Non-Standard-Datenbanken und Data Mining

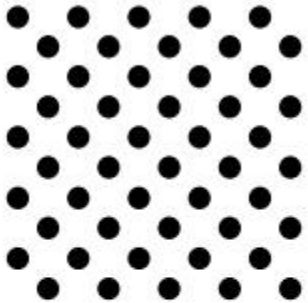
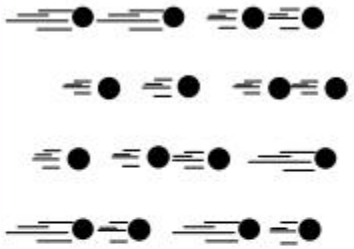
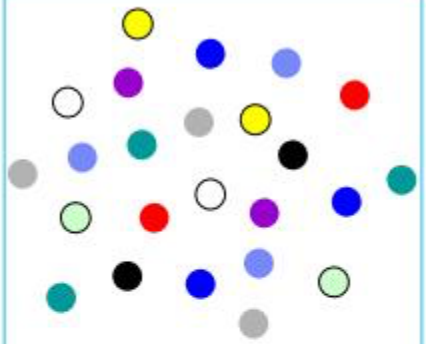
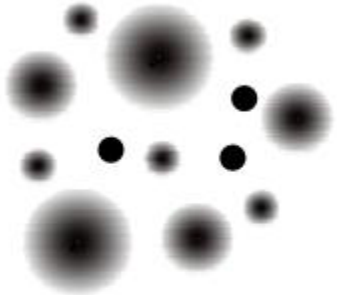
Von NoSQL zu NewSQL
CAP, CALM, CRON, Blockchain

Prof. Dr. Ralf Möller
Universität zu Lübeck
Institut für Informationssysteme

Übersicht

- Semistrukturierte Datenbanken (JSON, XML) und Volltextsuche
- Informationsrecherche, Informationsextraktion, Einbettungsräume
- Mehrdimensionale Indexstrukturen
- Cluster-Bildung
- Einbettungstechniken
- First-n-, Top-k-, und Skyline-Anfragen
- Probabilistische Datenbanken, Anfragebeantwortung, Top-k-Anfragen und Open-World-Annahme
- Probabilistische Modellierung, Bayes-Netze, Anfragebeantwortungsalgorithmen, Lernverfahren,
- Temporale Datenbanken und das relationale Modell, SQL:2011
- Probabilistische Temporale Datenbanken
- SQL: neue Entwicklungen (z.B. JSON-Strukturen und Arrays), Zeitreihen (z.B. TimeScaleDB)
- Stromdatenbanken, Prinzipien der Fenster-orientierten inkrementellen Verarbeitung
- Approximationstechniken für Stromdatenverarbeitung, Stream-Mining
- Probabilistische raum-zeitliche Datenbanken und Stromdatenverarbeitungssysteme: Anfragen und Indexstrukturen, Raum-zeitliches Data Mining, Probabilistische Skylines
- Von NoSQL- zu NewSQL-Datenbanken, CAP, CALM, CRON-Theoreme, Blockchain-Datenbanken
- Graphdatenbanken
- Gelernte Indexstrukturen
- Kausale Repräsentationen
- Kausales Data Mining

Big Data

Volume	Velocity	Variety	Veracity*
			
Data at Rest	**Data in Motion**	**Data in Many Forms**	**Data in Doubt**
Terabytes to exabytes of existing data to process	Streaming data, milliseconds to seconds to respond	Structured, unstructured, text, multimedia	Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations

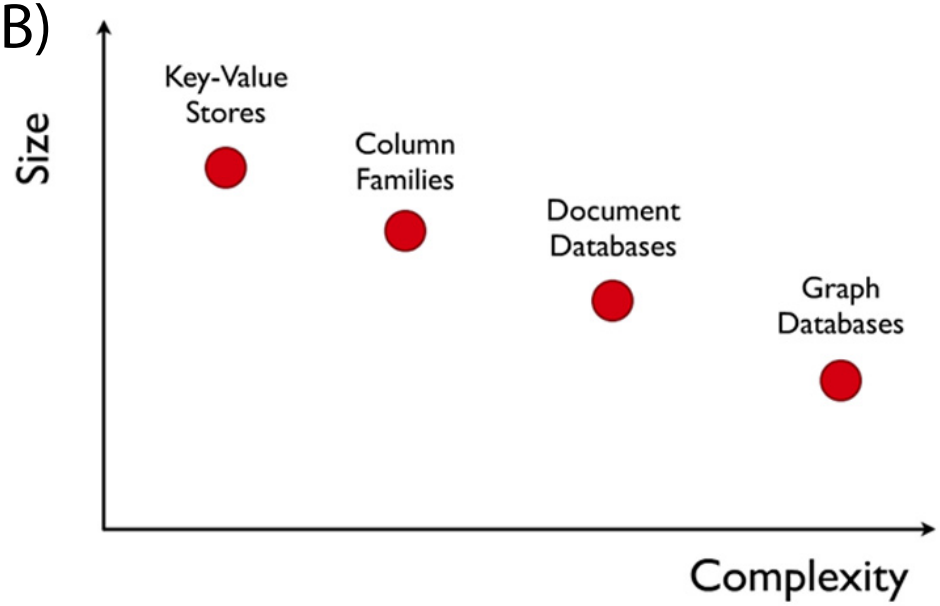
*Veracity = Aufrichtigkeit, Wahrhaftigkeit

NoSQL: Not Only SQL?

- Datenmengen werden groß (Big Data)
  - Horizontale Skalierung notwendig (→ Elastizität)
  - Virtualisierung (Cloud Computing) geht damit einher
- Heterogenität von Daten, Datenintegration
  - Schema-Freiheit (relationales Modell scheint zu starr)
  - Algorithmische Datenverarbeitung wird gewünscht
- Verteilung der Datenhaltung
  - CAP Theorem (Consistency, Availability, Partitioning tolerant: Eric Brewer)
    - Nur 2 aus 3 Kriterien erfüllbar
  - Abschwächung des Serialisierbarkeits-Konsistenzkriteriums: BASE
    - **B**asically **A**vailable
    - **S**oft-state (or scalable)
    - **E**ventually consistent

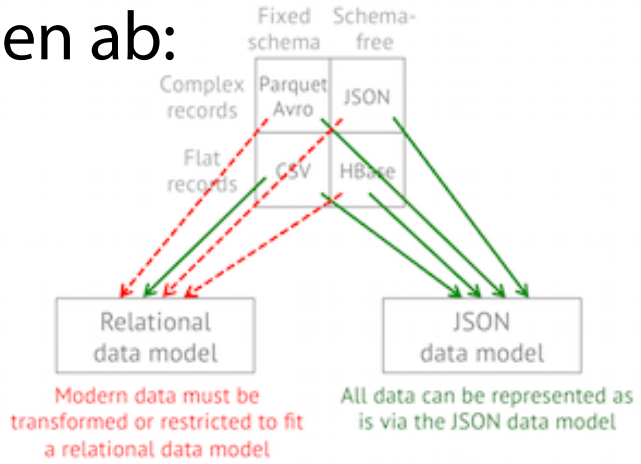
NoSQL-Datenbanktypen

- Key-Value Stores – Hashtabelle von Schlüsseln
  - Google Bigtable, Amazon Dynamo
- Column Stores – Block nur Daten aus einer Spalte
  - Supernormalisierung
- Document Stores (MongoDB)
  - XML-Strukturen
  - JSON-Strukturen
- Graphdatenbanken
  - RDF
    - SPARQL
  - Property Graphs
    - Cipher (Neo4J)
    - GQL als neuer ISO-Standard neben SQL (seit 2017 entwickelt)



NoSQL: Zusammenfassung

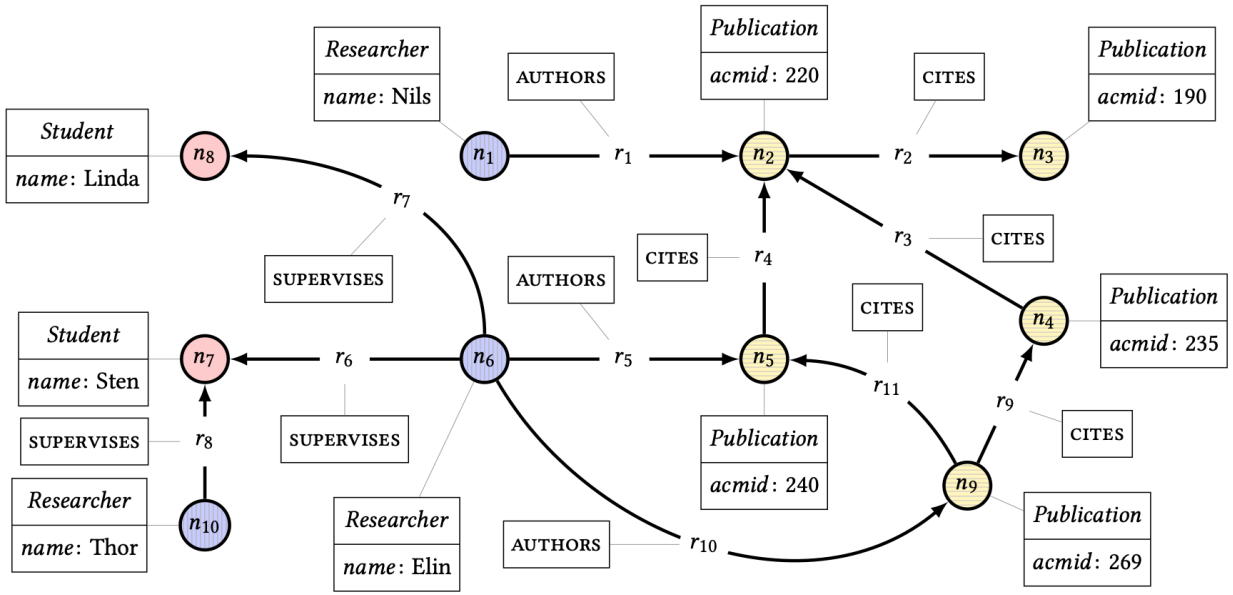
- Nutzer von NoSQL-Datenbanken lehnen ab:
  - Aufwand von ACID-Transaktionen
  - “Komplexität” von SQL
  - Aufwand des Designs von Schemata
  - Deklarative Anfrageformulierung
  - Ein-Prozessor-Technologie
- Programmierer wird verantwortlich für
  - Prozedurale Formulierung von Zugriffsalgorithmen
  - und Navigation zu den benötigten Daten




```
SqlString sql = select(ARTICLE.OID)
                .from(ARTICLE, ARTICLE_COLOR)
                .where(ARTICLE.OID.eq(ARTICLE_COLOR.ARTICLE_OID)
                .and(ARTICLE.ARTICLE_NO.is_not(NULL)));
```

Konkrete Ausprägung variiert

Cypher




```
MATCH (svc:Service)<-[:DEPENDS_ON*]-(dep:Service)
RETURN svc, count(DISTINCT dep) AS dependents
ORDER BY dependents DESC
LIMIT 1
```

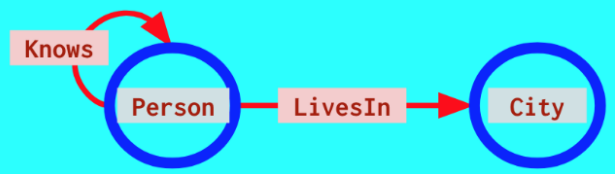
Nadime Francis, Alastair Green, Paolo Guagliardo, Leonid Libkin, Tobias Lindaaker, Victor Marsault, Stefan Plantikow, Mats Rydberg, Petra Selmer, and Andrés Taylor. 2018. Cypher: An Evolving Query Language for Property Graphs. In Proceedings of the **2018** International Conference on Management of Data (SIGMOD '18).

```
MATCH (accHolder:AccountHolder)-[:HAS]->(pInfo)
WHERE pInfo:SSN OR pInfo:PhoneNumber
                OR pInfo:Address
WITH pInfo,
    collect(accHolder.uniqueId) AS accountHolders,
    count(*) AS fraudRingCount
WHERE fraudRing > 1
RETURN accountHolders,
    labels(pInfo) AS personalInformation,
    fraudRingCount
```

GQL

Inspired by
- Cypher
- SQL/PGQ
- SPARQL

```
CREATE GRAPH SocialNetwork {
    (Person {name STRING, dob DATE}),
    (City {name STRING}),
    (Person)-[LivesIn]->(City),
    (Person)-[Knows]->(Person)
}
```



WG3:JCJ-015
DM32.2-2019-00999

ISO/IEC JTC 1/SC 32

Date: 2019-05-09

IWD 39075:202y(E)

ISO/IEC JTC 1/SC 32/WG 3

The United States of America (ANSI)

Information technology — Database languages — GQL

Technologies de l'information — Langages de base de données — GQL

SQL/PGQ querying – Example

Get the **creationDate** and **content** of the **messages created by one person** ("email1") and **commented on by another person** ("email2").

```
SELECT GT.creationDate, GT.content
FROM myGraph GRAPH_TABLE (
  MATCH
   (Creator IS Person WHERE Creator.email = :email1)
      -[ IS Created ]->
   (M IS Message)
      <-[ IS Commented ]-
   (Commenter IS Person WHERE Commenter.email = :email2)
      WHERE ALL_DIFFERENT (Creator, Commenter)
  COLUMNS (
      M.creationDate,
      M.content )
 ) AS GT
```

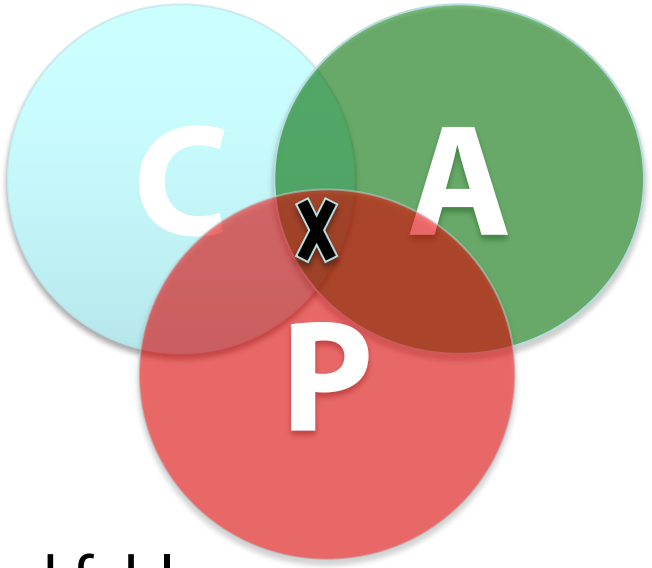
Standardisierung von Graph Datenbanken

SQL/GQL Implementierungen werden erscheinen

- Indexstrukturen
- Approximative Anfragebeantwortung
- Ströme von Graphstrukturen

CAP Theorem

- **C**onsistency:
  - Alle Knoten sehen die gleichen Daten zur gleichen Zeit
- **A**vailability (Verfügbarkeit):
  - Fehler von Knoten beeinträchtigen nicht die Funktionsfähigkeit der Überlebenden
- **P**artitionierungstoleranz:
  - System arbeitet weiter, auch bei Partitionierung durch Netzwerkfehler

