

The Blockchain & The Internet of Things



Niels Olof Bouvin

The Blockchain & the Internet of Things

- **The blockchain**
- **Blockchains for the Internet of Things**

The problem of distributed trust

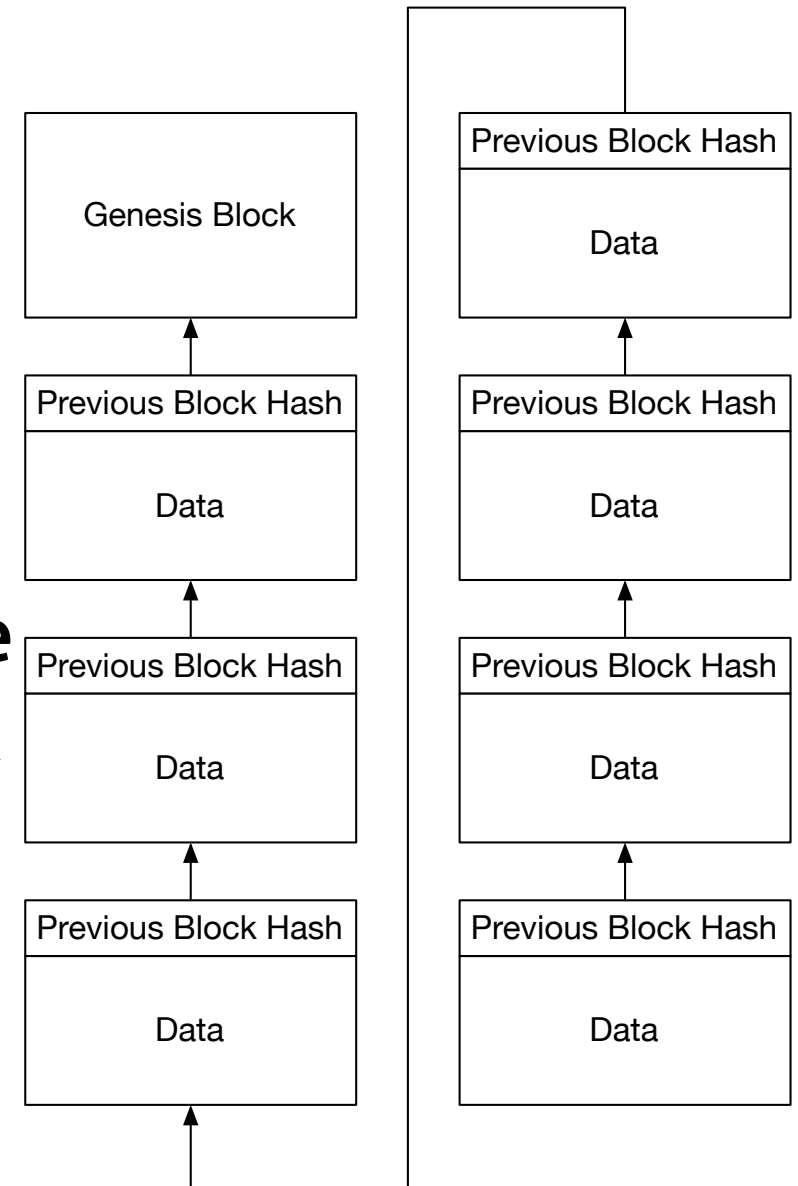
- **We have touched upon this before**
- **How do you establish trust in something important shared with faceless strangers?**
- **You can choose to put your trust in an authority**
 - like MobilePay, PayPal, eBay, etc
- **or you can do something else**

Requirements for public trust

- **Transparency**
 - all is public—no special privileges required except participation
- **Verifiability**
 - everybody can check and verify what takes place
- **Integrity & Immutability**
 - once committed, records cannot be changed
- **Consistency**
 - all will have the same records (eventually)

The blockchain

- A linked list of blocks containing data and a (crypto) hash value of the previous block (e.g., SHA256)
- Each hash validates the previous block, and thus the whole chain of blocks can be verified from the newest back to the genesis block
- Once it exists, a block cannot be modified without detection as that would invalidate the next and thus all subsequent blocks



What use is an immutable list?

