Introduktion til Kryptovaluta

Joakim Sandroos

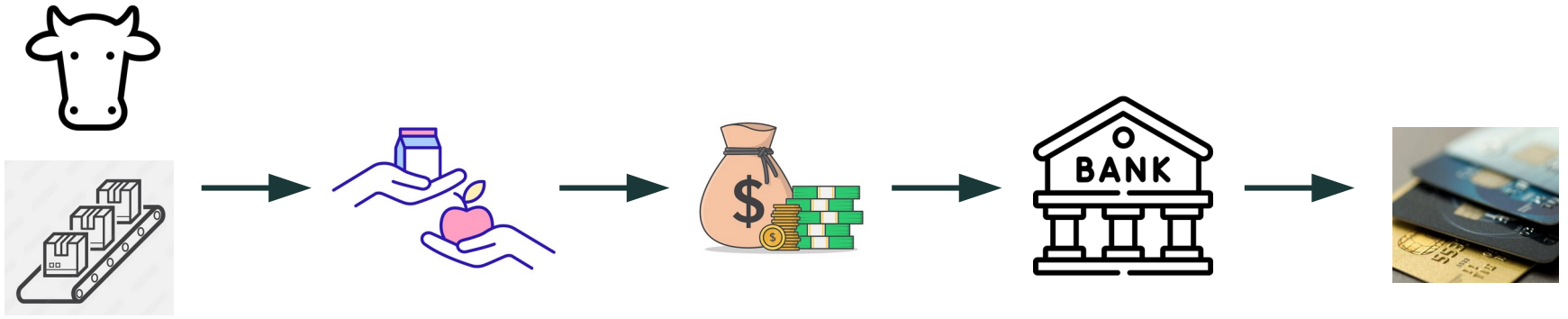
Longship
Invest

Agenda

- Penge!
- Krypto, konceptuelt
- Byg-en-kryptovaluta
- Mining og Marked
- Scams

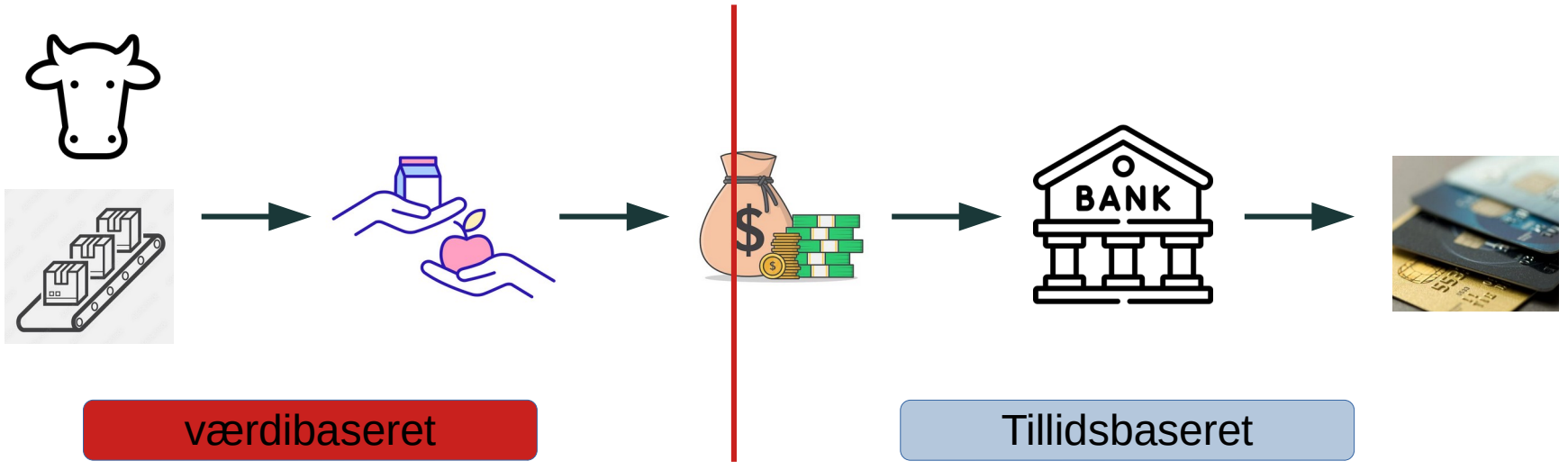
Penge!

