HLT..:: The Data Science Company**Research Report**

Autor: Wolfgang Wester

State: public
Letzte Überarbeitung: 18.06.2023

Titel

The First 1000 Bitcoin Rewards…

Vorbemerkung

Es handelt sich hier um einen Research Report auf Basis von statistischen Methoden und Arbeitshypothesen. Insofern sind die aufgeführten Ergebnisse und Schlussfolgerungen als eine mögliche (plausible) Lösung anzusehen.

Reportziele

Statistische Erfassung und Visualisierung der ersten 1000 Bitcoin-Rewards (Block #0 – 999) und der daran beteiligten Miner und eingesetzten Resourccen.

Begriffsdefinitionen

Agent #xyz – Bezeichnung für einen Miner
Special CPU-Miner – nicht öffentliche Spezial-Minningsoftware von Satoshi Nakamoto
Public CPU-Miner – die öffentlich verfügbare Minningsoftware
Reward – der Gewinn, der an den Miner ausgeschüttet wurde (in 2009 & 2010 jeweils 50 BTC)
KDI – Key Data Indikatoren (Schlüsseldaten wie z.B. Hashrate eines Minning-Computers)
Key Facts – wesentliche Kernpunkte aus der Untersuchung als Zwischenergebnis
Themenspeicher – ToDo-Liste

Datenbasis

Als Datenbasis für die Untersuchung dienten:

- Bitcoin-Blockchain
- interne nicht öffentliche HLT-Bitcoin-DB
- verschiedene öffentliche Internet-Daten (z.B. Blogs, Foren, …)

Methoden

- Datenanreicherung und Formatierung
- Ausschlußverfahren, Näherungsverfahren, Verhältnisverfahren
- Address-Linking Verfahren (Extranonce, Hashrate, Extranonce Start Point, First DateTime Reward Transferpoint, Transfer-Behaviour)
- Transaktions-Graphen
- Grafiken
- Miner-Clustering (Plausibilität der Ergebnisdaten gegen bekannte Miner-Reward-Daten wie Hal Finney, Dustin Trammell prüfen)

Arbeitshypothese

- Satoshi Nakamoto hat von Beginn an einen Special Miner 24/7 eingesetzt
- Satoshi Nakamoto hat von Beginn an mehrere Public Miner 24/7 eingesetzt

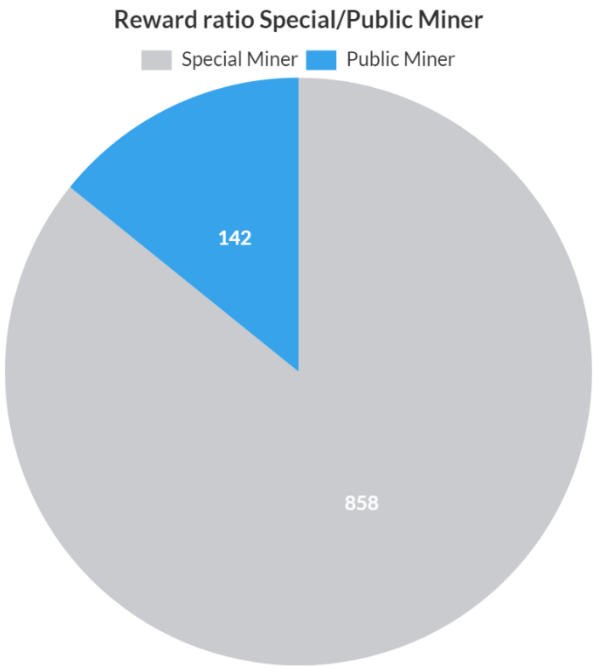
Beschreibung der Vorgehensweise

Aus der HLT-Datenbank haben wir die Blockchain-Informationen der Blöcke # 0 – 999 in eine eigene neue Datenbank kopiert, die als Datengrundlage für unsere Analyse diente.

Dann haben wir die Daten aufgeteilt in Rewards, die mit dem Special Miner gewonnen wurden und Rewards, die mit dem Public Miner gewonnen wurden. Die Separierung erfolgte anhand des Patoshi-Pattern und KDI-Plausibilitätsprüfungen (Hashrate, Nonce/Extranonce, Extranonce Start Point).

Ergebnis:

