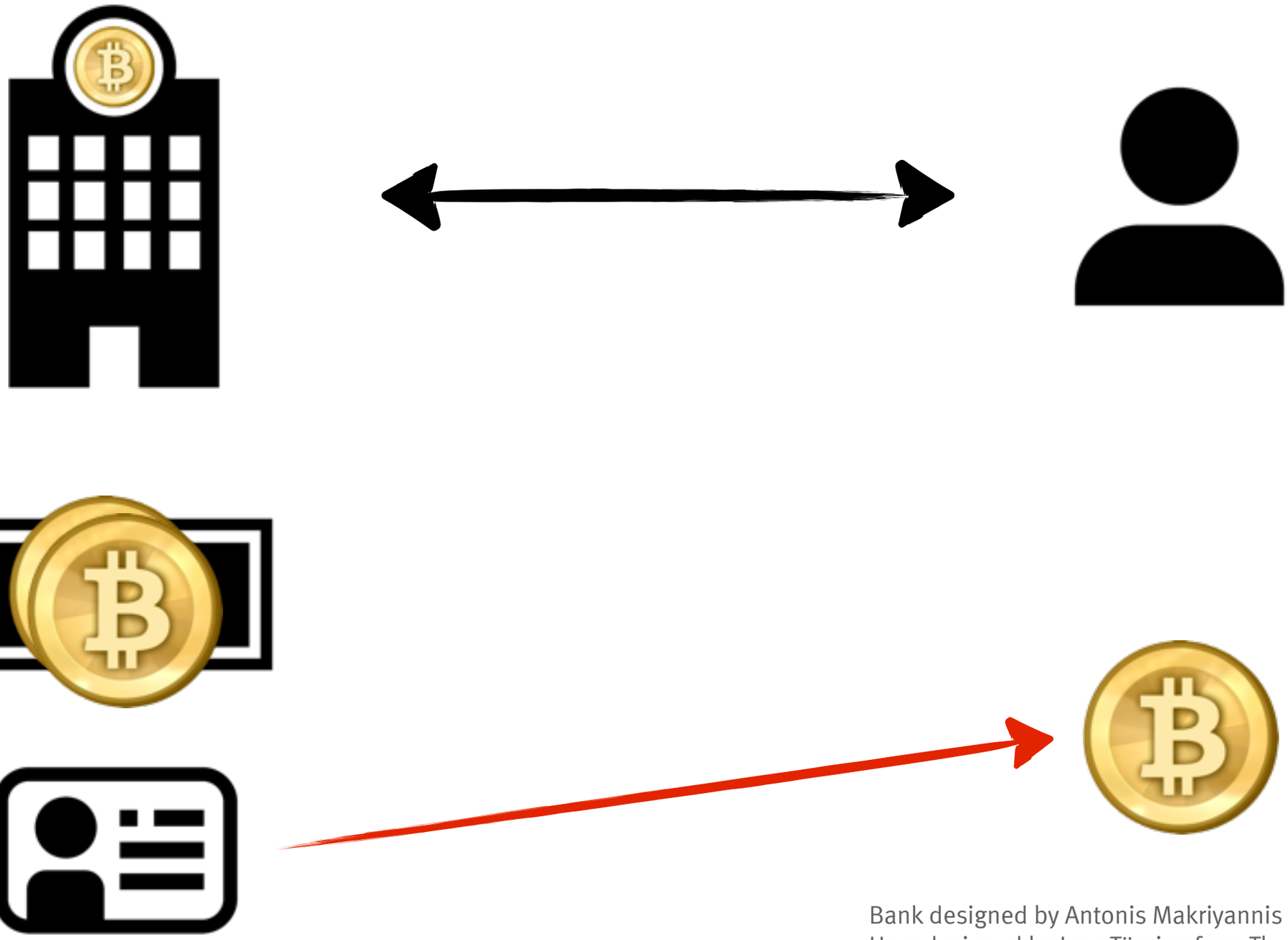
http://www.wired.co.uk/news/archive/2013-05/7/bitcoin-101

Damit ist Bitcoin.de der erste Bitcoin-Handelsplatz Europas mit einer direkten Bankenkooperation und orientiert sich an den Finanzmarkt-Vorschriften wie z. B. dem Geldwäschegesetz.

Pressemitteilung 10.07.2013: Bitcoin.de und Fidor Bank AG vereinbaren weitgehende Partnerschaft

https://blog.bitcoin.de/bitcoin-de-und-fidor-bank-ag-vereinbaren-weitgehende-partnerschaft

BITCOINS KAUFEN



Bank designed by Antonis Makriyannis from The Noun Project
User designed by Jens Tärning from The Noun Project
Dollar designed by Christopher Beach from The Noun Project
Identification designed by Rémy Médard from The Noun Project