- Tillidsbaseret system til overførsel af værdi



Penge! (Hvad er det?)

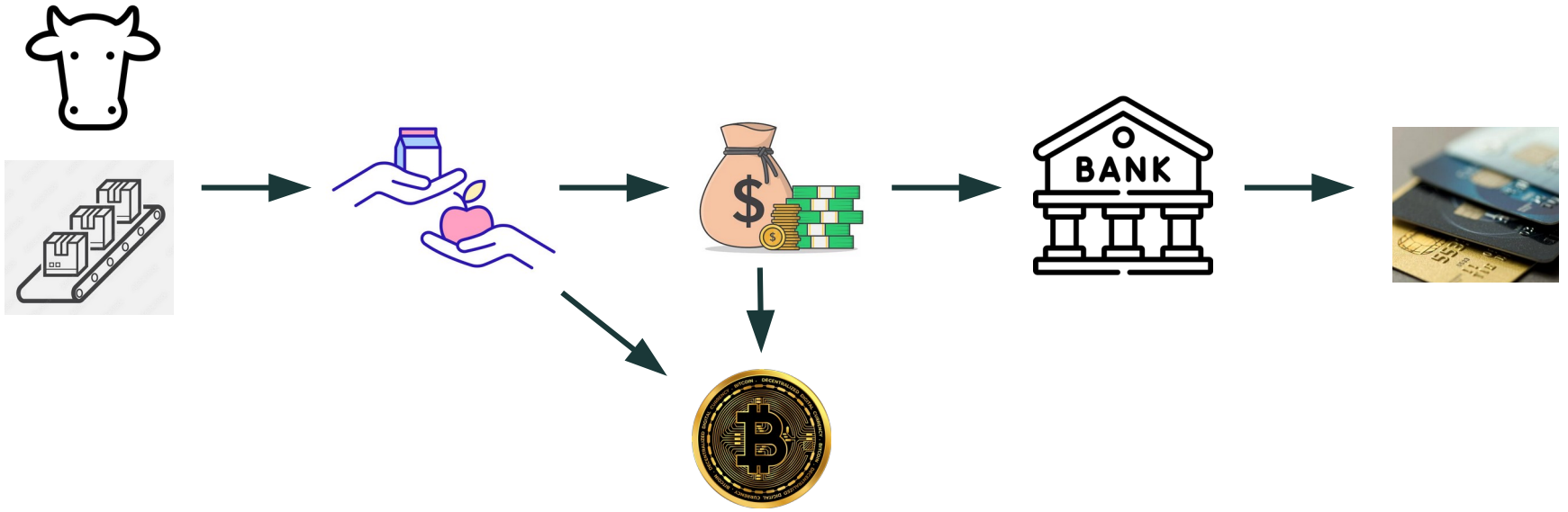
- Tillidsbaseret system til overførsel af værdi



1870 – 1971

Bitcoin

- Tillidsbaseret system til overførsel af værdi



KR/EUR/USD vs Bitcoin

FIAT ("let it be done.")

- Tillidsbaseret
- Falskmøntneri
- Kredit
- Anonymt
- Uendelig tilgængelighed
- Statskontrolleret

Bitcoin

- Tillidsbaseret
- Kryptografisk garanteret
- Hård forbrugsgrænse
- Sporbart
- Begrænset resource
- Decentral / Ukontrolleret

Kryptovaluta

Byg En kryptovaluta – 1: Setup

- 4 venner
- Én stor notesblok
- “jeg skylder” (“I owe you”/ IOU)
- Alle 4 kan skrive
  - Fx: Anders giver Joakim 50 kr
  - Mikkel giver Anders 23 kr
- Afregn fx én gang om måneden- via den totale historik

- Ledger

Byg En kryptovaluta – 1: Setup

Ledger:

- Anders giver Joakim 50 kr
- Mikkel giver Anders 23 kr
- Christian giver Mikkel 12 kr

- Ledger

2: Signatur

- Problem:
  - Hvad nu hvis nogen skriver falske transsaktioner?
- Løsning:
  - Kræv betalers signatur på hver transsaktion
  - Kryptografisk nøgle

- Ledger
- Signatur

2: Signatur, Krypto

- 2 nøgler: Private & Public
- Private: Krypterer. Public validerer
- Signatur baseret på indhold OG private key

$$sign(private\ key, indhold) = signature$$

- Validere signatur:

$$valid(signature, content, public\ key) = Sandt / Falsk$$

Nemt

Umuligt

- Fx, 0 og 1 konverteret til bogstaver og tal (64 lang):
  5c3beee676c460b530984477054ab01f71f3c5d70676c173e8b9118915d872ed

- Med private key kan man underskrive – keep them safe!

