Blockchain

Opbygning og Implementering

Gymnasietjenesten DIKU
Department of Computer Science

1. Dagens program
2. Blockchain kort fortalt
3. De 3 hovedområder
4. Anvendelses Muligheder
5. Opsamling og Spørgsmål

Program for idag

Agenda

- Introduktion
- Primære områder
- Python Introduktion
- Data struktur
- Øvelser - implementering af data struktur
- Gennemgang af “Proof of Work” konsensus mekanismen
- Øvelser - implementering af konsensus mekanisme
- Anvendelses-områder

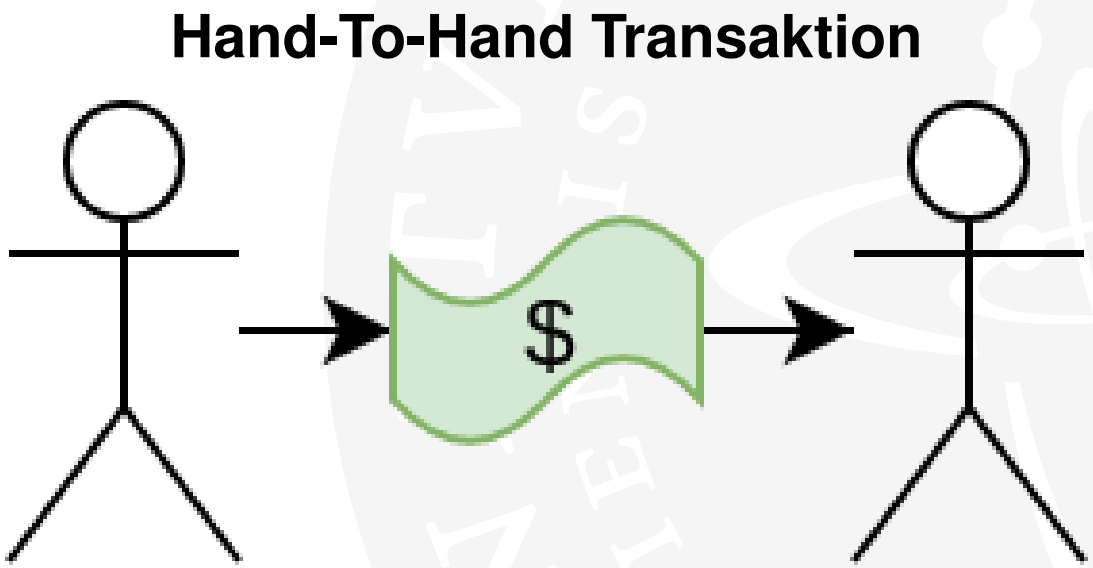
Det Første Eksempel

Lad os starte med et scenarie:

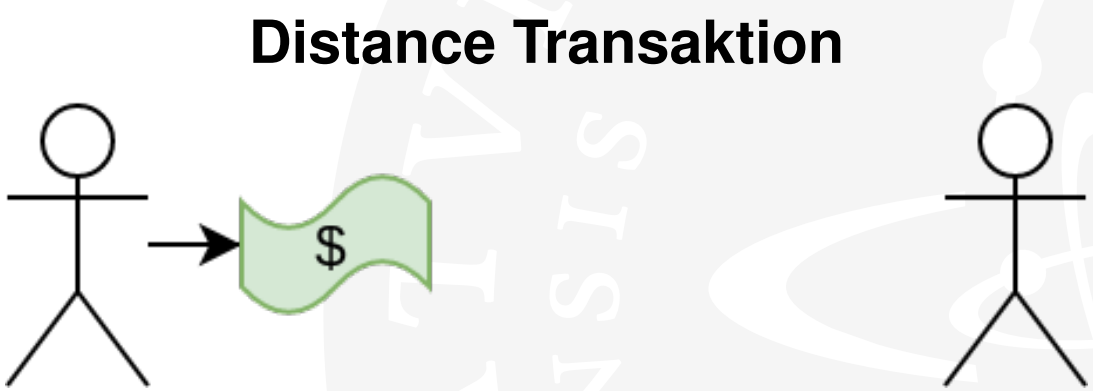
Scenarie

Vi ønsker at overfører nogle midler til en anden person, dette kan udspille sig på to måder.

