Digitale Demokratie

13. September 2018, 18.00 Uhr, Impact Hub, Bern

Referat Dubuis

Mehr Informationen zur Vortragsreihe
bfh.ch/treffpunkt

Berner Fachhochschule

Medienpartner

BZ Berner Zeitung

Der Bund

Bringt die Blockchain das Vertrauen beim E-Voting?

- Prof. Dr. Eric Dubuis
- Departement Technik und Informatik
- Leiter des Research Institute for Security in the Information Society (RISIS)
- Mitbegründer des Swiss E-Voting Competence Center
- Forschung zu elektronischen Wahlen übers Internet

Was soll uns ein Wahlsystem garantieren?

«Demokratie»-Regeln:

- Nur Stimmen von Stimmberechtigten fliessen ins Resultat ein («Berechtigung»)
- Eine stimmberechtigte Person ←→ eine Stimme («Eine-Stimme-Eigenschaft»)
- Das Resultat ist erst nach Urnenschluss bekannt («Fairness»)

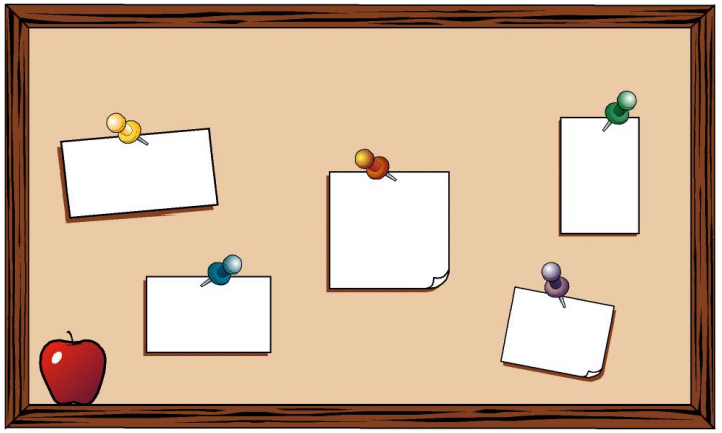
Regeln zum Schutz der Privatsphäre:

- Die Stimme ist geheim («Stimmgeheimnis»)
- Abstimmende Person kann nicht beweisen, wie sie gestimmt hat («keine Quittung»)

Verifizierbarkeit:

- Wurde meine Stimme richtig gezählt? («individuelle Verifizierbarkeit»)
- Wurden alle gültigen Stimmen gezählt? («universelle Verifizierbarkeit»)

Das elektronische Anschlagbrett



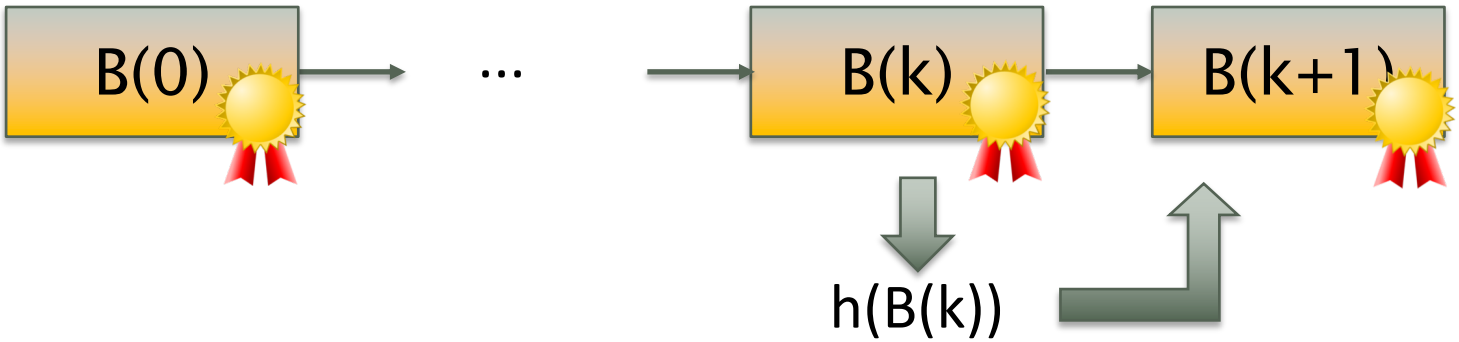
Publiziert Daten wie:

- Digitale Zertifikate mit öffentlichen Schlüsseln
- Wahldaten wie Kandidierende und Wahlberechtigte
- Eingetroffene, verschlüsselte und identifizierbare Stimmen
- Die verschlüsselten Stimmen nach der Entkopplung durch ein kryptografisches Mischnetzwerk (mit Beweisen)
- Die entschlüsselten Stimmen (mit Beweisen)
- Das Resultat

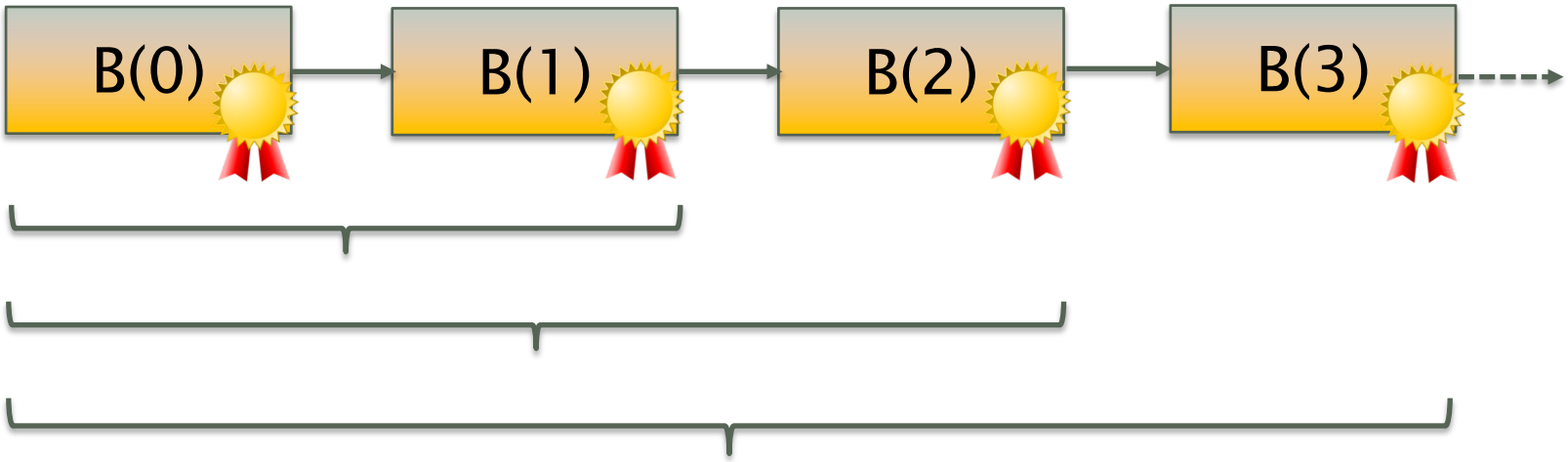
Das elektronische Anschlagbrett muss «fälschungssicher» sein!

Wie funktioniert das Anschlagbrett?

- Einträge können nur angefügt werden
- Die Vorgeschichte eines Eintrages wird kryptografisch an diesen gekoppelt:
  - Aus dem Eintrag und dem Hashwert des vorhergehenden «Blocks» wird ein digital signierter, neuer «Block» erstellt