- Satoshi Special Miner 858 Rewards
- Public Miner 142 Rewards

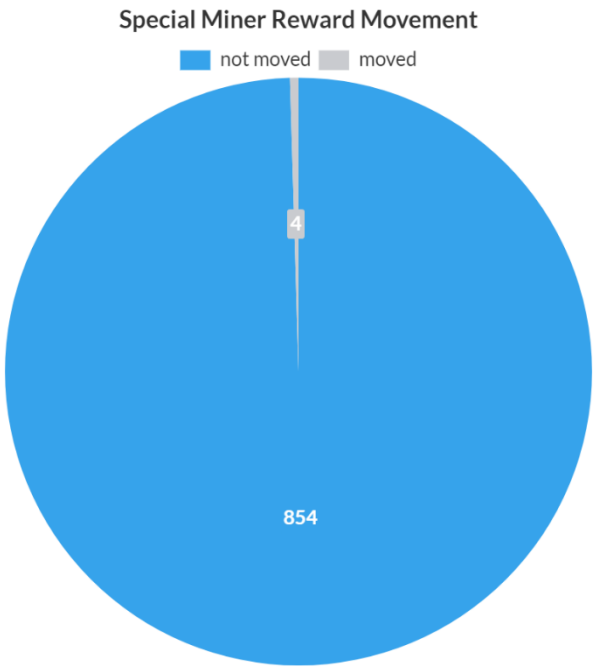


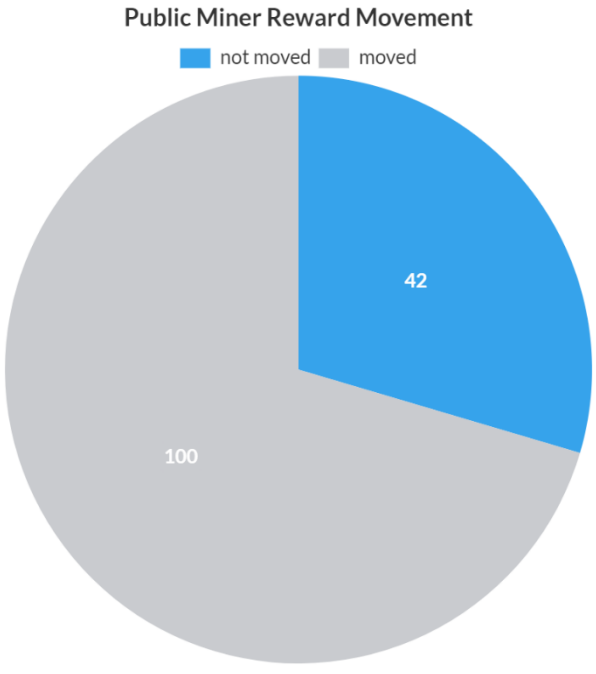
Die Daten liegen als Anlage 1 & 2 in Textform bei

Im nächsten Schritt haben wir die Rewards unterteilt nach bewegt bzw. nicht bewegt. Damit ist gemeint, welche Rewards wurden von den Originaladressen zu anderen Adressen bewegt (moved) und welche nicht (not moved).

Ergebnis:

- Special Miner
    - 854 not moved
    - 4 moved
- Public Miner
    - 42 not moved
    - 100 moved

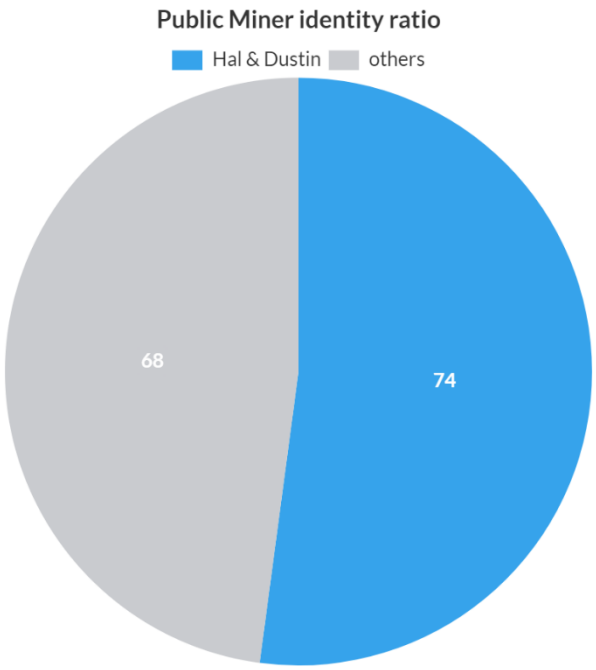




Bekannte Miner der ersten Stunde waren Hal Finney und Dustin Trammell. Die Rewards können damit für unsere weiteren Analyseschritte verwendet werden. Beide haben sämtliche Rewards bewegt. Aus den KDI Hashrate und Extranonce kann man weiterhin ableiten, dass Hal mit einem Rechner gemint hat und Dustin mit zwei Rechnern parallel.

