Blockkedjor utan hype

från en akademikers perspektiv

Tobias Pulls

- lektor datavetenskap
  - doktor 2015 kring kryptoprotokoll
  - misslyckad start av spin-off 2012-2016
- CAT, PAPAYA, HITS, WISR

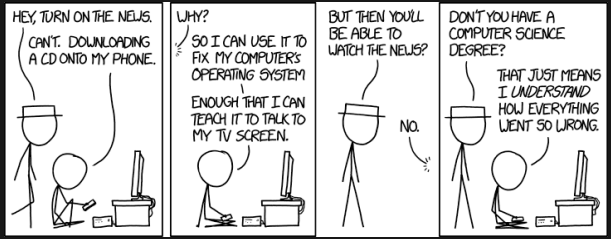
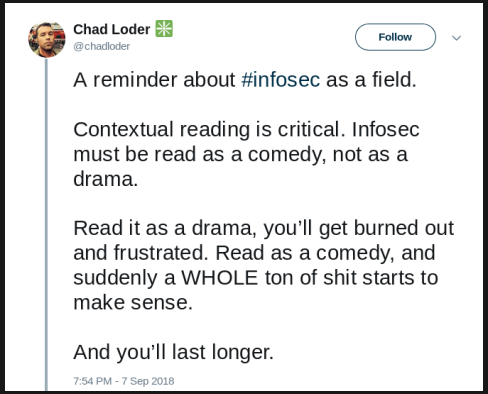


Bild: https://xkcd.com/1760/


Chad Loder
@chadloder
Follow
A reminder about #infosec as a field.
Contextual reading is critical. Infosec must be read as a comedy, not as a drama.
Read it as a drama, you'll get burned out and frustrated. Read as a comedy, and suddenly a WHOLE ton of shit starts to make sense.
And you'll last longer.
7:54 PM - 7 Sep 2018


1
NO
POVERTY

SUSTAINABLE DEVELOPMENT GOALS

17 GOALS TO TRANSFORM OUR WORLD

Home About Goals Partnerships Take Action News and Media Social Media Watch and Listen

Goal 1: End poverty in all its forms everywhere

Extreme poverty rates have been cut by more than half since 1990. While this is a remarkable achievement, one in five people in developing regions still live on less than $1.90 a day, and there are millions more who make little more than this daily amount, plus many people risk slipping back into poverty.

Poverty is more than the lack of income and resources to ensure a sustainable livelihood. Its manifestations include hunger and malnutrition, limited access to education and other basic services, social discrimination and exclusion as well as the lack of participation in decision-making. Economic growth must be inclusive to provide sustainable jobs and promote equality.

Källa: https://www.un.org/sustainabledevelopment/poverty/

Become a member

Medium

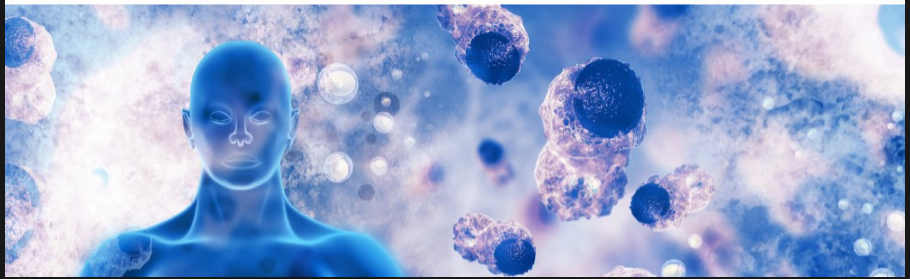
Sign in | Get started

Charlie Caruso Follow

Head of Global Growth for direct democracy NGO MiVote & CMO for Soar.Earth an innovative geospatial organisation putting mapping on the blockchain

