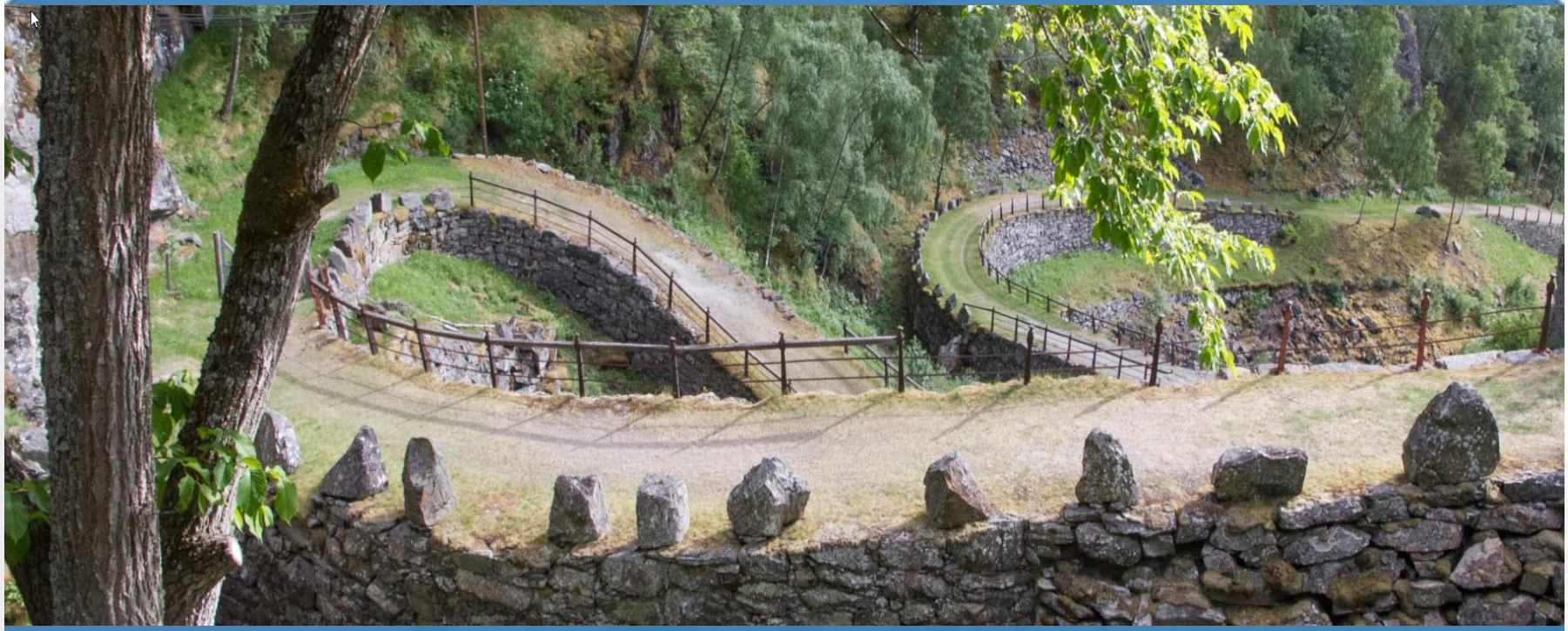


Bitcoin og blokk-kjedeteknologi - også for offentleg sektor

Svein Ølnes, Vestlandsforsking, 19. okt. 2017

WESTERN NORWAY RESEARCH INSTITUTE
VESTLANDSFORSKING
www.vestforsk.no

Bitcoin kan rasere velferdsstaten

En kryptovaluta gjør det enklere å risikofritt snyte på skatten, droppe å betale moms eller ta del i korrupsjon. Derfor skal vi frykte anonyme betalingsmidler som Bitcoin.

