# What (could) make blockchains useful?

Or at least interesting to me!

blockchain
workspace

Truth is confirmed by inspection and delay; falsehood by haste and uncertainty.

- Tacitus

blockchain
workspace

# Bitcoin Original Design Goals

- Hey Bas, why are you saying Bitcoin and not Blockchain?
  - The problem solved with Bitcoin was not “create a DLT that is safe”.
  - The problem that was solved was **monetary**, hence you cannot logically say “blockchain is disconnected from Bitcoin”. Bitcoin was the solution, “blockchain” at most a side product.
  - The corollary to this conclusion is that you cannot compare Bitcoin and “blockchain” as they may look alike, but are not. They occupy different niches.

blockchain
workspace

# Bitcoin Original Design Goals

- https://bitcoin.org/bitcoin.pdf

- “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.”

- “the main benefits are lost if a trusted third party is still required to prevent double-spending.”

blockchain
workspace

# Bitcoin Original Design Goals

- Goal:
  - “directly” -> Self-sovereignty
- Means:
  - Peer-to-peer
  - Digital Signatures
  - Hashes
  - Etc.

**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.

blockchain
workspace

# Bitcoin Original Design Goals

## My Old List

1. Immutability
2. Timestamping
3. Public key cryptography
4. Peer to peer network

blockchain
workspace

# Bitcoin Original Design Goals

## My New List

1. Immutability

blockchain
workspace

# Bitcoin Original Design Goals

- Failure state:
  - Trusted Third Party needed
    - Immutability compromised
      - Chain loses all usefulness in determining whether coins are legit.

**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.

blockchain
workspace

# Simplicity is Bliss


- While extremely simple and limited in scope, Bitcoin is exciting, as it is dangerous in its thinking.

- Its simplicity makes assumptions easy to test, which sharpens the dialogue.

blockchain
workspace

# Blockchain Design Goals

blockchain
workspace

# “Blockchain” Issues


Without knowing what you want to achieve,
you cannot know how to engineer a system.

blockchain
workspace

# “Blockchain” Issues

“Blockchain” products are all over the place because they do not strongly define what they want to achieve.

blockchain
workspace

# “Blockchain” Issues

- Quite a lot of projects just threw out the central tenet: disintermediation: Hyperledger Fabric, Corda, Multichain, and many more.

- Disintermediation can also be thrown out in the application, even if the protocol is still disintermediated.
  - Membership plans
  - Asset-backed Tokens
  - Centralised consensus plans

blockchain
workspace

# “Blockchain” Issues

- Blockchains can no longer make a fresh start. No “Immaculate Conception”. As a result, joiner incentives are completely different, leading to multiple distribution problems.

- Many projects do not think from first principles:
  - Decentralisation ditched: DPOS consensus, “governance” instituted badly with (just) voting
  - Badly written code (or not at all)
  - Naïve assumptions: “people won’t hurt their economic value”, “investors will want the project to succeed”, “entrepeneurs want control”.

blockchain
workspace

# Blockchain Talks (pun intended)


- “Blockchain” tech, as it stands is all over the place and riddled with contradictions. As such, it is extremely hard to discuss, as it is very easy to keep moving the goalposts.

- As a result, “blockchain” discussions tend to be like bar talk: wide ranging and rambling. Entertaining at first, but if you do it daily, exhausting and boring.

blockchain
workspace

# “Blockchain” Recommendations


- Statement #1: Blockchain projects that jettison core design principles are useless at best, fraudulent at worst.

- Statement #2: Blockchain projects should start from a very clear insight into the problem they want to solve, not naïve assumptions about the problem they find interesting (voting, identity, security, trading, money, whatever)

- Statement #3: Blockchain projects cannot assume because Bitcoin works, this automatically means they will work. Blockchains in their simplicity are HARD. Emergent behaviour will bite you in the bum if you mess up.

blockchain
workspace

# “Blockchain” Ideas


- Having talked, as a layman, to people inside banks, supply chain management, (semi)-government, it’s clear structures “work”, but are organisationally frequently a mess.

- We have a true opportunity to work to solve (some of) this mess.

- “Blockchain” alone will certainly not be a solution to any mess. It requires a structural action from the ground up. Start from first principles, most of which have been articulated, but not implemented (properly).

blockchain
workspace

# Blockchain Simple Proposal


Let's make the engineering clear and hard by making our goals simple.

blockchain
workspace

# Bas Wisselink

Teacher, trainer, writer

bas@baswisselink.com

https://www.linkedin.com/in/bwisselink/

www.baswisselink.com

Twitter: @DamelonBCWS

blockchain
workspace