Transaktion - Type 1



Transaktion - Type 2



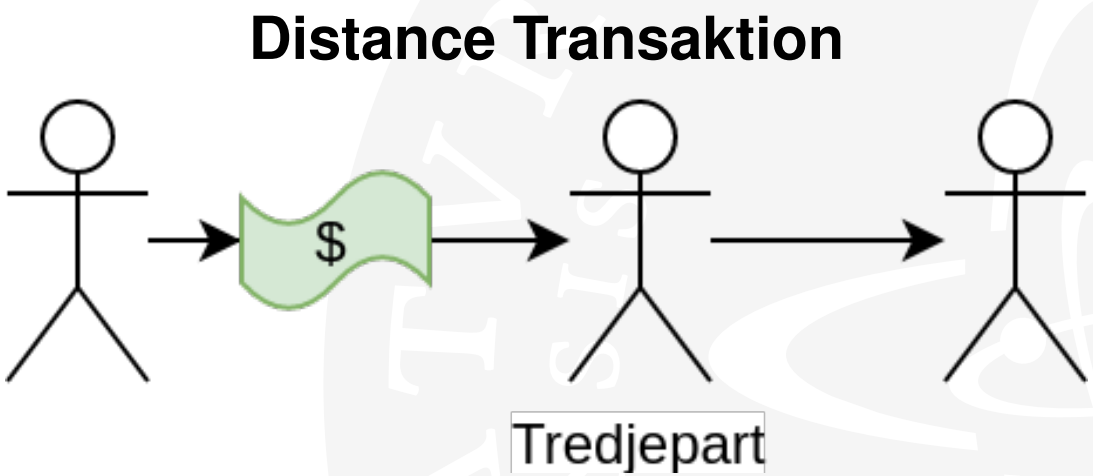
Transaktion - Type 2

Distance Transaktion

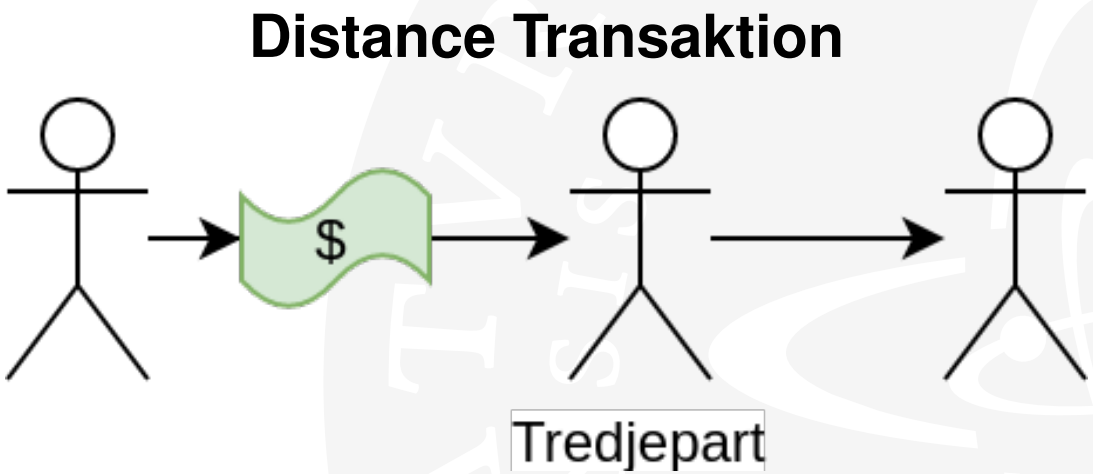
Problem

Hvordan overfører vi midler over distancer?

Transaktion - Mellemmand Løsning



Transaktion - Mellemmand Løsning



Tillidsløst Alternativ?

Finder der andre løsninger der ikke forudsætter tillid til tredjeparten?

blockchain?

Blockchain teknologien har rejset utallige spørgsmål i medier de seneste år:

- Hvordan virker den?
- Hvad kan teknologien bruges til?
- Sikker nok til at anvendes?
- Hvorfor skulle vi bruge den?

asia murphy, aCaDeMiC (35%) @am_an... · 17. aug. 2018

i still don't get bitcoin

corndog bayonet
@Theophite

imagine if keeping your car idling 24/7 produced solved Sudokus you could trade for heroin

♡ 17,8 t 00.49 - 17. aug. 2018

Ideen bag blockchain

”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.”

— Satoshi Nakamoto

Problem

”Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments.”

Problem

”Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments.”

1. Mægling omkostninger forøger transaktions omkostninger.
2. Begrænset praktisk minimums grænse ved transaktioner, hvilket medfører færre små transaktioner.
3. Ingen ikke-reversible overførsler.
4. Med reversible overførsler opstår behovet for tilled.