Previous Block Hash
Transaction
Transaction
Transaction

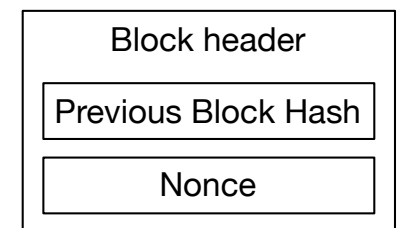
- It can be used to represent a *ledger*, i.e., a series of financial (or other) transactions collected in a block
 - a transaction might be 'Bob paid Alice ₿100'
- To defend against fraud, a transaction should be cryptographically signed by the issuer
 - i.e., (Bob paid Alice ₿100)_{signed by Bob} where Bob's public key is known by all
- Once bundled up in a published block, the information cannot be modified

Fraud prevention

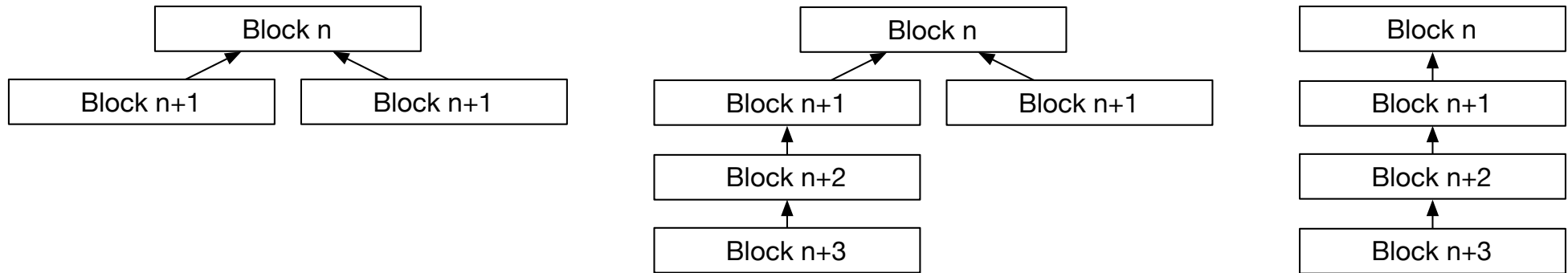
- Does Bob even have \$100?
- This can be checked by transversing all prior transactions, looking for Bob
- All Bob's previous financial transactions are public, so doing a sum of all transactions adding to or subtracting from to Bob's account will yield Bob's net worth
- Sounds like hard work! Who should do this and why?

Mining

- **Miners gather transactions, verify, and bundle them**
 - in return for a small transaction fee from the payer
 - as well as the *block reward* for creating and publishing the completed block
- **Before they can publish the transactions in a block, they have to perform a computational heavy task, so that it becomes infeasible to recreate (parts of) the blockchain for fraudulent purposes**
- **This is most often a Proof-of-Work, consisting of generating a nonce (a number) so that the hash of the block header satisfy some requirement:**
 - $\text{SHA256}(\text{block header}) < \text{some slowly decreasing target threshold}$



Forking



- Two miners may well create each a valid block at approximate the same time, but *there can be only one*
- The network prefers the more difficult, i.e., longer, chain, so if a fork happens, the longer of the forks will be accepted as the consensus chain
- Thus, the miners race to complete new blocks in order to protect already generated blocks and their rewards
 - currently at a global rate (for Bitcoin) of 50×10^{18} hashes per second (!)