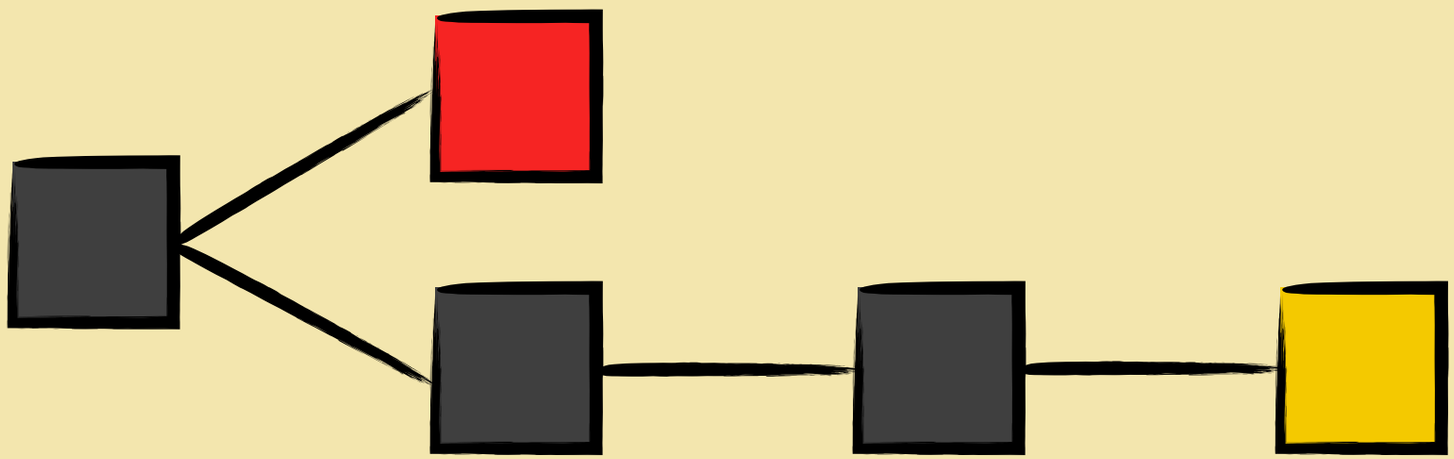
2

BITCOIN GRUNDLAGEN

Account-IDs sind öffentliche Schlüssel

Digitale Signaturen verhindern unrechtmäßigen Zugriff

Alle Transaktionen sind öffentlich in der block chain gespeichert



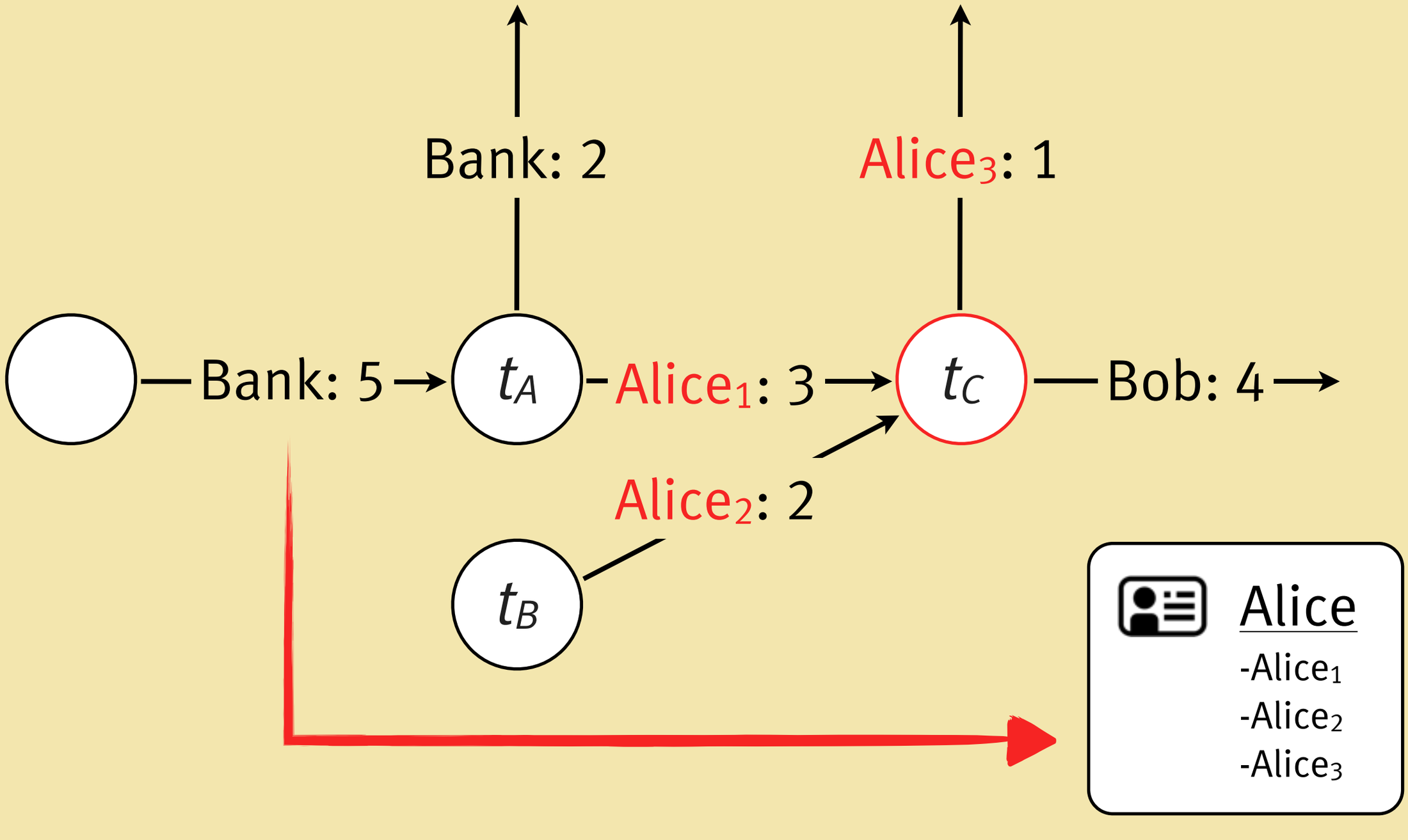
Eine Transaktion besteht aus Listen von Inputs und Outputs

Transaktionen

Adressen

Der Wert einer Transaktion muss vollständig verbraucht werden

TRANSAKTIONSGRAPH

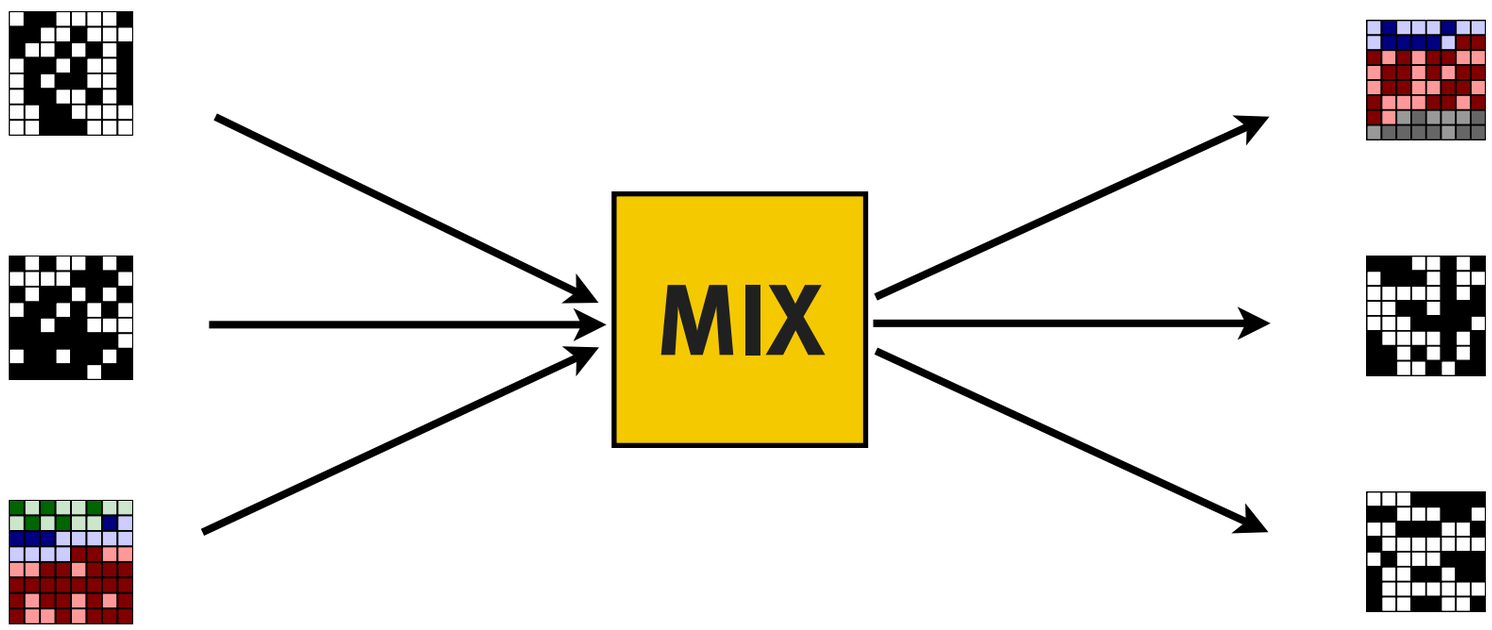


3 BITCOIN MIXER

Ziel: Beziehung zwischen Sender und Empfänger anonymisieren

CHAUM‘S MIX

anonymisiert Beziehung zwischen Sender und Empfänger in Kommunikationsnetzwerken



$c_M\ (z_1,\ c_A(z_0,\ m),\ A) \rightarrow c_A(z_0,\ m),\ A$

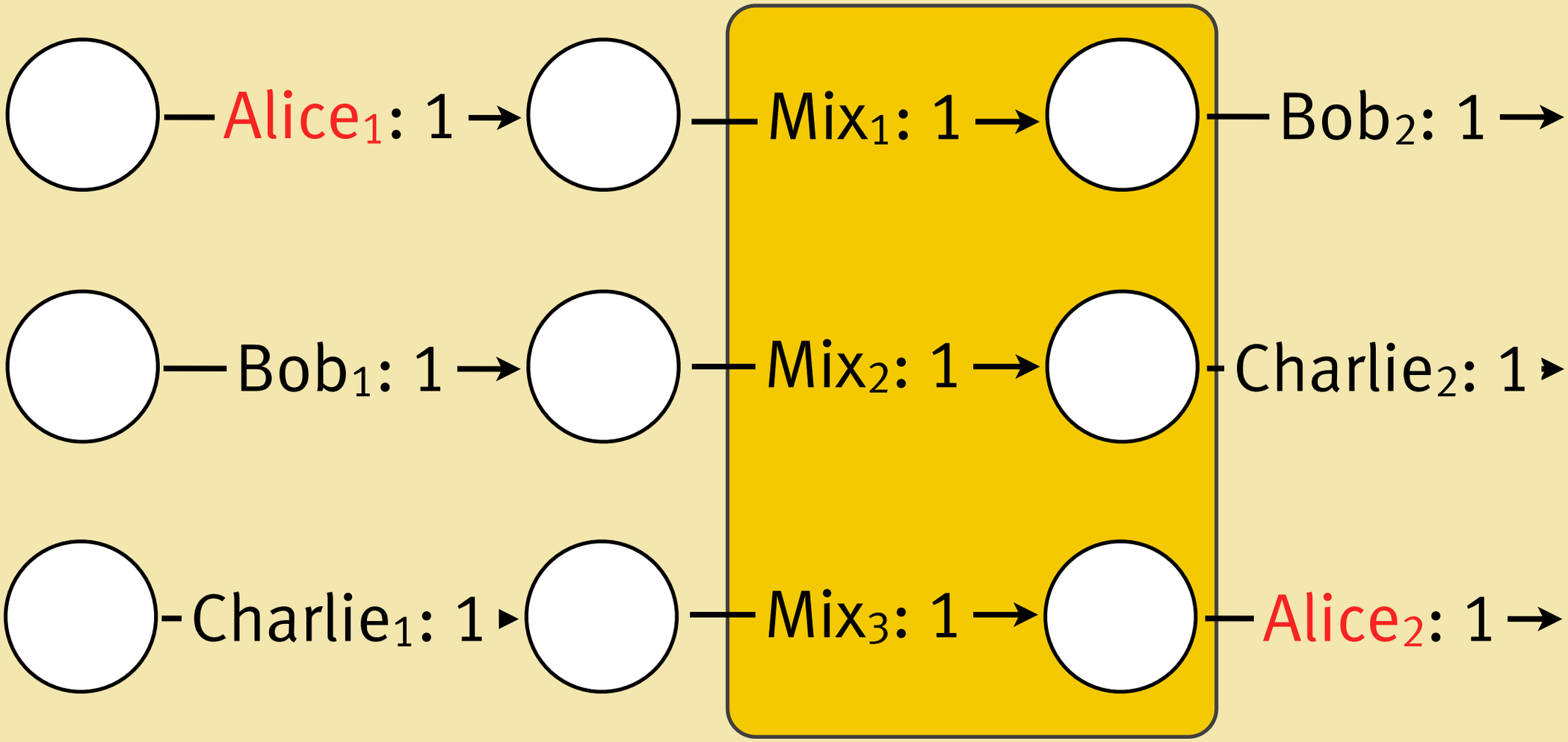
Chaum 1981, Grafik in Anlehnung an Böhme

