Blockkedjeteknikens fördelar och framtidens utmaningar I datahantering

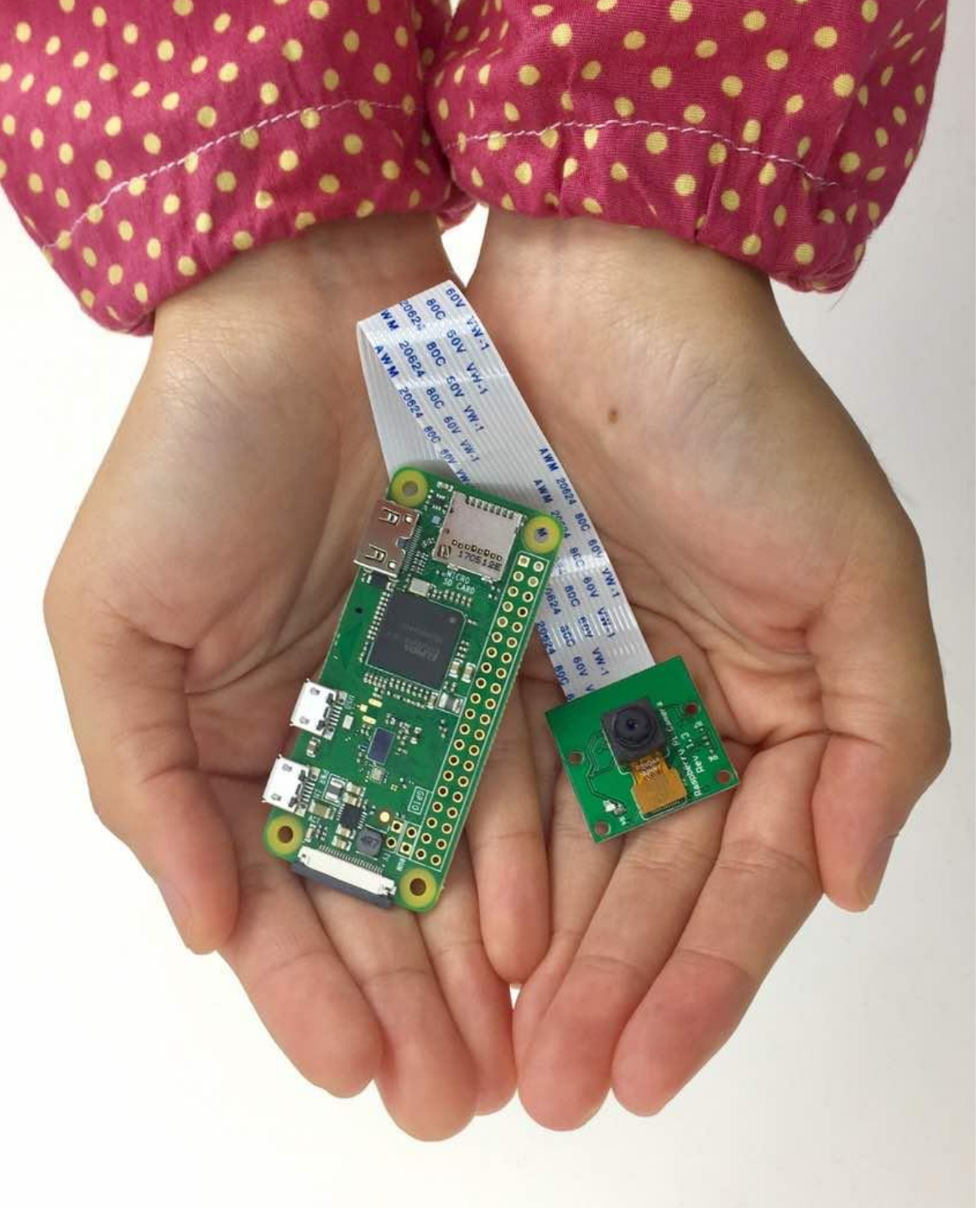
Andreas de Blanche
andreas.de-blanche@hv.se