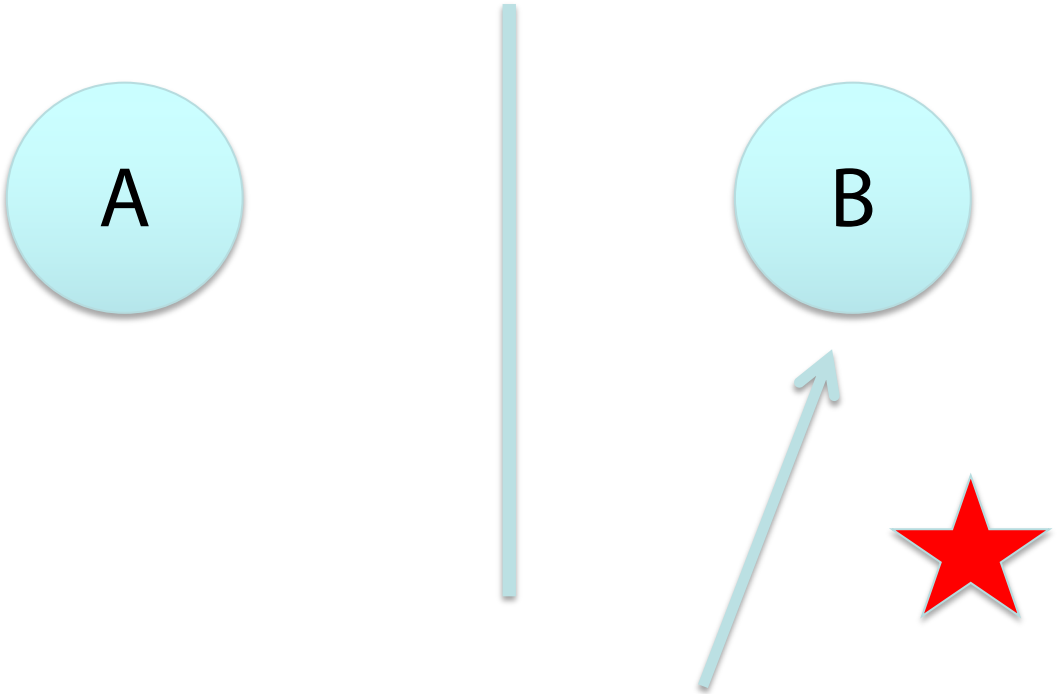


- Theorem: Ein verteiltes System kann nur jeweils zwei Kriterien erfüllen, nicht aber alle drei

Seth Gilbert and Nancy Lynch. "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services." ACM SIGACT News 33.2 (**2002**): 51-59

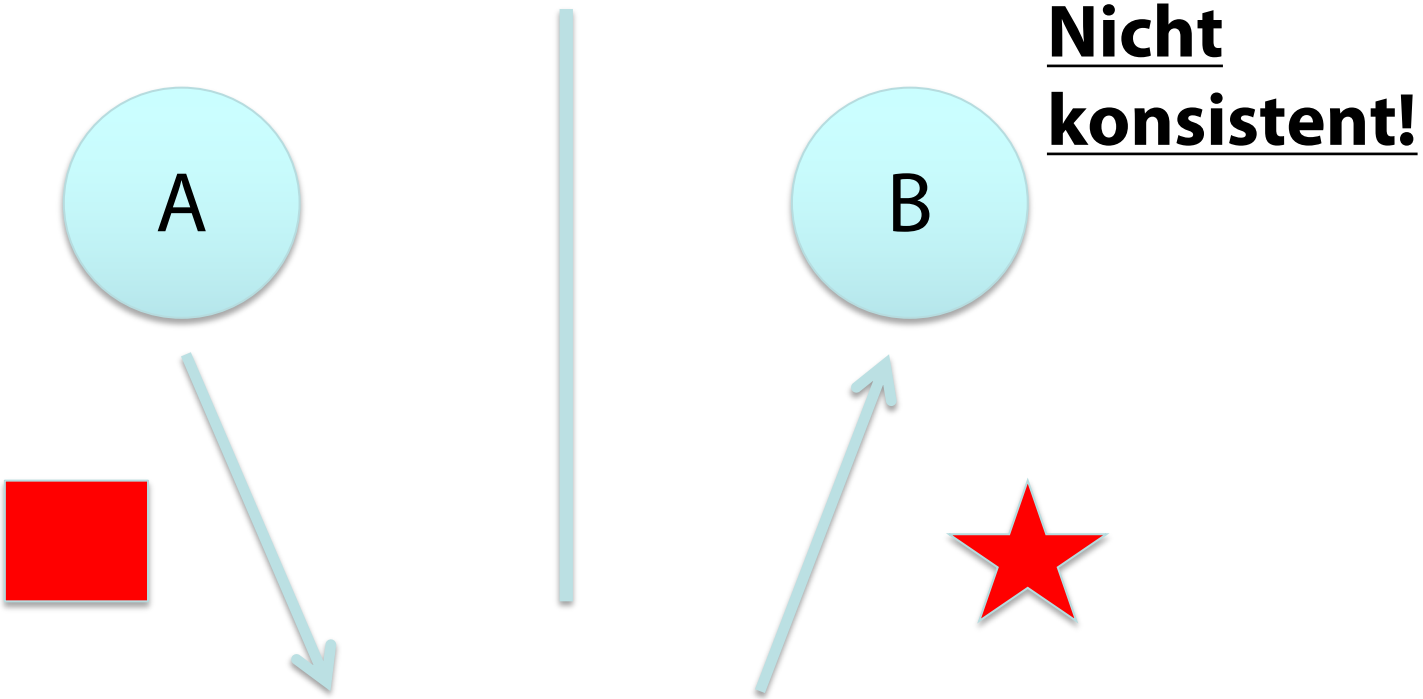
CAP Theorem: Argumente

- Nehmen wir an, es gibt zwei Knoten:



CAP Theorem: Argumente

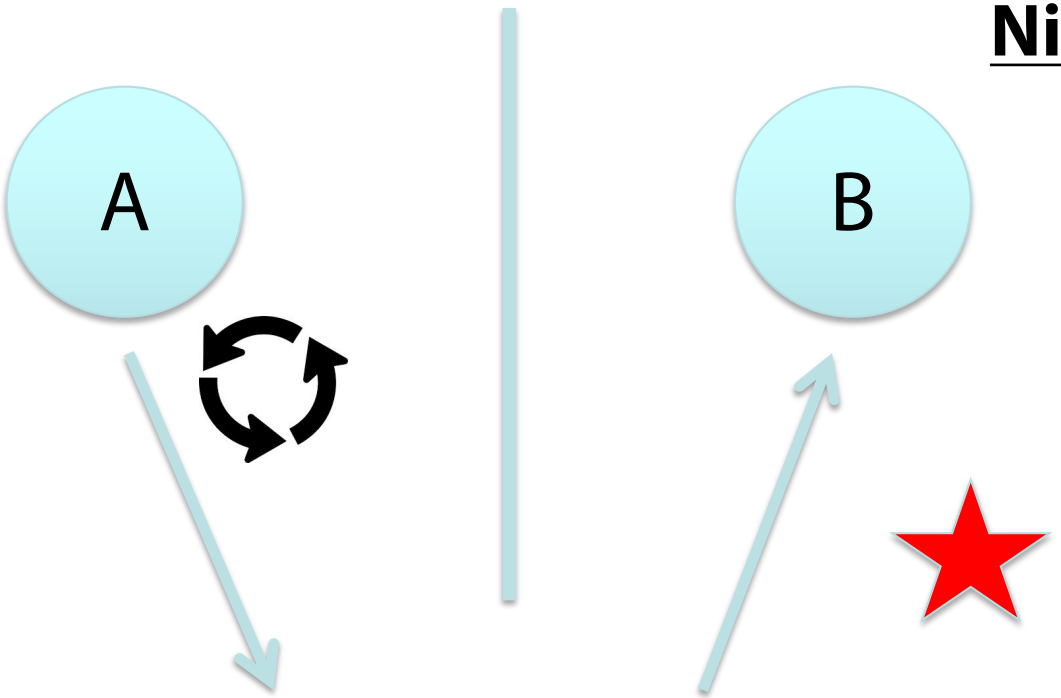
- Nehmen wir an, es gibt zwei Knoten:



CAP Theorem: Argumente

- Nehmen wir an, es gibt zwei Knoten:

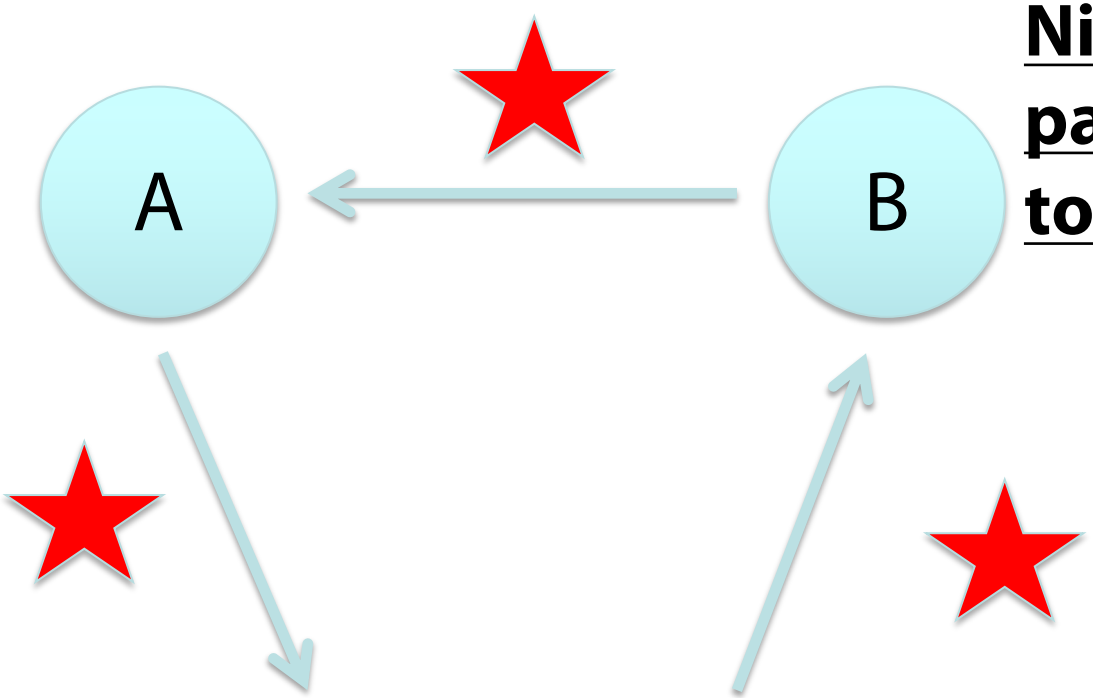
Nicht verfügbar!



Warten auf Aktualisierung

CAP Theorem: Argumente

- Nehmen wir an, es gibt zwei Knoten:



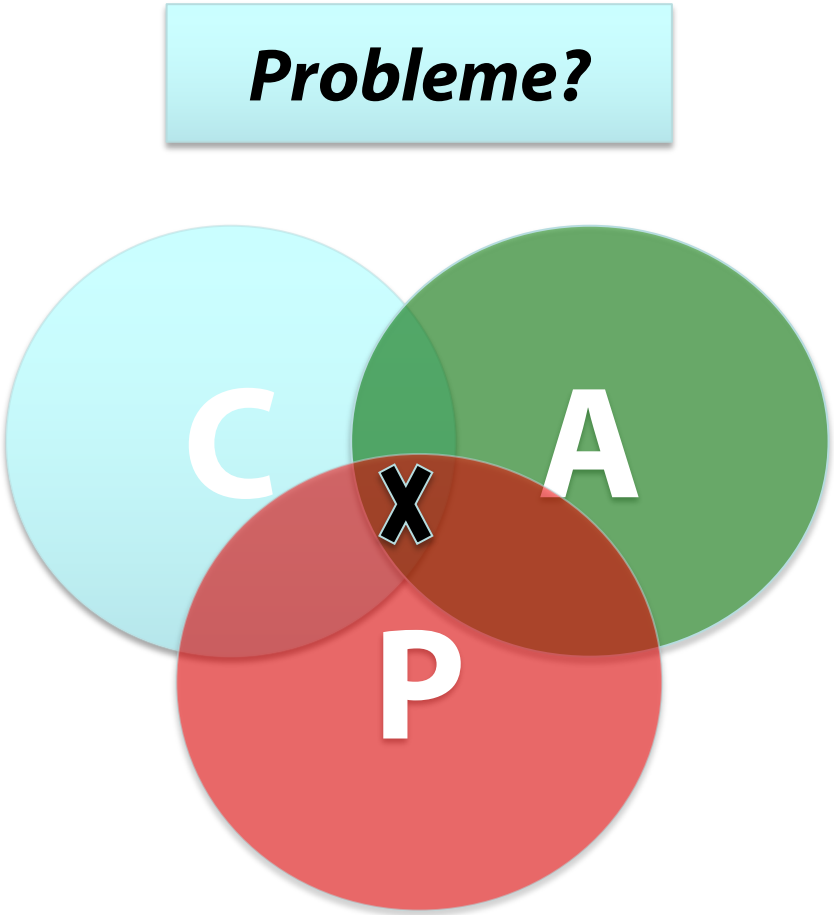
Nicht partitionierungs-tolerant!

A erhält Aktualisierung von B

Partitionierung:
System zerfällt in (mindestens) zwei unverbundenen Teile

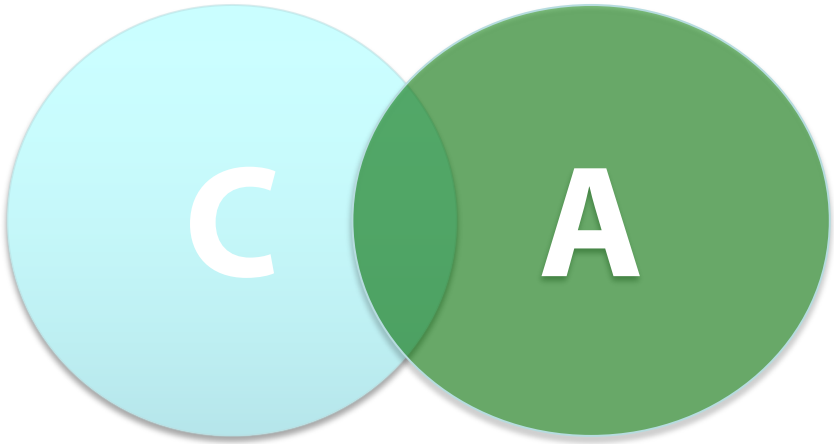
Neubetrachtung CAP Theorem

- Von den folgenden Garantien angeboten von verteilten Systemen:
  - Consistency
  - Availability
  - Partition tolerance
- Wähle zwei
- Drei Möglichkeiten :
  - CP
  - AP
  - CA (relationales DMBS)



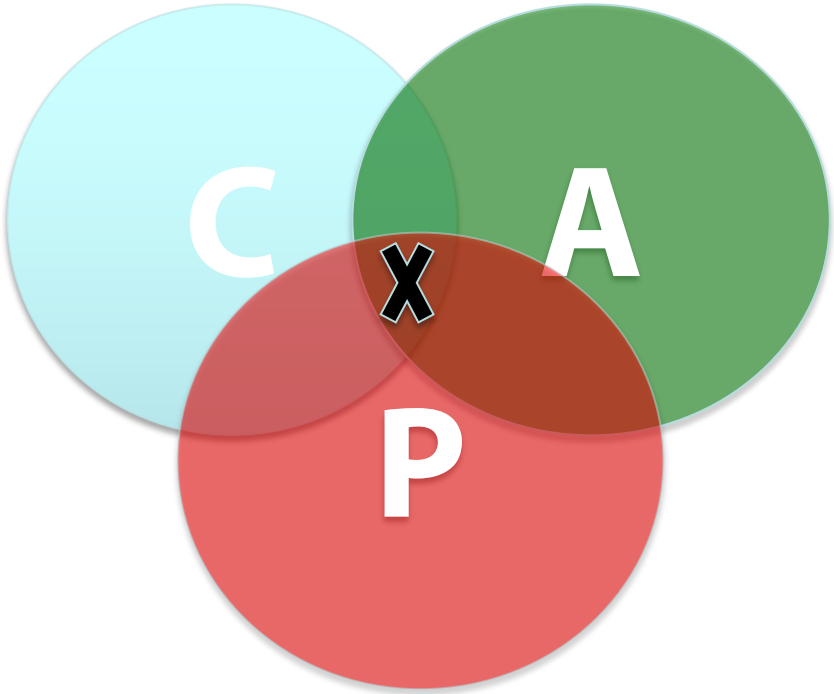
Häufiges Missverständnis: 2 von 3

- Was ist mit CA?
- Kann ein verteiltes System (mit unzuverlässigem Netzwerk) wirklich nicht partitionierungstolerant sein?



