Which year ???

p2p Electronic Cash System

2008

BITCOIN

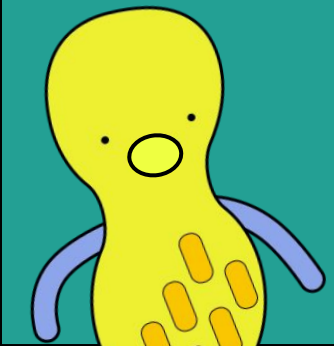
A PEER-TO-PEER
ELECTRONIC
CASH SYSTEM

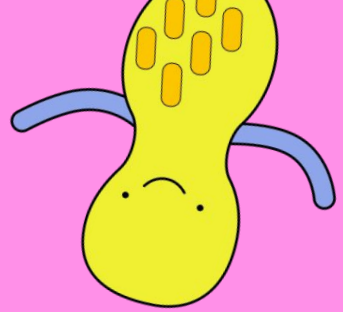
Abstract. *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.*

STILL HAS NOT TAKEN OVER THE WORLD :(

2008

Ancient...



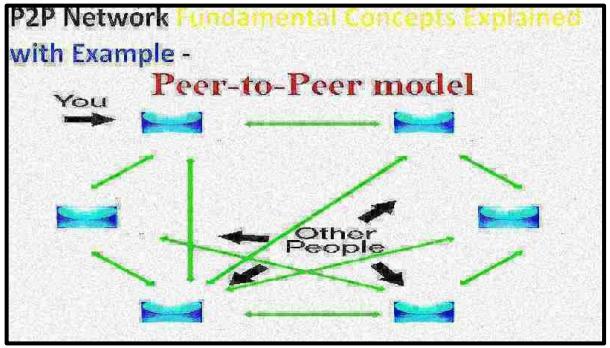


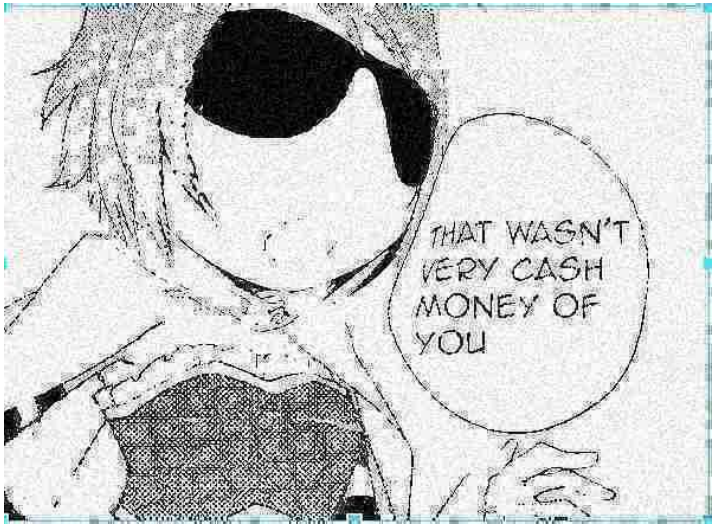
BRRRR

hehe

Answer to 2007-8 crisis?

