Westfälische Wilhelms-Universität Münster

ERCIS
European Research Center for Information Systems

# ANREIZE IN MINING-POOLS

## BITCOIN VERTIEFUNGSMODUL

Ulrich Schmidt

18. Juli 2013

# AGENDA

- Grundlagen Mining
- Mining-Pools
- Bekannte Mining-Pools
- Verteilungsmechanismen
- Beliebtheit der Mechanismen
- Fazit/Ausblick

# GRUNDLAGEN MINING

- Ziel: Transaktionen überprüfen, Betrug verhindern (Double-Spending)
- Block als Transaktionsbündelung
- Überprüfung des Blocks mittels Hashberechnung
- Zwei Verdienste:
  - Bonus/Reward (abnehmend)
  - Transaktionskosten

# SOLO-MINING VS. POOL-MINING

$$\text{Anzahl Blocks} = \frac{h \cdot t}{2^{32} \cdot D}$$

h≙Hashrate, t≙vergangene Zeit, D≙Difficulty, $2^{32}$≙ mögliche Änderungen Nonce

- Alleiniges Minen:

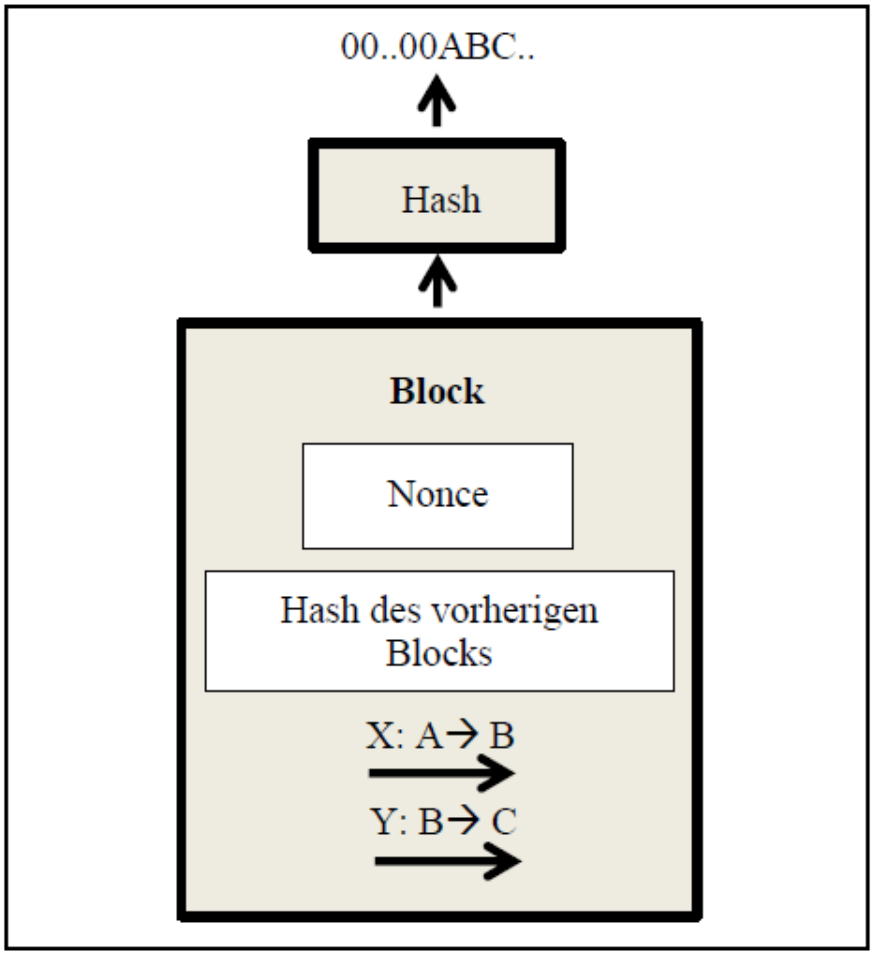
$$1\,[\text{Block}] = \frac{100\,[\frac{\text{MHash}}{\text{s}}] \cdot t}{2^{32} \cdot 12153411,71} \Leftrightarrow t = 16,55\,[\text{Jahre}]$$

