De digitale euro: Wat kunnen we leren van crypto?

Jacob Boersma
Warren Brandeis

Geschiedenis van geld: ruil, munt, papier

Eigenschappen van geld

1. Store of value
2. Medium of exchange
3. Unit of account

Dus behoefte aan:

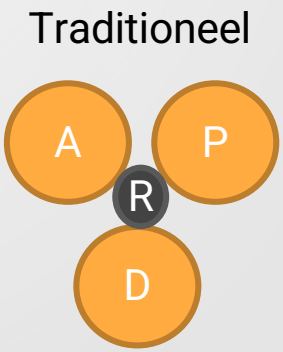
- Vaste waarde (niet teveel fluctuatie)
- Controleerbaar (vertrouwde uitgever, moeilijk vervalsbaar)
- Eenvoudige uitwisseling (zonder een derde partij)
- Brede adoptie (bereik, rekeneenheid)

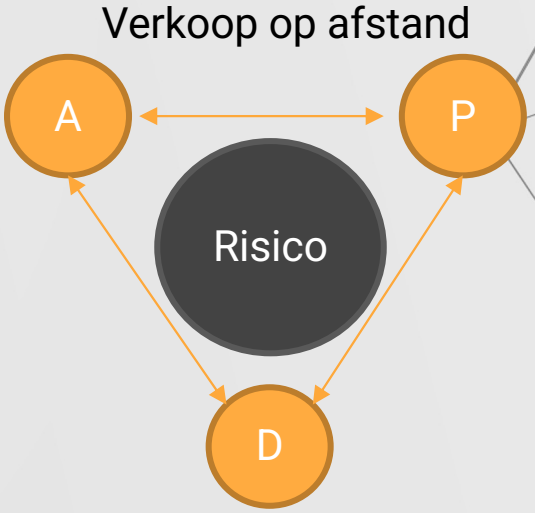
Op afstand betalen: banken, kaarten, internet

Wat maakt op afstand betalen een uitdaging?

Doordat de context verandert, neemt het risico toe:

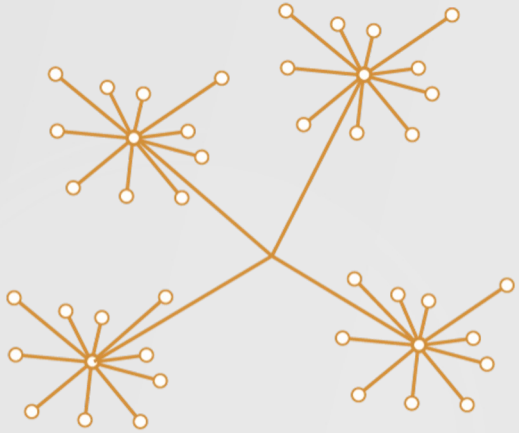
1. Relatie (tussen koper en verkoper)
2. Locatie
3. Timing





Centraal vs. decentraal vs. gedistribueerd

Network: Centralised



Decentralised

Distributed network

Bitcoin: A Peer-to-Peer Electronic Cash System

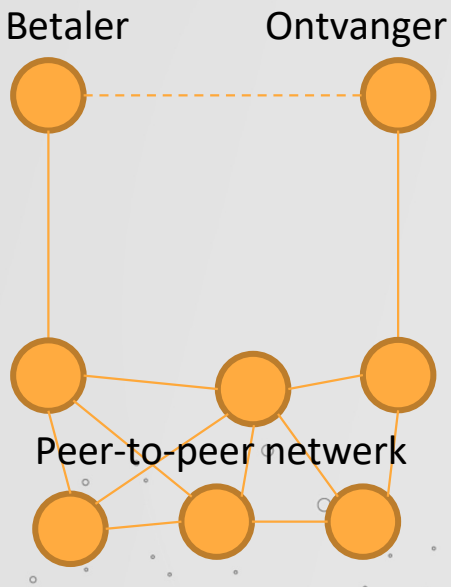
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

Peer-to-peer: de ultieme decentralisatie



- Iedere gebruiker zelf de controle
- Was voorheen niet mogelijk online, sinds kort door blockchain (maar nog in kinderschoenen)
- Wat is het verdienmodel, ook voor bv. banken?
- Trust vs. verification

Cryptocurrencies als geld

Sterke eigenschappen

- Transparantie, controleerbaarheid
- Oncensureerbaar
- Robuust
  (geen single point of failure, 100% uptime)
- Veel innovatie

(open source, open standaarden)

Nadelen

- Volatiliteit
- Moeilijk Schaalbaar
  (begint te komen met layer 2 solutions)
- Traceerbaarheid
- Scams
- Beperkte adoptie
  (banking the unbanked)

- Store of value +
- Medium of exchange +/-
- Unit of account –

Stablecoins

Gekoppeld aan euro, dollar of andere valuta
Oplossing voor volatiliteit probleem → betere store of value, unit of account

Veel (gecentraliseerde) organisaties geven al stablecoins uit:

- Collateralized (Tether, USDC)
- Algorithmic (Terra/USD, DAI)