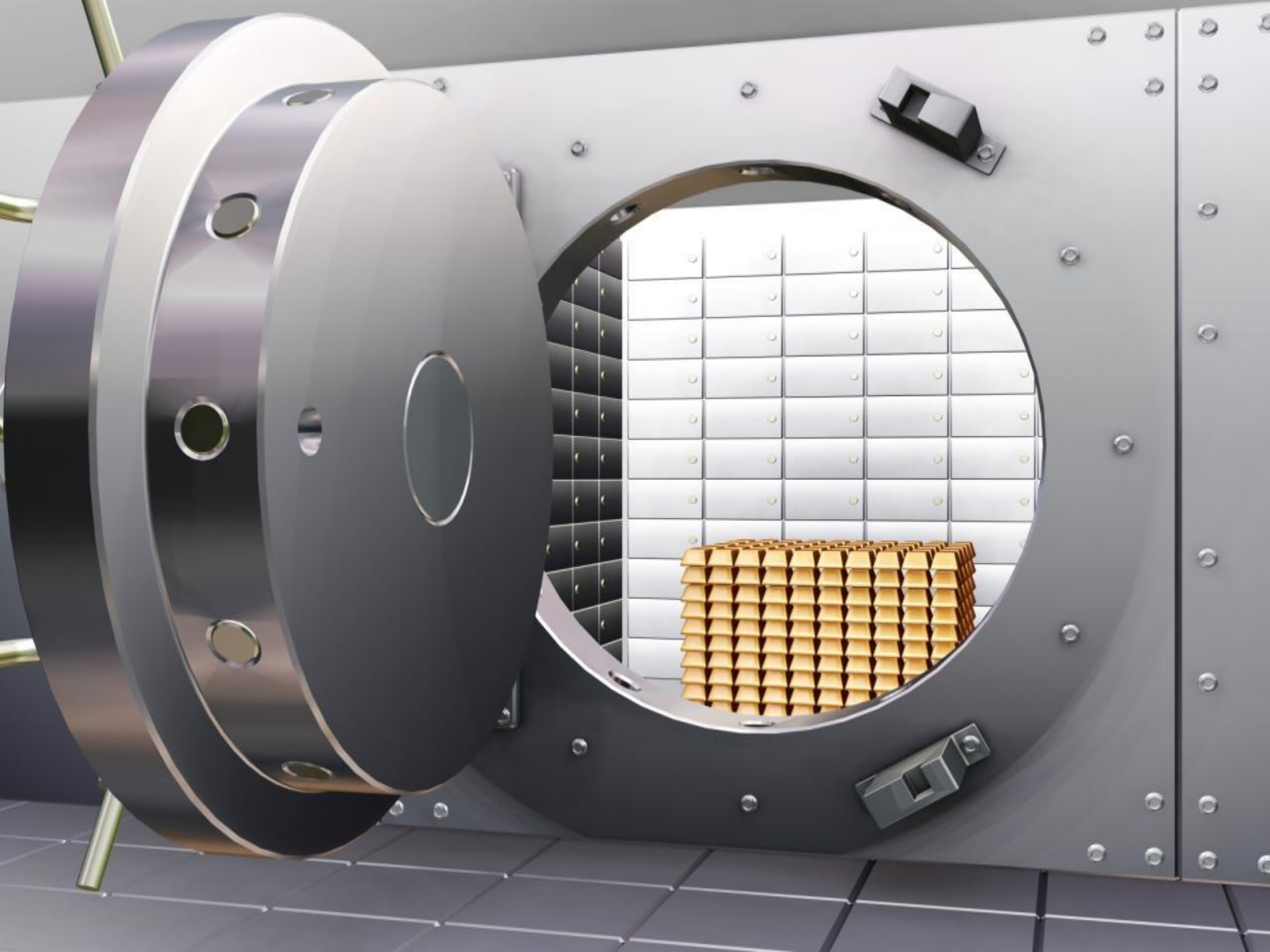
Det etablerte finansielle systemet med myndigheter, sentralbanker, tilsyn og banker tilfører penger dets viktigste egenskap, tillit. Bitcoin og andre kryptovalutaer står helt utenfor dette systemet, advarer kronikkforfatterne. (Ill.foto)

FOTO: 3D ILLUSTRATION OF BITCOIN OVER CYBER BACKGROUND WITH CPU, 3D ILLUSTRATION OF BITCOIN OVER

Tom Staavi
Informasjonsdirektør, Finans Norge

Eivind Gjemdal
Adm.dir., Bits

Oppdatert 20.09.2017, kl. 10:14



www.vestforsk.no

Det viktigaste

- **Blokk-kjede («blockchain») som frittståande omgrep gir lite meining**
- **Konsensus-modellen, ikkje blokk-kjeda, er det geniale!**
- **Skilnad på opne og lukka blokk-kjeder**
- **Bitcoin og kryptovaluta er langt meir enn pengar og betalingssystem**
  - men valutaen er likevel viktig for funksjonen i opne system
- **Blokk-kjede er ingen erstatning for databasar generelt!**
  - «Do you really need a blockchain for that?» (Gideon Greenspan)

Vestlandsforsking

- **Forskingsinstitutt lokalisert i Sogndal, stifta i 1985**
- **Forskingsområde:**
  - Klima og miljø
  - Reiseliv
  - Teknologi og samfunn
- **Rundt 30 tilsette**

- **Del av forskings-infrastrukturen i Norge**

Om meg

- **Forskar ved Vestlandsforsking sidan 1996**
- **Forskingsfelt: IT i offentleg sektor**
- **Interessert i Bitcoin/blokk-kjede sidan 2011**
  - har følgt utviklinga nøye sidan då
  - interessert i skjeringspunktet teknologi, økonomi og samfunn
  - har gjennomført master-programmet *Digital Currencies* ved universitetet i Nicosia
  - ser Bitcoin/blokk-kjedeteknologi som eit viktig område også for offentleg sektor
  - eig bitcoin og andre kryptovaluta + ei Bitcoin-gravemaskin (!)