Ergebnis:

- Public Miner
    - Hal & Dustin 74 Rewards
    - others 68 Rewards

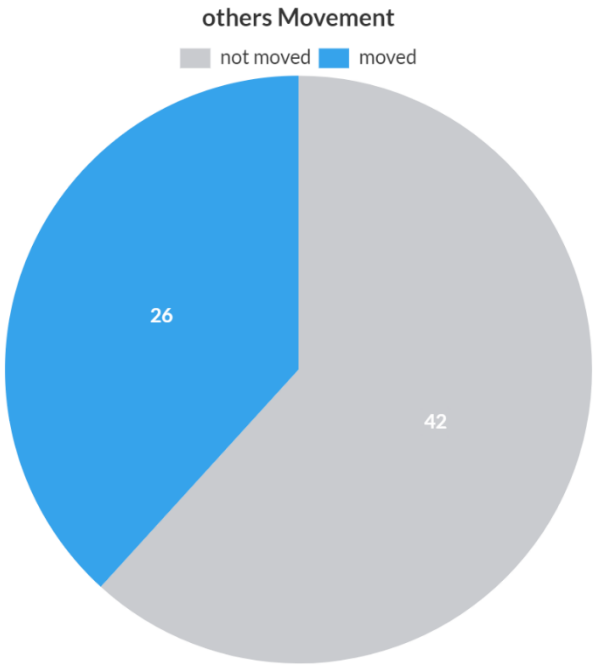


Die Daten von others liegen als Anlage 3 in Textform bei

Laut unserer Arbeitshypothese hat Satoshi Nakamoto von Anfang an mit mehreren Public Minern gearbeitet. Also müsste er in den restlichen Daten ***others*** dominant und über den kompletten Range (Block 0 – 999) enthalten sein. Deshalb beziehen sich die nachfolgenden Untersuchungen nur noch auf den Datenbestand ***others***. Zuerst haben wir uns das Verhältnis von bewegten und nicht bewegten Rewards angeschaut.

Ergebnis:

- others
    - 42 not moved
    - 26 moved



Die Daten liegen als Anlage 4 & 5 in Textform bei

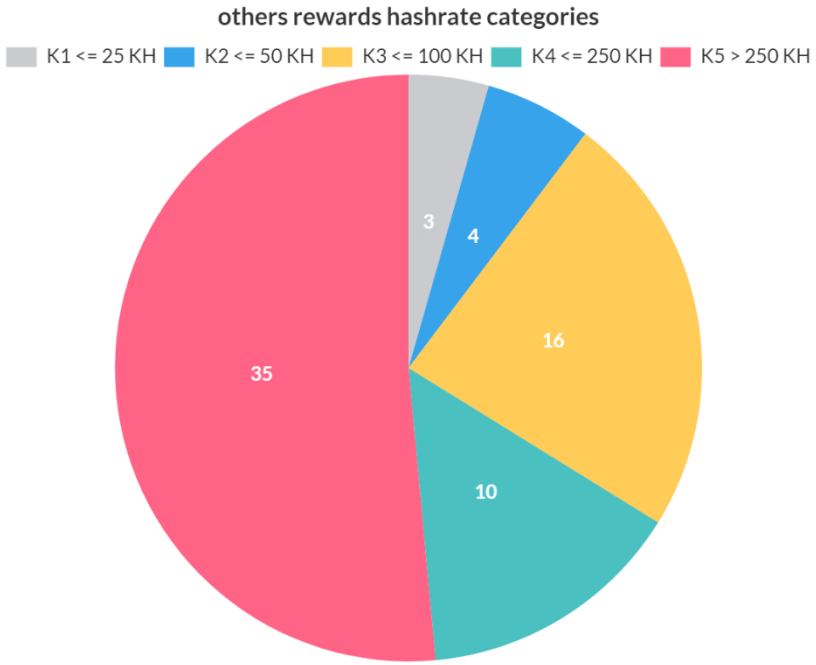
Dann haben wir anhand der KDI Hashrate 5 Kategorien definiert:

- K1 <= 25 KH
- K2 <= 50 KH
- K3 <= 100 KH
- K4 <= 250 KH
- K5 > 250 KH

wobei KH = Hashrate in 1000, beispielweise 10 KH = 10.000 Hash pro Sekunde, Obergrenze +3 %

Ergebnis:

- K1 = 3 Rewards, Blockbereich 189 – 885
- K2 = 4 Rewards, Blockbereich 204 – 986
- K3 = 16 Rewards, Blockbereich 236 – 998
- K4 = 10 Rewards, Blockbereich 127 – 993
- K5 = 35 Rewards, Blockbereich 12 – 996



Fazit

K5 erfüllt die Arbeitshypothese und stellt unserer Ansicht nach die Public Miner-Aktivitäten von Satoshi Nakamoto dar. Weiterhin ist zu beachten, dass der erste Reward in K5 in Block #12 erzielt wurde. Anhand der Extranonce = 12 kann man sofort sehen, dass dieser Miner direkt am Anfang von Bitcoin gestartet wurde. Das kann nur durch Satoshi Nakamoto selbst erfolgt sein.

00000012|09-01-2009 05:21:28|0C|6A|59|3F|0000000012||0000394500|1PYELM7jXHy5HhatbXGXfRpGrgMMXmpobu

Ferner sind 5 Rewards aus K5 bewegt worden. Wir glauben, dass es sich dabei um Transaktionen von Satoshi Nakamoto handelte.

Um hier mehr Klarheit zu bekommen, werden wir

1. eine neue Untersuchung durchführen mit erweitertem Blockbereich (0 – 2999)
2. eine Untersuchung der 5 bewegten Rewards und aller damit verbundenen nachfolgenden Rewards