HÖGSKOLAN VÄST

Andreas de Blanche

Universitetslektor datateknik
Inst. för ingenjörsvetenskap
Högskolan Väst

andreas.de-blanche@hv.se



Dataingenjör
Högskolan Väst

HÖGSKOLAN VÄST

- ☑ programmering
- ☑ nätverksteknik
- ☑ cyber security
- ☑ internet of things

Industrins digitalisering

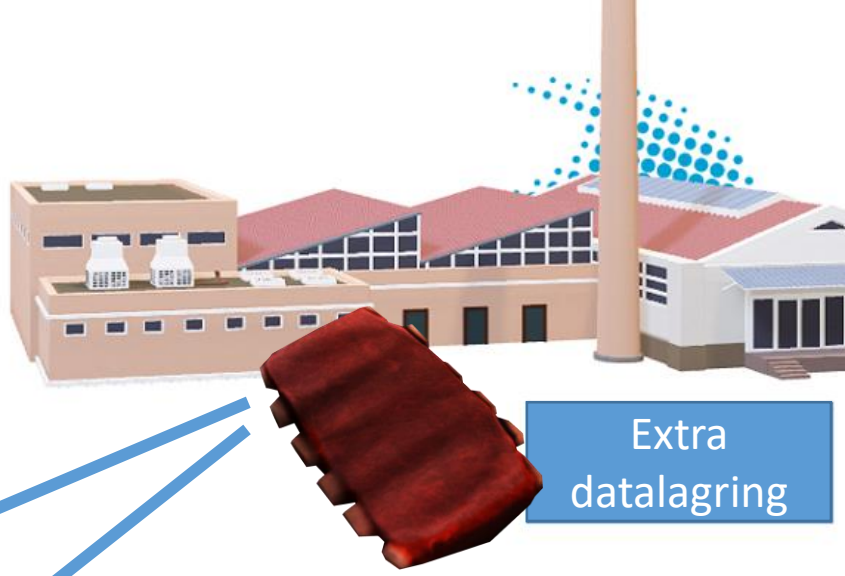
- Industri 4.0, tekniker och möjligheter
- Cyber security
- Internet of things