Innhald

- Introduksjon til Bitcoin og blokk-kjede
- Mytar og mistydingar
- Eksempel på bruk i offentleg sektor
- Spørsmål og diskusjon

Bitcoin – «alle blokk-kjeders mor»

Bitcoin: A Peer-to-Peer Electronic Cash System

Publisert 31.10.2008 (Halloween Day)

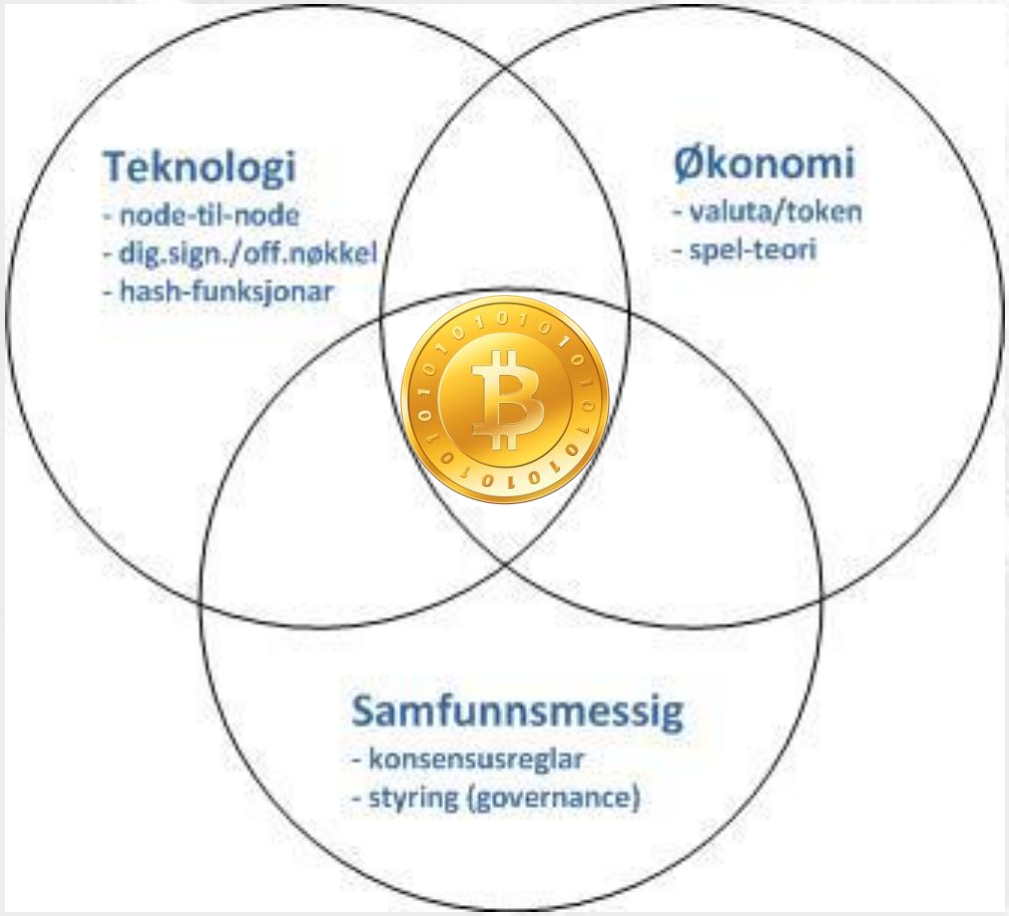
Sett i drift 03.01.2009

Har gått kontinuerleg sidan då