Konsistenz oder Verfügbarkeit

- Konsistenz und Verfügbarkeit sind keine binären Entscheidungen
- AP-Systeme schwächen Konsistenz zugunsten von Verfügbarkeit (sind aber nicht notwendigerweise inkonsistent)
- CP-Systeme opfern Verfügbarkeit zugunsten der Konsistenz (sind aber durchaus meist verfügbar)
- Quintessenz: AP- und CP-Systeme können Konsistenz, Verfügbarkeit und Partitionierungstoleranz graduell zur Verfügung stellen -- theoretisch



Arten der Konsistenz

- Starke Konsistenz
  - Nach einer Datenaktualisierung muss jeder nachfolgende Zugriff (egal auf welcher Kopie) den neuen Wert liefern
- Schwache Konsistenz
  - Es wird nicht garantiert, dass nachfolgende Zugriffe auf Kopien den aktualisierten Wert liefern
- Letztendliche Konsistenz (Eventual consistency)
  - Spezielle Form der schwachen Konsistenz
  - Es wir garantiert, dass schließlich alle Prozesse den letztmalig aktualisierten Wert sehen, wenn keine neuen Änderungen erfolgen (verzögerte Propagierung von Änderungen in die Kopien)

Daniel Abadi. 2012. Consistency Tradeoffs in Modern Distributed Database System Design: CAP is Only Part of the Story. Computer 45, 2. pp. 37–42. **2012**.

AP, CP greift zu kurz: CAP/ELC

- **AP/EL-System:** Gib Konsistenz C auf zugunsten der Verfügbarkeit A und kleinerer Latenz L
  - Dynamo, Cassandra, Riak
- **CP/EC-System:** Verweigere, die Konsistenz C aufzugeben, und zahle die Kosten von Verfügbarkeit und Latenz
  - BigTable, Hbase, VoltDB/H-Store
- **AP/EC-System:** Gib Konsistenz auf, wenn Partitionierung erfolgt, und erhalte Konsistenz im normalen Betrieb
  - MongoDB
- **CP/EL-System:** Erhalte Konsistenz, wenn Partitionierung erfolgt, gebe Konsistenz für kleine Latenz im normalen Betrieb auf
  - Yahoo! PNUTS

EL=Else Latency
EC=Eventual Consistency

CAP Theorem – Leider Komplexitätsproblem

- Ignoriere die Komplexität: Alles kann passieren: schlecht
- Vemeide Komplexität: Nicht möglich: Einfachste Beispiele zeigen Read-Write- und Write-Write-Konflikte
- Einkapselung der Komplexität: Transaktionen und Cache-Kohärenzprotokolle regeln das, aber zum Preis von Sperren, Deadlocks und Rücksetzungen

Bloom Programmierspache

- Kann die Programmierumgebung helfen, einfachen und effizienten verteilten Code zu schreiben?

```
state do
  table :link, [:from, :to]
  scratch :path, [:from, :to]
end

bootstrap {link <+ [['a', 'b'], ['a', 'c'], ['b', 'd']]}

bloom do
  path <= link
  path <= (path * link).pairs(:to=>:from) {|p,l| [p.from, l.to]}
end
```

- Datalog:
  - Monoton (kleinster Fixpunkt existiert (LFP), PTIME-vollständig)
  - Mit stratifizierter Negation (immer noch PTIME)
    - Versiegelung oder Snapshot Closed World Assumption (SCWA), LFP per Stratum bottom up
- Versiegelung in verteilten Systemen: Koordination

Interlandi, Matteo & Tanca, Letizia. A datalog-based computational model for coordination-free, data-parallel systems. Theory and Practice of Logic Programming. 18. 874-927. **2018**.

Theorie der Verteilten Systemen

- Begriff der Kausalität,
  - der Programmierern ermöglicht ungewollte Dinge zu vermeiden (z.B. die Ausführung von Instruktionen in der falschen Reihenfolge)
  - Töte-deinen-Großvater-Paradoxon
- Kausalität wird durch Protokolle mit verteilten Uhren erreicht
  - Richtige Ordnung der Ausführung durch Nachrichten erreichen
    Warten auf Nachrichten: schlecht
- Das CRON Prinzip:
  - Zur Hölle mit den verteilten Uhren

CALM

- Vermutung: Konsistenz und logische Monotonie
- LM => C. Monotone Logik erzeugt konsistente Ergebnisse unabhängig von der Reihenfolge der Nachrichtenübermittlung
  - Beweis scheint recht einfach: Konstruktion über Pipeline-orientierte semi-naive Auswertung
- C => LM? Sind denn alle konsistenten Programme monoton? Nun, jedenfalls nicht auf den ersten Blick
- LM + Koordination => C. Wenn wir an den Schichtungsgrenzen eines verteilten Datalog-Programms Koordination einführen, erhalten wir ein ordnungsunempfindliches Programm
- Wir können LM syntaktisch prüfen! (Nun ja, wir können es konservativ prüfen)

Alvaro, P., Conway, N., Hellerstein, J.M., & Marczak, W.R.. Consistency Analysis in Bloom: a CALM and Collected Approach. CIDR. **2011**.

CRON

- CRON-Hypothese:
  - Kausalität nur für nicht-monotone Logik erforderlich
- Ziemlich sichere Vermutung:
  - Monotone Programme erfordern keine kausalen Ordnungen.
  - Bewiesen von Ameloot und Van den Bussche
- Vermutung:
  - Nicht-monotone Programme erfordern kausale Ordnungen
  - Oder äquivalent: "Jedes Programm, das Nicht-Kausalität toleriert, ist äquivalent zu einem positiven Programm"
  - Widerlegt von Ameloot und Van den Bussche

Bloom, CALM, CRON

- Komplexität ignorieren: Angenommen, ich ignoriere die Probleme der Gleichzeitigkeit und des Ausfalls. Was ist das Schlimmste, was passieren kann?
  - Antwort: Sowieso kein Problem, wenn Ihr Programm monoton ist. Wir können aber auch automatisch Koordination in ein Benutzerprogramm injizieren, das nicht monoton ist. Oder wir können die potenziell nicht monotonen "Ordnungspunkte" identifizieren, und Sie können Ihr Programm so erweitern, dass es diesen "Makel" trägt, wenn Sie möchten.

- Vermeiden von Komplexität: Kann ich meine Programme so umschreiben, dass die Notwendigkeit der Koordination vermieden wird? Immer?
  - Antwort: Ja: Es scheint, dass wir theoretisch keine dieser Techniken für irgendwelche polynomialzeitlichen (d.h. vernünftigen) Aufgaben brauchen sollten. Offene Frage, ob das praktisch ist.

- Einkapselnde Komplexität: Kann ich meine Probleme mit verteilten Systemen einmal in einer wiederverwendbaren Bibliothek lösen und die Komplexität verstecken?
  - Antwort: Man kann garantieren, dass ein Modul all seine Nicht-Monotonie mit irgendeinem Koordinationsprotokoll schützt. Auf ähnliche Weise können Sie eine Art Koordinationsdienst bauen und sich auf diesen verlassen, wenn Sie ihn intelligent aufrufen.

Hellerstein, Joseph & Alvaro, Peter. Keeping CALM: When Distributed Consistency is Easy. Communications of the ACM, September 2020, Vol. 63 No. 9, pp. 72-81 **2020**.

Überwindung der imperativen Programmierung

- Koordination ist das letzte wirklich teure Gut
  - Anwendungsprogrammierung baut auf mutierbarem Zustand und geordneten Strukturen
  - Nicht sehr gut für Cloud-Architekturen geeignet
  - Sperren und Kommunikation verlangsamen Berechnungen
- Wie kann man Koordination vermeiden, ohne Inkonsistenzen zu erzeugen?
  - Geht nicht mit klassischen Read/Write-Betrachtungen (Transaktionen)
  - Vermeidung auf Applikationsebene mit neuen Programmiertechniken (implizites strat. Datalog)
    - Z.B. Bloom http://bloom-lang.net

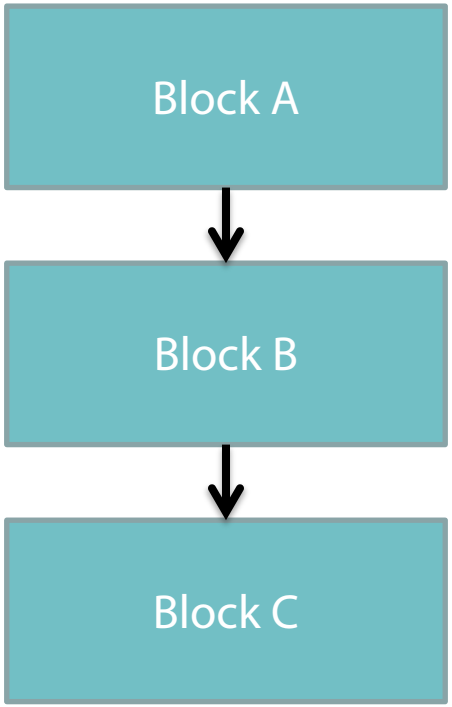
Blockchain-Datenmanagement

Was ist eine Blockchain?

Wie der Name schon sagt, eine **Kette** von **Blöcken**

Was enthalten die **Blöcke**?

- Prinzipiell alle möglichen Daten
  - Währungen
  - Verträge
  - Grundbücher
  - Wikipedia Einträge
  - Stammbäume



Was ist mit der **Kette**?

- Dokumentiert eine Erweiterung der Daten

Ziel: **Konsistente** und **nachvollziehbare** Speicherung der Erweiterung von Daten!

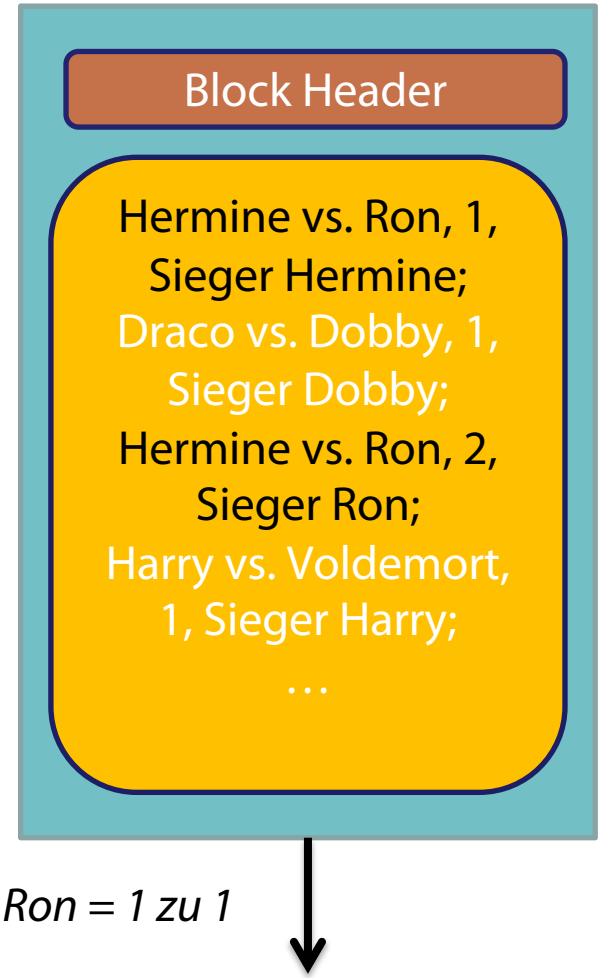
Beispiel Zaubererduell

Was enthält unserer **Block**?

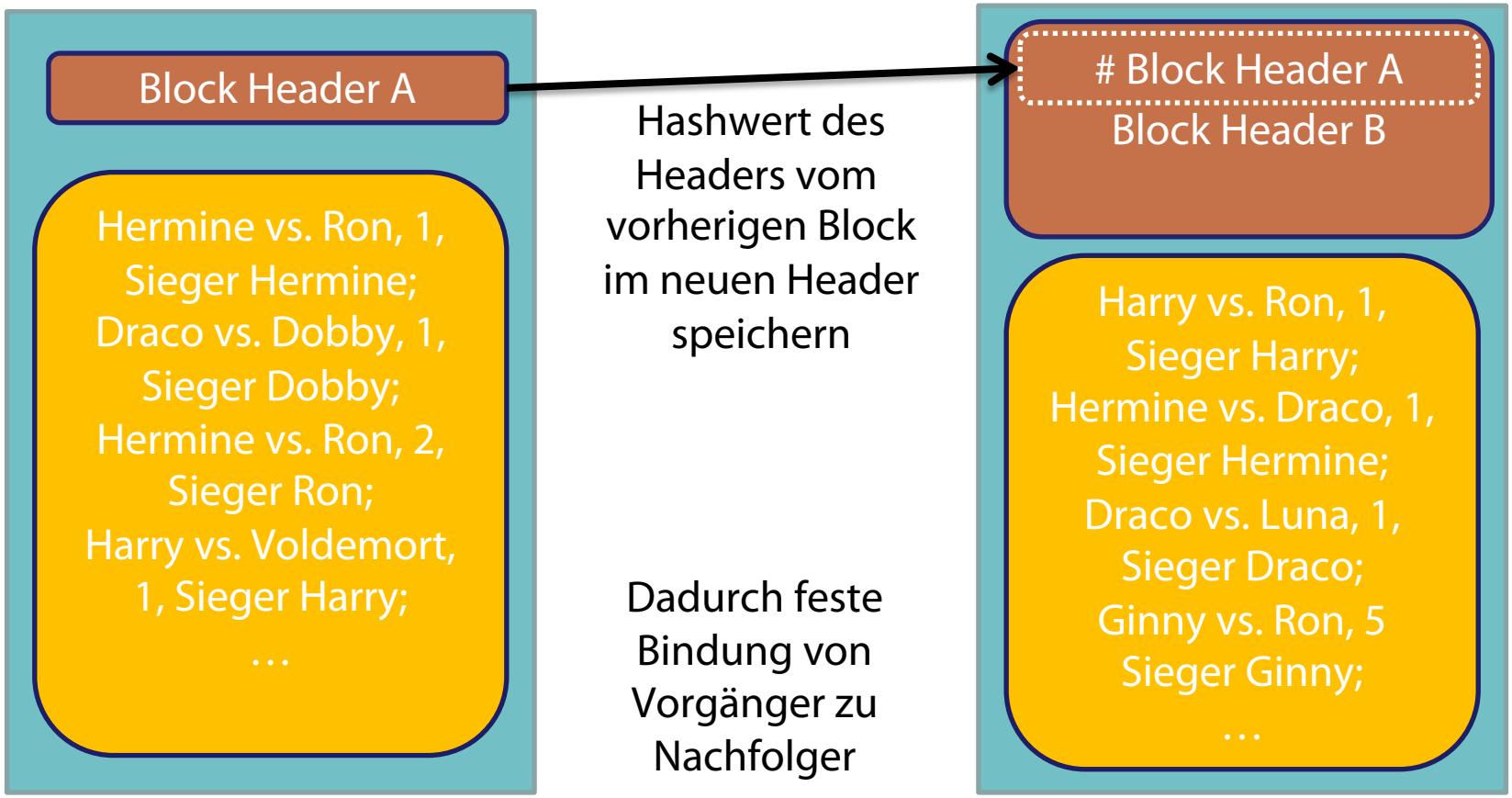
- Duelle zwischen 2 Zaubernden
- Sieger des Duells
- (Duellant A, Duellant B, DuellNr. zwischen Beteiligten, Sieger)

Was können wir damit **nachweisen**?