PROBLEM

- Transaktionen können nicht verschlüsselt werden
- Herkunft einer Transaktion muss immer bekannt sein

Alle Bitcoins haben (theoretisch) den gleichen Wert

BITCOIN MIXER



ANGRIFFSPOTENZIALE

2013-07-12
08:45
1.337 BTC

2013-07-12
09:46
1.337 BTC

ANGRIFFSPOTENZIALE

2013-07-12
08:45
1.337 BTC

2013-07-12
09:46
1.2 BTC

- Auszahlungsgröße verändern

ANGRIFFSPOTENZIALE

2013-07-12
08:45
1.337 BTC

2013-07-12
09:46
0.5 BTC

2013-07-12
09:46
0.7 BTC

- Auszahlungsgröße verändern
- über mehrere Transaktionen verteilen

ANGRIFFSPOTENZIALE

2013-07-12
08:45
1.337 BTC

2013-07-12
11:42
0.5 BTC

2013-07-13
01:10
0.7 BTC

- Auszahlungsgröße verändern
- über mehrere Transaktionen verteilen
- über einen längeren Zeitraum verteilen

ungelöstes Problem:

der Bitcoin Mixer

könnte der Angreifer

sein

4 ANALYSE

ANSATZ

Funktionsweise?

Einzahlung → Bitcoin Mixer → Auszahlung

Direkte Verbindungen?

VORGEHEN

1. Transaktionen erstellen
2. Daten von Blockchain.info abrufen
3. Transaktionsgraphen erstellen
4. Direkte Verbindungen suchen
5. Taint Analyse[1] nutzen
6. Graph mit Gephi visualisieren

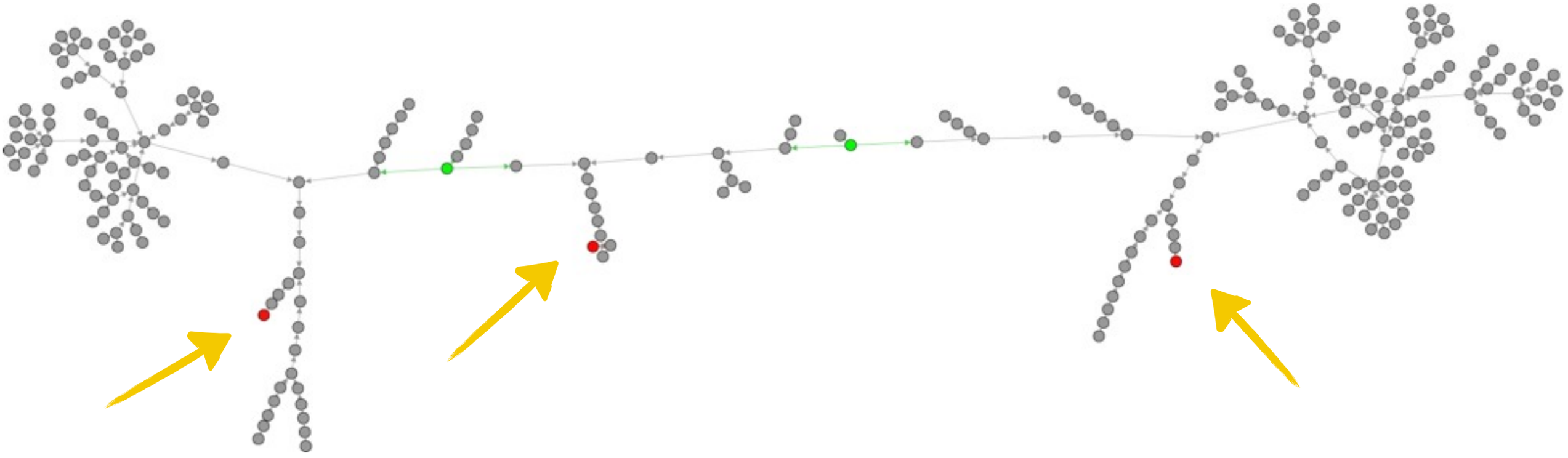
[1] https://blockchain.info/taint/_ADRESSE_

AUSGEWÄHLTE BITCOIN MIXER

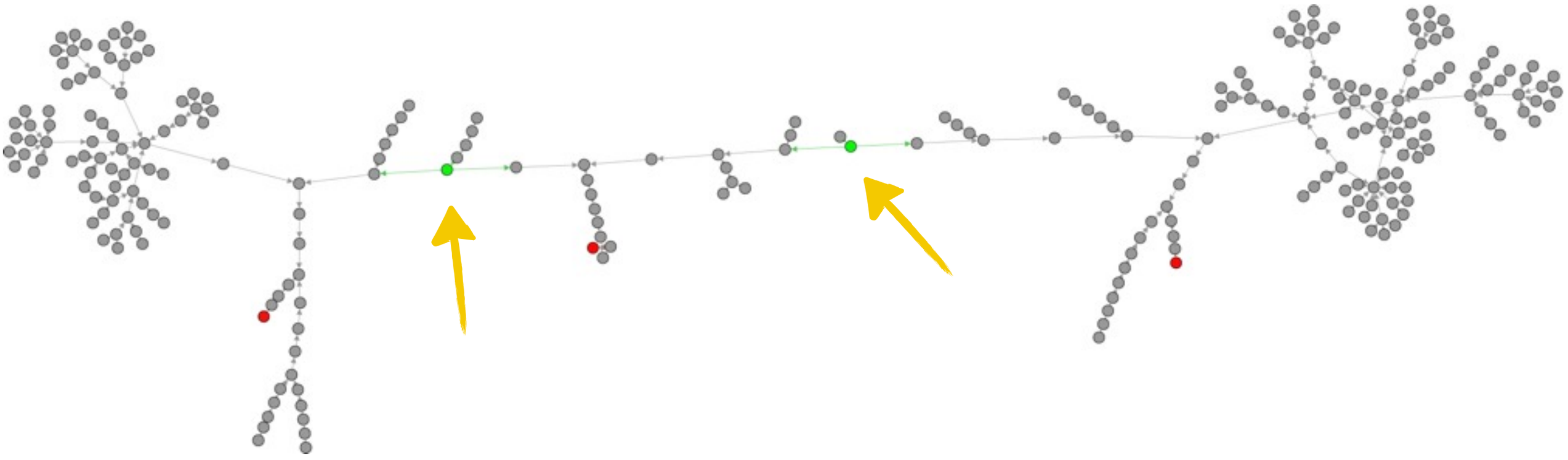
	Blockchain.info	Bitcoin Fog	BitLaundry
Gebühr	0.5 %	1–3%	2.49% + 0.00249 pro Tx
Min. Größe	0.2 BTC	0.2 BTC	0.25 BTC