- Pool-Mining
  - Höhere Hashrate
  - Stetigere Auszahlung

  → bessere Planung

# POOL-MINING

## HASHSUCHE



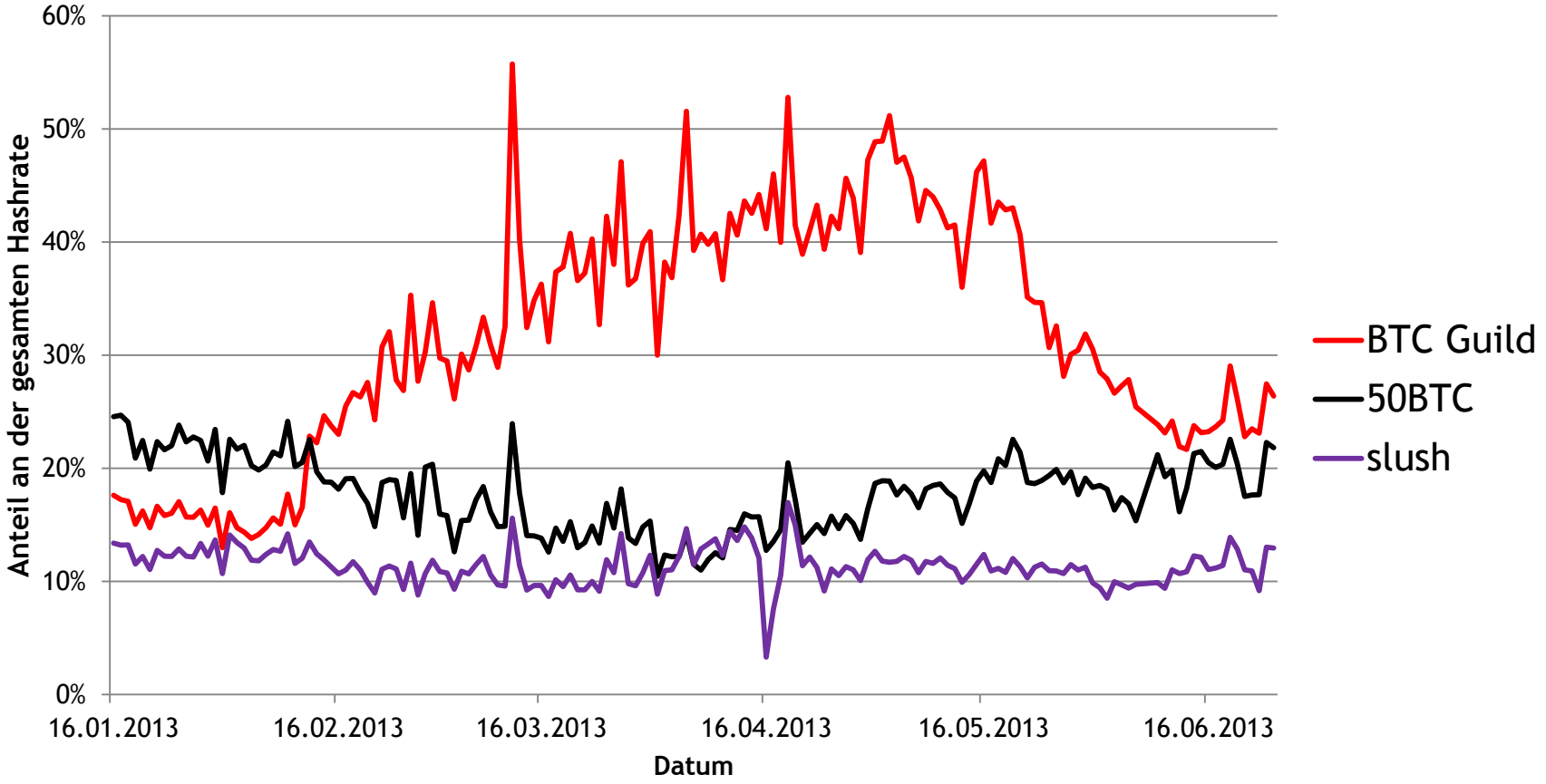

- Berechnung von Shares

$$1\,[\text{Share}] = \frac{100\,[\frac{\text{MHash}}{\text{s}}]\cdot t}{2^{32}\cdot 1} \Leftrightarrow t \approx 43\,[\text{Sek}]$$