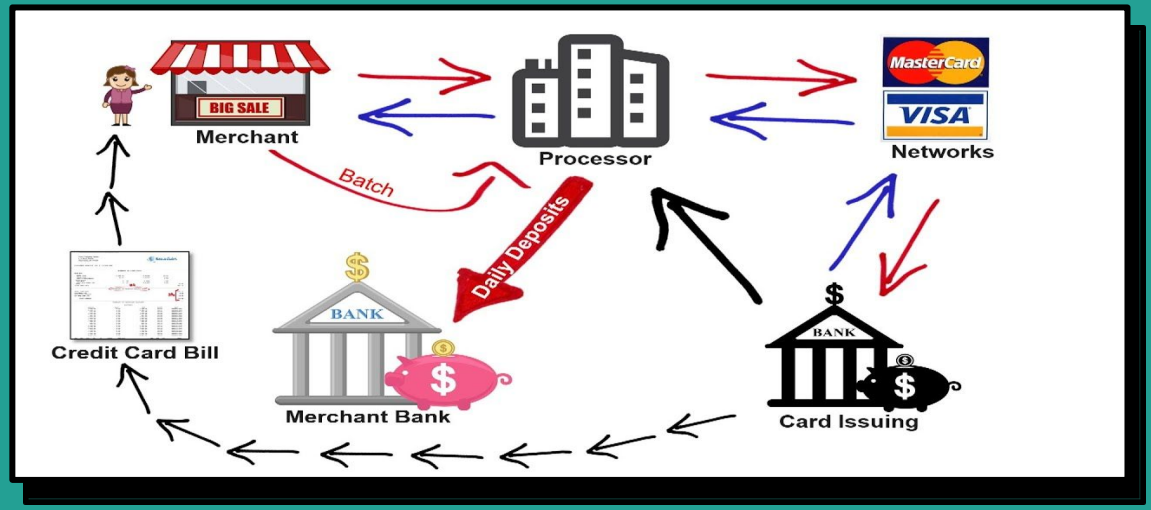
P2P





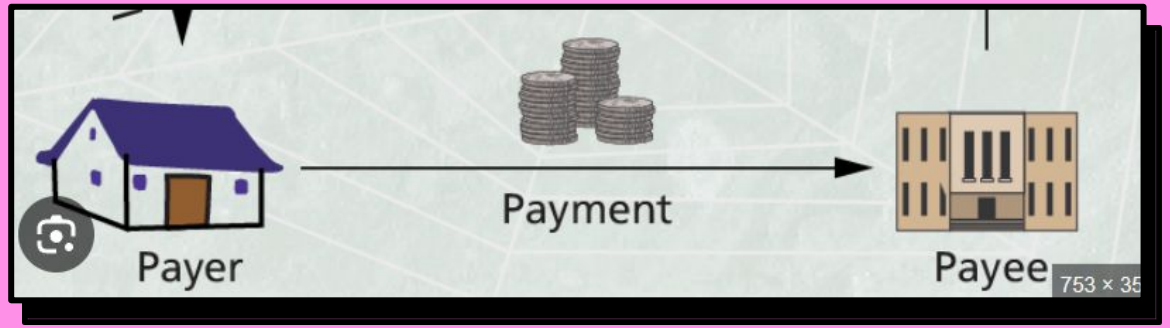
CASH =/= GOLD

CASH == RAW PAYMENT



Cards:

- *Chargebacks.*
- *Credit / Debit.*
- *POINTSSSS & rewards lol.*



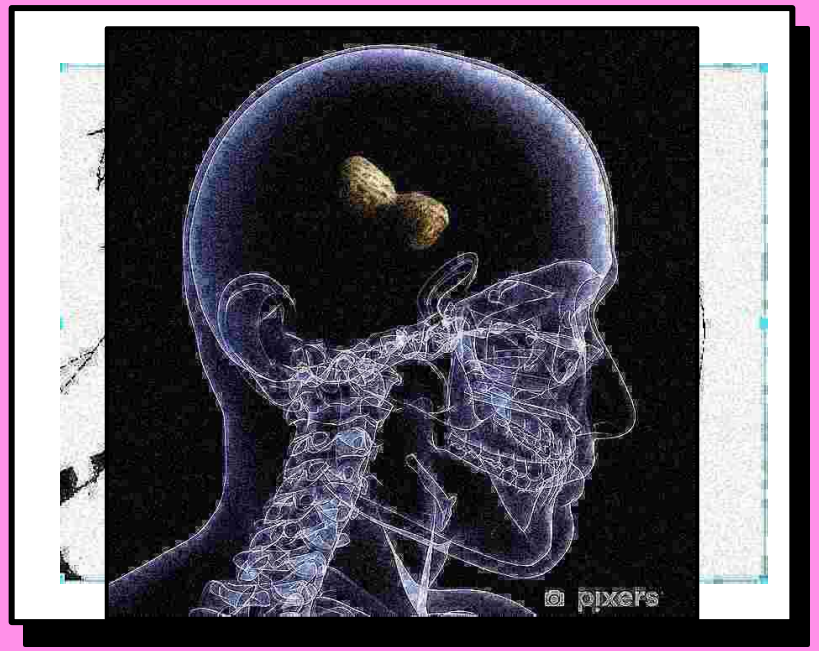
AGENDA

> Mini intro
> Mini-History

y no p2p cash yet?

5 blocker candidate:
> Scalability
> Privacy
> Stablecoins
> Account management
> Interop

kkonrad ☺️ peanut brain at peanut

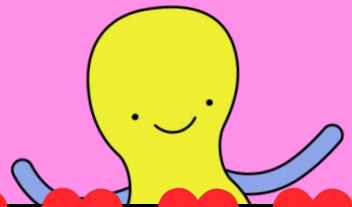


kkonrad.com ☺️ peanut.to ☺️
t.me/kkonrad

HISTORY

HONOUR THY ANCESTORS

Bitcoin - 2008
Litecoin - 2011
Ripple - 2012
Dogecoin - 2013
Nxt - 2013
Ethereum - 2013
Dash - 2014
Stellar - 2014
Monero - 2014
Zcash - 2014



THE BOOTSTRAP PROBLEM

2017

2024

1 token 1 chain

AGENDA

~~> Mini History~~

y no p2p cash yet?