Løsning

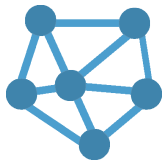
”What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”

Løsning

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

1. Distribueret Netværk - globalt uden central styring,
   - Undgå mægling omkostninger
   - ingen praktisk minimums grænse ved transaktioner
2. Kryptografisk bevis - stol på matematikken ikke personen.
   - Tillidsfrit system
3. Blok struktur - Lænket og svært at forfalske.
   - ikke-reversible overførsler - alt er hugget i sten

Blockchain kerne områder



- Distribuerede database

- Blok struktur

- Konsensus mekanisme

Database?

Hvad er en database?

Database?

Hvad er en database?

En måde at opbevare information på.

Centraliserede vs Decentraliserede?

Database?

Hvad er en database?

En måde at opbevare information på.

Centraliserede vs Decentraliserede?

- **Central Database** - Al information holdes samlet og tilgås fra samme udgangspunkt.
- **Decentraliseret Database** - Information spredt ud over flere lokationer, forskellige arkitekturer.

Centraliserede Database

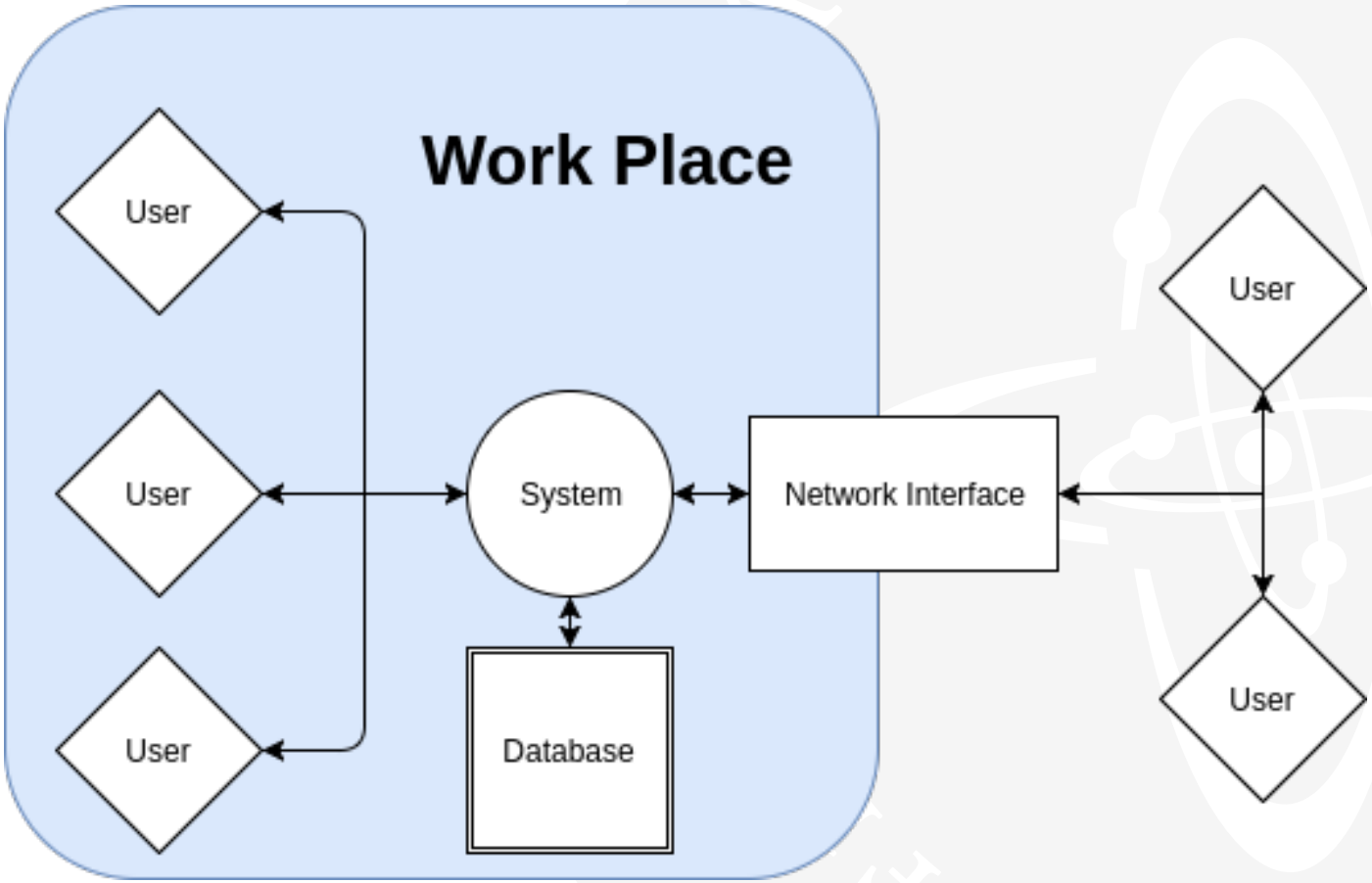


Figure: Centraliseret

Decentraliserede Database

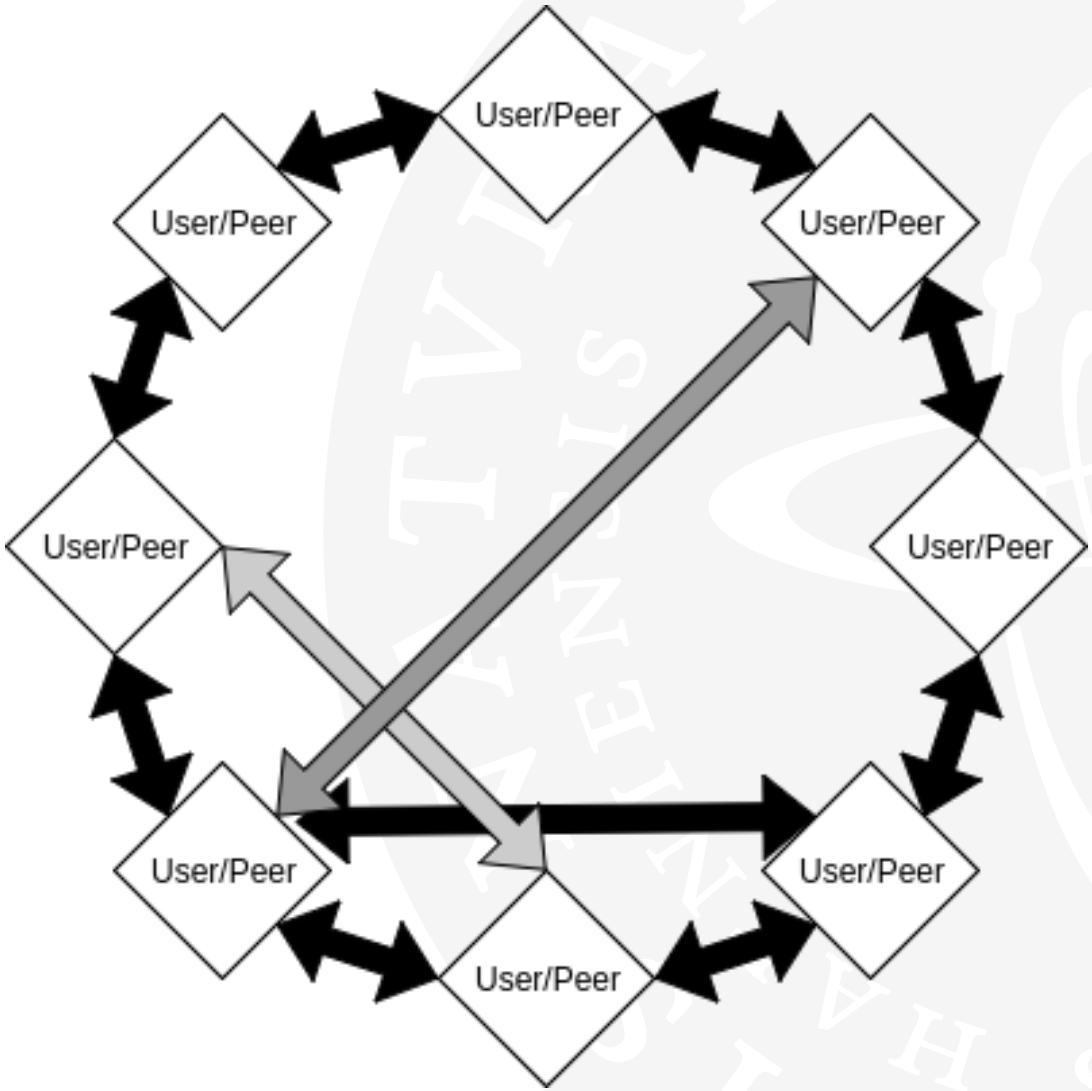
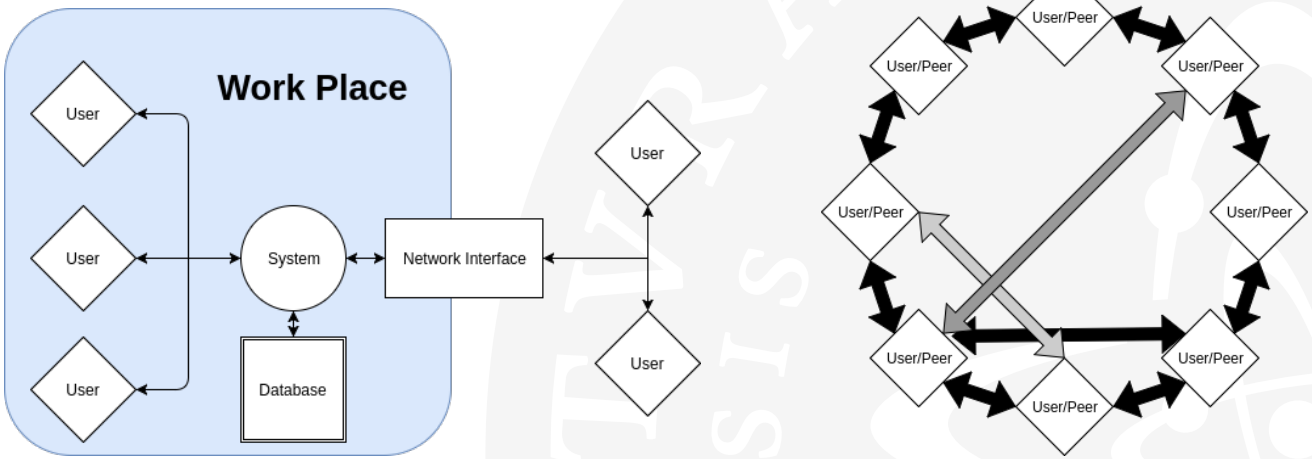