Dr. Andreas de Blanche
Det digitala djuret 2019

Carrefour extends food traceability blockchain

Pig traceability goes live on public blockchain

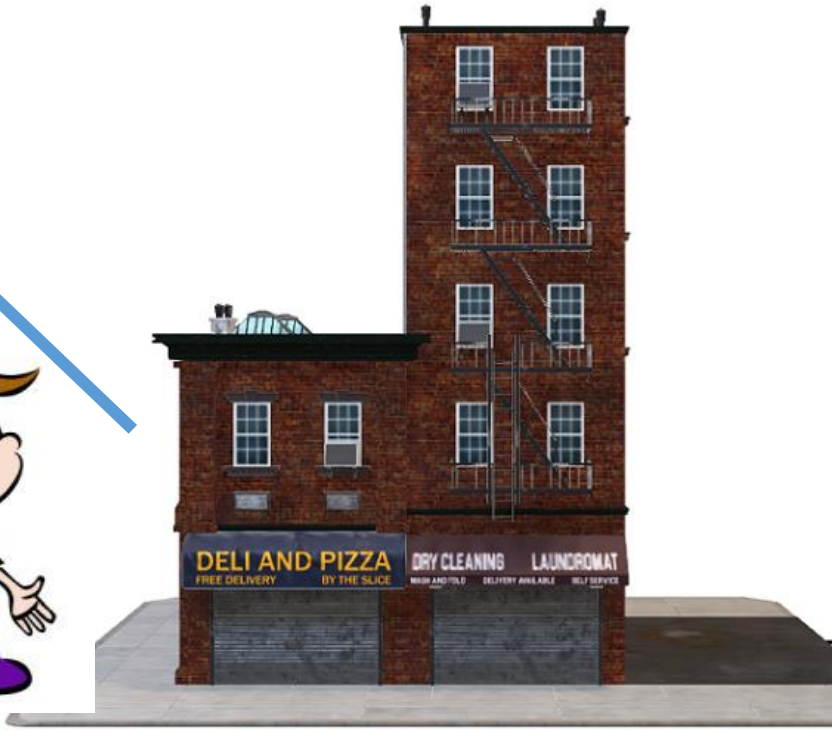
Subway and Tyson



Extra datalagring

Blockkedja

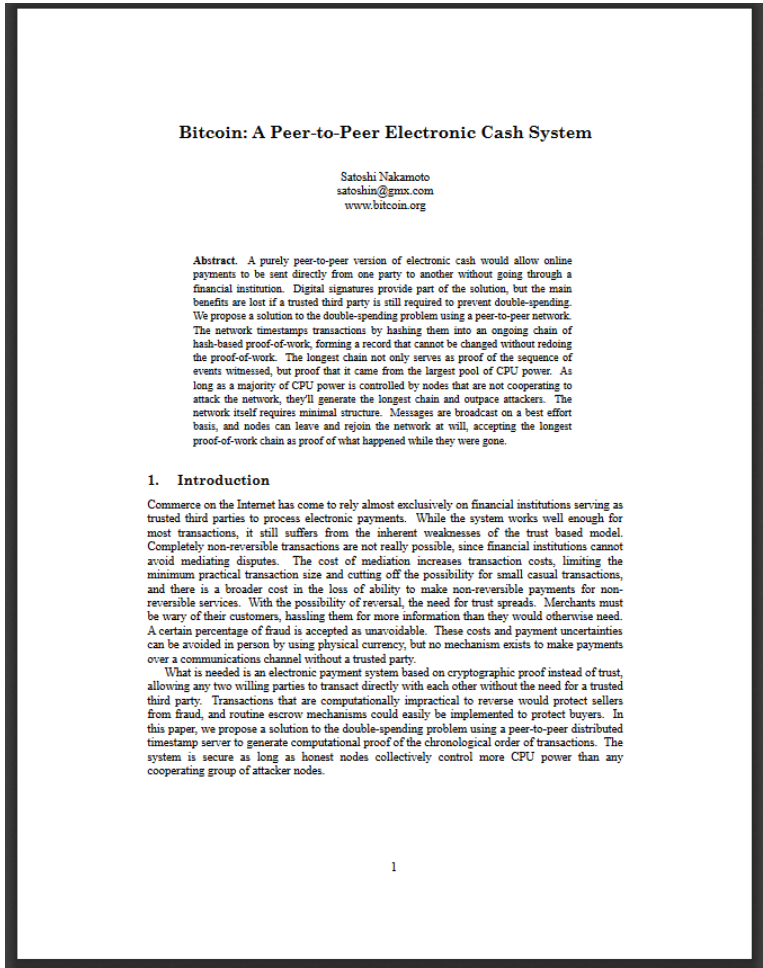
extra datalagring



BITCOIN OCH BLOCKCHAIN

HÖGSKOLAN VÄST

- Januari 2009 presenterade Satoshi Nakamoto Bitcoin och blockkedjetekniken.
- Blockkedjan och konsensus algoritmen är den teknik som gör Bitcoin möjlig!
- Blockkedjor har precis fyllt tio år.



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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

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. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