5 blocker candidates:
> Scalability
> Privacy
> Stablecoins
> Account management
> Interop

SCALABILITY

SCALABILITY

> *In order to compete with tradfi payments, we have to be similarly cheap and fast. Visa has 24k TPS.*
> *Btw, my new altchain has 69k tps.*

SCALABILITY

1. This mistakes card payments (e.g. chargebacks, rewards) with cash (raw payment).
2. Some payments should already be cost effective
   a. Large
   b. Rare international pairs (many hops)

SCALABILITY

> Startup idea: a TransferWise but with crypto rails.
> Replace just what's costly. No need for e2e.

SCALABILITY

You need two banks to agree to not ban you. But if you can get two banks to sign contracts then you might as well just use tradfi IOUs.

PRIVACY

PRIVACY

Hard privacy: Monero & Zcash.
Obfuscation: CEXes.

STABLE VALUE

STABLECOINS

> You can’t make payments in a highly volatile currency.

STABLECOINS

1. That’s false. Many national currencies are highly volatile.
2. Rails thesis (only use crypto for settlement, but not e2e) still holds.

ACCOUNTS

AA

> AA is necessary for mass adoption in payments. Better onboarding, account recovery, granular permissions etc.

Again, a subset works. Yet, we've not even seen a subset.

UNLOCK FOR MASS PAYMENTS?

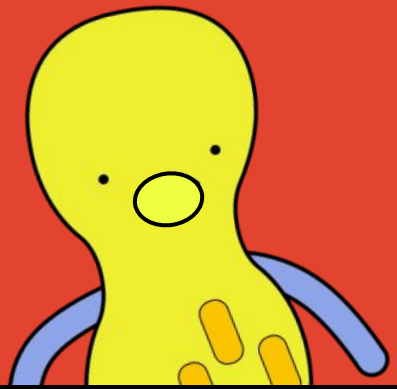
INTEROP

(To avoid the 1 chain 1 token bootstrapping problem)

INTEROP THESIS

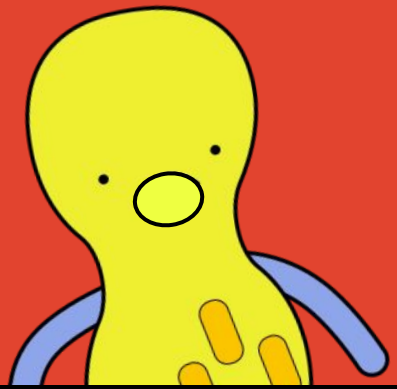
Interoperability is a necessary condition for interchangeability, which is a necessary condition for any new payments network.

“I have coins on Scroll, and I want to pay [you] for coffee … you are only set up to receive coins on Taiko. Wat do?”
- Vitalik, Ethereum Intern



MULTICHAIN MADNESS MULTICHAIN MADNESS

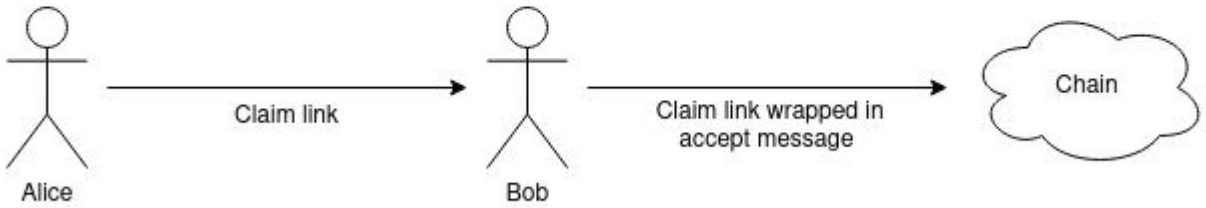
“I have coins but you want fiat. Wat do?”
- peanut brain at peanut protocol