BLOCKCHAIN.INFO

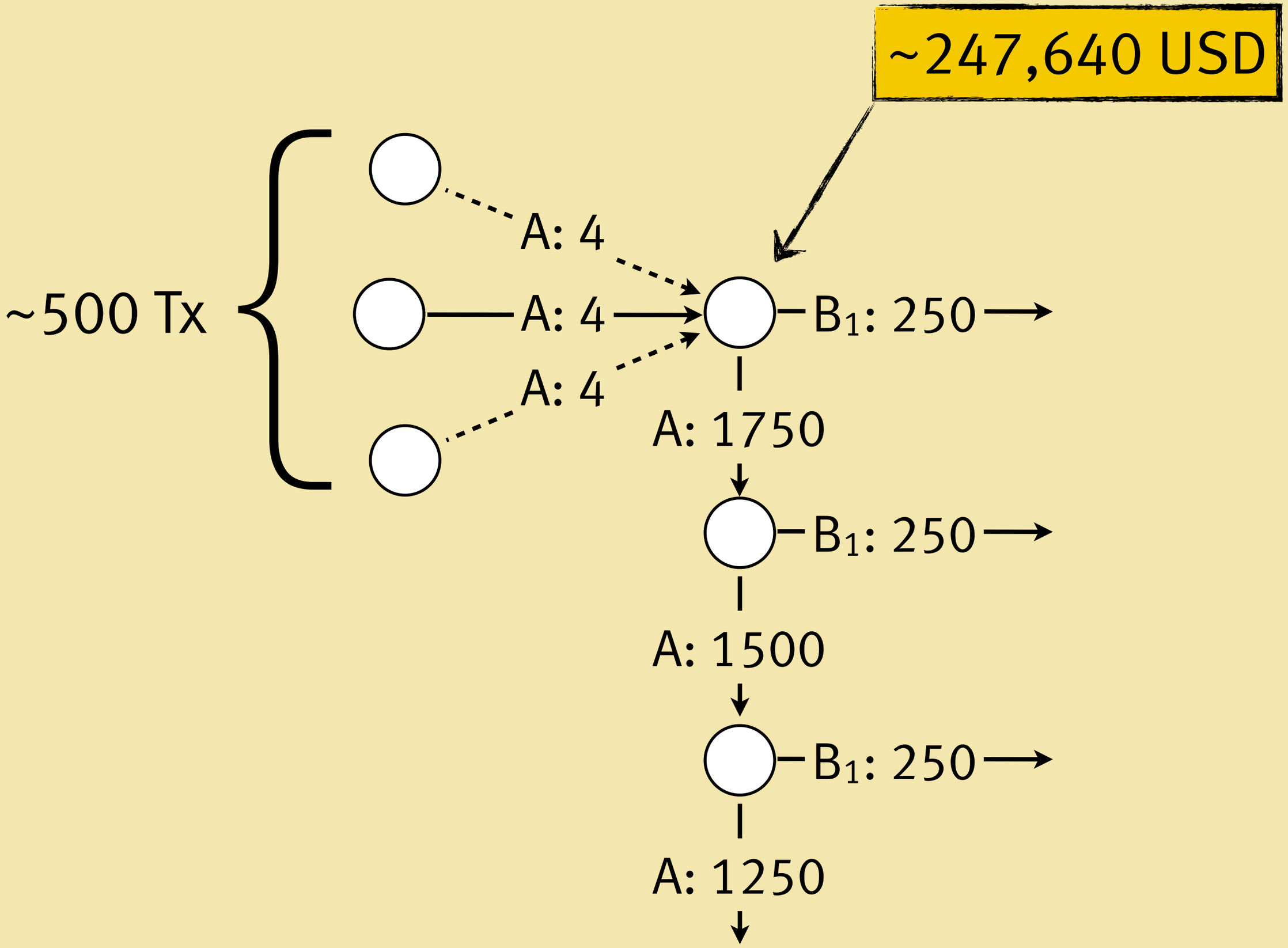
- 12 Transaktionen
- keine direkte Verbindungen
- 8 Graphen → Zusammenhänge



Auszahlungen



Transaktionen, die in mehrere Auszahlungen eingehen

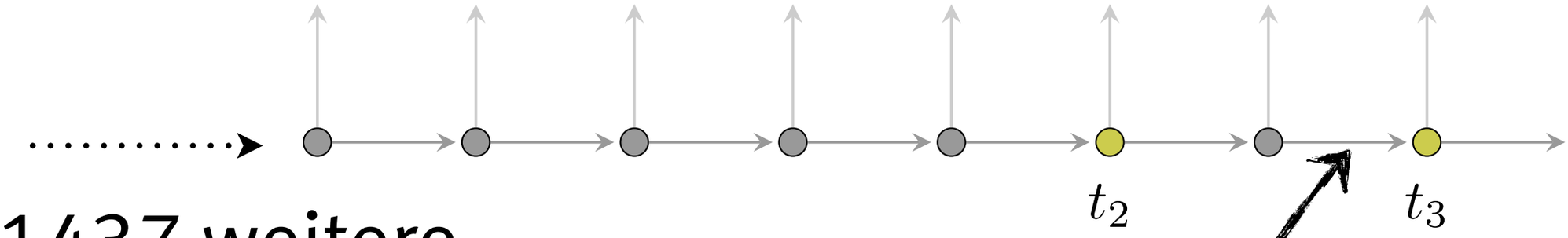

~247,640 USD
~500 Tx
A: 4
A: 4
A: 4
B1: 250
A: 1750
B1: 250
A: 1500
B1: 250
A: 1250

BITCOIN FOG

- 2 Experimente
- Einzahlungen bleiben (Monate lang) unberührt
  → keine direkten Verbindungen