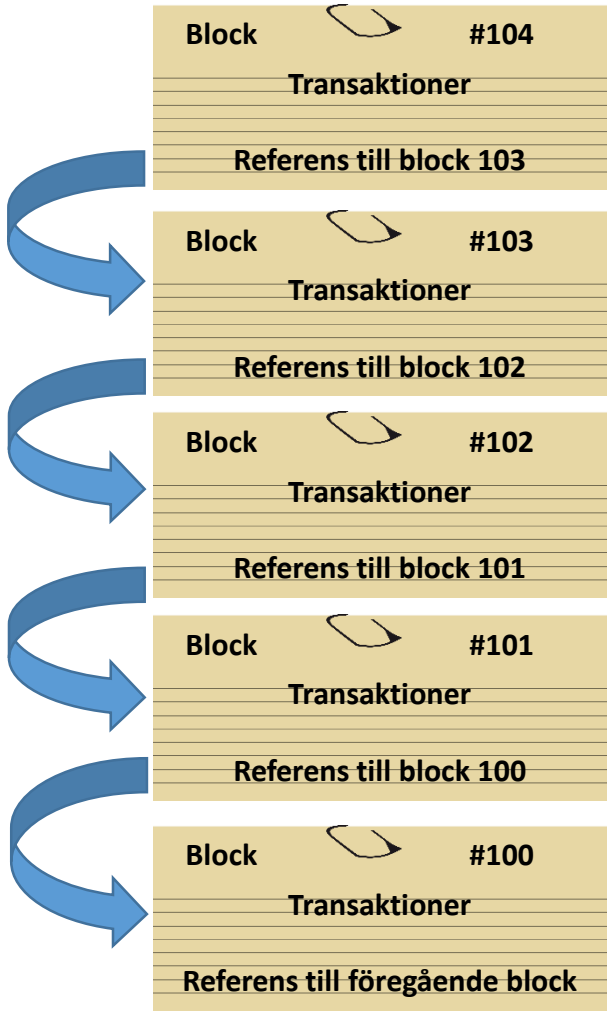
1

BLOCKKEDJAN

HÖGSKOLAN VÄST

- En blockkedja består av block.
- Ett block innehåller
  - information om blocket (header)
  - referens till föregående block
  - godtycklig information
- Publik blockkedja
  - **ALLA** får läsa och lagra
  - **INGEN** bestämmer (distributed trust)
  - betyder inte att man förstår vad man läser
- Privat blockedja
  - bara vissa får läsa och lagra

https://blockchain.com/

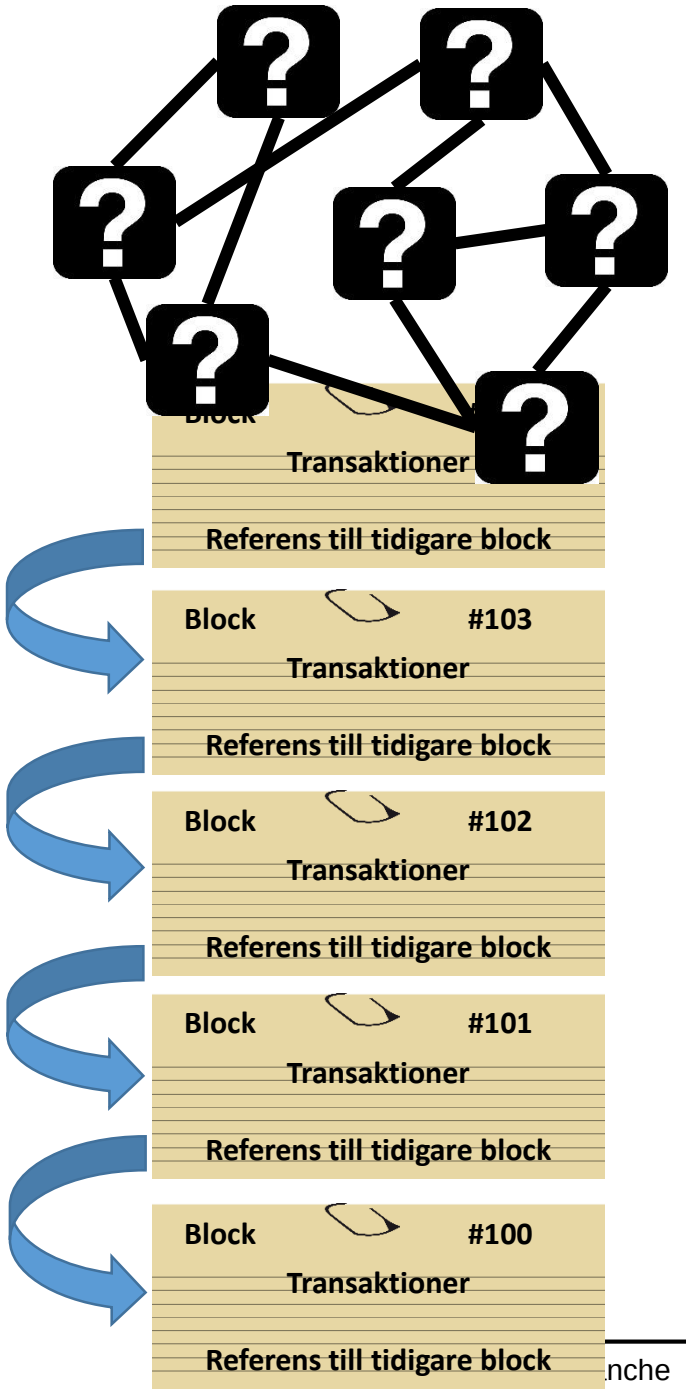


DISTRIBUTED TRUST

Garanterar säkerheten i blockkedjan

- Ingen vet vem som kommer att skapa nästa block.
- Vem som helst får försöka
- Den som skapar ett block får en belöning

- Blockskapandet i *Proof-of-Work* använder mycket energi.



IDENTITET

HÖGSKOLAN VÄST

- Alice och Bob har privata ”krypto-nycklar”
  - En nyckel motsvarar en adress.
  - Alice och Bob kan ha oändligt många nycklar.
  - Man skapar själv sina nycklar.