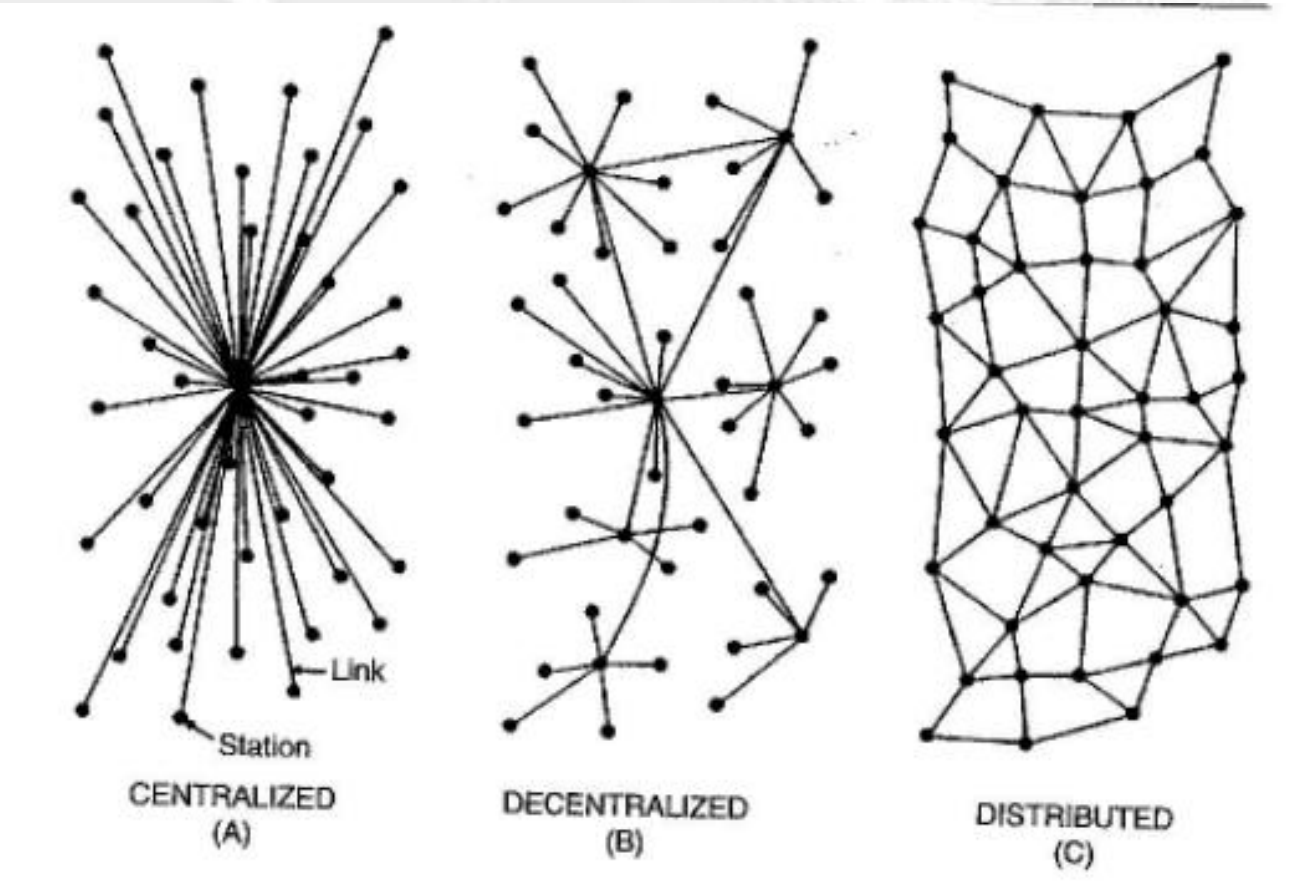
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort

Tverrfagleg!

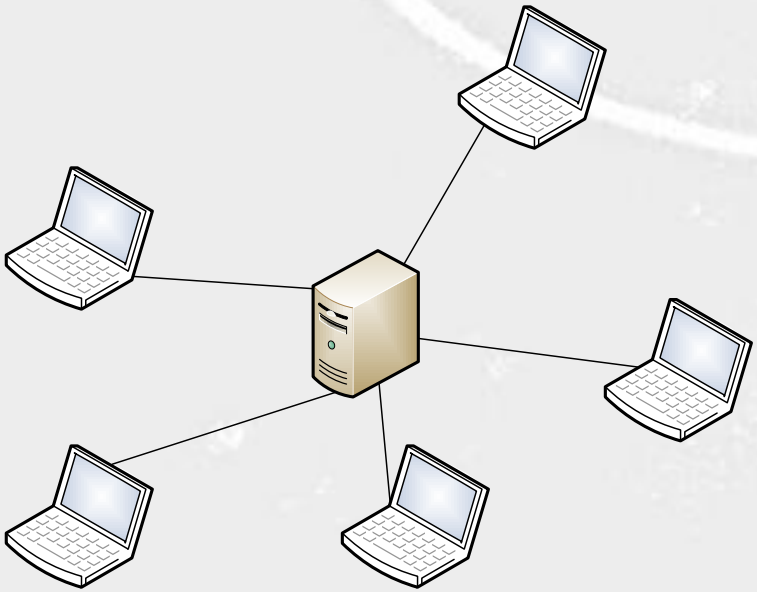


Tilbake til start: det distribuerte Internettet

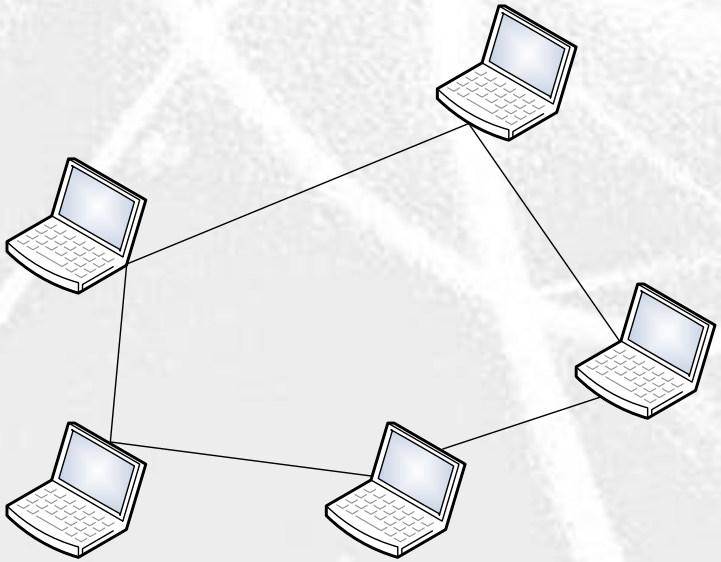


Paul Baran: «On Distributed Communications Network» (1964)
[Baran fann opp pakke-svitsjing, saman med (og uavh.) av Donald Davies, UK]