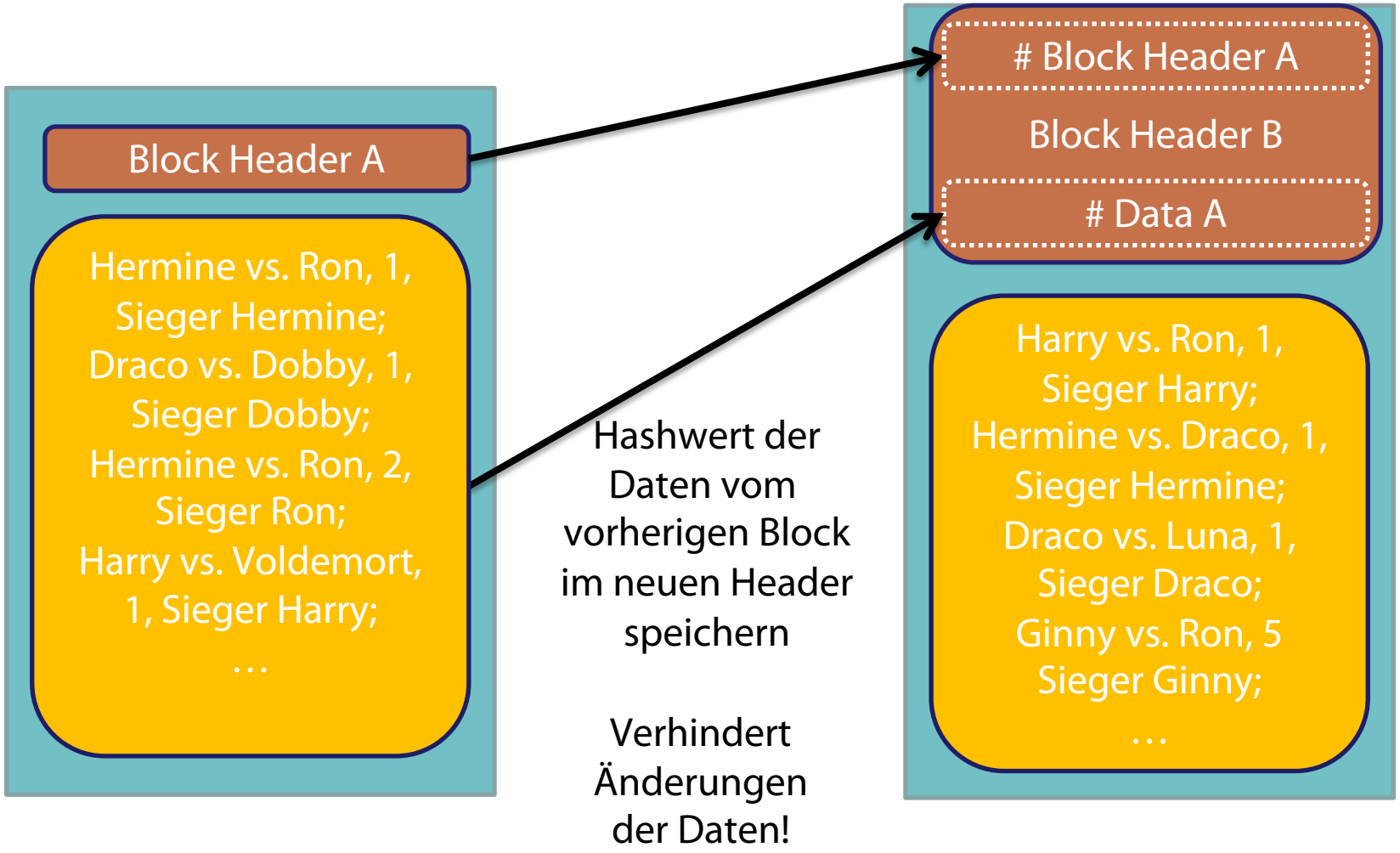
- Wer gegen Wen
- Häufigkeit Sieger/Verlierer über gesamte Kette



Wie sind die Blöcke verbunden?



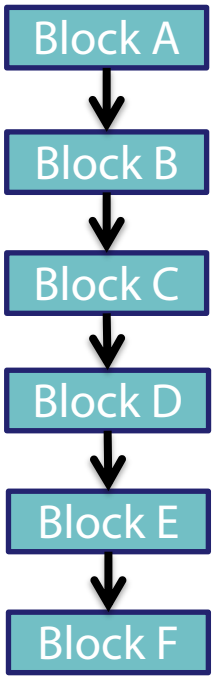
Wie sind die Blöcke verbunden?



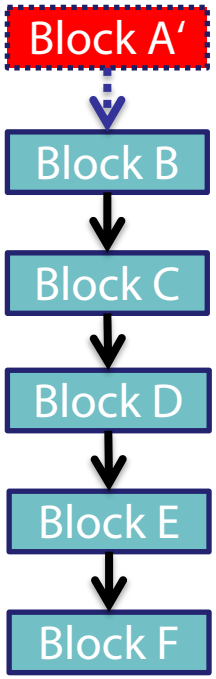
Kann Draco schummeln?

Problem: Verändere die Kette so, dass Draco in der Vergangenheit gewonnen hat.

Aktuelle Kette:



Dracos Kette:



Hashwert anders wegen veränderter Daten!
Block B erkennt seinen Vorgänger nicht an!

Schummeln am **Anfang** oder in der **Mitte** der Kette nicht möglich.

Was ist mit dem **Ende**?

Wer entscheidet über einen neuen Block?

Prinzipell: **JEDER** Teilnehmer an der Blockchain

Heißt in unserem Fall jeder Zaubernde, **ABER** es muss **Konsens** herrschen!

Wir brauchen somit ein dezentrales **Konsensverfahren**!
Häufig wird die sog. **Proof-of-Work-**Methode verwendet:

- Aufwendiger Arbeitsnachweis des Blockerstellers
- Einfache Prüfung für jeden anderen Teilnehmer

BEISPIEL: Ein neuer Block darf nur erstellt werden, wenn eine Abbildung des Blockinhalts auf einen Zauberspruch genannt werden kann, so dass z.B. der:

- Zauberspruch mit A anfängt,
- aus 2 Worten besteht und
- genau 2 Mal ‚v' enthält

Beispiel: **Avada Kedavra (man muss erst einmal viele Zauberspruchbücher durchsehen, um so eine Abbildung zu finden)**
Einfach zu prüfen, aber Abbildung aufwendig zu finden.

Anforderungen wechseln für jeden neuen Block, da neuer Inhalt gegeben

Erstellen eines neuen Blocks

1. **Verteile** alle neuen **Daten (bsp. [Harry, Draco, 3, Harry])** an alle bekannten Zauberer
2. Zauberer sammeln **Daten** in Blöcke und verteilen neue **Daten** weiter
3. Zauberer arbeiten am **Proof of Work**, um ihren Block zu veröffentlichen
4. Falls **Proof of Work** erfüllt, **verteile Block** an alle anderen bekannten Zauberer
5. Andere Zauberer **akzeptieren** den **Block** oder stellen **ungültige*** Daten fest
6. **Akzeptanz** wird durch Erstellung eines **Nachfolgeblocks** an den neuen Block ausgedrückt

** Was als ungültig angesehen wird, hängt auch von den Daten ab. In unserem Beispiel :*

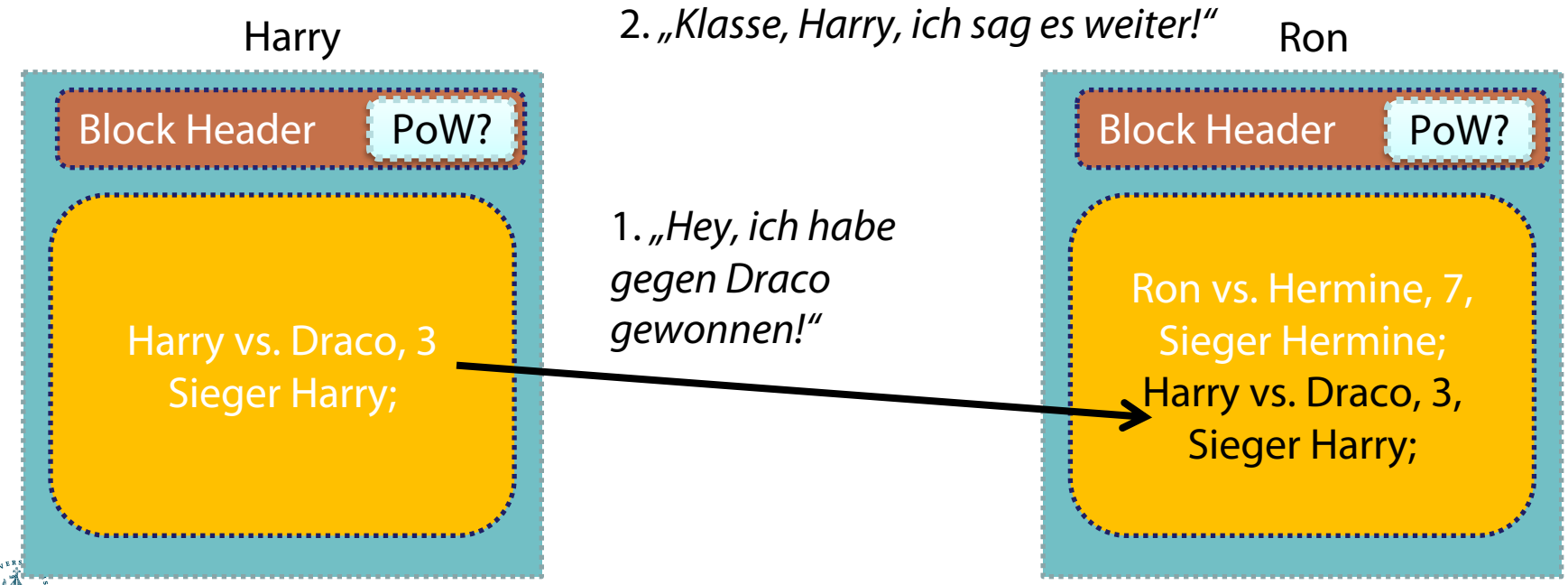
- *Duell gegen sich selbst verboten*
- *Duell mit 2 Siegern/Verlierern (keine doppelte Version eines Duells)*
- *Lücke/Reihenfolge falsch (Duell 3 vor 2, Wo ist Duell 1?)*

Schritte aus https://bitcoin.org/bitcoin.pdf

Erstellen eines neuen Blocks

1. **Verteile** alle neuen **Daten (bsp. [Harry, Draco, 3, Harry])** an alle bekannten Zauberer
2. Zauberer sammeln **Daten** in Blöcke und verteilen neue **Daten** weiter

3. Zauberer arbeiten am **Proof of Work**, um ihren Block zu veröffentlichen
4. Falls **Proof of Work** erfüllt, **verteile Block** an alle anderen bekannten Zauberer
5. Andere Zauberer **akzeptieren** den **Block** oder stellen ungültige Daten fest
6. **Akzeptanz** wird durch Erstellung eines **Nachfolgeblocks** an den neuen Block ausgedrückt

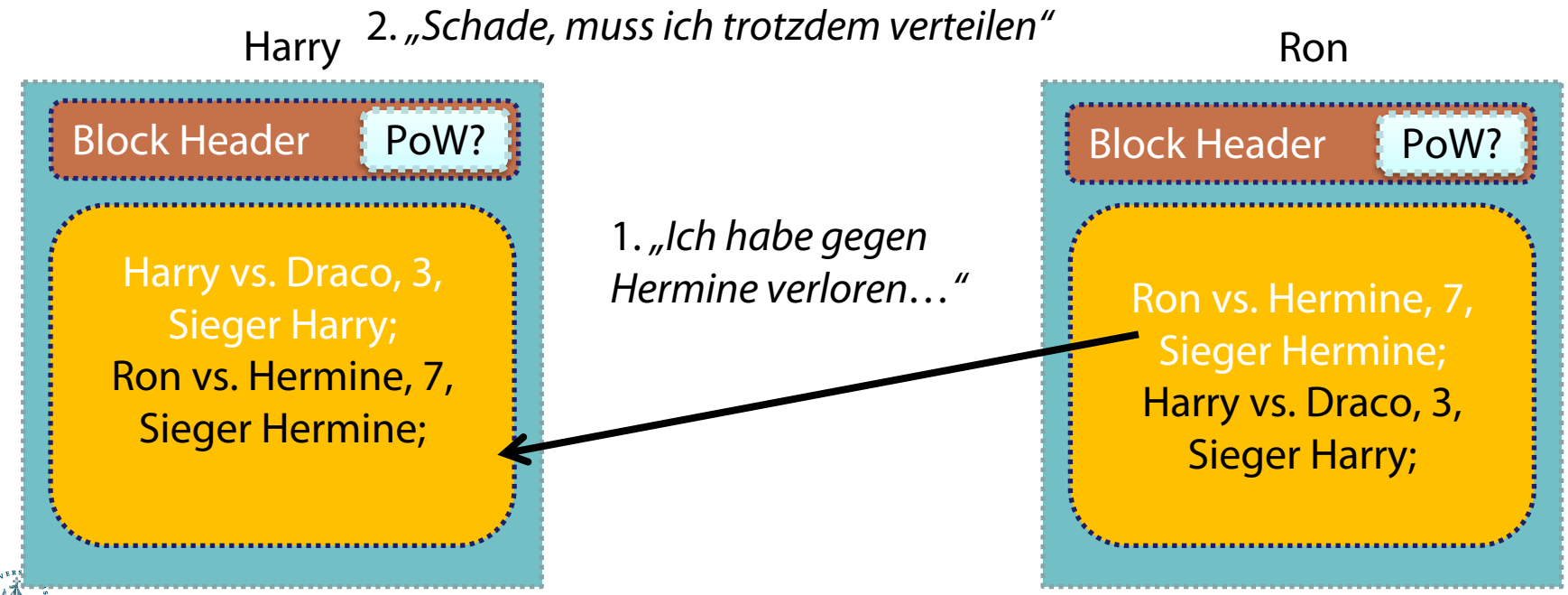


Schritte aus https://bitcoin.org/bitcoin.pdf

Erstellen eines neuen Blocks

1. **Verteile** alle neuen **Daten (bsp. [Harry, Draco, 3, Harry])** an alle bekannten Zauberer
2. Zauberer sammeln **Daten** in Blöcke und verteilen neue **Daten** weiter

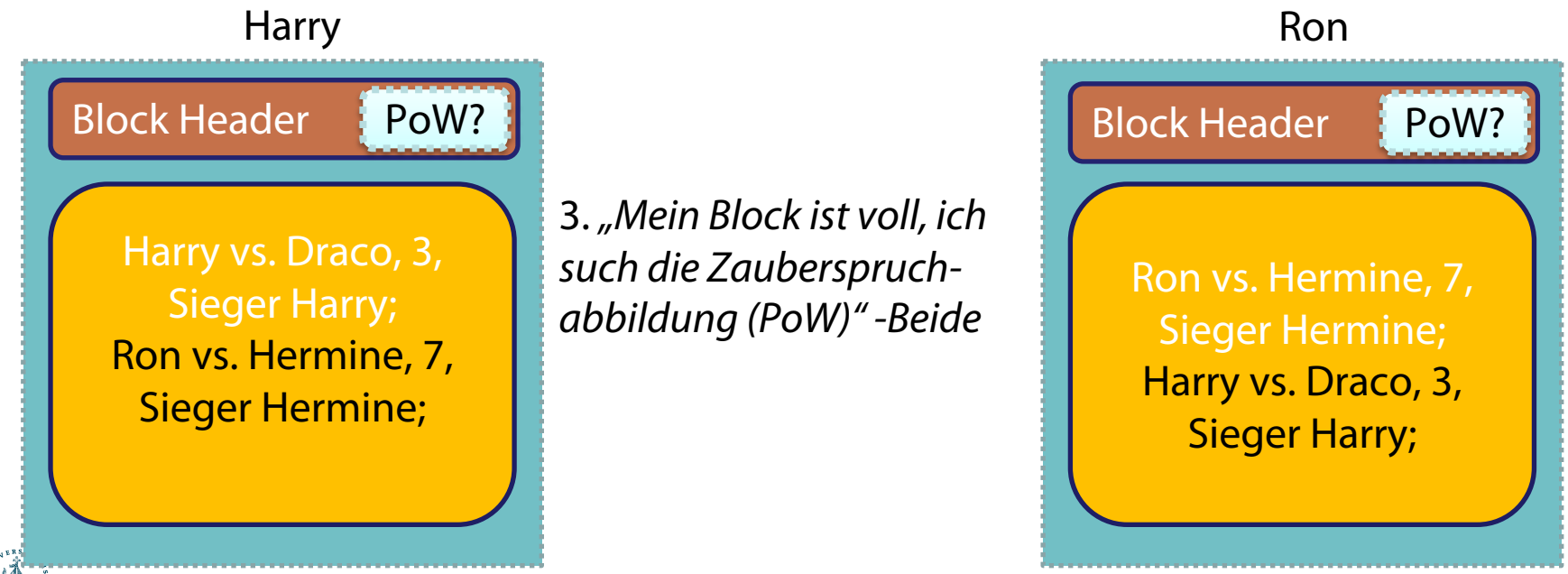
3. Zauberer arbeiten am **Proof of Work**, um ihren Block zu veröffentlichen
4. Falls **Proof of Work** erfüllt, **verteile Block** an alle anderen bekannten Zauberer
5. Andere Zauberer **akzeptieren** den **Block** oder stellen invalide Daten fest
6. **Akzeptanz** wird durch Erstellung eines **Nachfolgeblocks** an den neuen Block ausgedrückt