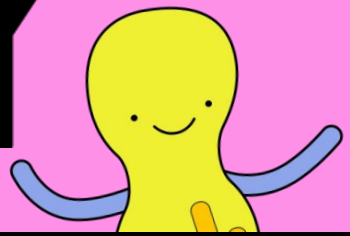


TRADFI INTEROP

NNN Challenge

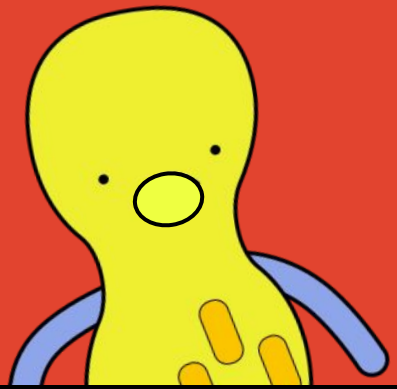
Another category of solutions has to do with abandoning the concept of user-facing addresses altogether, in a similar spirit to the Bitcoin payment protocol. One idea is to rely more heavily on direct communication channels between the sender and the recipient; for example, the sender could send a claim link (either as an explicit URL or a QR code) which the recipient could use to accept the payment however they wish.





VITALIK VITALIK VITALIK VITALIK

Is visa just eating our lunch?



TRADFI INTEROP

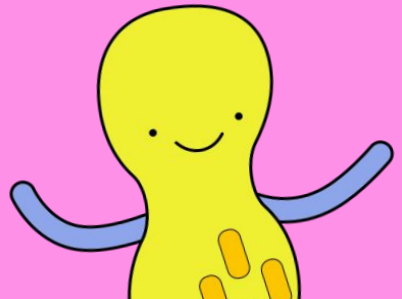
BITCOIN

“Bitcoin … discovered how to send value or money over the internet … especially for the people around the world that are unbanked”

Interview Jinyoung Lee Englund, Bitcoin Foundation - Zermatt Summit 2014

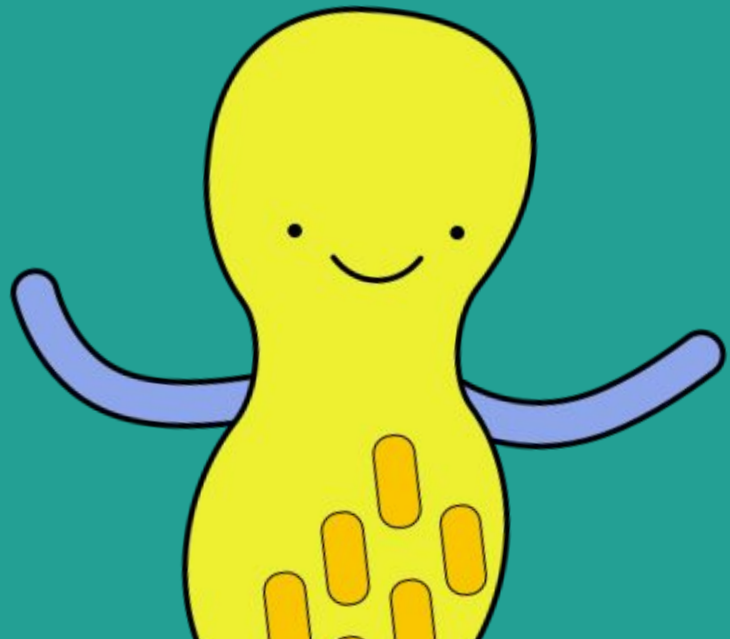
This is where crypto shines!

Permissionless, accessible.

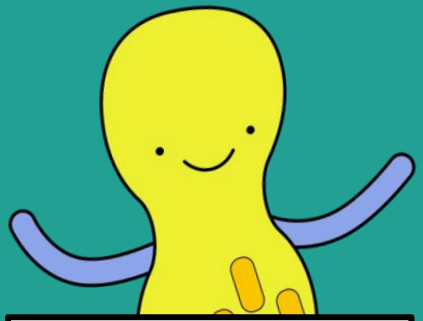


1. **Scalability**
2. **AA + onboarding**
3. **Stablecoins**
4. **Privacy?**
3. **Interop & reg?**

All we need for a borderless & bankless world!



NEXT GEN NEXT GEN

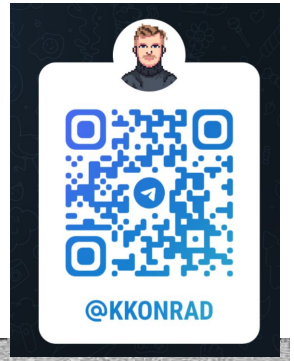


For simple finance all we need is:
Spend, receive, save.

BANKS → ~~**NEOBANKS**~~ → **ONCHAIN BANKS**

INTEROP

DM me. I WILL send you money.



peanut.to
t.me/kkonrad
@0xkkonrad