Frå klient-tenar til likeverdige nodar



Tradisjonell web-teknologi



Likeverdige nodar, ingen sentral tenar

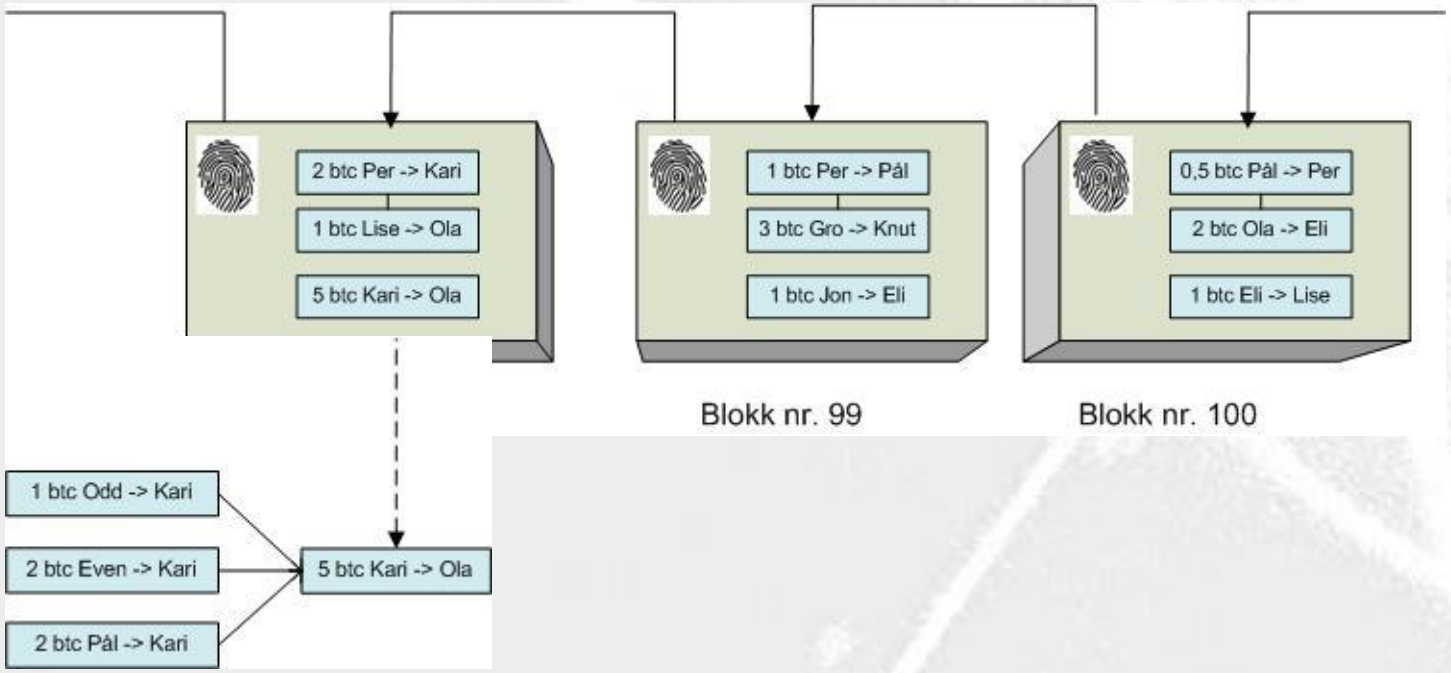
Kva er det spesielle med Bitcoin/blokk-kjede?

- **Bevis av eigarskap utan bruk av tredjepart**
  - NB! Dette gjeld opne blokk-kjeder!
- **Digital knappheit («digital scarcity»)**
- **«The Internet of Money»**
  - men også mykje meir..
- **Uforanderlege («immutable») data**
  - vel, ikkje nødvendigvis..