2: Signatur, Ledger

Ledger:

- Anders giver Joakim 50 kr, 00111001
- Mikkel giver Anders 23 kr, 01011011
- Christian giver Mikkel 12 kr, 11001010

- Ledger
- Signature

3: Kopier

- Problem:
  - Hvad hvis man kopierer en transsaktion

- Ledger
- Signature

3: Kopier

Ledger:

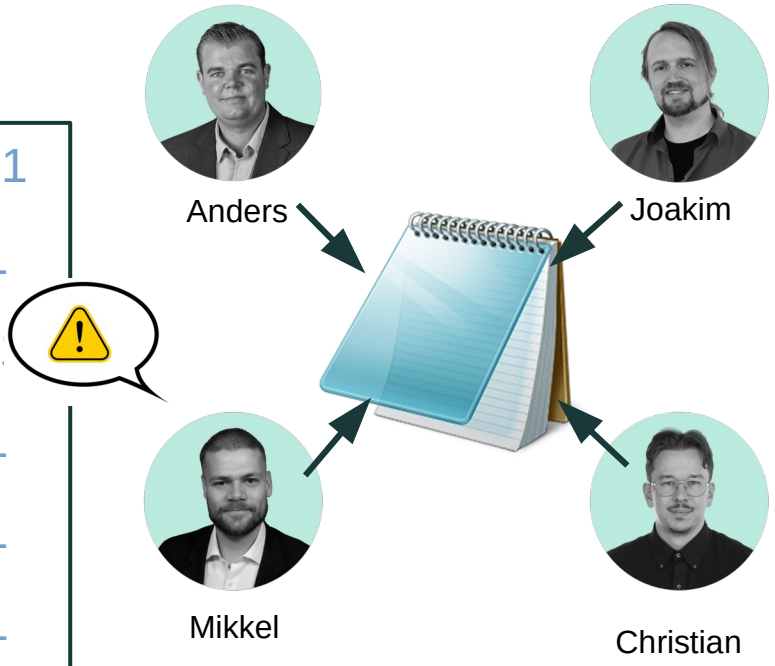
- Anders skylder Joakim 50 kr, 00111001
- Mikkel skylder Anders 23 kr, 01011011
- Christian skylder Mikkel 12 kr, 11001010

- Ledger
- Signature

3: Kopier

Ledger:

- Anders skylder Joakim 50 kr, 00111001
- Mikkel skylder Anders 23 kr, 01011011
- Christian skylder Mikkel 12 kr, 110010
- Mikkel skylder Anders 23 kr, 01011011
- Mikkel skylder Anders 23 kr, 01011011
- Mikkel skylder Anders 23 kr, 01011011
- Mikkel skylder Anders 23 kr, 01011011



- Ledger
- Signature
- ID

3: Kopier

- Problem:
  - Hvad hvis man kopierer en transsaktion
- Løsning:
  - Alle transsaktioner får et unikt ID
  - ID bliver en del af underskriften

- Ledger
- Signatur
- ID

$$sign(ID, private\ key, content) = signature$$

3: Kopier, Ledger

Ledger:

1) Anders skylder Joakim 50 kr, 10011100
2) Mikkel skylder Anders 23 kr, 110110110
3) Christian skylder Mikkel 12 kr, 10010101

- Ledger
- Signatur
- ID

4: Regler (protocol)

- Problem:
  - Hvad nu hvis nogen ikke betaler hvad de skylder?
- Løsning:
  - Indbetal eller indsæt beløb fra start
  - Lav regel om ikke at overskride beløbet

- Ledger
- Signature
- ID’s

Protocol

4: Regler, Ledger

Ledger:

1) Anders modtager 100 kr
2) Joakim modtager 100 kr
3) Mikkel modtager 100 kr
4) Christian modtager 100 kr

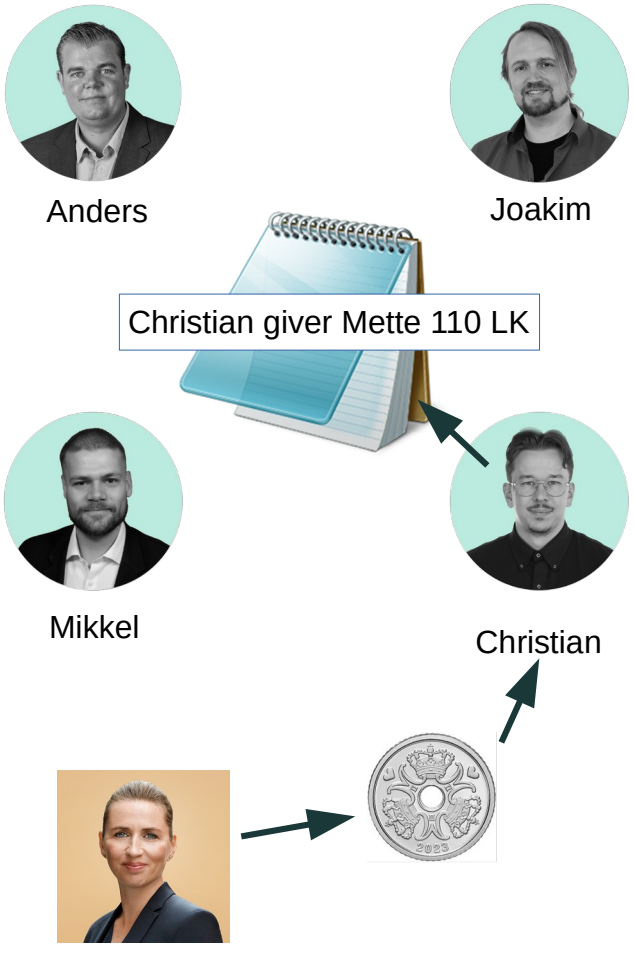
5) Anders giver Joakim 50 kr, 10011100
6) Mikkel giver Anders 23 kr, 110110110
7) Mikkel giver Anders 80 kr, 10010101

Ulovlig Transsaktion!

- Ledger
- Signature
- ID’s
- Protocol

4: Regler, Resultat

- Penge bliver overflødige,
  kr → LK
- Kan veksle mellem kr og LK:
  - Nye deltagere
  - Fx: Mette giver 100 kr til Christian
  - Christian skriver: Christian giver rose 110 LK i ledgeren
- Vekslekurs er fri
- LK er uafhængig
- Nyt frit valutamarked



- Ledger
- Signature
- ID’s
- Protocol
- Valuta

Kryptovaluta: Hvad **er** det?

- Kryptovalutaen = Transsaktions historikken
- Din private key tillader at du kan skrive transsaktioner
  - men kun op til din kreditværdighed
- Din public key gør at din transsaktion kan valideres
- Cryptografisk verificeret system
- White Paper: Beskriver blockchainen og programmerne bag

KR/EUR/USD vs Bitcoin

FIAT

- Tillidsbaseret
- Falskmøntneri
- Kredit
- Anonymt
- Statskontrolleret
- Uendelig tilgængelighed

Bitcoin

- Tillidsbaseret
- Kryptografisk garanteret
- Hård forbrugsgrænse
- Sporbart
- Decentral / Ukontrolleret
- Begrænset resource

5: Decentral

- Problem:
  - Central ledger
  - Kan slettes eller modificeres
  - Kan vi stole på Udbyderen?
- Løsning:
  - Alle har deres egen kopi af ledgeren
  - Udsend alle transsaktioner
  - Alle skriver alle transsaktioner ned.

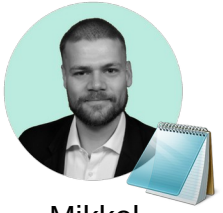
- Ledger
- Signature
- ID’s
- Protocol
- Valuta

6: Authoritative?

- Problem:
  - Hvad er den rigtige orden?
  - Hvilken Ledger er den rigtige?