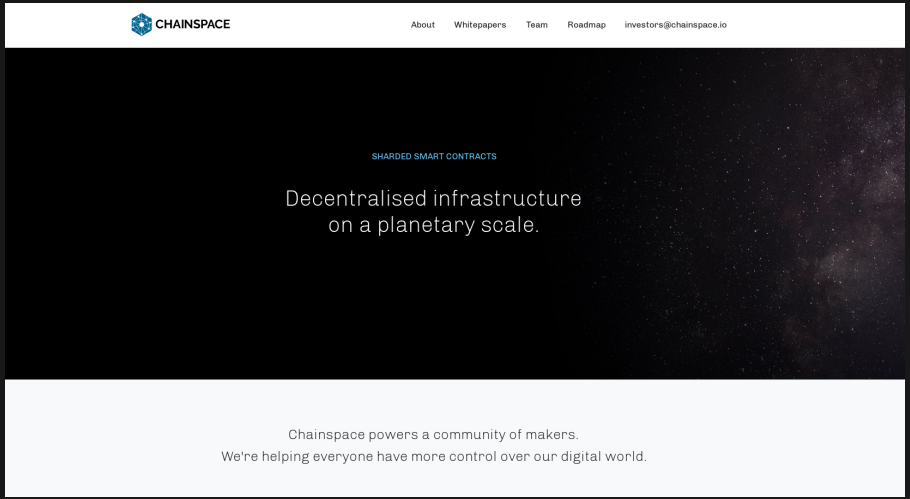
May 21 · 5 min read

How Blockchain could cure cancer



Källa: https://medium.com/@charliecaruso/how-blockchain-could-cure-cancer-e8afc0f173ef

Källa: https://www.dfinity.org/



Källa: https://chainspace.io/

Blockchain may resolve Irish border Brexit problem: Hammond

1 MIN READ

BIRMINGHAM, England (Reuters) - A solution to providing frictionless trade across the Irish border after Britain leaves the European Union might be found using technology such as Blockchain, finance minister Phillip Hammond said on Monday

Källa: https://www.reuters.com

Tre delar

1. **Datastruktur**: blockkedja eller “grafkedja”
2. **Nätverk**: öppet eller slutet (“permissioned”)
3. **Konsensus**: PoW, PBFT, PoS...

Tre delar

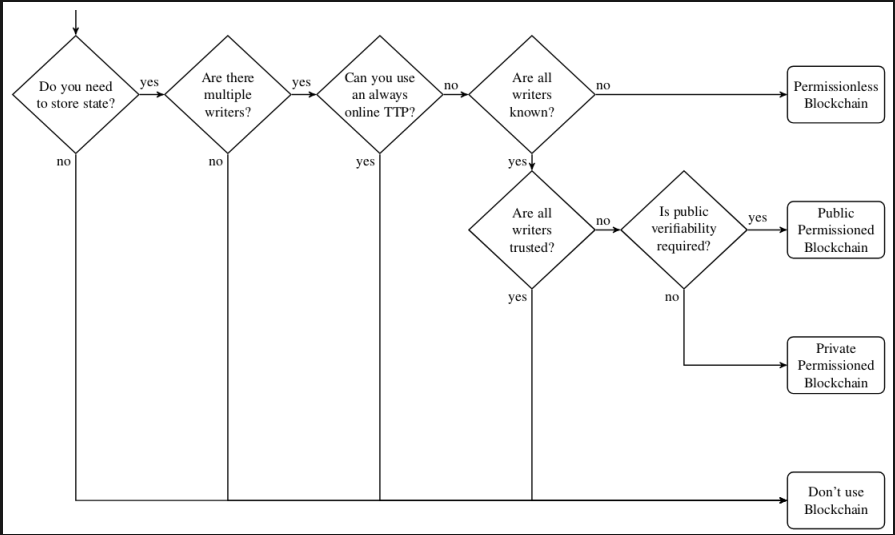
1. **Datastruktur**: blockkedja eller “grafkedja”
2. **Nätverk**: öppet eller slutet (“permissioned”)
3. **Konsensus**: PoW, PBFT, PoS...

Sedan

- data/kod i blocken
- samt logik för att tolka datan

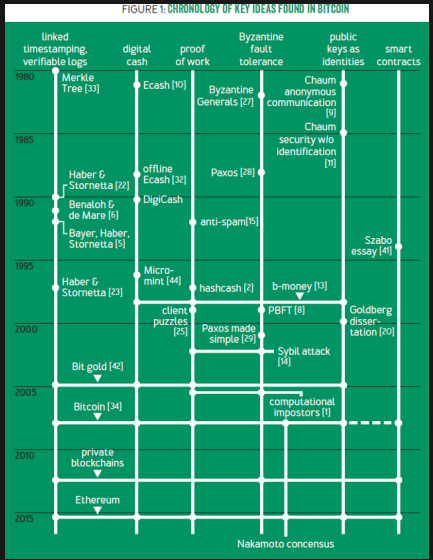
Bild: First Styles (CC-BY-3.0), https://www.iconfinder.com/firststyles

“Do you need a blockchain?”