Bitcoins kjernearkitektur

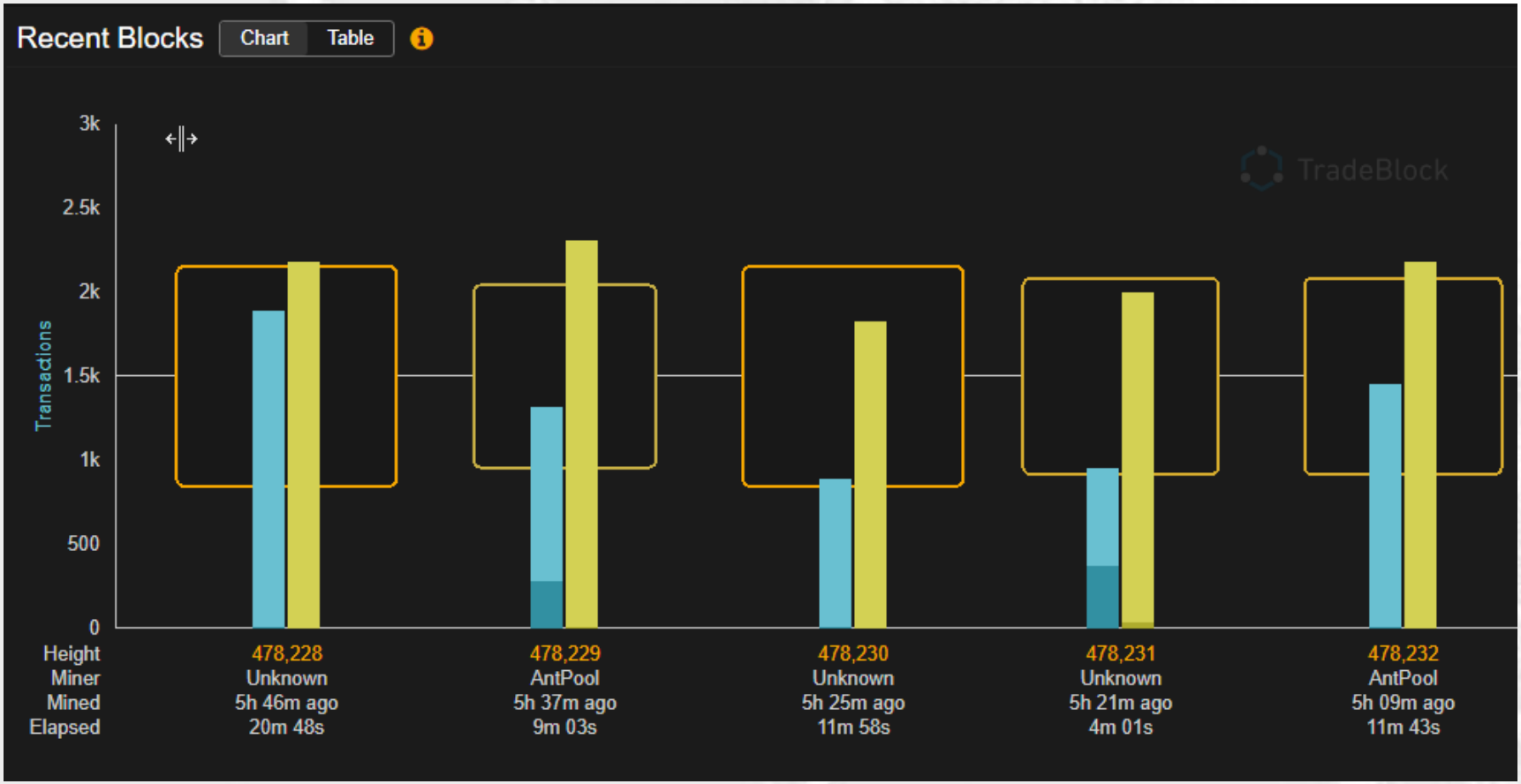
- **Byggjer på kjend teknologi:**
  1. Node-til-node-teknologi («peer-to-peer», kjent frå Internet)
  2. Digitale signaturar (oppfunne på 1970-talet)
  3. Hash-funksjonar (fleire ti-år gammalt)
- **Blokk-kjede som lagringsstruktur**
- **Konsensus-modell (Nakamoto-konsensus)**
  - Nodar som validerer transaksjonar and blokker
  - Gravarar («miners») som sikrar transaksjonane med arbeidsinnsats («Proof of work»)
    - Det er dette som avvergar kopiering av transaksjonar («double spending»)
- **Konsensus-modellen er det verkeleg disruptive! (ikkje blokk-kjeda!)**

Kjede av blokker OG transaksjonar!



Bitcoin kunne like godt vore kalla ei *transaksjons-kjede*!

Bitcoin i praksis (tradeblock.com)



Innhald

- Introduksjon til Bitcoin og blokk-kjede
- **Mytar og mistydingar**
- Eksempel på bruk i offentleg sektor
- Spørsmål og diskusjon

Myter og mistydingar om Bitcoin og blokkjede

1. **«Blokk-kjede»/»Blockchain» som generelt omgrep er nokså meiningslaust**
   - Må spesifisera kva type blokk-kjede ein snakkar om
     - Open eller lukka? Kva sikkerheitsmodell?

2. **Bitcoin er berre for kriminelle eller lyssky aktivitetar**
   - Forsking tilbakeviser dette (Tasca et al., 2016)

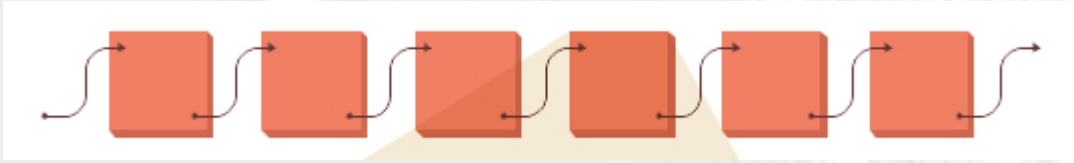
3. **Det er stor skilnad på opne og lukka blokk-kjeder**
   - Opne blokk-kjeder har det største innovasjonspotensialet (MIT)
   - Lukka blokk-kjeder kan også vera nyttig i enkelte samanhengar - men må stilla spørsmålet: Kvifor ikkje heller ein distr. database?