Figure: Decentraliseret

Decentraliseret Vs Centraliseret

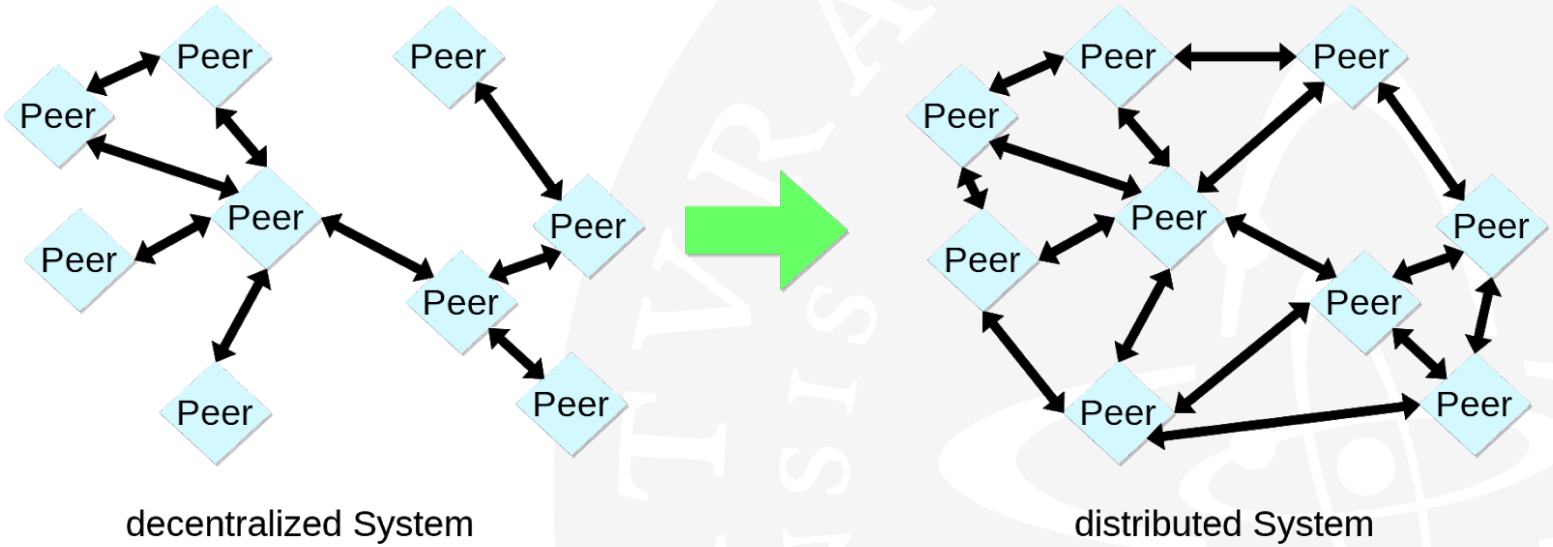


(a) Centraliseret (b) Decentraliseret

Pros and Cons?

Hvilke fordele og ulemper er der ved brug af centrale kontra decentaliserede databaser?