Källa: Karl Wüst och Arthur Gervais, `https://eprint.iacr.org/2017/375`

“Bitcoin’s Academic Pedigree”

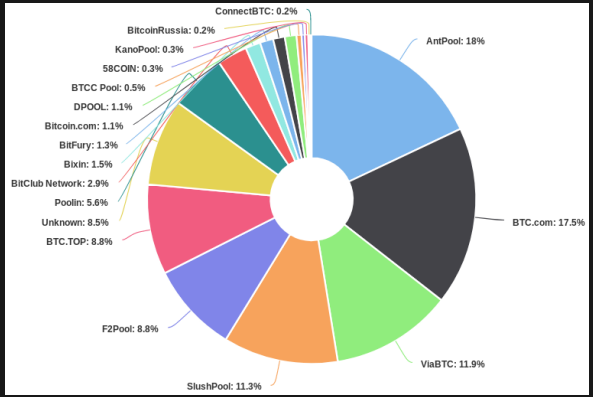


Källa: Arvind Narayanan och Jeremy Clark, `https://queue.acm.org/detail.cfm?id=3136559` (ACM)

Tre utmaningar

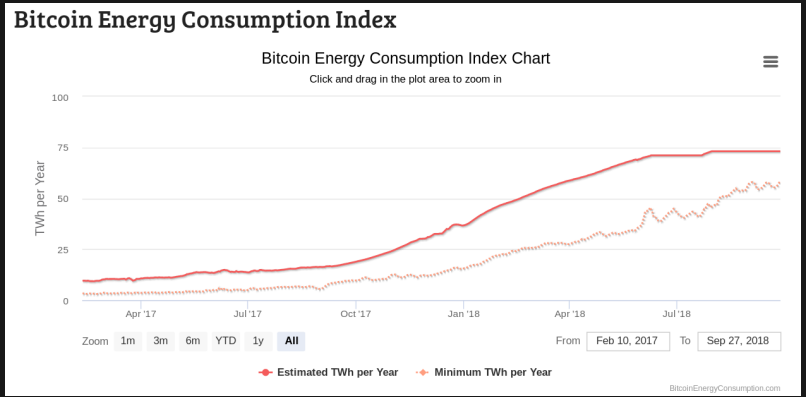
1. Konsensus: “säker” blockkedja?
2. GDPR
3. Mognad

1. Konsensus: “säker” blockkedja? (publika)



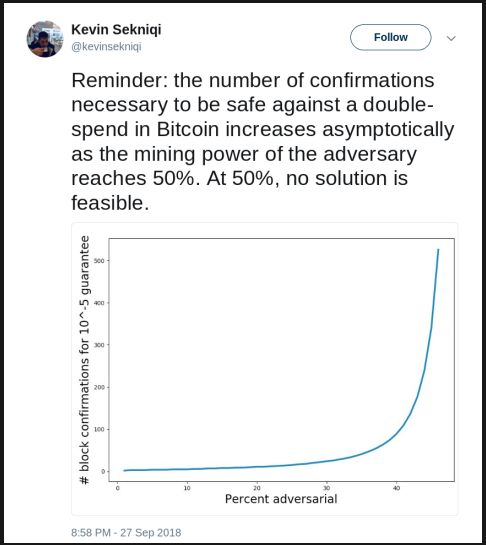
Källa: `https://www.blockchain.com/pools`

1. Konsensus: “säker” blockkedja? (publika)



Källa: `https://digiconomist.net/bitcoin-energy-consumption`

1. Konsensus: “säker” blockkedja? (publika)



1. Konsensus: “säker” blockkedja? (publika)

At a conceptual level, the barriers stem from the following: all cryptocurrencies require some source of (pseudo)randomness. In Proof-of-Work, this pseudorandomness is in some sense external to the cryptocurrency: the first miner to successfully find a good nonce produces the next block, and this miner is selected completely independently of the current state of the cryptocurrency.

In Proof-of-Stake, it is highly desirable that the pseudorandomness comes from within the cryptocurrency itself, versus an external source (due to network security concerns discussed in Section 2). One might initially suspect that with sufficiently many hashes or digital signatures of past blocks, this can indeed serve as a good source of pseudorandomness for future blocks. However, we formalize surprising barriers showing a fundamental difference between external pseudorandomness and pseudorandomness coming from the cryptocurrency itself.