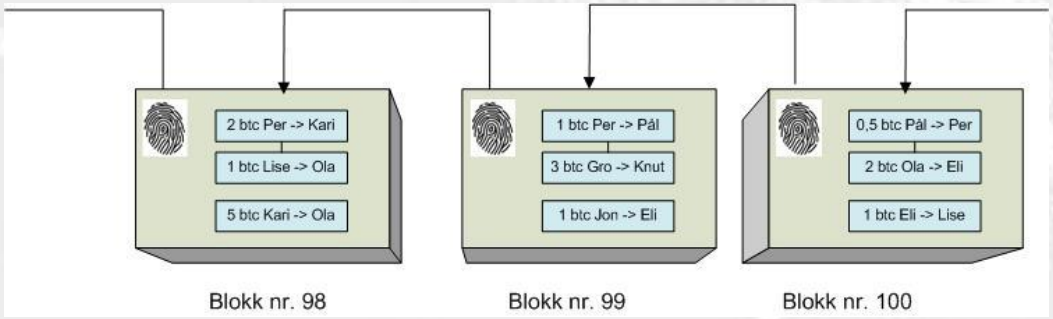
4. **Blokkjede som universalmiddel**
   - Blokk-kjedeteknologi er nyttig på mange område, men ikkje alle

Opne vs. lukka blokk-kjeder

	Opne («permissionless)	Lukka («permissioned»)
Kven oppdaterer	Alle som vil	Utvalde pers./org.
Kven produserer data	Alle som deltek	Kundar av org.
Insentiv til å følgja reglar	Direkte økonomiske (gulrot & pisk)	Omdømme
Lagring	Distribuert	Sentralisert
Stola på sentrale aktørar	Nei	Ja
Transaksjonskostnader	-	+
Fart (trans./sek.)	-	+
Uforanderleg	+	-
Valuta/»token»	Ja	Nei
Eksempel	Bitcoin, Ethereum	HyperLedger, Corda

Blokk-kjede og sikring mot endringar





På grunn av blokk-kjedestrukturen blir endringar **lett synlege**.

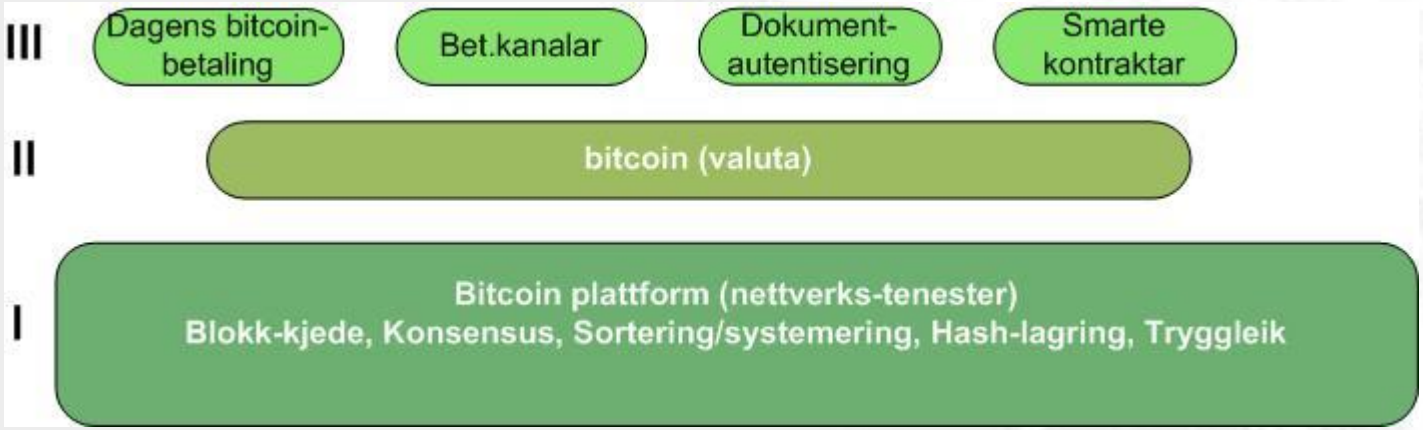
NB! Det betyr ikkje at det er umuleg å endra blokk-kjeda!