13gWtMQJdg3H6XBpFjMELcHLJc1HHp79vD

F1EnPrivatHemligNyckel

1Bob42389sdAdgjdlsoe92MELcHLJc1HklE53X

F1lSomGerTillgångTillAdressen.

SÄKERSTÄLLA DOKUMENT

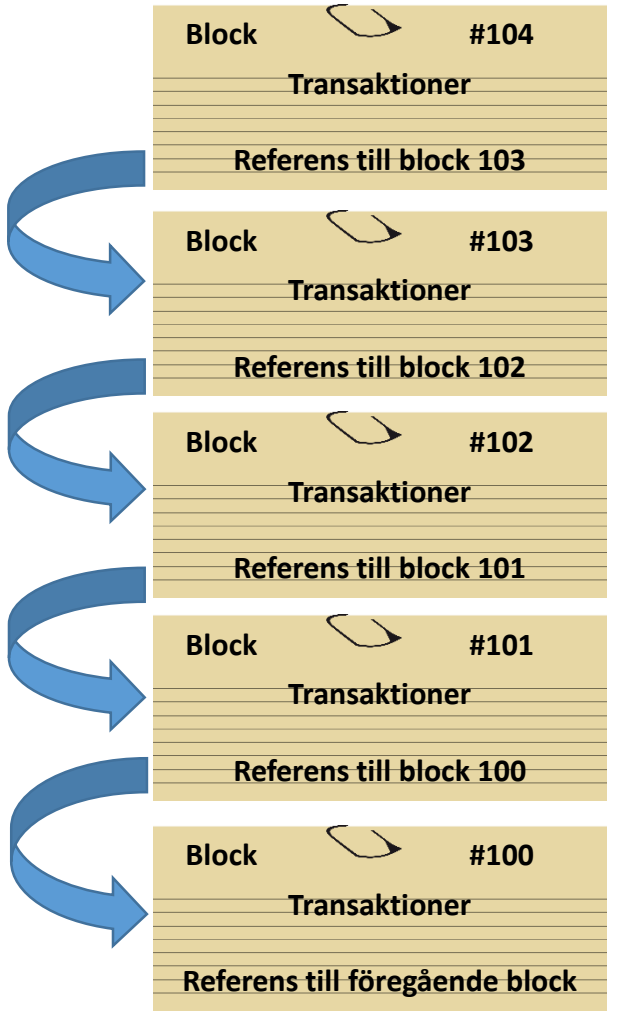
HÖGSKOLAN VÄST

- Dokumentet lagras någonstans.

F0456779297E6074F698030CB623E6FB7F2C0FFC65EB1BD45C58FAD53C3C9397

- Dokumentets hash (fingeravtryck) lagras i blockkedjan.
  - Hashen är liten.
  - Hashen avslöjar inte innehållet.
  - Har man dokumentet kan man bekräfta att det är rätt.

- Lagringen signeras
  - ”Transaktionen” signeras av en eller flera parter.
  - Det går då att se ”vem/vilka” som lagt in hashen
  - och ungefär när.