Källa: Brown-Cohen et al., Formal Barriers to Longest-Chain Proof-of-Stake Protocols

1. Konsensus: “säker” blockkedja? (privata)

“vi litar inte på varandra,
men vi litar på att inte mer än en tredjedel av oss vill göra något elakt tillsammans”

1. Konsensus: “säker” blockkedja? (privata)

$\rightarrow$ om någon verkligen vill så går det snett

2. GDPR

Första formella analysen av en tillsynsmyndighet i EU

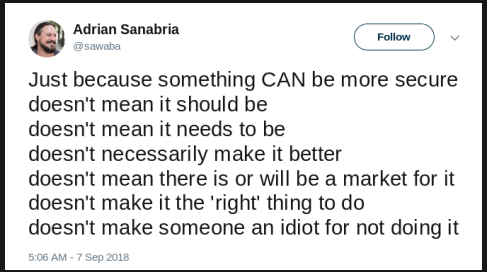
- blockkedjor + inbyggd integritet ≠ ❤️
- personuppgifter + publik blockkedja = nej
- personuppgifter inte direkt på kedjan
- kan vara personuppgiftsbiträden
  - kontraktsutvecklare
  - “mining”/konsensus noder
- automatiserade beslut (=från att kontrakt körs) måste gå att ändra

Bild: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

2. GDPR

$\rightarrow$ hejdå till väldigt många användningsområden (?)

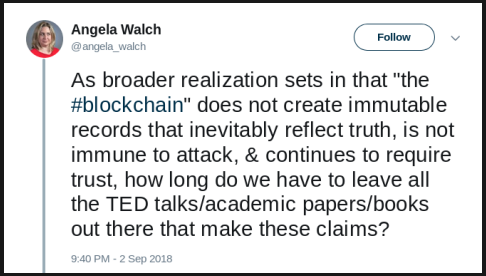
3. Mognad


Adrian Sanabria
@sawaba
Follow
Just because something CAN be more secure
doesn't mean it should be
doesn't mean it needs to be
doesn't necessarily make it better
doesn't mean there is or will be a market for it
doesn't make it the 'right' thing to do
doesn't make someone an idiot for not doing it
5:06 AM - 7 Sep 2018

3. Mognad


Sergio Caltagirone
@cnoanalysis
Follow
So true 👇 in #infosec you spend a career studying a small part of business risk - it's everything to you. But, only part of the picture for others. Respect that. If they don't do something you suggest, it may not be that they're stupid but they MIGHT actually know better than you
Patrick C Miller @PatrickCMiller
Replying to @cnoanalysis
It's ok if Managment wants to accept risk. Give them the best advice you can and move on.
1:30 AM - 31 Aug 2018

3. Mognad


Angela Walch
@angela_walch
Follow
As broader realization sets in that "the #blockchain" does not create immutable records that inevitably reflect truth, is not immune to attack, & continues to require trust, how long do we have to leave all the TED talks/academic papers/books out there that make these claims?
9:40 PM - 2 Sep 2018

3. Mognad


Arvind Narayanan
@random_walker
Following
5. The final agenda item: can blockchains improve the cybersecurity of the grid? The core of infosec is based on cryptography, network security, fault tolerant computing, etc. Blockchains can augment these classical technologies in some cases, but their role is at best marginal.
8:43 PM - 21 Aug 2018

Avrundning

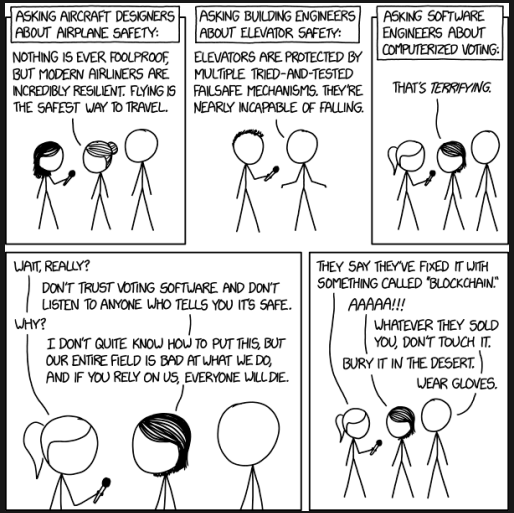


Bild: https://xkcd.com/2030/

tack!