Anders


Joakim


Mikkel


Christian

6: Authoritative: Løsning

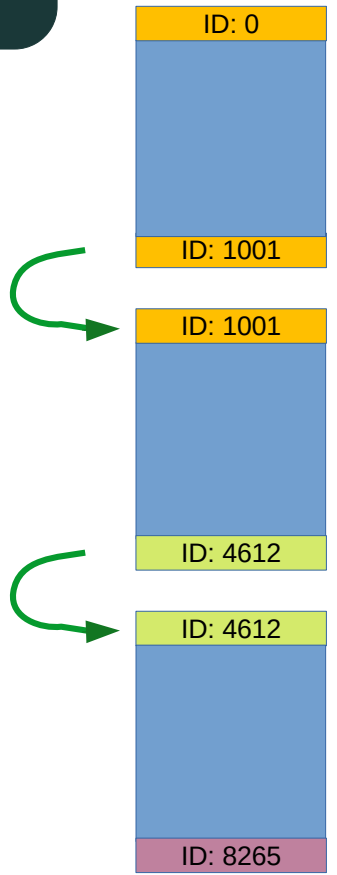
- Løsning: ID-search
  - Indfør et ukendt Ledger ID
  - Brug hash funktion på
  - Kræv fx 30 første tal er nuller
  - ledger er signed, når det ukendte ID er fundet

$$sign(\text{Ledger-ID},\ private\ key\ , content) = ledger\ signature$$

- Kan kun finde Ledger ID ved at gætte (maaaange kombinationer → meeeeget computerkraft)
- Hvis ledgeren er signeret med kravet **ved** vi at der er brugt arbejde på at validere den.

7: Blocks

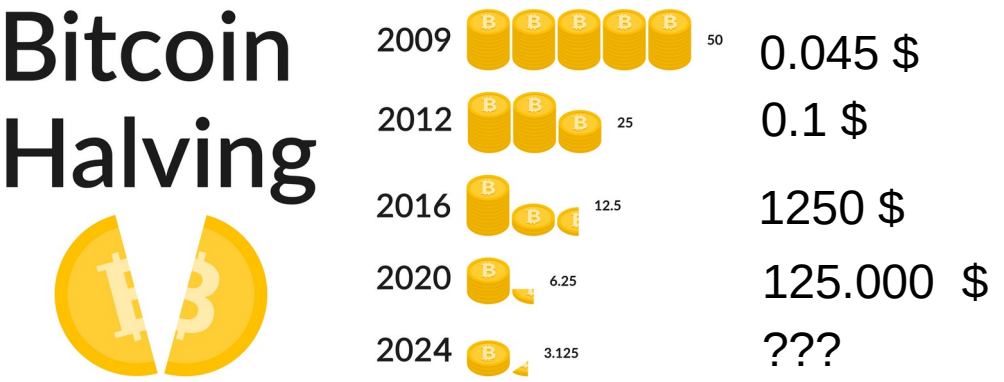
- Problem:
  - ét unikt ledger-ID medfører
  - Ledgeren kan ikke verificeres igen (hvorfor systemet dør)
  - Eller verifikation tager uendeligt længe
- Løsning:
  - Del ledgeren op i ‘blokke’
  - Slutte med unikt block-id (før ledger-id)
  - Starte med forgængers unikke block-id
- Resultat:
  - Alle blokke er kryptografisk forbundet
  - Umuligt at ændre eller snyde uden at skulle gentage alt ‘gætte’ arbejdet



$$sign(\text{Block-ID},\ private\ key, content) = Block\ signature$$

Kryptografisk Validering

- Hver block må valideres via ID-search
- Find et block-id: Modtag Belønning
- Eneste måde at skabe nye bitcoin → Bitcoin Mining!
- Belønning Halveres hvert 4 år
- “Mini lotteri”