- Eingereichte Shares dienen als Verteilungskriterium

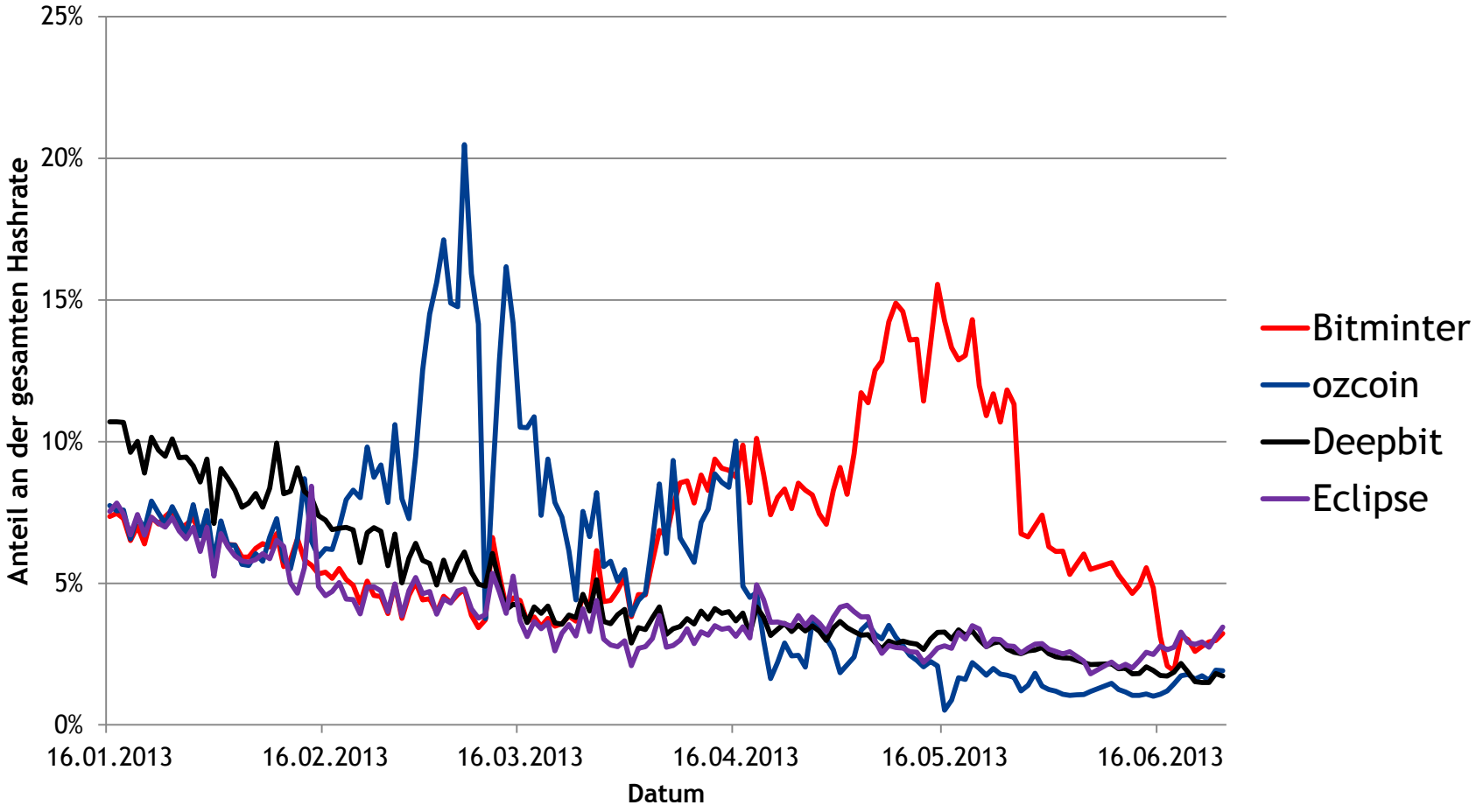
# BEKANNTE MINING-POOLS

## TOP 3



# BEKANNTE MINING-POOLS

## TOP 4-7



# TEILNAHMEGEBÜHREN

| Poolname | Internetadresse | Gebühr |
|---|---|---|
| 50BTC | https://50btc.com/ | 3 % (PPS) |
| Bitminter | http://bitminter.com/ | 1 % (PPLNS) |
| BTC Guild | https://www.btcguild.com/ | 3 % (PPLNS)<br>7,5 % (PPS) |
| Deepbit | https://deepbit.net/ | 3 % (Prop.),<br>10 % (PPS) |
| Eclipse | https://eclipsemc.com | 0 % (DGM),<br>5 % (PPS) |
| ozcoin | https://www.ozcoin.net/ | 1 % (DGM),<br>3 % (PPS) |
| slush | http://mining.bitcoin.cz/ | 2 % (Score) |

# VERTEILUNGSMECHANISMEN

- Faire Aufteilung des Rewards an Teilnehmer

- Fairness
  - Betreiberrisiko einstellbar
  - Kein opportunistisches Verhalten möglich
  - Erwartete Auszahlung immer gleich