SIGNERING ÖVERFÖRING AV ÄGANDE

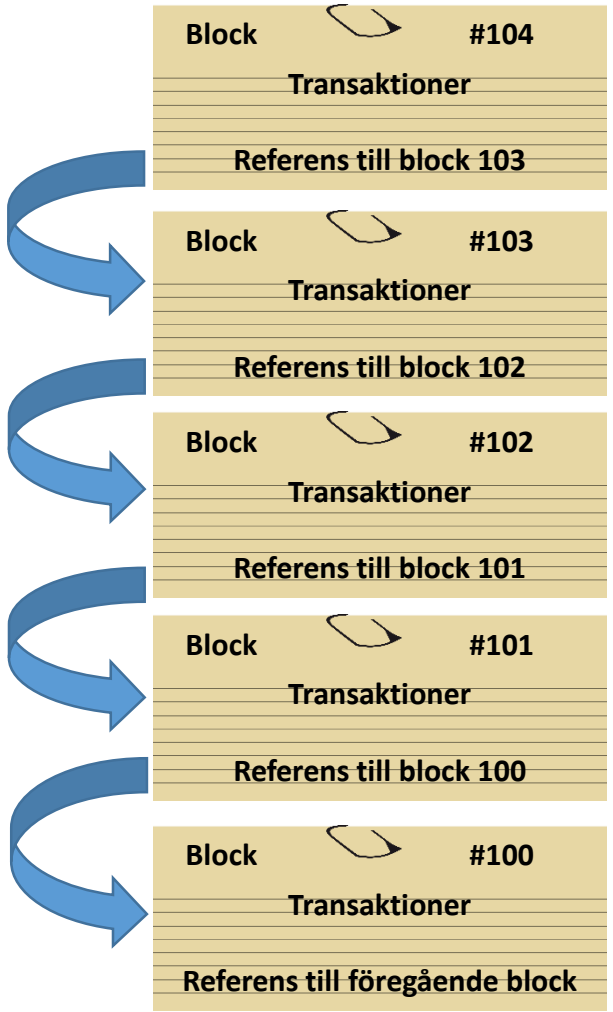
HÖGSKOLAN VÄST

4) Lastar av vid slutdestination. Flyttar ägande, signerar.

3) Tullen godset (id) mot blockedjan, ser att det finns en kedja. Lägger till att det tullats.

2) Lastar om godset till båt i hamnen. Chaufför och båt signerar överföring till båt

1) Lastar gods på lastbil. Tillverkare och chaufför signerar, överföring till chaufför



DET STORA PROBLEMET

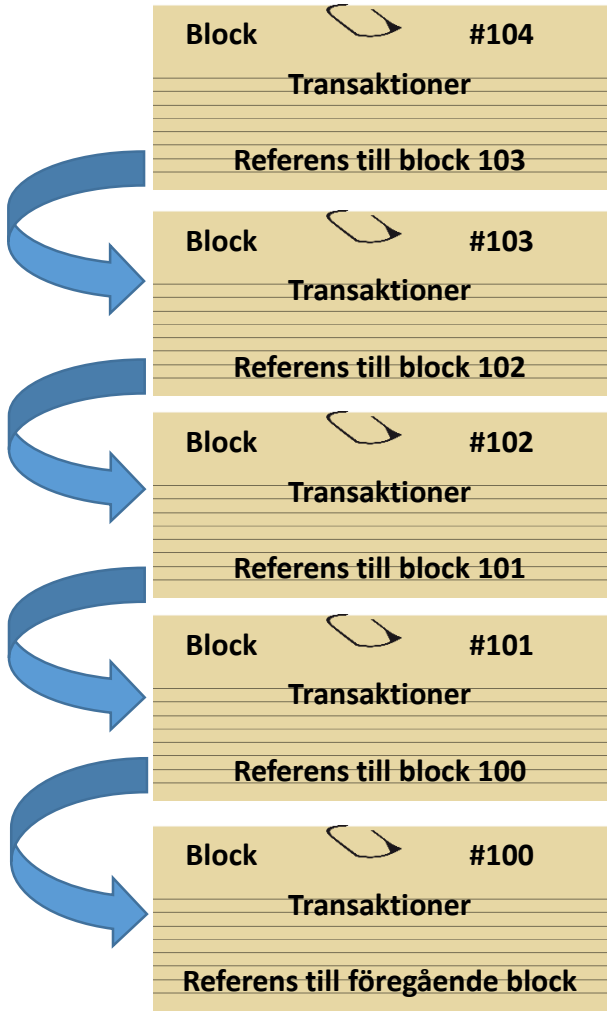
KNYTA FYSISK ENTITET TILL DIGITAL ENTITET

HÖGSKOLAN VÄST

- Dokument kan hashas.