En toen was er: Meta

- Libra
- Diem
- …

Bloomberg

How $60 Billion in Terra Coins Went Up in Algorithmic Smoke

By Muyao Shen
21 mei 2022

If you put $1 under your mattress, you know you'll get $1 back when you go looking for it. When you deposit $1 with a bank, you can be pretty sure you'll get it back even if they do more with it than lock it in a vault, thanks to regulations developed over centuries. A branch of cryptocurrencies called stablecoins has been trying to replicate that kind of dependability in totally new ways. Some have used the equivalent of a digital vault to back up

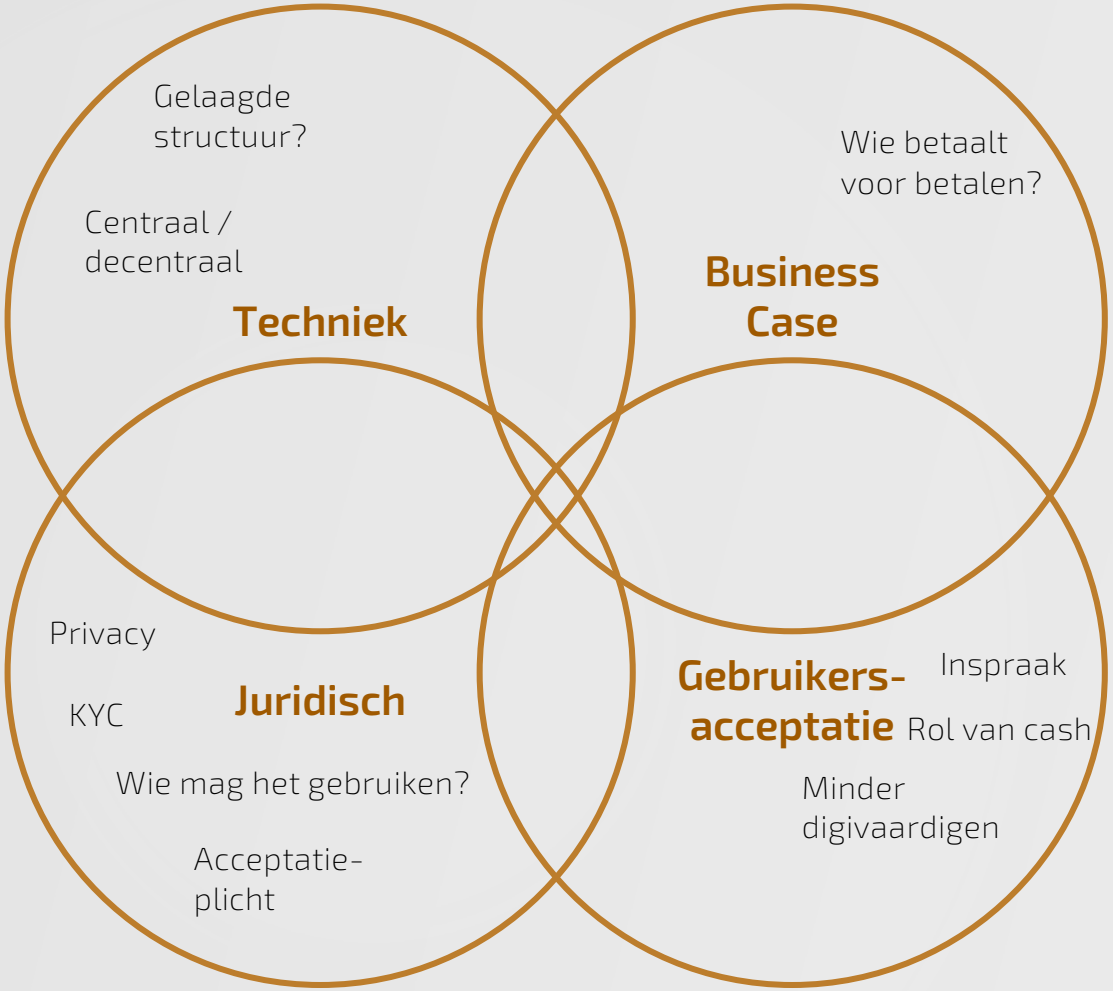
Wat willen we in een digitale euro?

- Traceerbaarheid?
  (banken kijken al steeds meer mee)
- Transparantie?
- Peer-to-peer?
- Offline bruikbaar?
- Programmeerbaarheid?
- Open stelsel?
  (banking the unbanked)
- Grootschalige adoptie

De rol van de wallet:
Bij betalen en bij Digital Identity

Wallet applicatie is er voor de gebruiker (consument, burger)
Openheid (keuzevrijheid) en transparantie zouden centraal moeten staan

Discussie op meerdere vlakken



Welke waarden liggen ten grondslag aan ons geldsysteem, en hoe vullen we die in?


“In the future we will still need banking,
but we may no longer need banks”
– Bill Gates
$3,812.57
BUY

Jacob.Boersma@warrenbrandeis.io
warrenbrandeis.io