Decentraliseret $\neq$ Distribueret



decentralized System

distributed System

- Splittet Database
- Mist-bar Data
- Få updates

- Spejlet Database
- Sikker Data
- Utallige updates

Data Struktur

Hvad er en Data Struktur?

Data Struktur

Hvad er en Data Struktur?

En betegnelse for data det er struktureret i elementer, således at disse kan tilføjes eller fjernes.

Data Struktur

Hvad er en Data Struktur?

En betegnelse for data det er struktureret i elementer, således at disse kan tilføjes eller fjernes.

Eksempler:

- **Array** - Simpel datastruktur indelt efter en specifik orden.
- **Linked List** - Data struktur hvor hvert element, eller ”node”, henviser til det næste element i listen.
- **Hash maps** - Data struktur formet efter navn og værdi, ingen specifik orden men yderst brugbart som opslagsværk.

Linked list

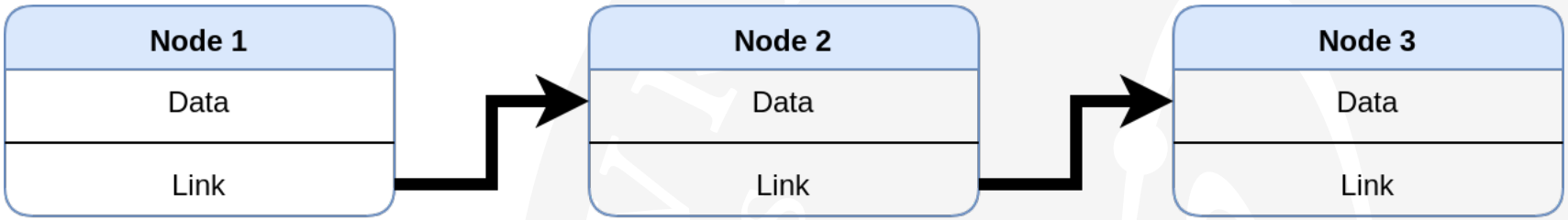


Figure: Linked List

Brugbart i vores tilfælde?

Sammensætning af data på denne måde via referencer giver en manøvrerbar strøm af data. Man kunne også kalde dette for en kæde?