Schritte aus https://bitcoin.org/bitcoin.pdf

Erstellen eines neuen Blocks

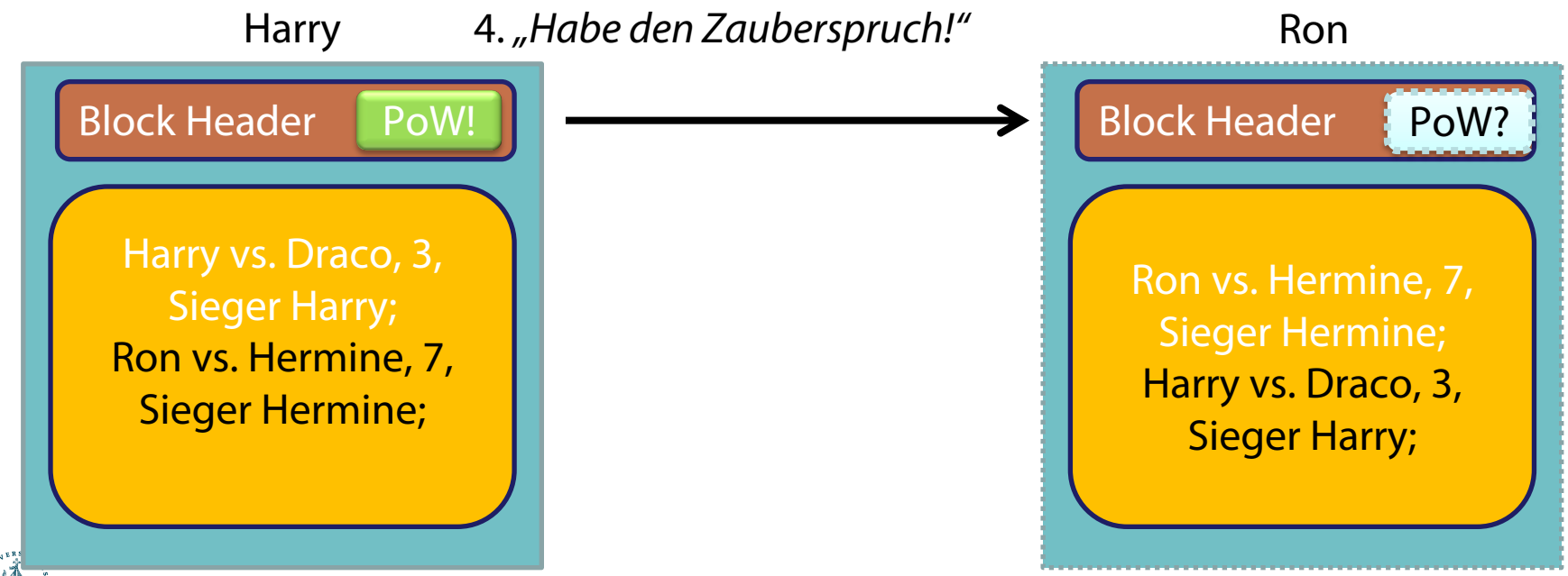
1. **Verteile** alle neuen **Daten (bsp. [Harry, Draco, 3, Harry])** an alle bekannten Zauberer
2. Zauberer sammeln **Daten** in Blöcke und verteilen neue **Daten** weiter
3. Zauberer arbeiten am **Proof of Work**, um ihren Block zu veröffentlichen
4. Falls **Proof of Work** erfüllt, **verteile Block** an alle anderen bekannten Zauberer
5. Andere Zauberer **akzeptieren** den **Block** oder stellen invalide Daten fest
6. **Akzeptanz** wird durch Erstellung eines **Nachfolgeblocks** an den neuen Block ausgedrückt



Schritte aus https://bitcoin.org/bitcoin.pdf

Erstellen eines neuen Blocks

1. **Verteile** alle neuen **Daten (bsp. [Harry, Draco, 3, Harry])** an alle bekannten Zauberer
2. Zauberer sammeln **Daten** in Blöcke und verteilen neue **Daten** weiter
3. Zauberer arbeiten am **Proof of Work**, um ihren Block zu veröffentlichen
4. Falls **Proof of Work** erfüllt, **verteile Block** an alle anderen bekannten Zauberer
5. Andere Zauberer **akzeptieren** den **Block** oder stellen invalide Daten fest
6. **Akzeptanz** wird durch Erstellung eines **Nachfolgeblocks** an den neuen Block ausgedrückt



Schritte aus https://bitcoin.org/bitcoin.pdf

Erstellen eines neuen Blocks

1. **Verteile** alle neuen **Daten (bsp. [Harry, Draco, 3, Harry])** an alle bekannten Zauberer
2. Zauberer sammeln **Daten** in Blöcke und verteilen neue **Daten** weiter
3. Zauberer arbeiten am **Proof of Work**, um ihren Block zu veröffentlichen
4. Falls **Proof of Work** erfüllt, **verteile Block** an alle anderen bekannten Zauberer

5. Andere Zauberer **akzeptieren** den **Block** oder stellen invalide Daten fest
6. **Akzeptanz** wird durch Erstellung eines **Nachfolgeblocks** an den neuen Block ausgedrückt

Schritte aus https://bitcoin.org/bitcoin.pdf

Wie sieht ein realer Proof of Work aus?

Es wird ein Ziel festgelegt, das vom Hashwert erfüllt werden muss,
beispielweise:

Hashfunktion(Header, Daten, RandomNumber) < Ziel

Da **Header** und **Daten** vorgegeben sind, kann nur die **RandomNumber** verändert werden.

Nach längerem ‚**Raten**' kann eine Lösung gefunden werden.

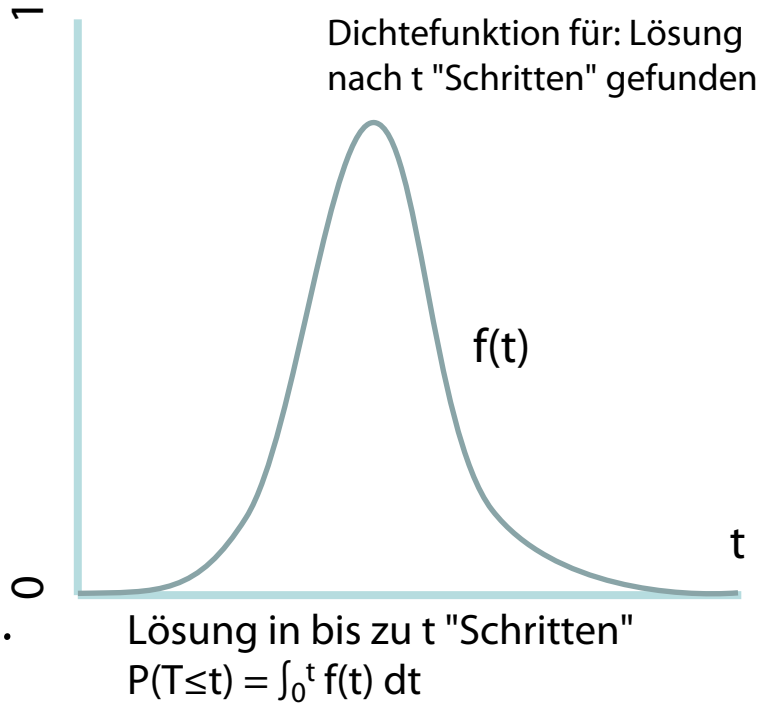
*Hashfunktion(4EF…, 3GH…, **1**) < 100…*

*Hashfunktion(4EF…, 3GH…, **2**) < 100…*

*Hashfunktion(4EF…, 3GH…, **3**) < 100…*

…

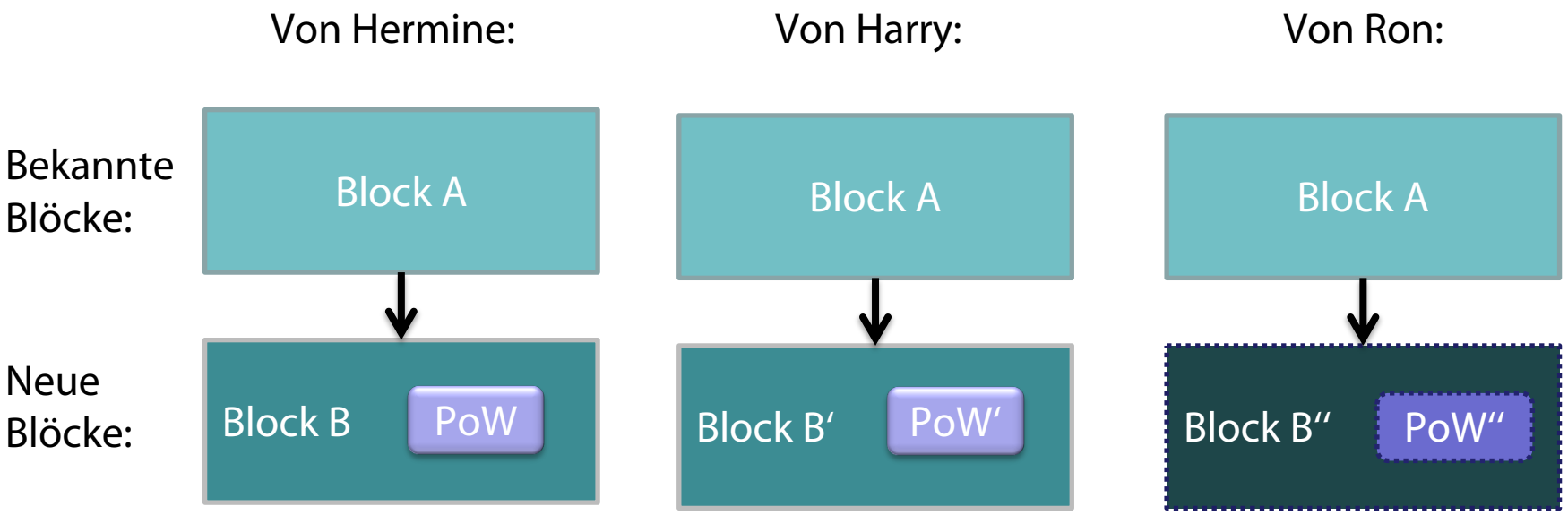
*Hashfunktion(4EF…, 3GH…, **578.321**) < 100…*



Welche Ketten werden übernommen?

Problem: Zauberer sind verteilt, d.h. Ketten können am Ende variieren, wenn viele Zaubernde einen neuen Block erstellen.

Welchen Block soll Ron wählen?

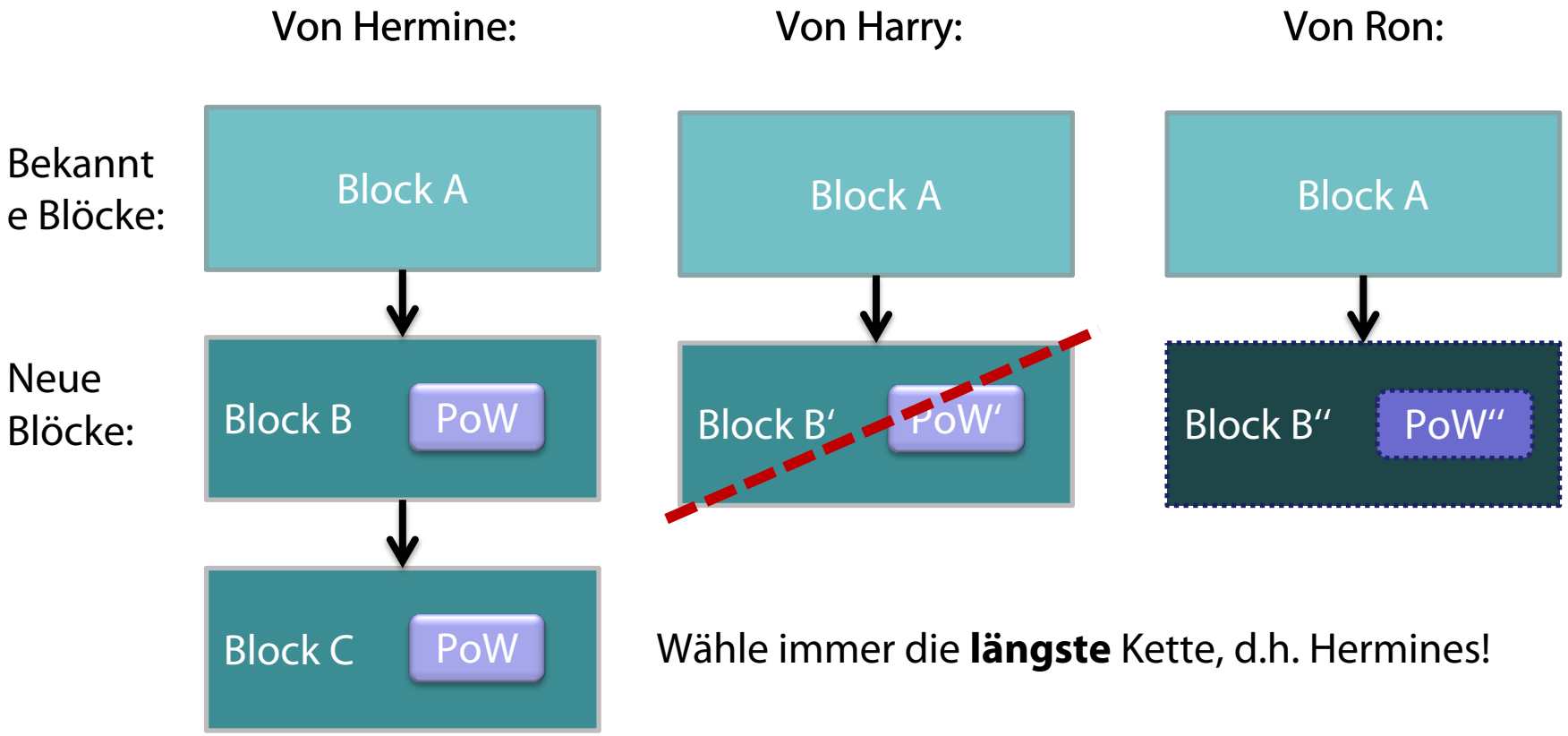


- PoW kann für beide Blöcke getestet werden
- Duelle sind konsistent und Blöcke gefüllt

→ Ron kann sich für einen von beiden entscheiden, denn noch ist keiner wirklich besser als der andere Block

Welche Ketten werden übernommen?

Problem: Zauberer sind verteilt, d.h. die Kette kann am Ende variieren, wenn viele Zaubernde einen neuen Block erstellen.



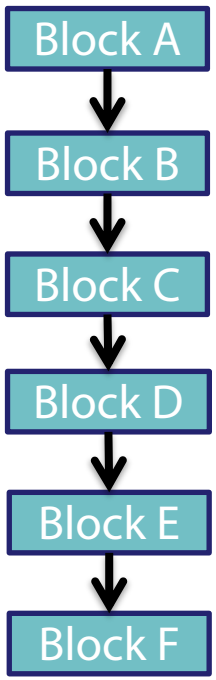
Wähle immer die **längste** Kette, d.h. Hermines!

Kann Draco schummeln? Neubetrachtung

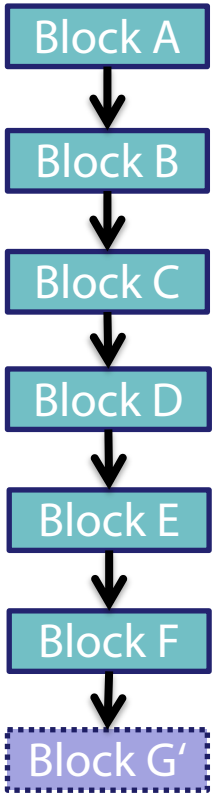
Draco kämpft gegen Harry, Harry gewinnt. Beide tragen Event in letzten Block ein

Problem: Verändere die Kette so, dass Draco in der Gegenwart gewonnen hat.