- Runde: Zeit zwischen Anfang und Ende der Blocksuche

# PROPORTIONALE VERTEILUNG

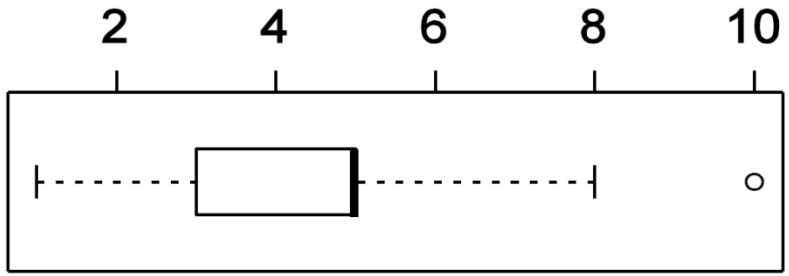
## EINFACHER VERTEILUNGSMECHANISMUS


- Auszahlung je nach Anteil an der Gesamtanzahl der Shares
- Bei gleichbleibender Anzahl Minern fair
- Aber: Poolhopping möglich
- Grundprinzip: Shares sind in kürzeren Runden mehr wert
- Beste Ausstiegszeit: nach 43,5% der Rundenzeit
- Gegenmaßnahme: Pool-Statistik nicht in Echtzeit
- Verfahren ist nicht fair!

# PAY-PER-SHARE (PPS)

## EINFACHER VERTEILUNGSMECHANISMUS

- Bestimmte Auszahlung für jeden eingereichten Share
  → Miner kann Auszahlungen gut planen
- Betreiber hat höheres Risiko
- Übersicht der prozentualen Gebühr:




- Methode für den Miner fair

# SLUSHS SCORE METHODE

## FORTGESCHRITTENER VERTEILUNGSMECHANISMUS

- Berechnung eines Scores für jeden Share
- Anteil des Scores am Gesamtscore bestimmt Auszahlung
- Score anfangs weniger wert
  → Verhinderung von Pool-Hopping
- Berechnung des Scores:

$$\text{Score} = \sum \exp\left(\frac{\text{Rundenzeit}}{C}\right)$$

- Kurze Runden attraktiver, da mehr Auszahlung
  → praktisch fair

# GEOMETRISCHE METHODE

## FORTGESCHRITTENER VERTEILUNGSMECHANISMUS


- Scorebasiert wie slush
- Verhinderung des Nachteils bei kurzen Runden
  → zusätzliche variable Gebühr (Score des Betreibers)
- Kurze Runden
  - Betreiber-Score hoch
  - Miner erhalten weniger
- Lange Runden
  - Betreiber-Score nahezu null
  - Miner erhalten „normale“ Auszahlung
- Verfahren ist fair

# PAY-PER-LAST-N-SHARE-METHODE (PPLNS)

## FORTGESCHRITTENER VERTEILUNGSMECHANISMUS


- Unabhängig von Runden, nur letzte N Shares relevant
- Geringeres Risiko für Betreiber
- Welches N?
  - Feste Größe: Änderungen der Difficulty ausnutzbar
  - Vielfache der Difficulty: Zeit direkt vor und nach Änderung der Difficulty ausnutzbar
  - Lösung: Speicherung der Difficulty zu jedem Share
- Abwandlung: Pay-per-last-N-shifts
  - Shares (z.B. 25 Mio) werden zu Shifts zusammengefasst
- Theoretisch angreifbar, praktisch fair