Blok Data

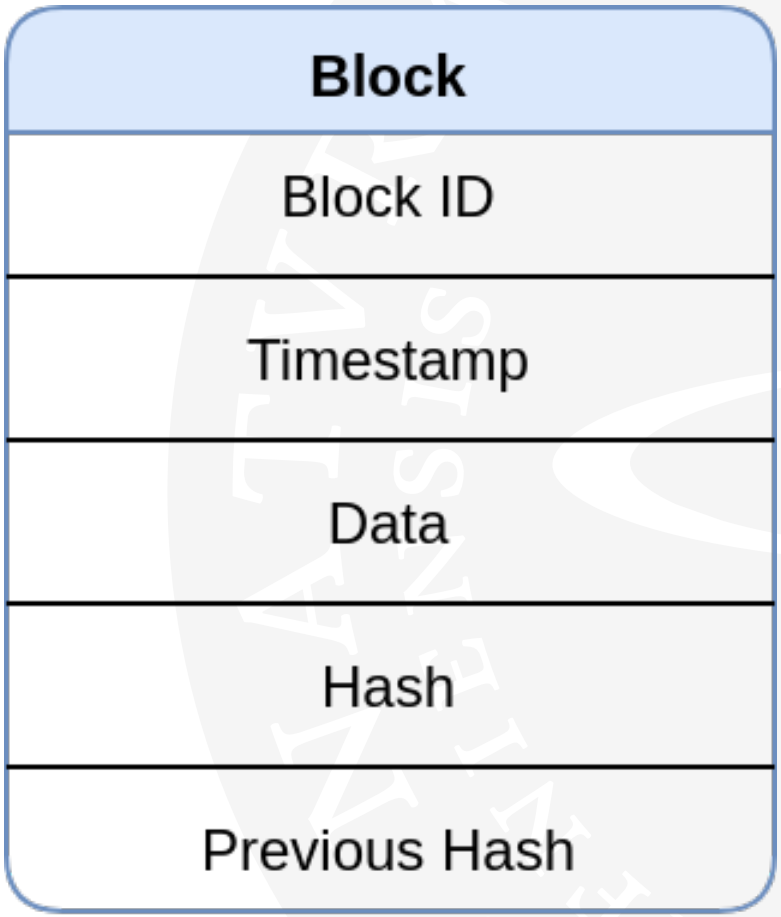


Figure: Data Blok

Blok Struktur

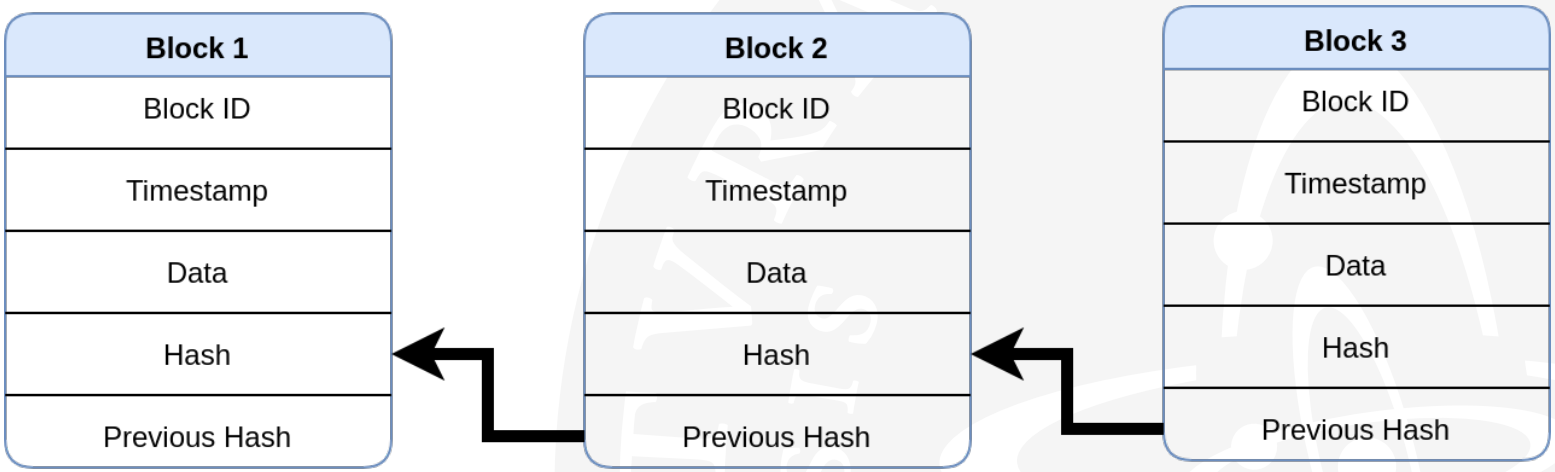


Figure: Bloks

Sikker nok?

Selvom vi nu har defineret en brugbar struktur mangler vi stadig en måde hvorpå vi kan garantere data'en ikke bliver ændret.

Konsensus Algoritme?

Hvad er en Algoritme?

En matematisk opskrift.

Konsensus?

En konsensus algoritme bruges til at garantere at datastrukturen forbliver u-kompromitteret

Hashing?

Hashing er en måde hvorpå man omdanner data til en mindre billedmængde.
F.eks. ved brug af en sha-1 kan man omdanne:

$$\texttt{Hello World} \rightarrow \texttt{Sha-1} \rightarrow \texttt{0a4d55a8d778e5022...}$$