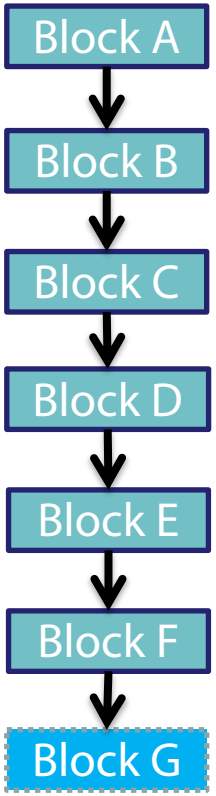
Aktuelle Kette:



Dracos Kette:



Harrys Kette:



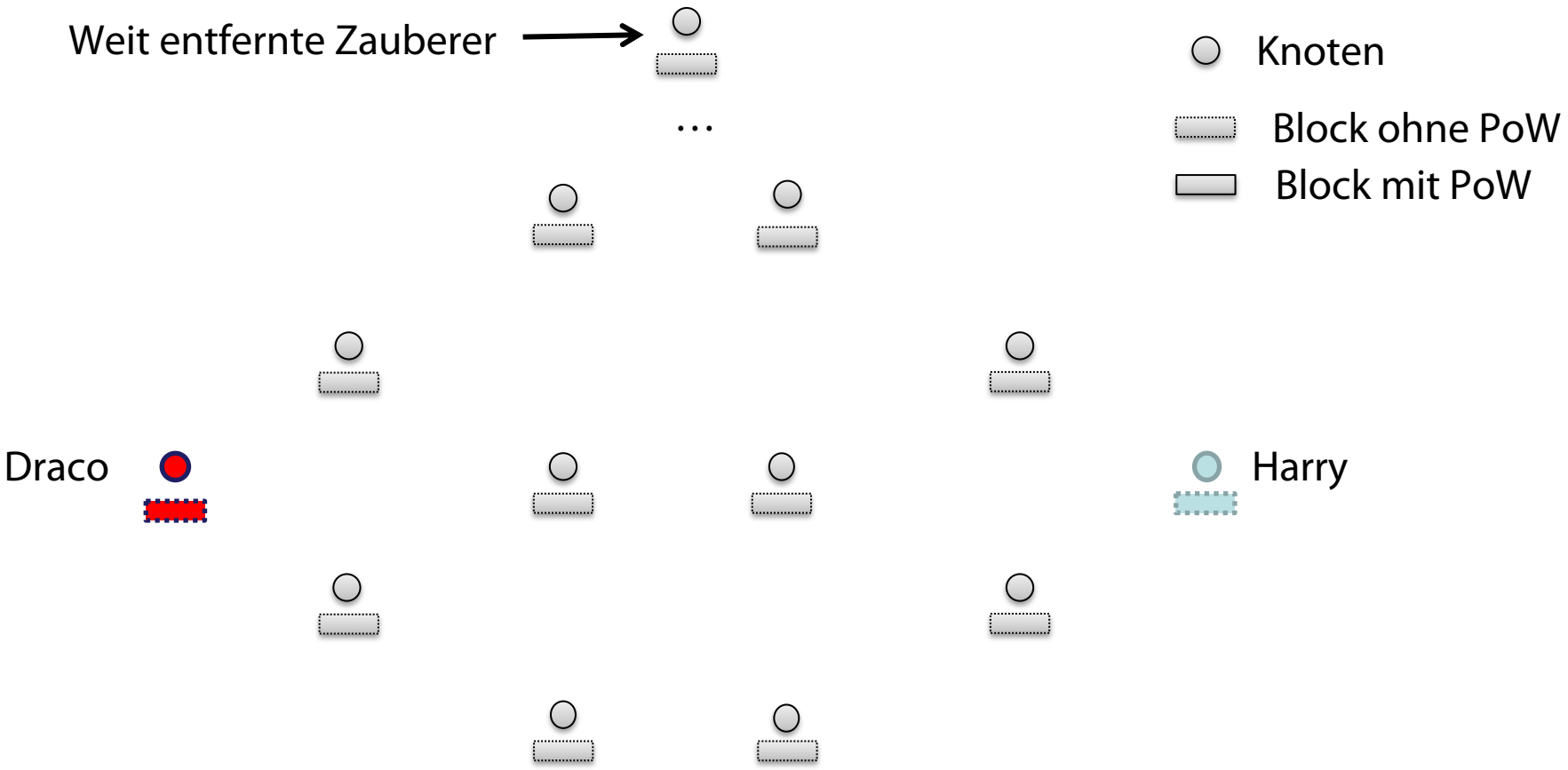
Draco muss erstmal einen PoW leisten, damit er seinen Block verteilen kann.

Draco muss schneller sein als Harry!

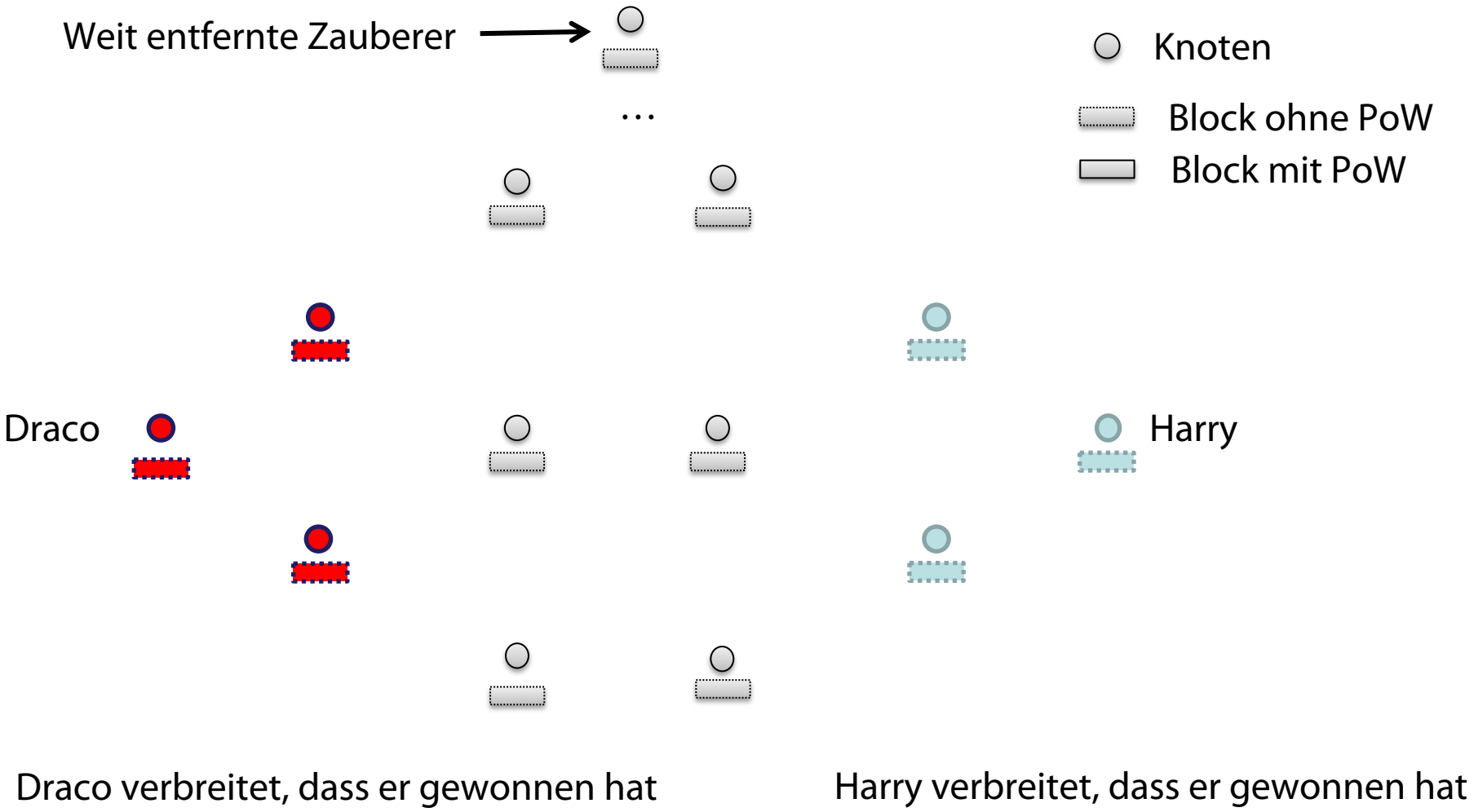
Gewinnchance: 50 zu 50*

*bei gleicher Reichweite im Netzwerk

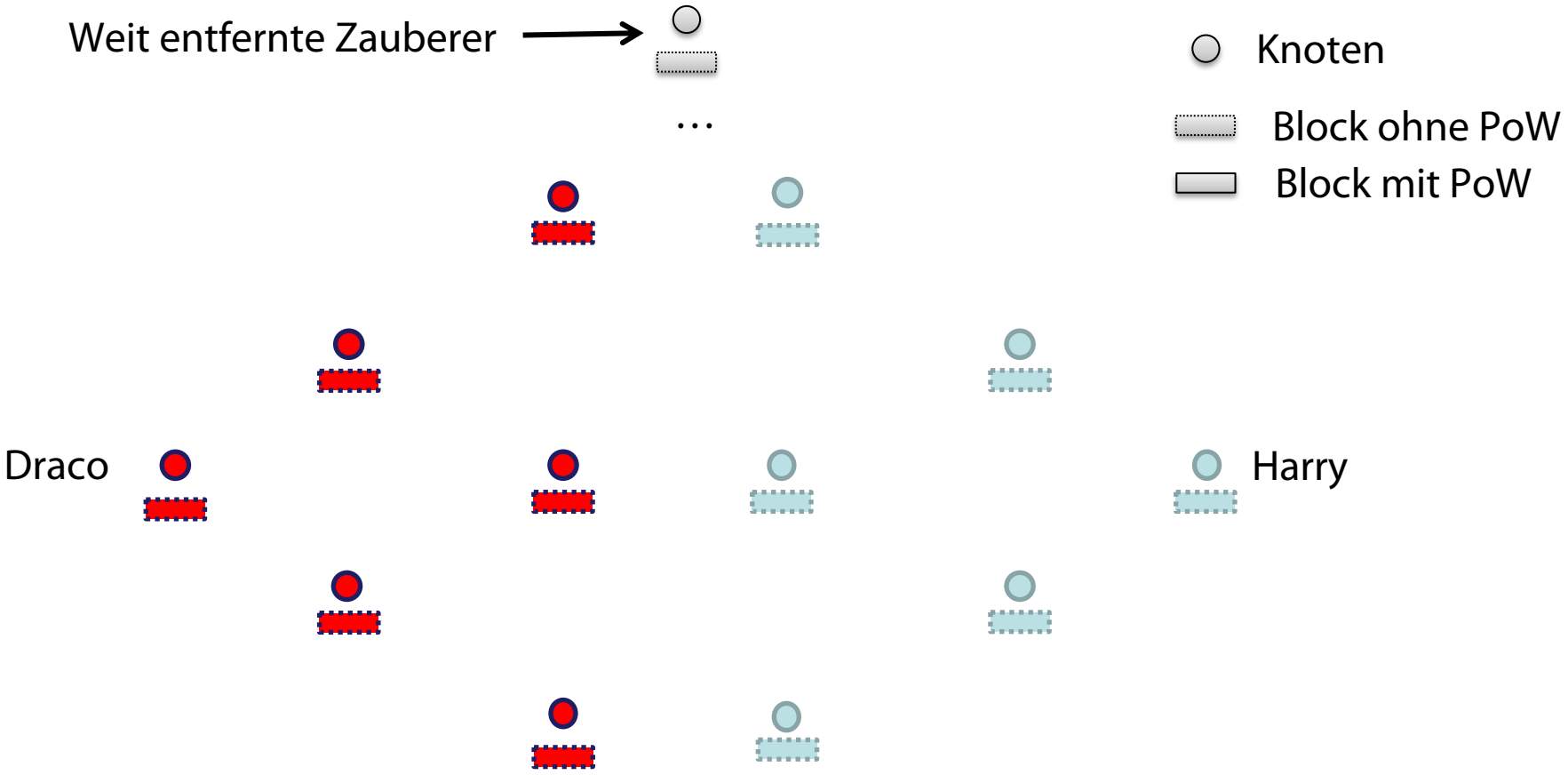
Kann Draco schummeln? Neubetrachtung



Kann Draco schummeln? Neubetrachtung

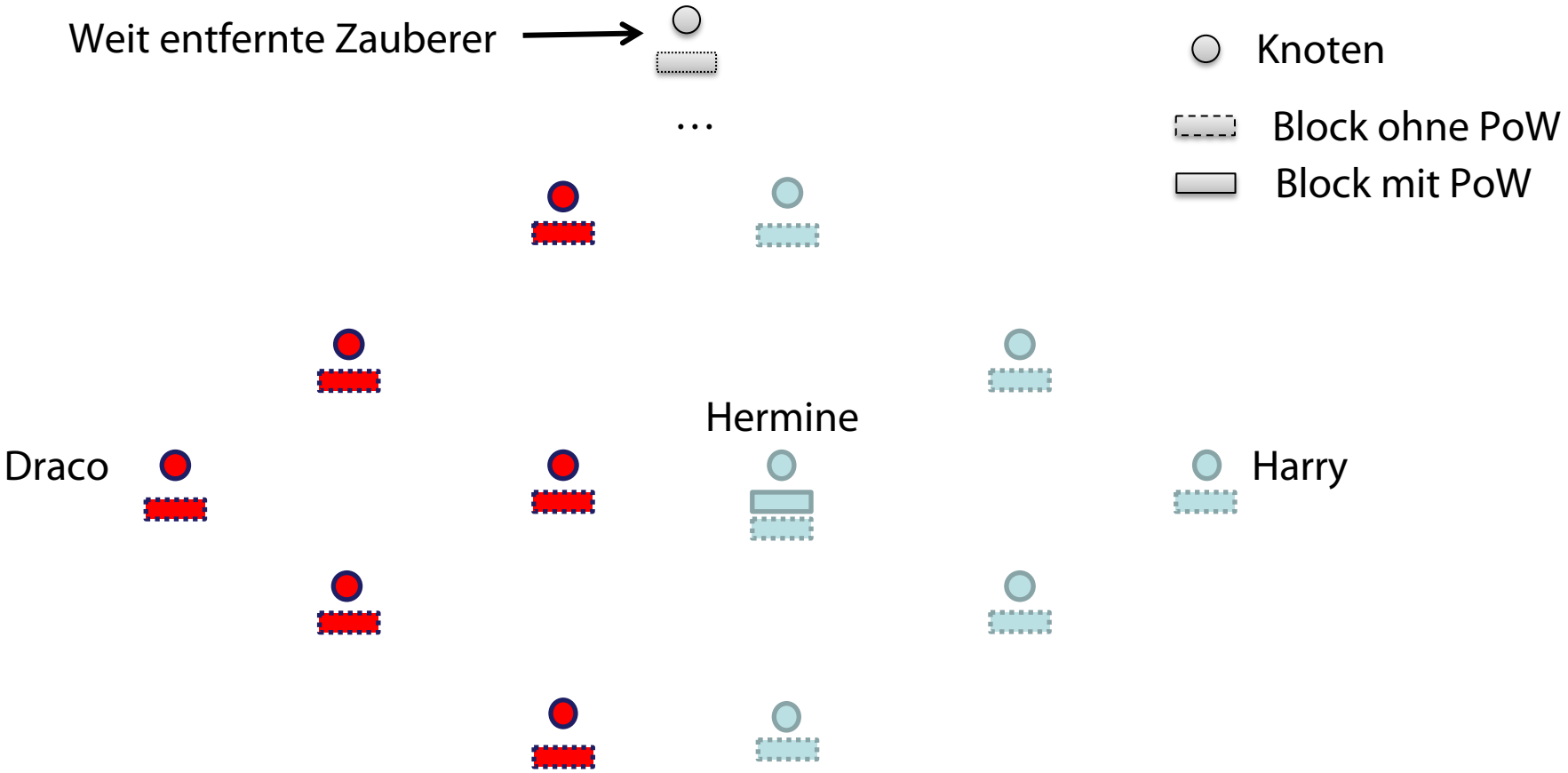


Kann Draco schummeln? Neubetrachtung



Es kann nur einen Sieger pro Duell geben!
Kein Knoten wird beide als Sieger in seinen Block aufnehmen.