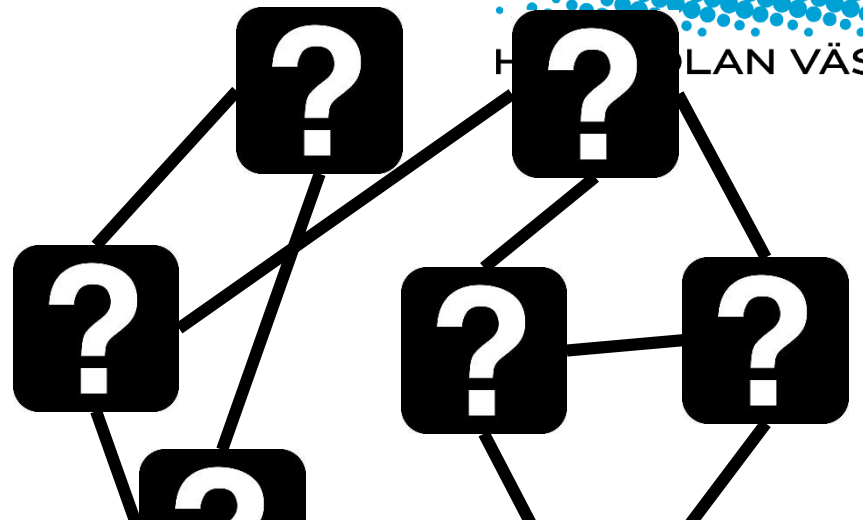
F0456779297E6074F698030CB623E6FB7F2C0FFC65EB1BD45C58FAD53C3C9397

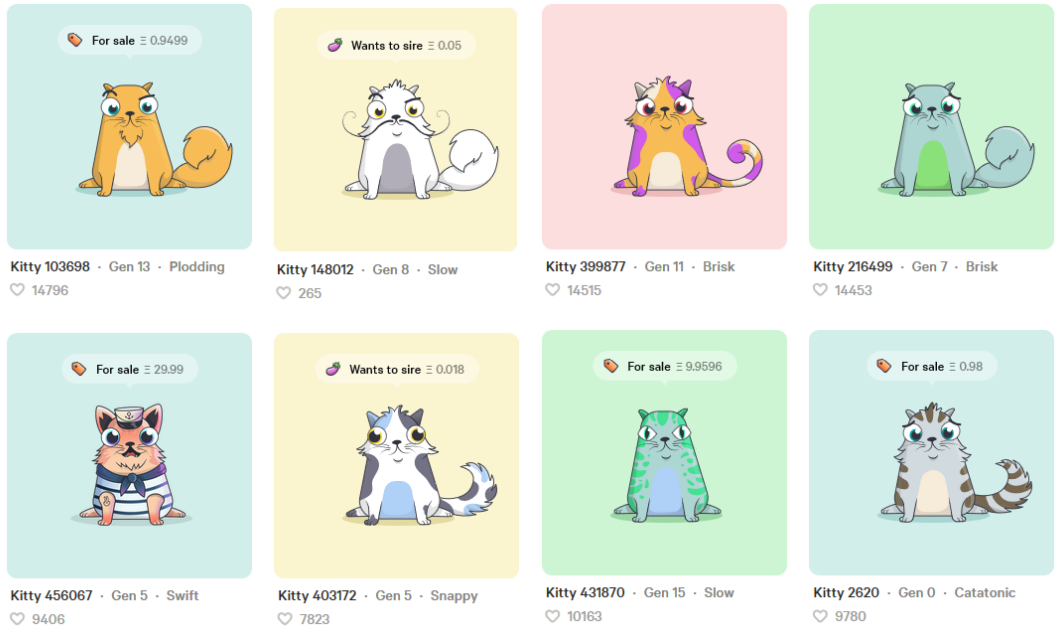
- Bilder kan hashas (ex: fiskar)
- Metallbalkar kan innehålla spårämnen.
- *Hur säkerställer man en tomat?*



VIKTIGASTE INNOVATIONERNA

- Distributed trust
- Digitalt ägande
- Smarta kontrakt





PASSAR BLOCKCHAIN?

- Finns det många inblandade parter?
- Litar inte alla på varandra?
- Behövs spårbarhet av händelser?
- Säkrar vi ägarskap av specifika resurser?
- Vill vi ha transparens mellan parterna?

Svarar man ja på flera frågor passar en blockkedja.

ANVÄNDNINGSOMRÅDEN

HÖGSKOLAN VÄST

Kryptovaluta
- digitala betalningar
- definitiva
- multisignatur
- billiga (lager 2)

Ägande
- ägarregister
- registrera köp och sälj
- ej duplicerbart

Dokument
- notarie
- tidsstämpling
- journaler
- kontrakt
- examina, …

Identitet
- lagra identitet
- bevisa identitet

Supply chain
- vem har produkten nu
- absolut spårbarhet

Maskinbetalningar
- program/prylar kan betala
- microbetalningar
- Ex: dator betalar för wifi

IoT
- uppdateringar
- kommunikation
- buggar

Smarta kontrakt
- självexekverande kontrakt
- autonoma program