Proof of Work - Algoritme

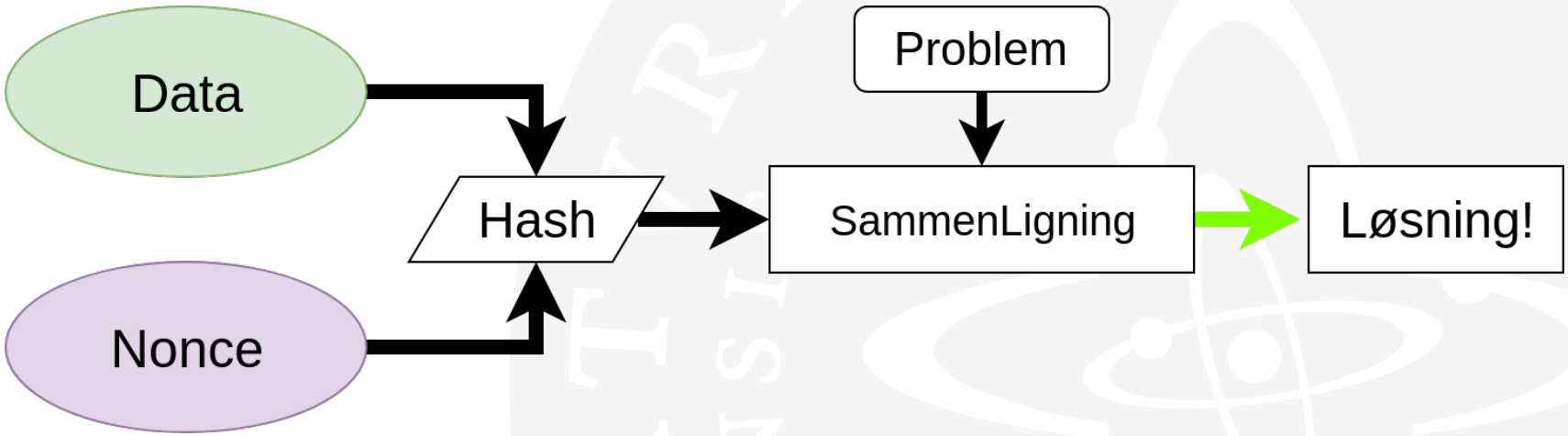
Algorithm 1

Input: Problem, data

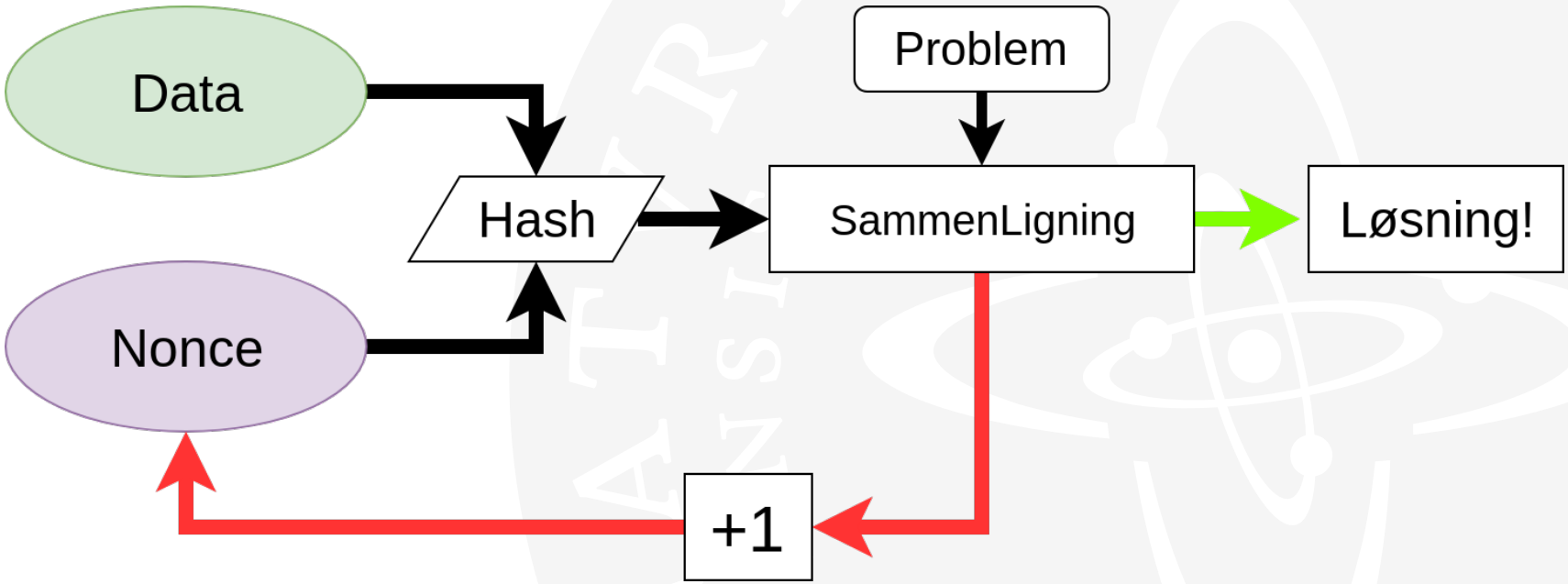
Output: Hash

```
hash = Hash_Funktion(data)
nonce = 0
while Hash ≠ Problem do
    nonce += 1
    data += nonce
end while
Return hash
```

Proof of Work



Proof of Work



Konsensus Algoritme/mekanismer - Alternativer

Der findes et antal alternativer til ”Proof of Work”

- Proof of Stake (PoS)
  - Belægger sig på brugerens værdi, jo større værdi jo større chance for at tilføje den næste blok.
- Proof of Elapsed Time (PoET)
  - Bruges i *”Permissional Blockchains”*, fungere ved at hver ”node” venter på det bliver deres tur til at ”commit” en block til kæden.
- Proof of Authority (PoA)
  - Bruges i mindre blockchain systemer, her vælges et antal brugere som ”validators”, og giver dem alene magten til at autorisere nye blokke.

Kun Krypto Valuta?

(a) Tracr - Diamond Track

(b) Uport - Zug ID

Spørgsmål

Nogen spørgsmål?