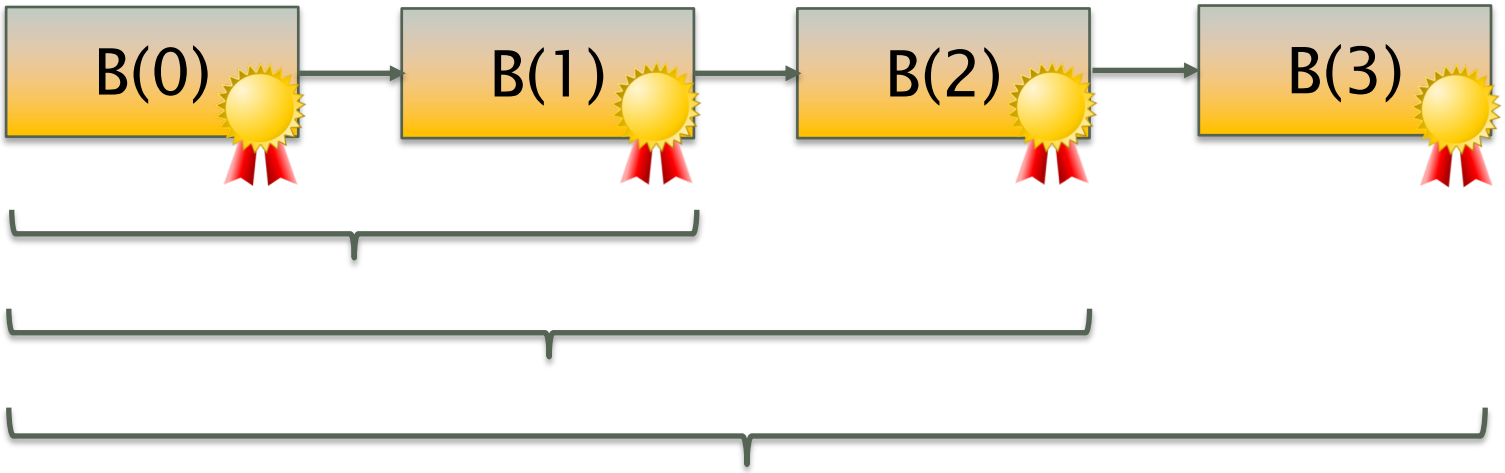


Verkettung der Blöcke veranschaulicht



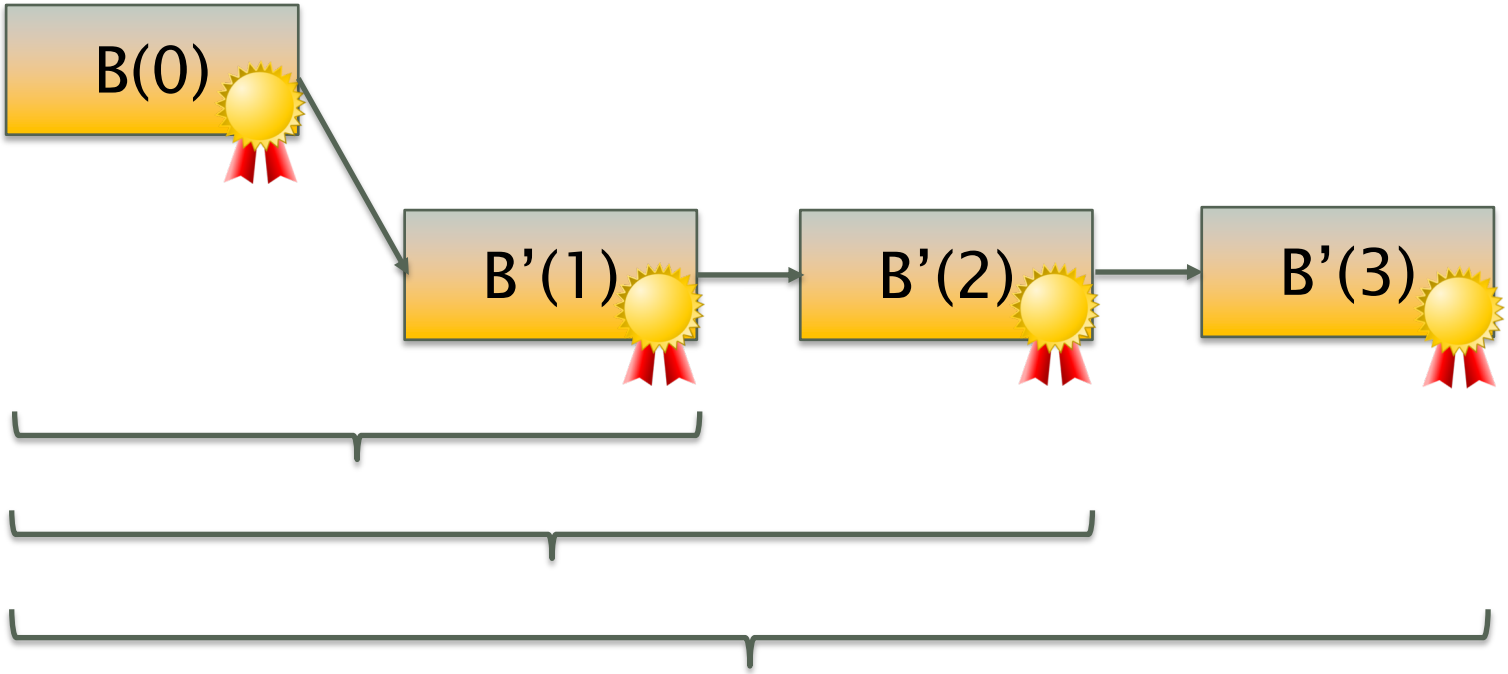
usw.