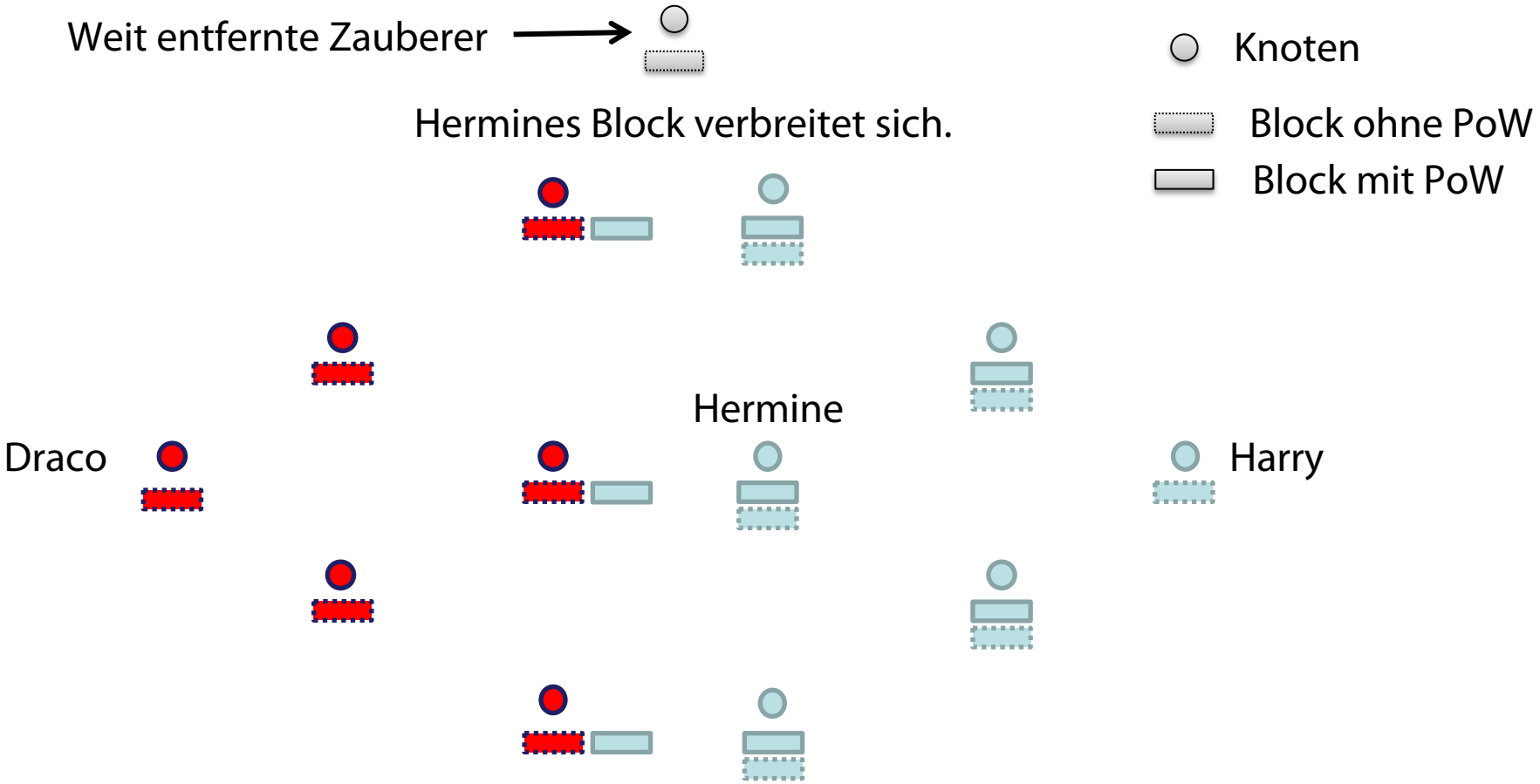
Kann Draco schummeln? Neubetrachtung



Der Knoten Hermine erfüllt den **Proof of Work** für Harrys Version.

Hermine arbeitet nun an Nachfolgeblock

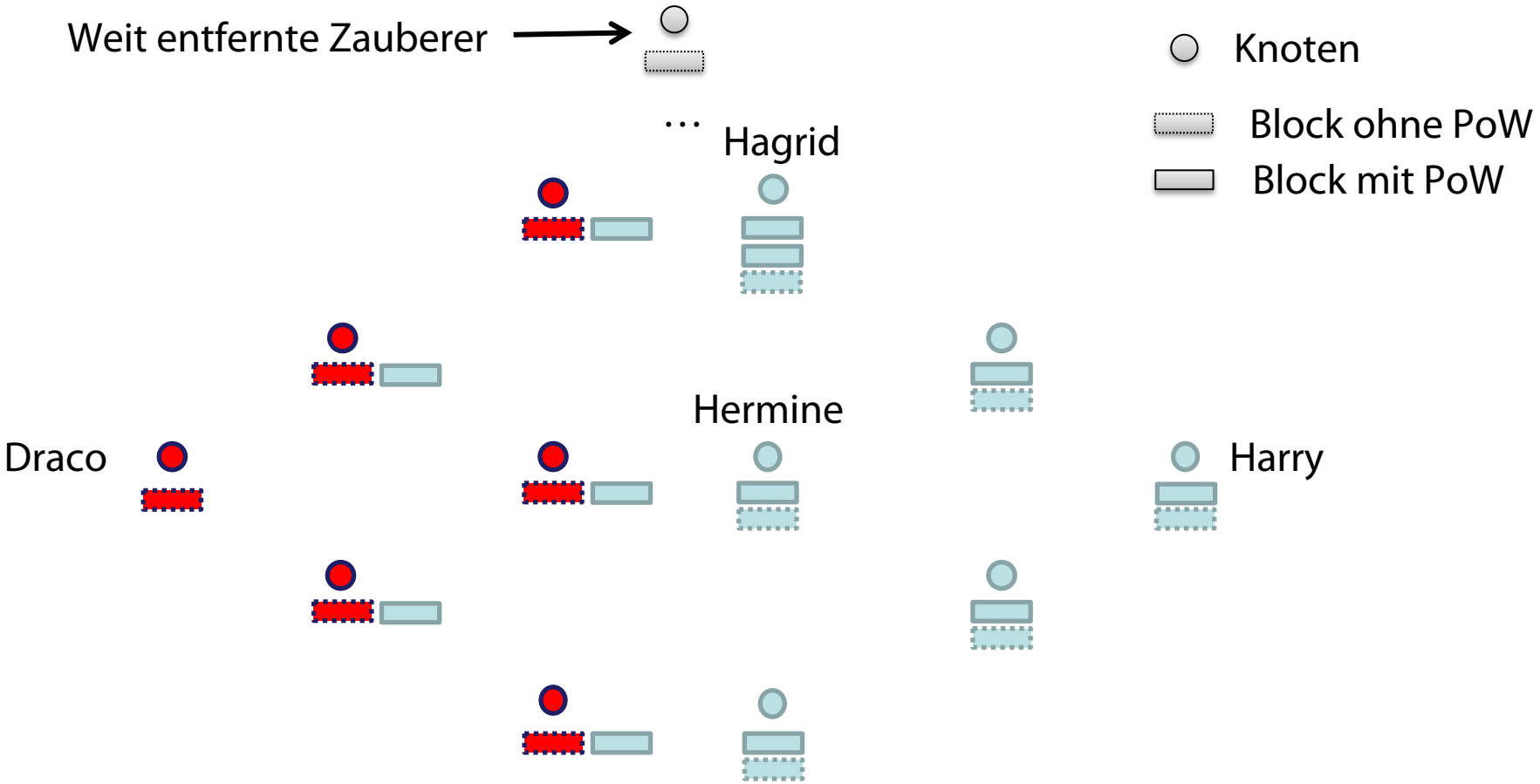
Kann Draco schummeln? Neubetrachtung



Gruppe Draco erhält Hermines Block, akzeptiert diesen aber nicht.

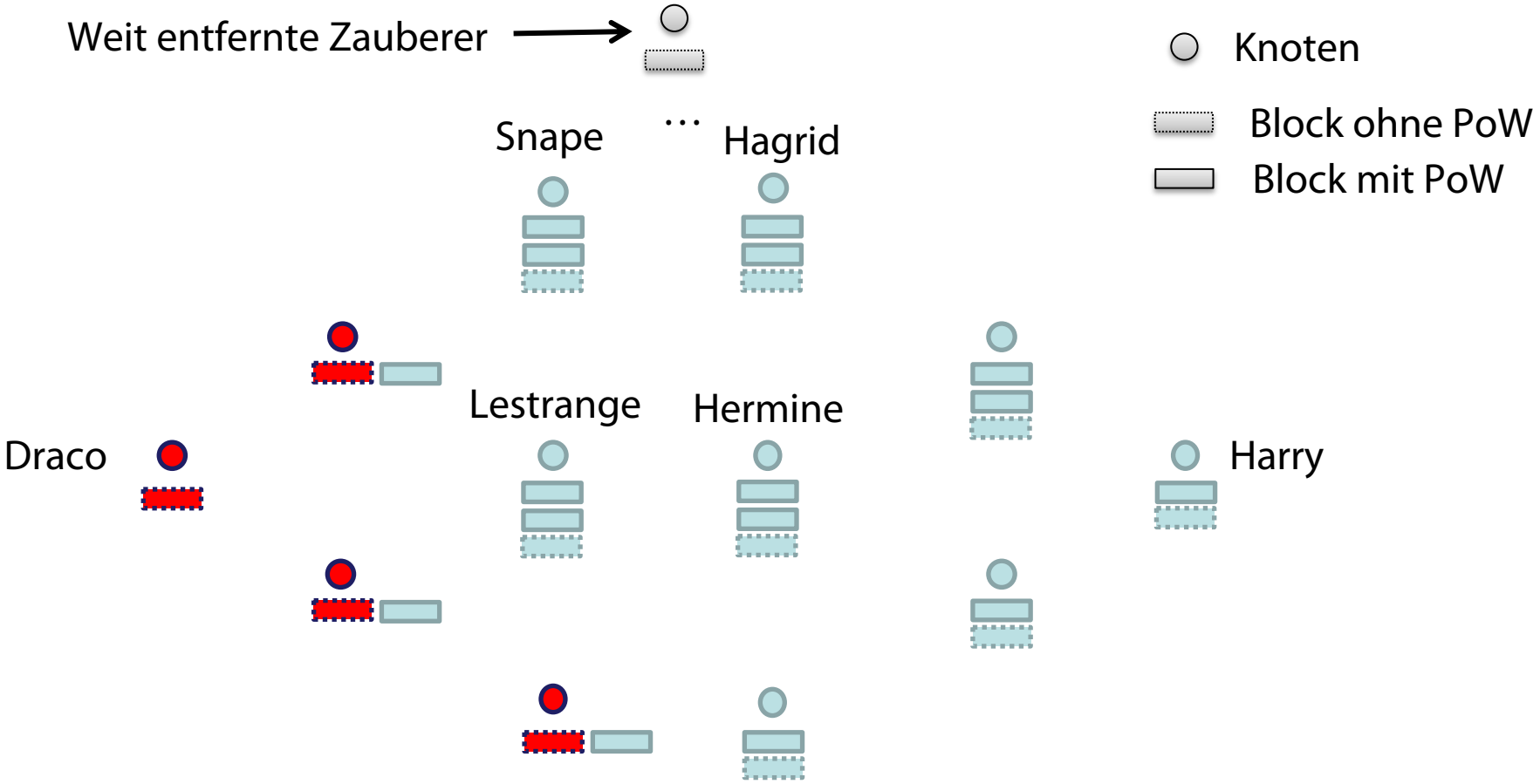
Gruppe Harry arbeitet nun an Nachfolgeblock

Kann Draco schummeln? Neubetrachtung



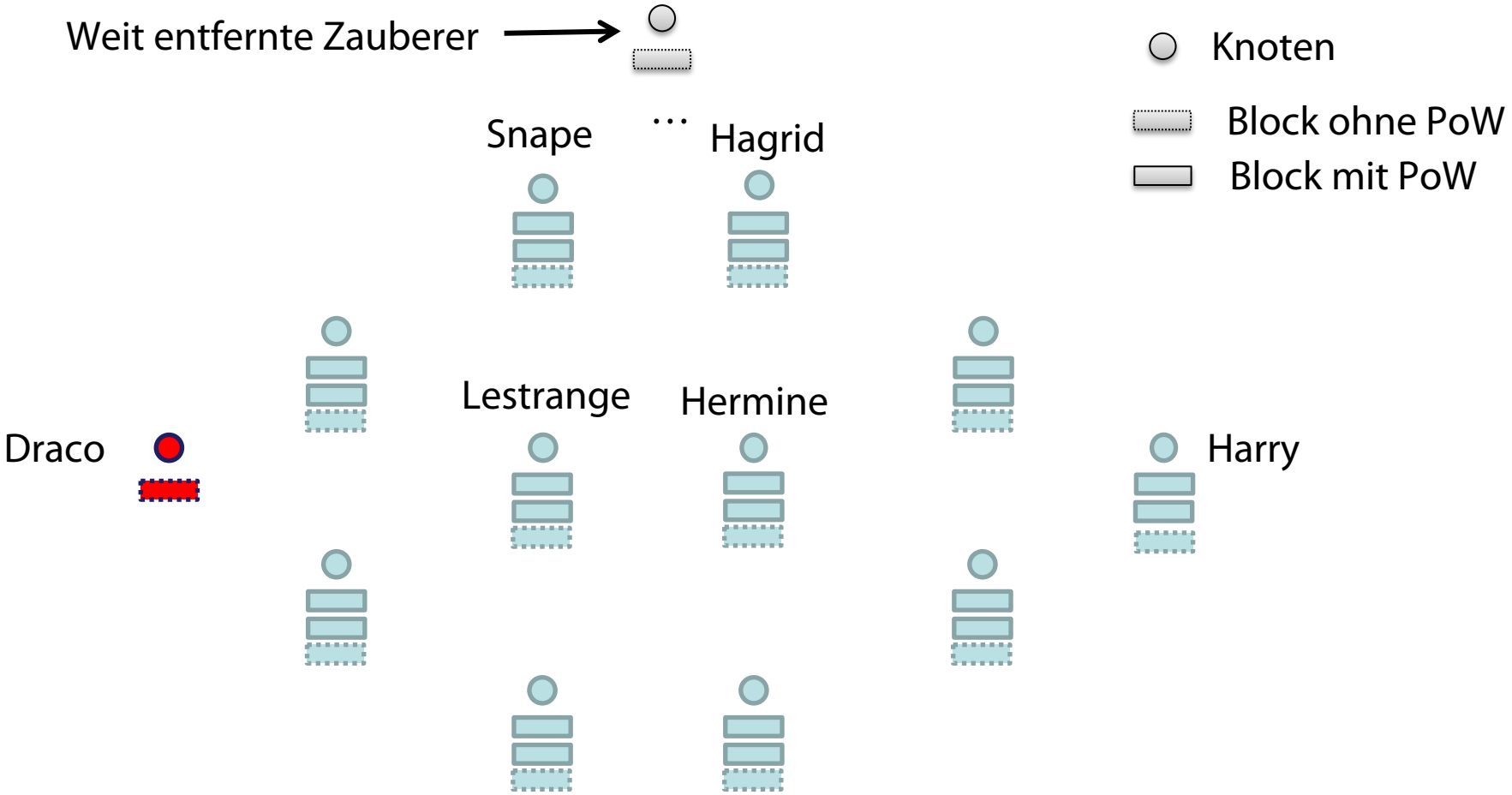
Hagrid erfüllt **Proof of Work** mit einem Block der auf Hermines aufbaut.

Kann Draco schummeln? Neubetrachtung



Snape und Lestrange erkennen längere Kette an und arbeiten nun an der Version in der Harry gewonnen hat.

Kann Draco schummeln? Neubetrachtung

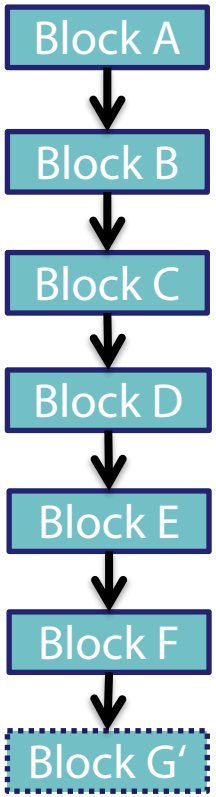


Es sieht schlecht aus für Draco…

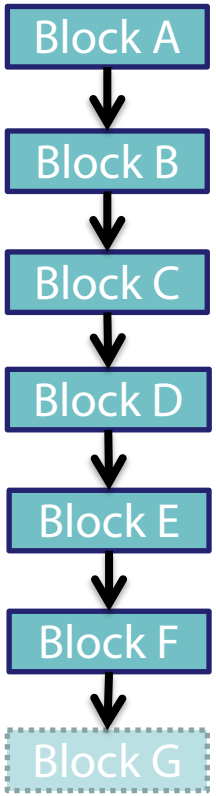
Kann Draco schummeln? Neubetrachtung

Problem: Verändere die Kette so, dass Draco in der Gegenwart gewonnen hat.