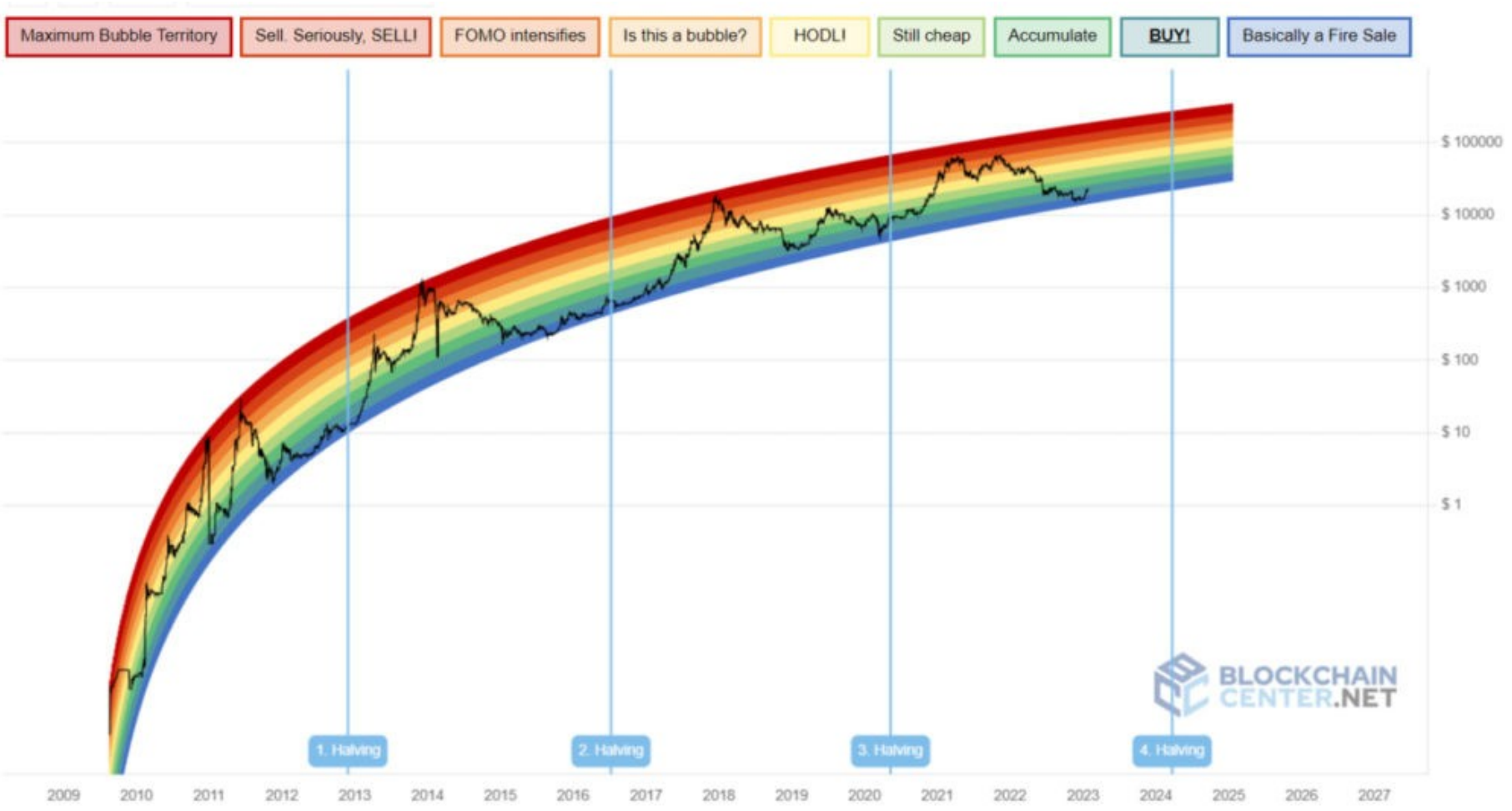


Værdi Fastsættelse

- Frit marked
- Sammenhæng mellem (begge klassisk udbud/efterspørgsel):
  - Mining værdien – transsaktioner kræver validering
  - Valutaens tilgængelighed – køb / salg
- Den coin vi har designet er Bitcoin
- Andre coins kan have andre protokoller og sikkerheder
  (eller manglen på samme)

- Gratis råd: Vid hvad I køber før I investerer

Historisk pris



Historiske Scams

- Andrew Tate: Hustler's University
  - "Lær at Trade" website
  - Pyramidespil + associerede coins