Kann die Geschichte nicht geändert werden?

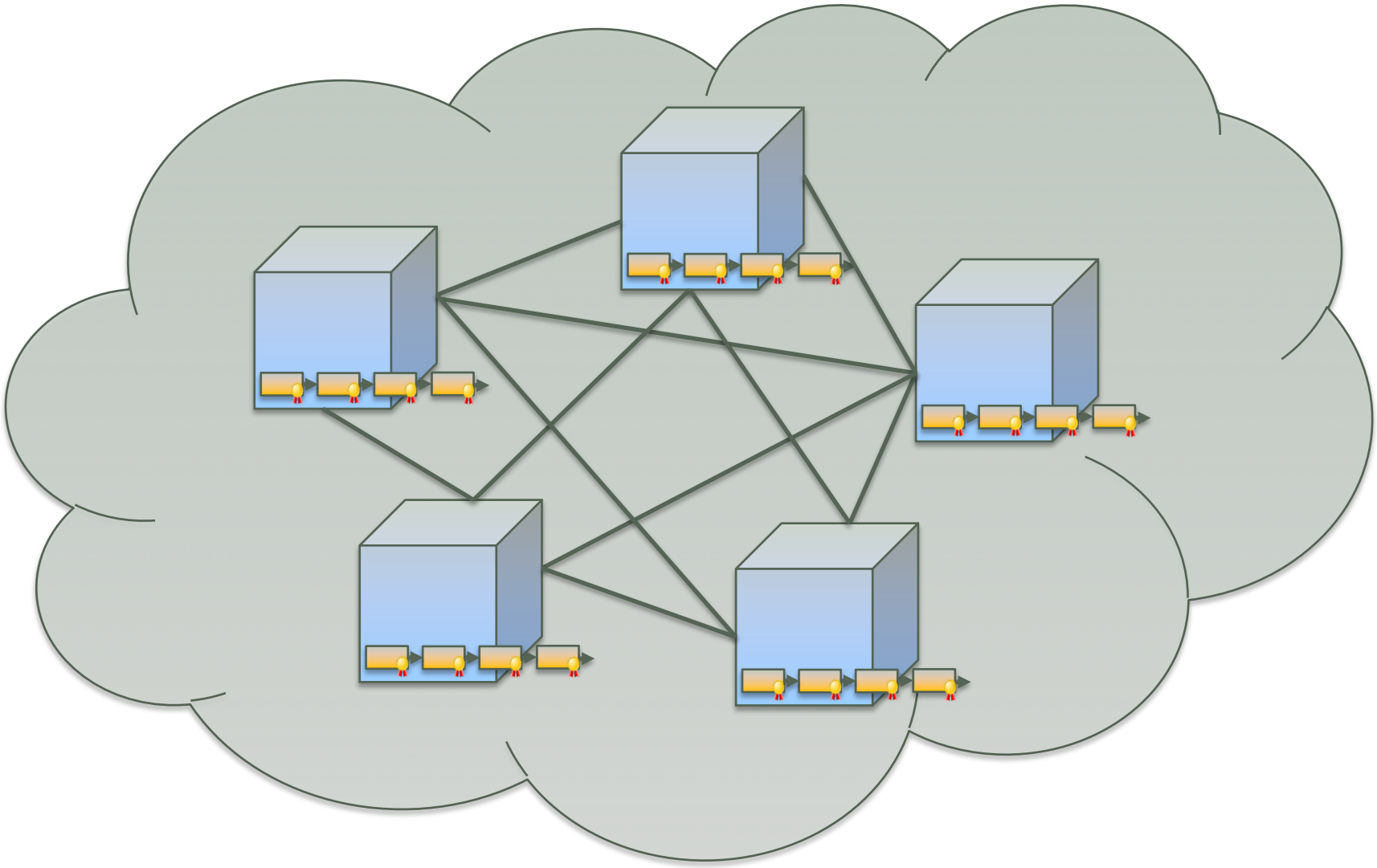


Kann die Geschichte nicht geändert werden?

Doch!



Verteilung der Blockchain auf viele Computer



Wie wird Konsens erreicht?

- Ein altes Informatik-Problem
- Im 2009 «erfindet» Satoshi Nakamoto (Pseudonym) eine neue Lösung:
- **Proof-of-Work**

Wie könnte die Blockchain beim E-Voting helfen?

- Die Blockchain hält alle Transaktionen unveränderbar fest
  - was wir uns beim E-Voting mit dem elektronischen Anschlagbrett wünschen («fälschungssicher»)
- Die Blockchain löst das sog. «*double spending*»-Problem
  - ähnliches Problem beim E-Voting: 1 Person ←→ 1 Stimme («Eine-Stimme-Eigenschaft»)
- In der Blockchain sind alle Daten für jedermann einsehbar
  - notwendige Bedingung für die «individuelle und universelle Verifikation»

Aber...

- Wie regelt man das Stimmrecht?
  - es bräuchte dennoch eine (zentrale) Autorität, die Wahlbehörde («Berechtigung»)
- Die Blockchain ist nicht *a priori* anonym, das Stimmgeheimnis ist nicht automatisch gewährt
  - eine zusätzliche Stufe zur Anonymisierung wäre notwendig («Stimmgeheimnis»)
- Das Stimmergebnis darf erst nach Urnenschluss ermittelbar sein
  - es bräuchte weiterhin einen Mechanismus, der das garantiert («Fairness»)

Fazit

- Die Blockchain garantiert ein «**fälschungssicheres**» Anschlagbrett, aber zu einem hohen Preis:
  - Latenzzeit
  - Energieverbrauch

- **Die Blockchain alleine löst das E-Voting-Problem nicht!**
  - Mechanismus für die «Berechtigung» wird benötigt
  - Mechanismus für die «Stimmgeheimnis» wird benötigt
  - Mechanismus für die «Fairness» wird benötigt

Fazit

- Die Blockchain garantiert ein «**fälschungssicheres**» Anschlagbrett, aber zu einem hohen Preis:
  - Latenzzeit
  - Energieverbrauch

- **Die Blockcha**
  - Mechanis
  - Mechanis
  - Mechanis

matt blaze @mattblaze · 5t

By the way, the committee agrees that blockchain has no role in civil elections. Time to stop this distracting nonsense and get on with the important work of securing or elections nationwide.

2 23 80

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Merci!

Wir diskutieren gerne weiter beim Apéro

www.societybyte.swiss