Blokk-kjede og sikkerheit

Innhald

- Introduksjon til Bitcoin og blokk-kjede
- Mytar og mistydingar
- Bitcoin/blokk-kjede som plattform og muleg infrastruktur
- **Eksempel på bruk i offentleg sektor**
- Spørsmål og diskusjon

Bitcoin som plattform/infrastruktur



I Nettverk/Protokoll
II Valuta/token
III Applikasjonar

Bitcoin og blokk-kjede i offentleg sektor

- **Sikker lagring og verifisering av dokument**
  - vitnemål
  - sertifikat
  - arkiv-dokument
  - Eksempel: Alle vitnemål frå høgare utd. lagra på blokk-kjeda
- **Bevis av eigarskap**
  - eigedommar
  - Eksempel: Matrikkelen på blokk-kjeda?
- **Identitetshandtering og personvern**
  - sikker, desentralisert identitetshandtering
  - Eksempel: MinID/eID som blokk-kjedeteknologi?
- **Tenk på Bitcoin/blokk-kjede som ei ny Internett-basert plattform!**

Blokk-kjede og arkiv

- **Kva rolle kan blokk-kjede spela for forvaltningsarkiva?**
  - Søknad til Riksarkivet (KDRS, HiOA, Trondheim kommune, Vestlandsforsking)
- **Skilja struktur og innhald**
- **Publisera struktur på ei blokk-kjede**
  - Opna for meir aktiv bruk av arkiv-informasjon

Estland

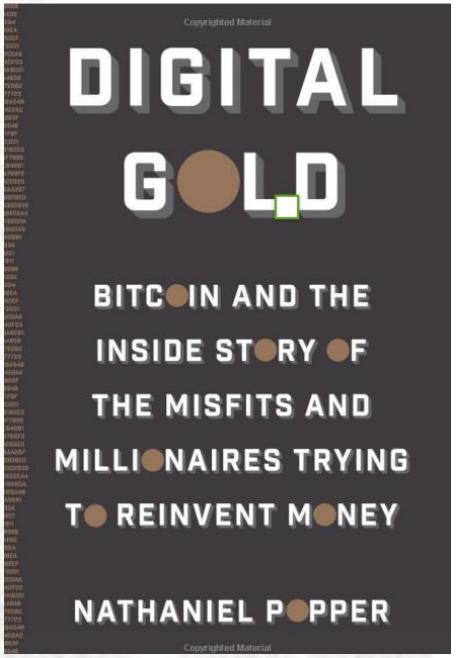
- **Fleire års bruk av blokk-kjedeinspirert teknologi til tidsstempling av dokument**
  - Garanti for når dokumentet er oppretta
  - Autentisering av dokumentet
  - Avtrykk av loggfiler for å verifisera innsyn i offentlege register

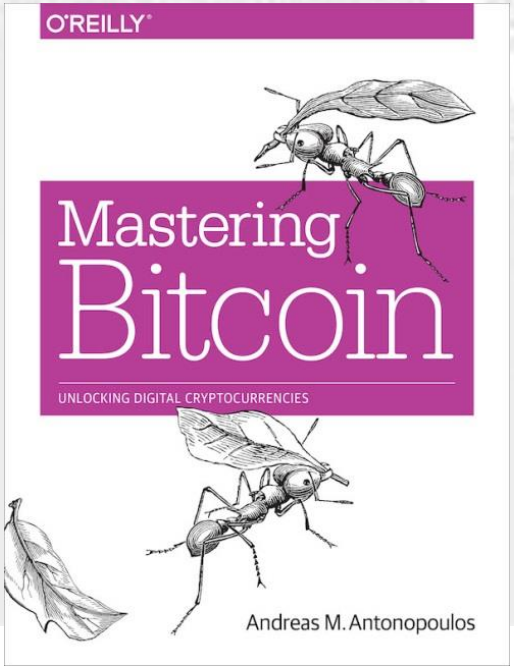
Aktuell litteratur

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.





Meir informasjon om Bitcoin og blokk-kjede

- **«Bitcon – A Peer-to-Peer Electronic Cash System»**
  Satoshi Nakamoto, 2008

- **«Open Matters - Why Permissionless Blockchains are Essential to the Future of the Internet”**
  Peter van Valkenburgh, Coin Center

- **«Beyond Bitcoin – Enabling Smart Government Using Blockchain Technology»**
  - Svein Ølnes, eGov 2016, Springer LNCS

- **«Deja vú all over again: Thinking through law & code, again**
  Lawrence Lessig, https://vimeo.com/148665401

Ressursar elles på nettet

- **Nytt om Bitcoin og blokk-kjedeteknologi**
  - CoinDesk (www.coindesk.com)
  - Coin Telegraph (www.cointelegraph.com)
  - Bitcoin Magazine (www.bitcoinmagazine.com)
  - + mange fleire
- **Bitcoin blokk-kjede i sanntid**
  - https://blockchain.info
  - https://blockchain.info
  - https://data.bitcoinity.org
  - http://statoshi.info
  - https://bitinfocharts.com
  - + mange fleire

Innhald

- Introduksjon til Bitcoin og blokk-kjede
- Mytar og mistydingar
- Bitcoin/blokk-kjede som plattform og muleg infrastruktur
- Eksempel på bruk i offentleg sektor
- **Spørsmål og diskusjon**

Takk for meg!

E-post: **sol@vestforsk.no**

Denne presentasjonen:
http://www.slideshare.net/sveino/Arkivraadet

Bitcoin-addresse:

332d75vrrdeyhfYo4V7cMZduWDmjvRFtQX