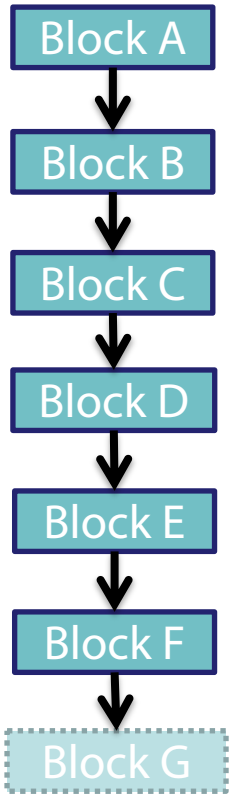
Dracos Kette:



Harrys Kette:



Kette von Dumbledore's Armee:

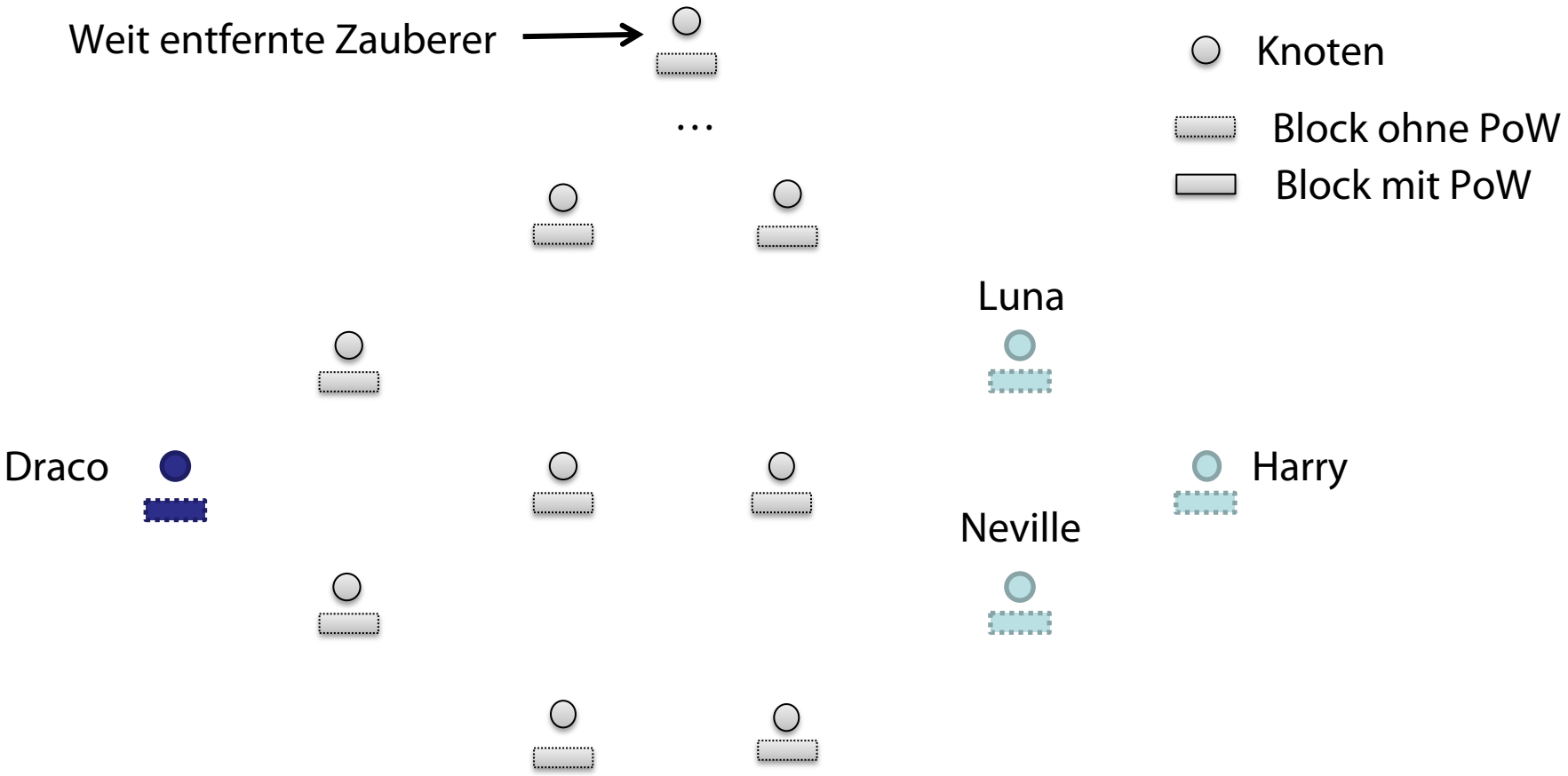


Wahrscheinlichkeit, dass einer der anderen Zauberer oder Harry seine Sicht veröffentlichen kann größer!

Plötzlich Rennen gegen viele andere!

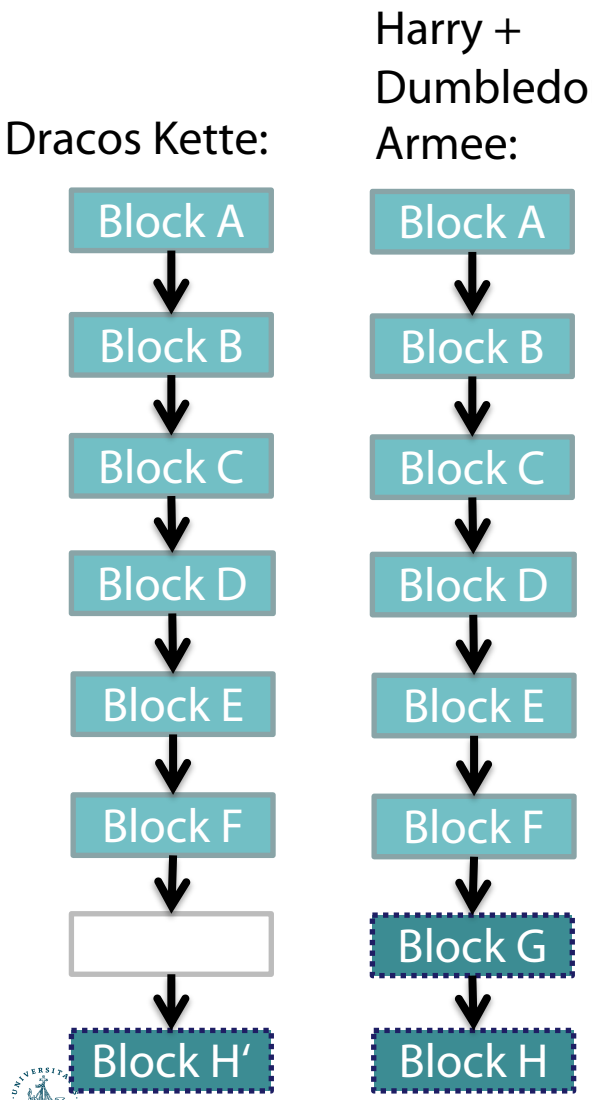
Dracos Chancen, einen neuen Block vor den anderen zu erstellen, sinken mit der Anzahl der anderen Beteiligten.

Kann Draco schummeln? Neubetrachtung



Schon von der Ausgangslage hat Draco ein Problem, hat aber trotzdem noch die Möglichkeit zu gewinnen

Kann Draco schummeln? Neubetrachtung



Problem: Verändere die Kette so, dass Draco in der Gegenwart gewonnen hat.

Draco hat trotzdem immer noch eine Chance seinen **Block G‘** zu verteilen.

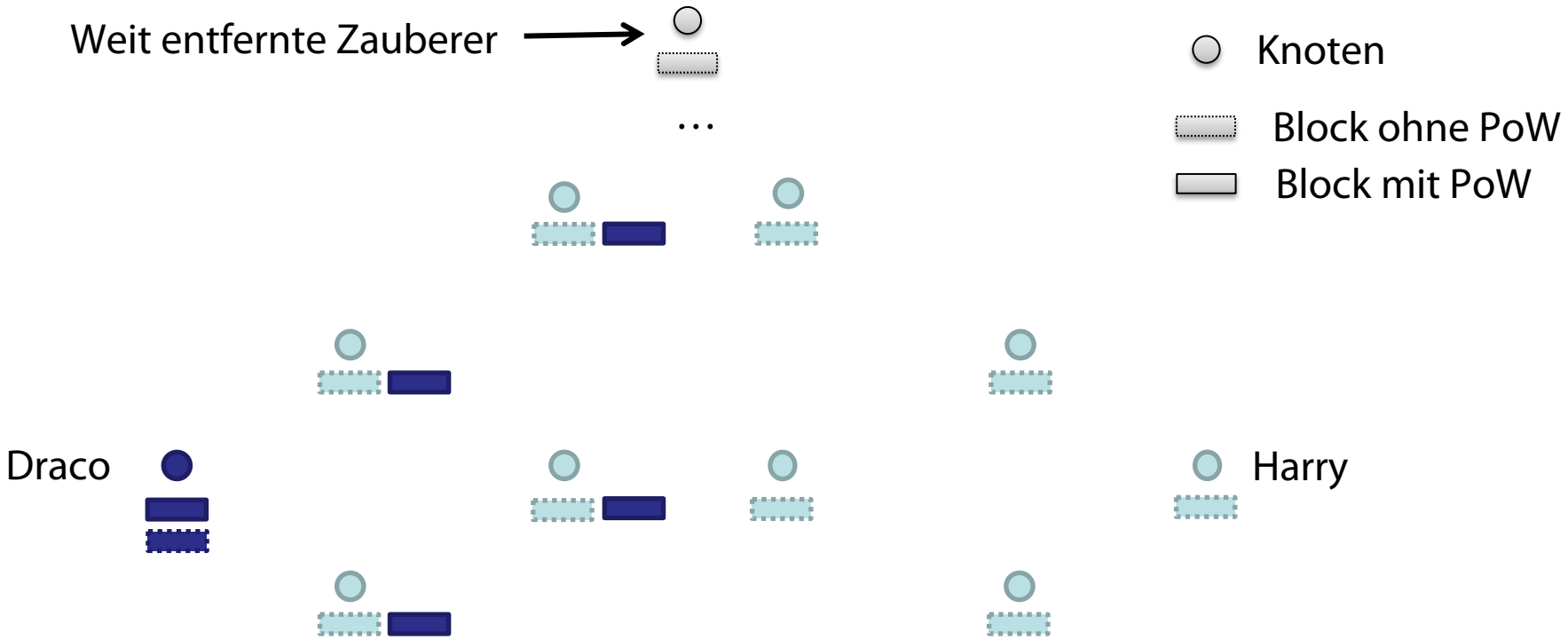
Damit ist der **Block H‘** durch den Hash allerdings anders als der von der anderen Gruppe.
Und Draco muss **erneut** seinen **Proof of Work** für diesen Block alleine leisten.

Die Wahrscheinlichkeit dafür, dass jemand aus Harrys Gruppe den **Proof of Work** für **G** und **H** findet, steigt mit der Anzahl der Teilnehmenden.

Dracos **G‘** würde verworfen, wenn die Blöcke **G** und **H** vor **H‘** veröffentlicht werden.

Mehrheiten haben bessere Chancen!

Kann Draco schummeln? Neubetrachtung



Trotz des Vorsprungs muss Draco alleine ein **Proof of Work** für den nächsten Block erfüllen, bevor der Rest umgestimmt wird.

Harrys Gruppe muss nachziehen, hat aber durch die Anzahl eine höhere Chance auf einen **Proof of Work.**

Wie sieht es mit CAP aus?

Konsistenz

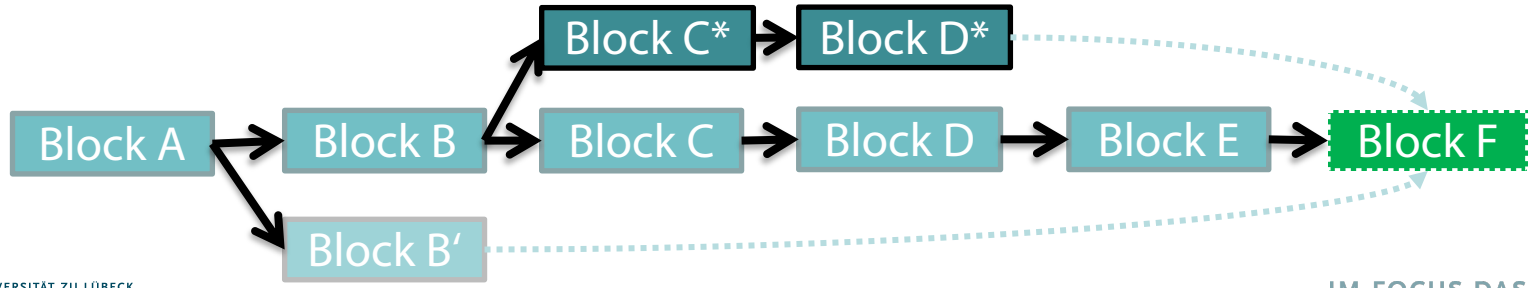
Pro:

- Neue Teilnehmer erhalten **immer** komplette Kette, heißt:
  - Eigenes Nachverfolgen **aller** Daten
  - **Anfang** und **Mitte** der Kette relativ sicher vor Veränderung
- Verworfene Blöcke können in neue Blöcke eingepflegt werden, um Transaktionen zu retten

Contra:

- Verteilung der Transaktionen, Proof of Work und Verteilung der Blöcke brauchen Zeit

Aussagen von unterschiedlichen Teilnehmern am **Ende** der Kette eher **inkonsistent**



Wie sieht es mit CAP aus?

Availability

Jeder Teilnehmende besitzt komplette Kette.
Direkte Antwort immer möglich

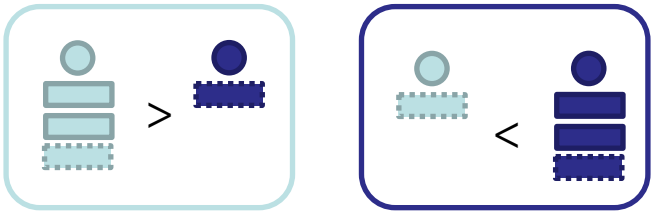
Knoten

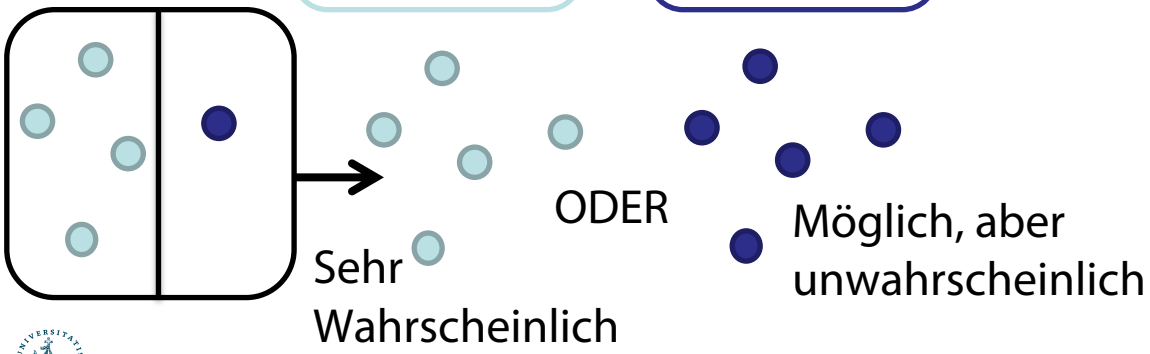
Block ohne PoW

Block mit PoW

Partitionierungstoleranz

Trennung in Subnetze möglich
Bei Wiedervereinigung setzt sich längste Kette durch





Damit ist eine Blockchain ein **AP**-System (AP/EC)!

Zusammenfassung

- Blockchains bestehen aus verketteten Blöcken, die **beliebige** Daten enthalten können.
- **Proof of Work** ermöglicht Konsensverfahren ohne zentrale Instanz und limitiert die neu generierten Blöcke.
- Die **längste** Kette gewinnt.
- Manipulation durch Hashverfahren innerhalb der Liste ausgeschlossen.
- Manipulation am **Ende** möglich, aber nur mit großer Mehrheit (>50%) erfolgsversprechend