AUSZAHLUNGSKETTEN

Auszahlungen

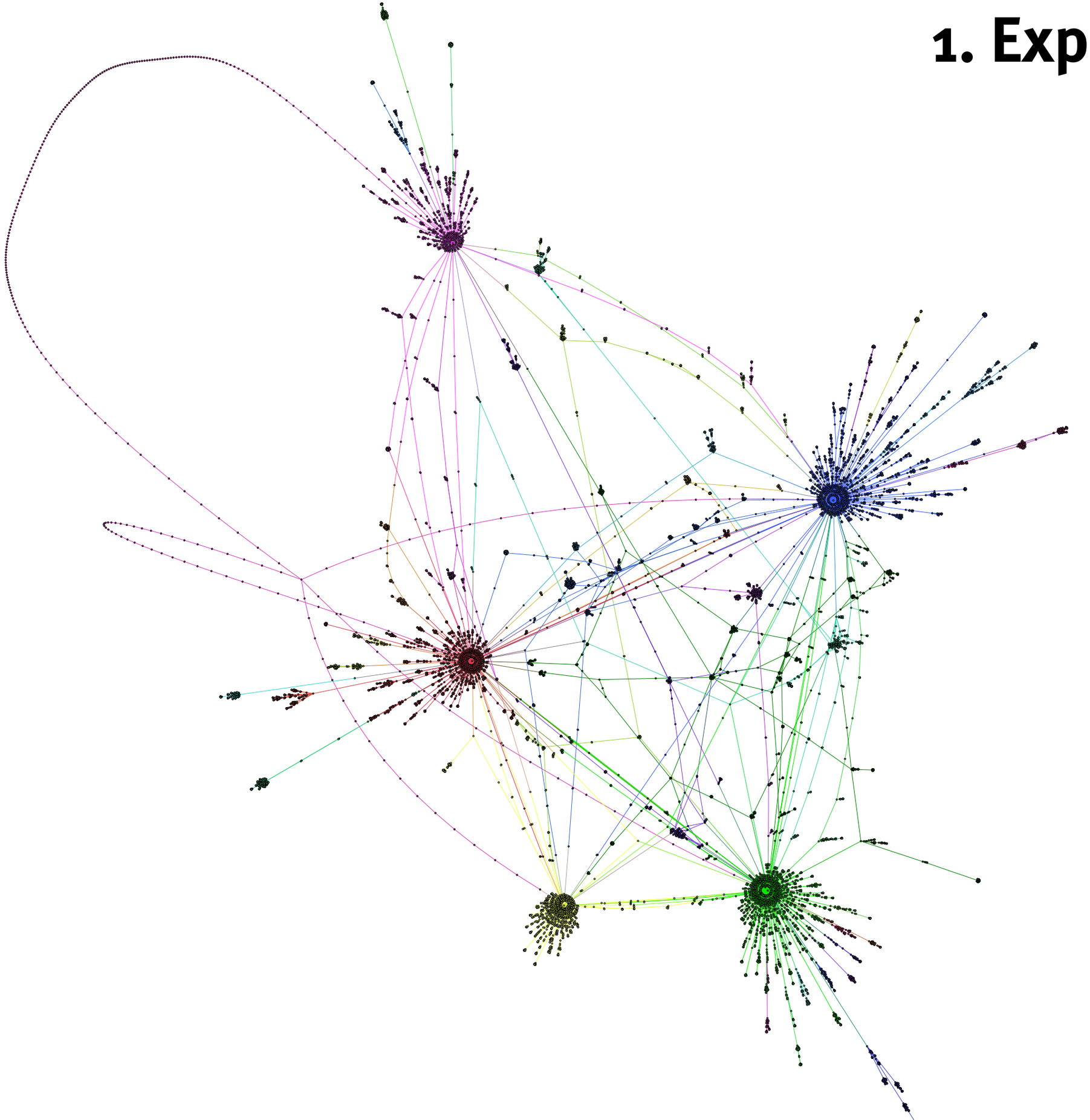


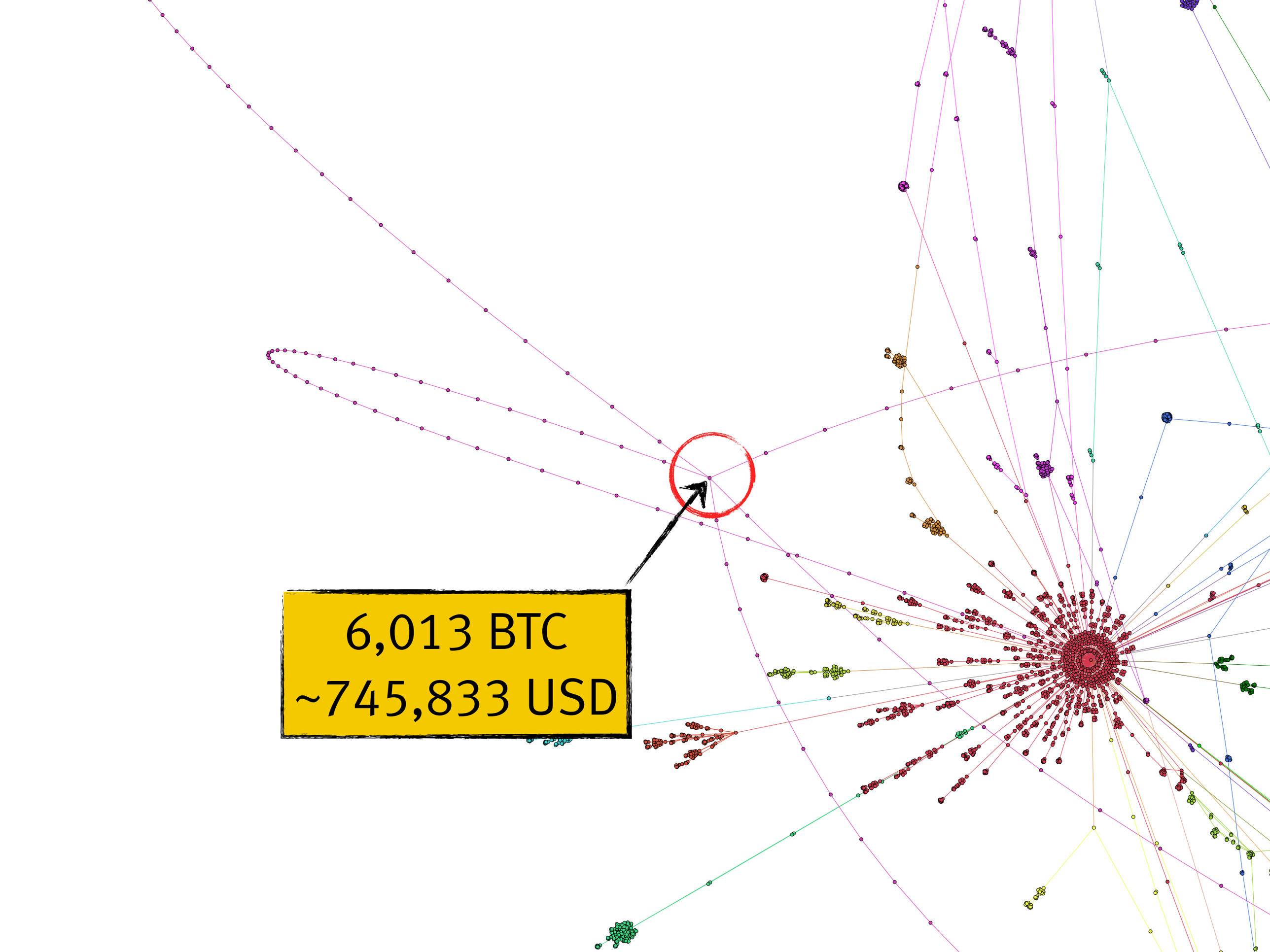
1437 weitere Transaktionen

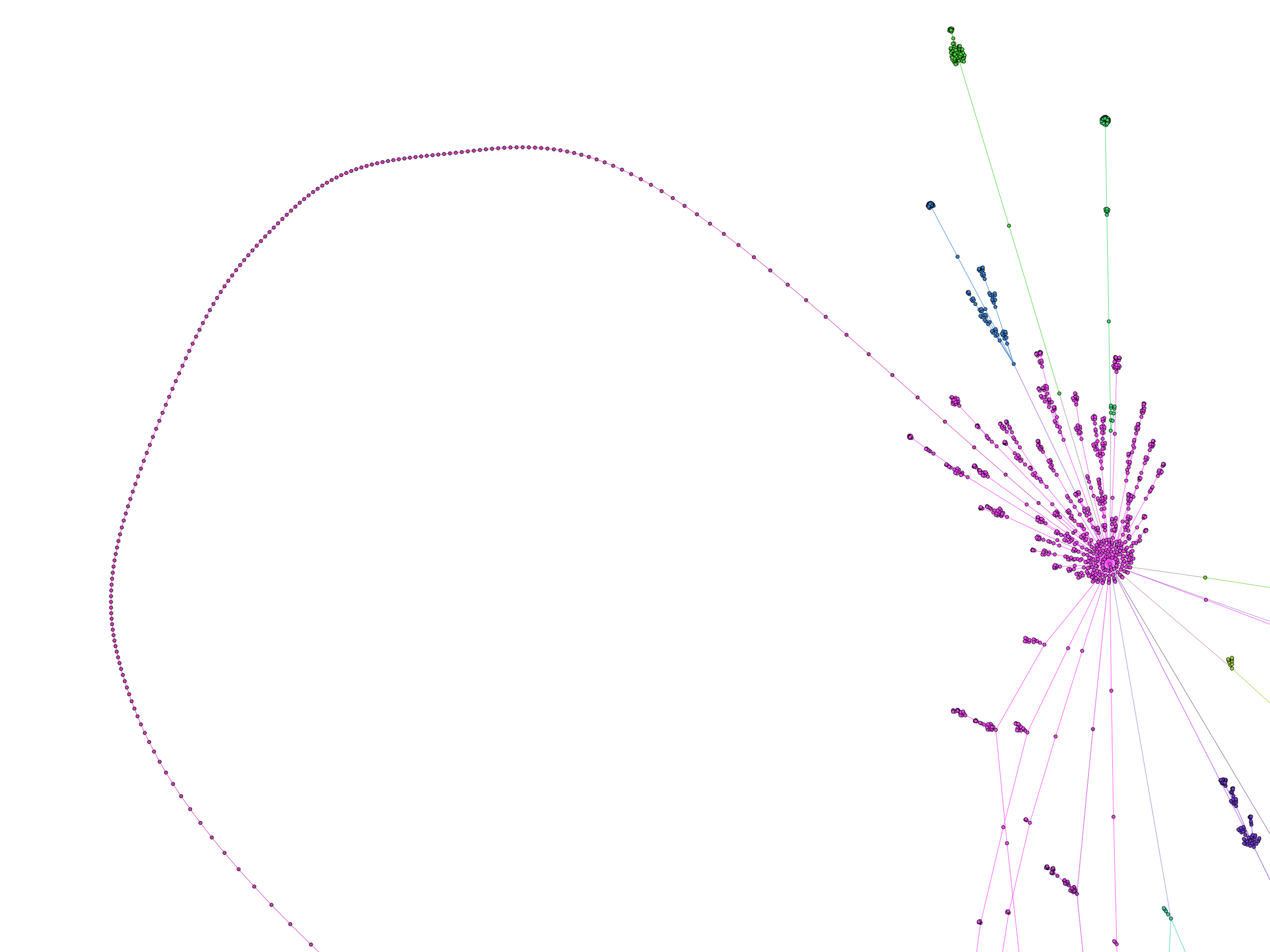
474 BTC
~66,298 USD

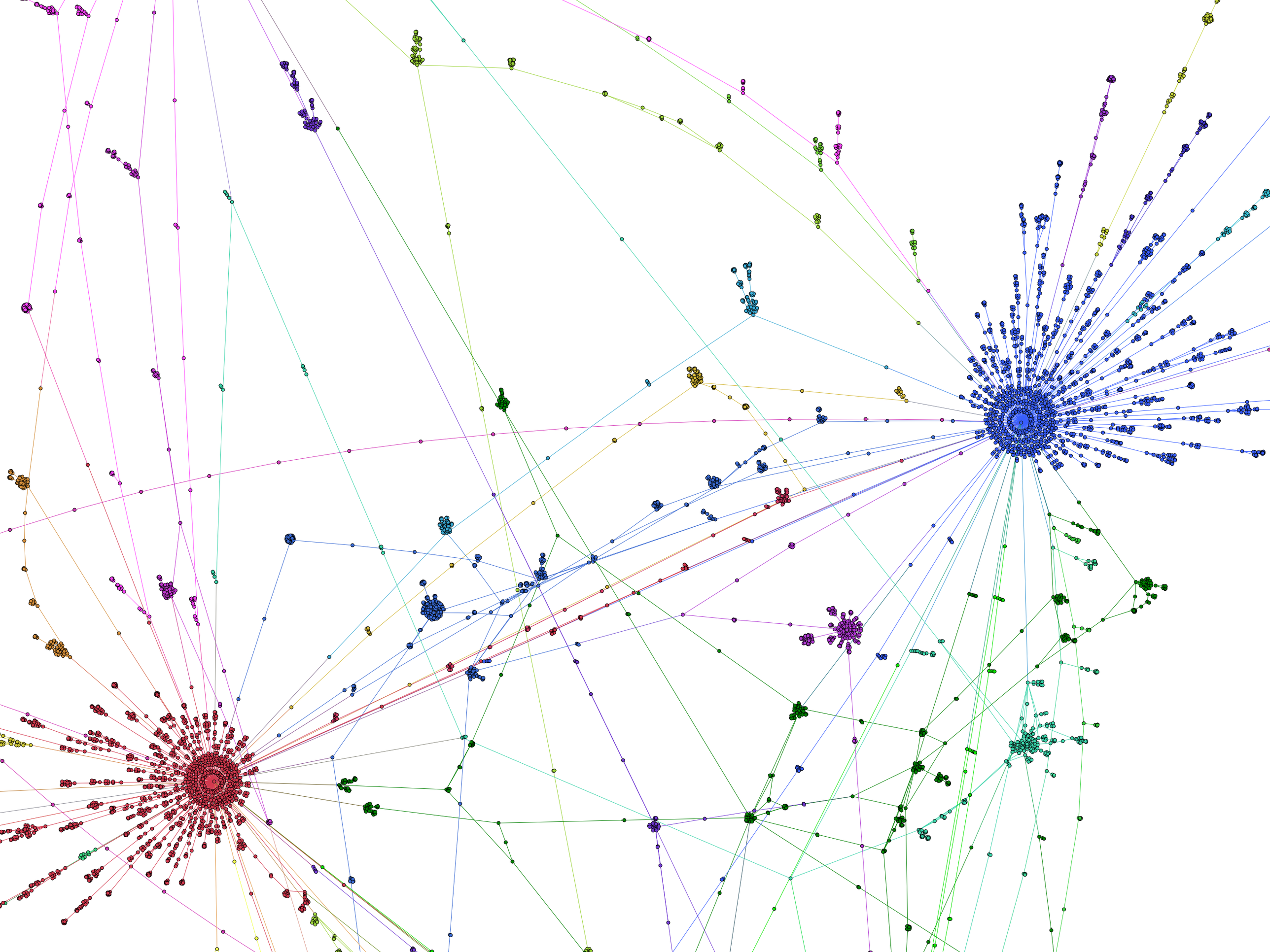
„Wechselgeld“

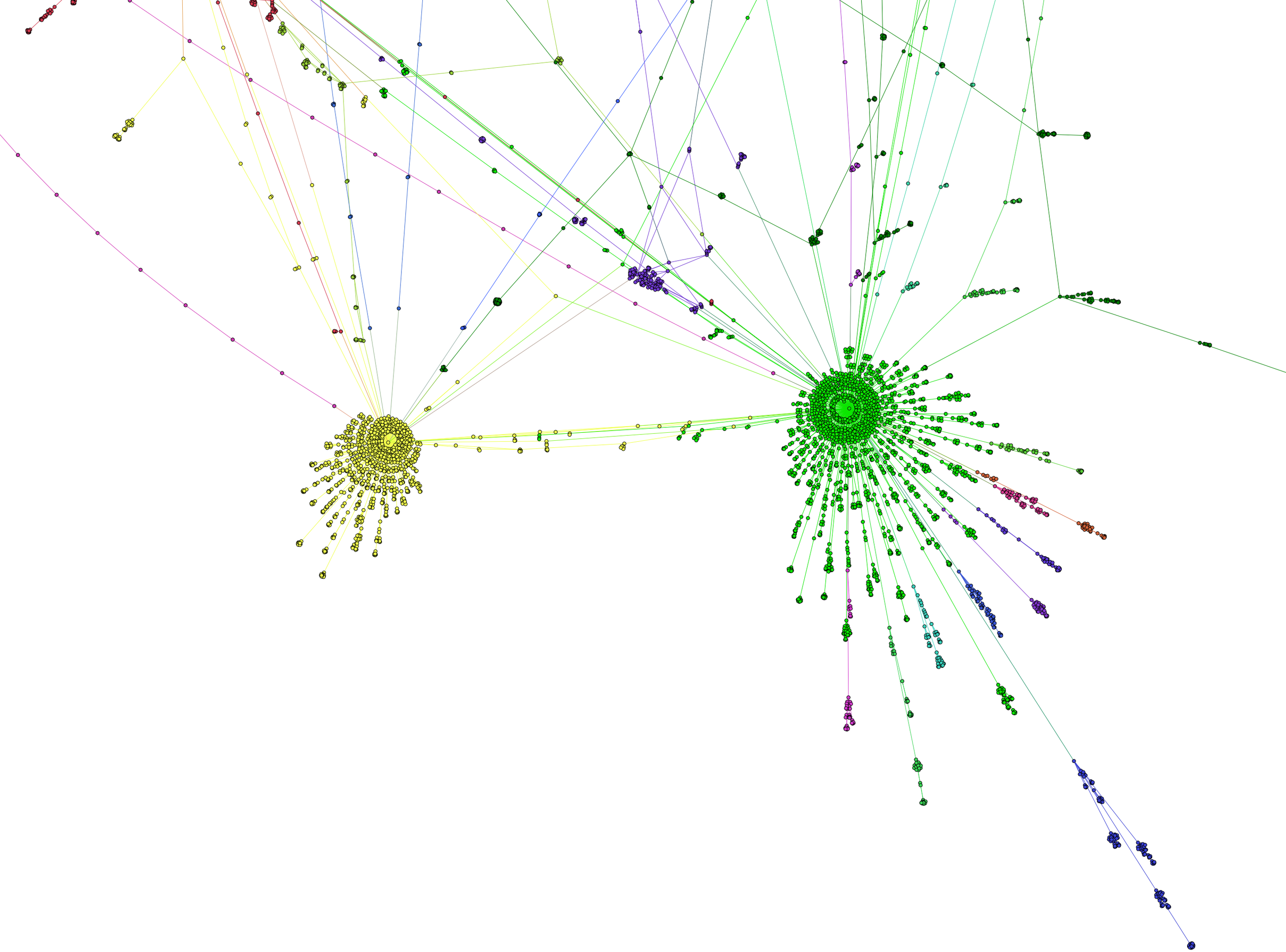
1. Experiment



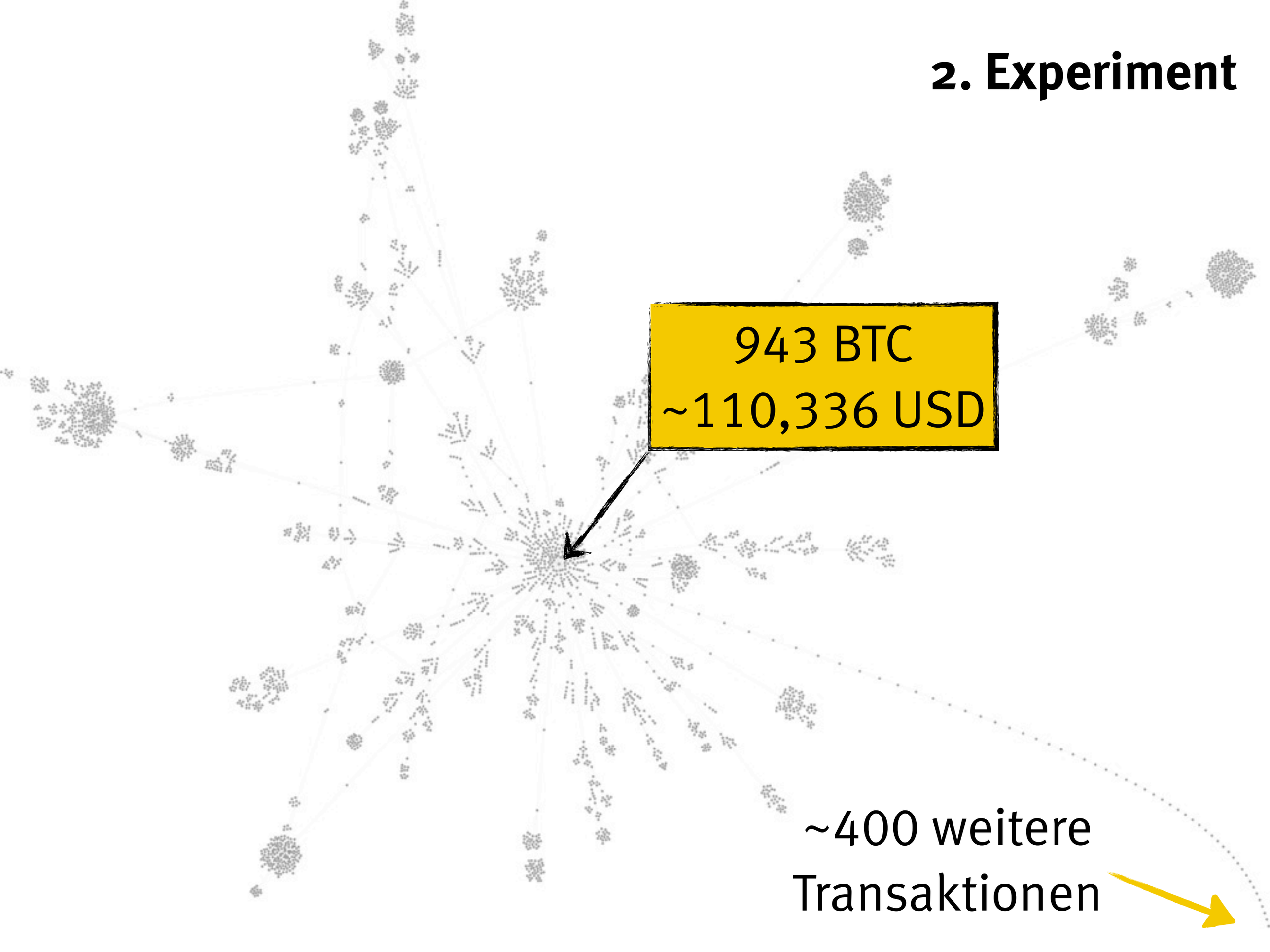

6,013 BTC
~745,833 USD



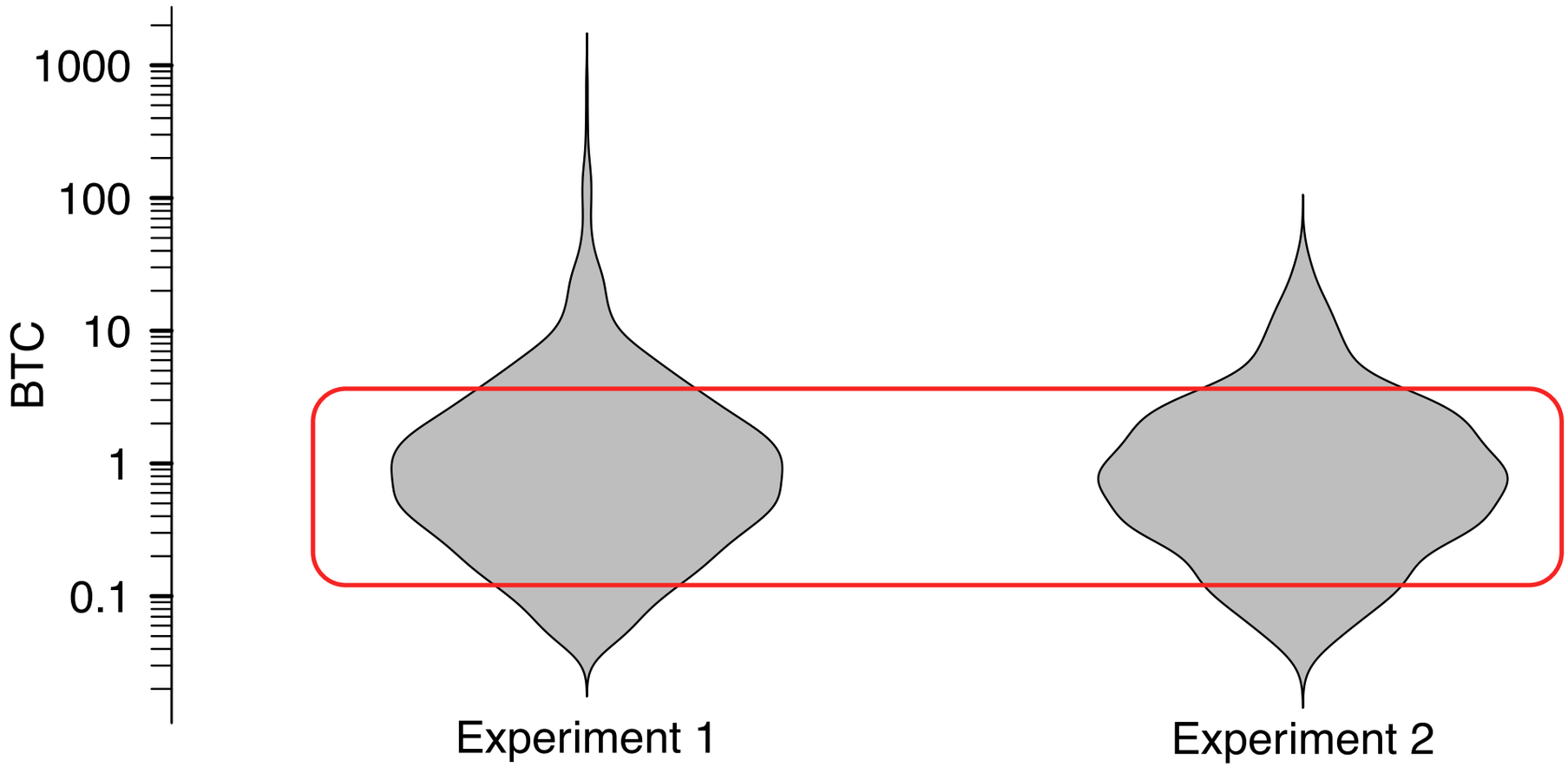