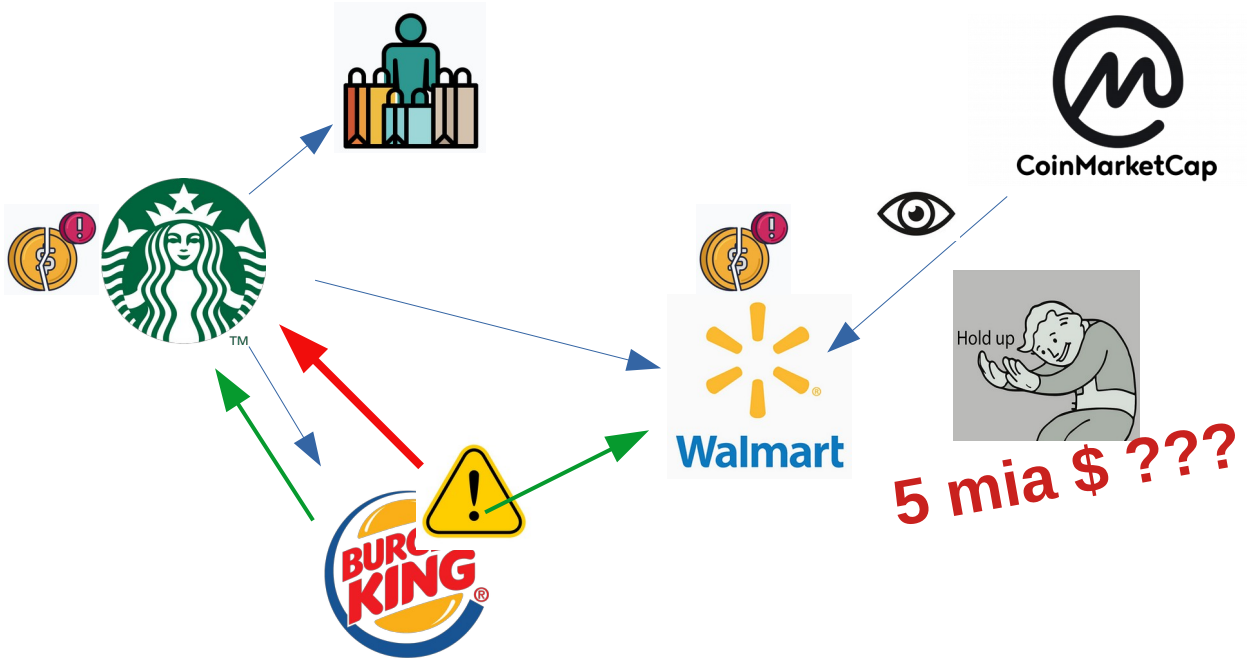
- Bitconnect: Guaranteed Investments
  - Ponzi Scheme:
    (Brug likviditet fra investorer til at betale investorer der vil trække deres midler ud)
  - https://www.youtube.com/watch?v=kNdp0I8AG40

- Squid game: Rug Pull
  - Hype Token så prisen stiger
  - Fine print: 2-1 køber / sælger ratio
  - ~16 mio $ op i røg

Bonus:
Falskt Advokatfirma Sagsøger!

FTX: Creative Liquidity

- sam bankman-fried & Caroline Ellison



- Starbucks udsteder 'starbucks' coins & kunderne køber – det går godt
- Burger king køber også en hel del
- Wallmart investerer/trader, og det går godt for deres kunder
- Prisen stiger
- Coinmarketcap: 5 MIA? Dém kan starbucks da ikke dække
- Burger king sælger ALLE deres starbucks coins
- Prisen kollapser
- Wallmar og Starbucks er på randen af konkurs
- Burger king melder ud: Vi opkøber jer – men skifter mening efter de ser regnskaberne
- Starbucks og Wallmart var ejet af samme ejere
- Begge går konkurs og ejerne flygter til Bahamas

Bot Scams

- Handler med algoritmer / “Bot” for simplere sprogbrug
- Høj return rate (fx 10% om ugen)
- Ekstremt høj ‘positiv handel’ rate (umuligt)