# DOUBLE GEOMETRIC METHOD (DGM)

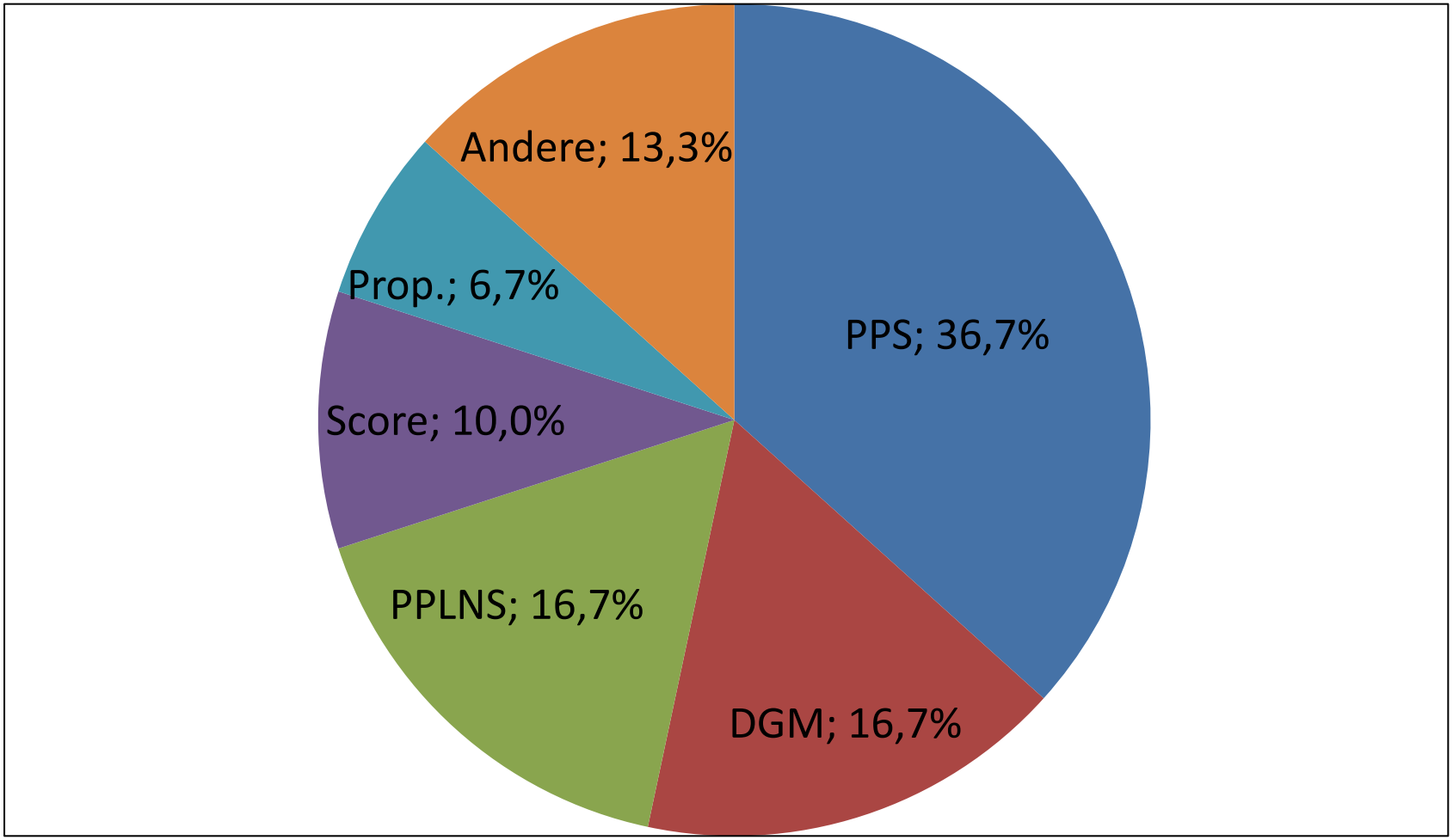
## FORTGESCHRITTENER VERTEILUNGSMECHANISMUS

- Kombination aus PPLNS und geometrischer Methode
  → scorebasiertes PPLNS
- Dadurch lassen sich minimieren:
  - Poolbasierte Streuungen: Abweichungen in der Anzahl und Häufigkeit der eingereichten Shares
  - Sharebasierte Streuungen: Abweichungen von Zahlungen pro eingereichten Share
- Teil des Rewards bleibt im Pool (variable Gebühr)
  - Langen Runde: geringe Gebühr
  - Kurze Runde: hohe Gebühr
- Verfahren ist fair

# FAIRNESS DER METHODEN

| Verfahren | Fairness Betreiber | Fairness Miner |
|---|---|---|
| Proportional | Ja, nur Auszahlung bei Fund eines Blocks | Nein, Pool-Hopping möglich |
| Pay-per-Share (PPS) | Nein, evtl. mehr Auszahlung als Gewinn | Ja, Auszahlungen gut planbar, keine Poolhopping |
| Slushs Score | Ja, nur Auszahlung bei Fund eines Blocks | Praktisch fair |
| Geometrische Methode | Ja, durch variable Gebühr | Ja, kein Pool-Hopping |
| Pay-per-last-N-Shares (PPLNS) | Ja, gleiche Auszahlung | Praktisch fair |
| Double Geometric Method | Ja, Streuung variabel | Ja, Streuung variabel |

# BELIEBTHEIT DER METHODEN



# FAZIT / AUSBLICK

- Viele Verfahren (bis auf proportionale Verfahren) sind in der Praxis sicher gegen opportunistisches Verhalten
- Gefahr des Missbrauchs bei großen Pools (>50%)
- Verfahren stehen im Wettbewerb zueinander
- Verlauf der beliebtesten Methoden in weiterer Forschung beobachten

# VIELEN DANK FÜR DIE AUFMERKSAMKEIT!

ERCIS
European Research Center for Information Systems

THE IS RESEARCH NETWORK

www.ercis.org