2. Experiment



AUSZAHLUNGSGRÖSSEN



$\tilde{x} = 0.8$

$\bar{x} = 3.83$

$\sigma = 24.5$

$\tilde{x} = 0.745$

$\bar{x} = 1.89$

$\sigma = 3.72$

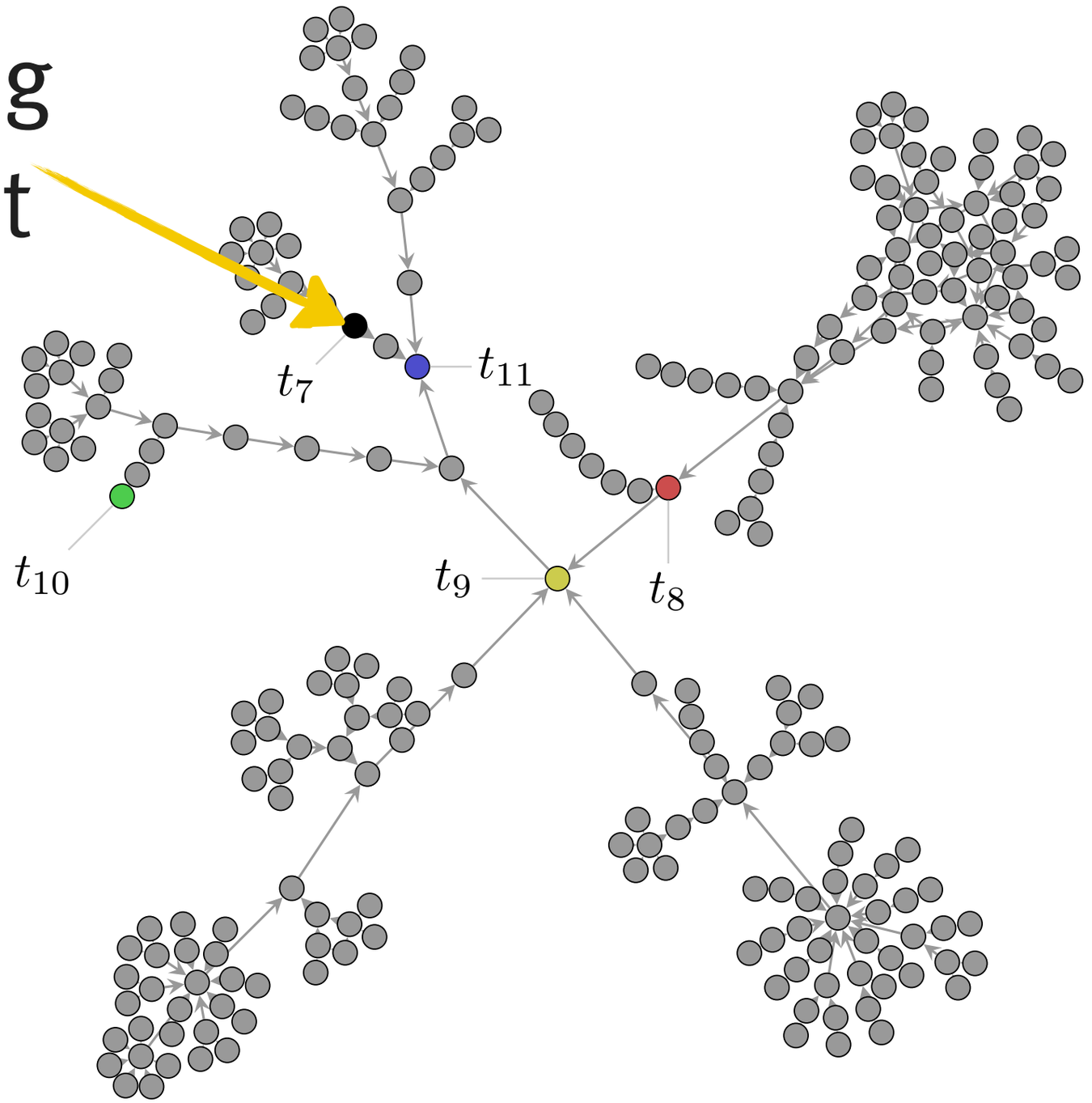
BITLAUNDRY

- 3 Experimente
- Dienst generiert Wegwerfadresse
- Zeitstempel weisen auf Bündelung der Auszahlungen hin

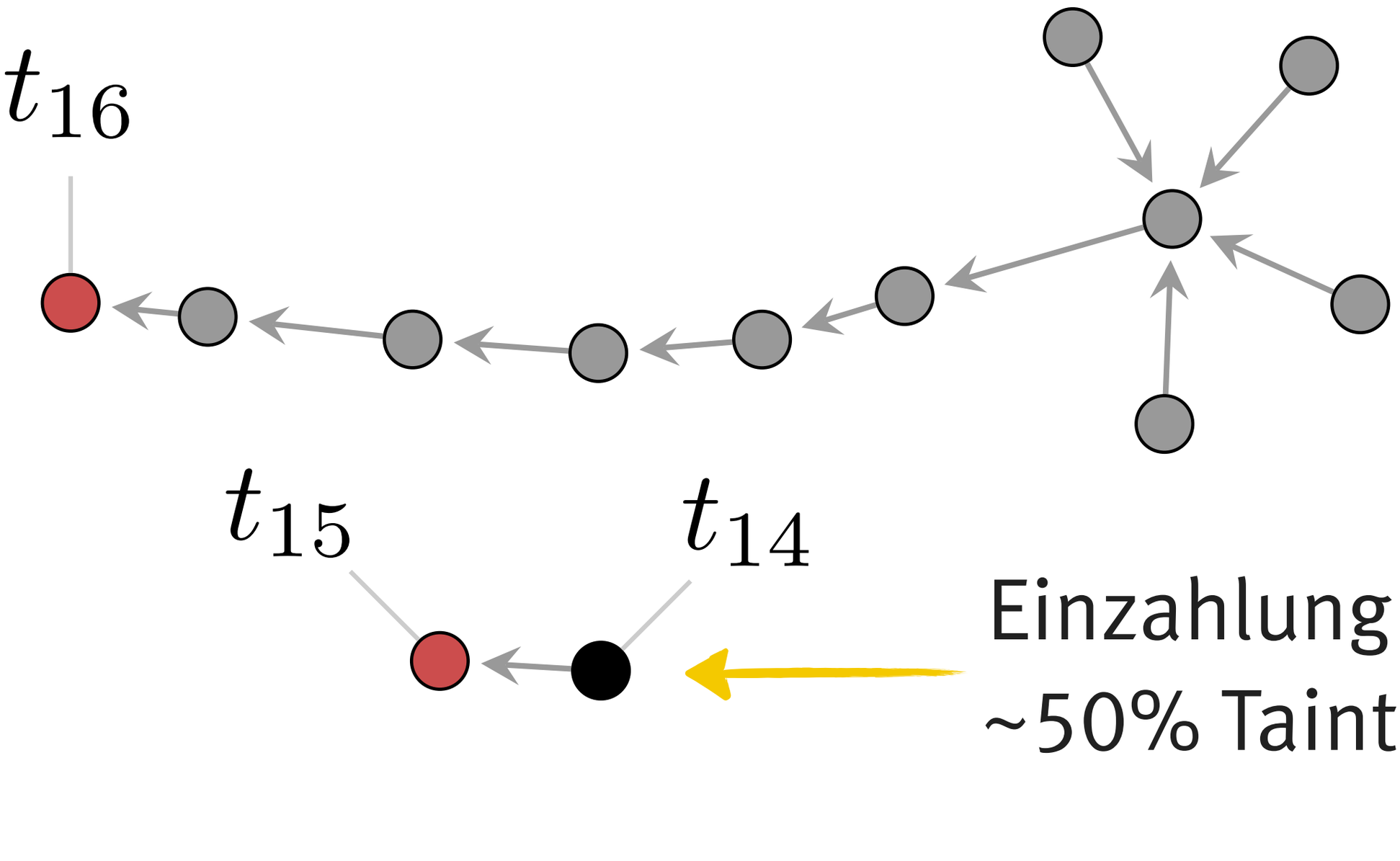
bietet kein https :(

ERSTES EXPERIMENT

Einzahlung
~7% Taint



DRITTES EXPERIMENT



ERGEBNIS

+ Bitcoin Fog und Blockchain.info anonymisieren erfolgreich
- offensichtliche Struktur bei Bitcoin Fog
- BitLaundry Transaktionen lassen sich zurückverfolgen

ZENTRALE INSTANZ

- Mix kann Angreifer sein
- Kombination mehrerer Dienste möglich
- hohe Gebühren: alle 3 Dienste kombiniert führen zu Gebühren i. H. v. 5%
- prinzipiell hohes Risiko

5 DISKUSSION UND FAZIT

EINSCHRÄNKUNGEN

- Nur Transaktionen betrachtet
- Keine Angriffe über Kontext/Timing/Wert
- Keine „großen“ Transaktionen anonymisiert

FAZIT

- Bitcoin Mixer entfernen die Verbindung zwischen Transaktion und Identität
- Kein dezentrales Mixer-Konzept vorhanden
- Bitcoin ist nicht anonym: Forschungspotenzial für anonyme Bitcoin-Alternativen (z. B. Zerocoin)

VIELEN DANK FÜR DIE AUFMERKSAMKEIT!

Gibt es Fragen?

Westfälische Wilhelms-Universität Münster

Malte Möser
MBC’13 Münster Bitcoin Conference