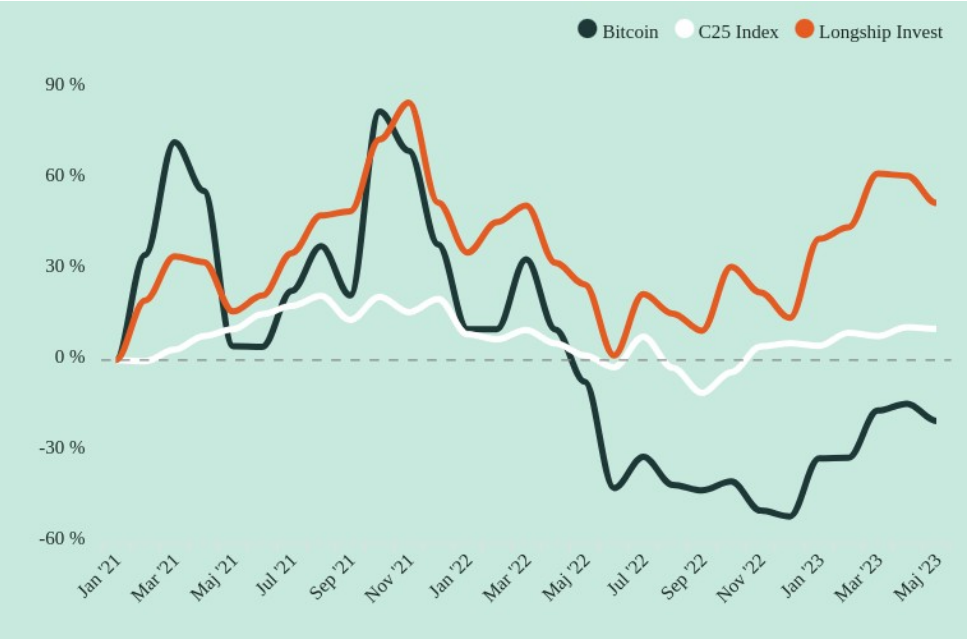
- Traders Domain: Ponzi Scheme,
  - ~500.000.000 $
  - Tidlige investorer kan få pengene ud
  - Ændrede handler ‘retroaktivt’
    → Bankrun
- EZBot: Pyramide Spil
  - Agressiv markedføring
  - Tidlige investorer kan få pengene ud & blive ‘founders club’ medlemmer
  - Hovedsæde I Dubai

Undgå scams: Checkliste

- Registreret virksomhed
- Åbent hvem der driver virksomheden og er ejere
- Realistisk afkast
- Kend din investering

Longship Invest

- Investerer kun i coins vi kender (!)
- Low frequency handel
- Algoritmer er historisk testet på 38 børser
  - Optimeret med metoder fra statistik, økonomi og partikelfysik
- Statistisk vist at det **ikke** er et tilfælde at vi slår markedet
  - **99.88%** sandsynlighed
- Find vores prospekt på
  - http://www.longshipinvest.dk/



Afsluttende Kommentarer

- Kryptovaluta: Kryptografisk sikrede penge
- Decentralt og frit
- Mange forskellige – Kend dem du investerer i

Tak for Opmærksomheden

- Spørgsmål / diskussion ?

Longship Invest

Appendix

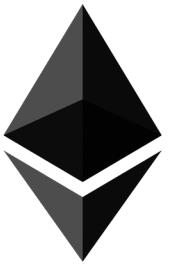
Blockchain Muligheder

- Finanssystemer
- Stemmesystemer
- Shipping og logistik ordrer
- Skøder og Kontrakter
- Sociale Medier
- E-faktura v.2.0

Mulighed for at gøre
centraliserede service
Udbydede forældede

Smarte Kontrakter

- Programmer af “hvis A, så B” logik
- Uintelligente – følger programmet 100%
- Statiske efter ‘søsættelse’
- Svært at gøre sikker / fuldt dækkende



ethereum

Ordforklaring

- Ledger: Regnskabsbog
- I-owe-you: Gældsbrev
- Pyramidespil: Ikke et spil, men ulovlig markedsføring der kræver flere og flere deltagere
- Coin: Kryptovaluta
- Decentral: Uden central autoritet eller kontrol
- White Paper: Beskriver blockchainen og programmerne bag

Moderne Monetært System

- Centraliseret økonomi
- Centralbanker
  - udsteder valutaer
  - Fastsætter renter
  - stats obligationer
- Banker m. Licens udsteder ‘I-owe-you’ – lån - essentielt penge