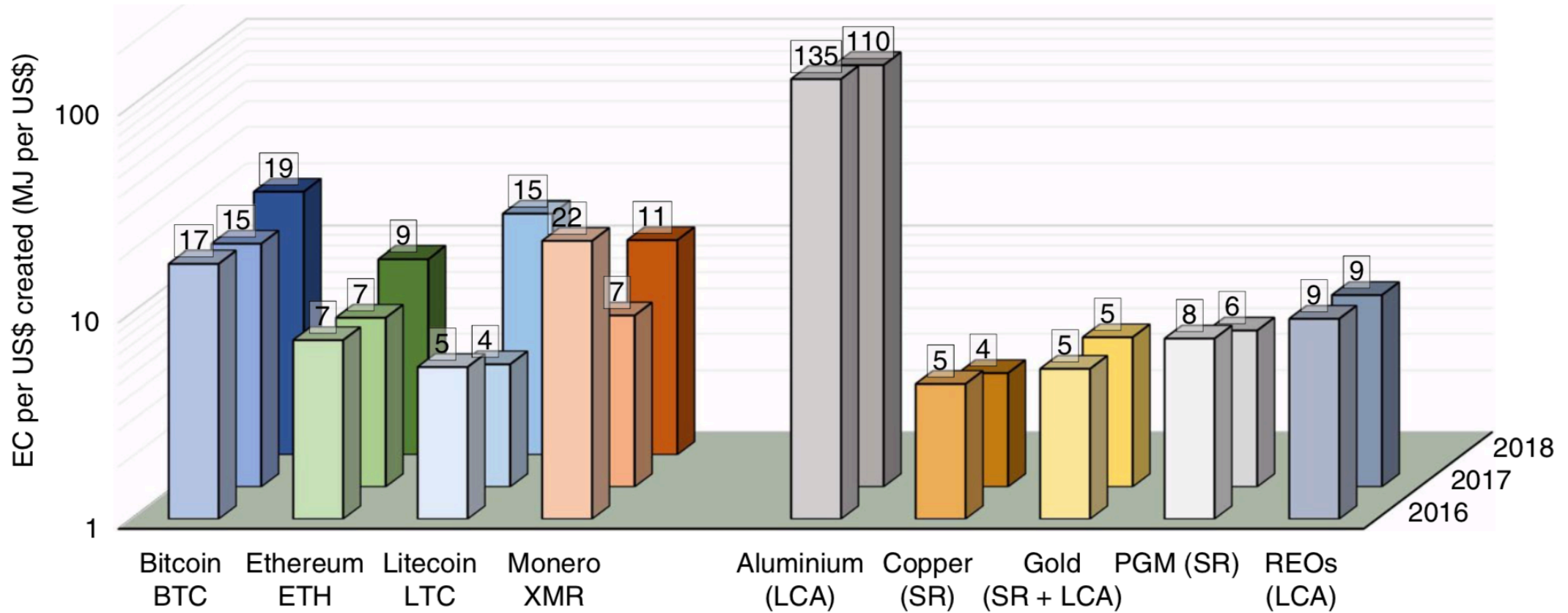
The cost of doing Proof-of-Work

- In the most popular blockchain, Bitcoin, the difficulty of the PoW has been steadily increasing to match the rising computation power of the miners
- The miners currently earn 12,5 bitcoin per block, approximately (8/11/2018) equivalent to 527.000 kr
 - thus, that is the upper bound cost of electricity spent to generate the block, ignoring other expenses such as rent and capital cost on mining equipment
- Current estimates put the electricity cost of a *single transaction (not block)* at 764 KWh (follow the link)
 - an average Danish family uses 5.200 KWh per year, so that is nearly **2 months worth of electricity (!)**

Is it *really* that bad?

- Study by Max J. Krause & Thabet Tolaymat published in Nature Sustainability (published 5/11/2018)
- A comparison of the four largest cryptocurrencies' energy and carbon costs juxtaposed with the same costs of gold, platinum, copper, aluminium, and rare earth metal mining

Results



- Energy costs (MJ)/US\$

Alternatives to Proof-of-Work

- **Proof-of-Stake**

- defer block creation to those, who have most to lose (have most at stake), if consensus is not reached
- not widely adopted, seems to be a hard problem to solve

- **Proof-of-Space**

- defer block creation to those, who can prove that they hold a specific (large) data structure/file—trades CPU cycles for disk space

- **Regardless, if a cryptocurrency is traded at a certain value, it will be worth spending up to that amount in resources to generate it**

Smart contracts

- **Apart from transactions (a simple form of code), the data in a block could also be used to store executable code, known as *smart contracts***
 - takes input from the blockchain, and generates output to the blockchain
 - the smart contracts run on all peers when triggered by a transaction pointing to it
- **The code is as public as the blockchain, and bugs and vulnerabilities are thus also visible to all**
 - however, in contrast to open source software, a faulty smart contract is not easy to withdraw, as it resides in an immutable block
 - Ethereum especially has suffered from time to time because of this

Does it scale?

- **Not very well**
 - Bitcoin (Core) blocks cannot (currently) be bigger than 1 MB
 - Estimates put transactions per second for Bitcoin around 3-4
 - Ethereum clocks in around 25 TPS
- **There are other systems that scale considerably better**
 - though shouldn't they then be the dominant ones?
- **Still, a private rather than public blockchain, might be made to scale better as PoW requirements may be different between trusted participants**
 - but they might as well use other, more classic and far, *far* faster, methods to handle their transactions

Is it P2P?

- **Well, yes...**
 - no central authority
 - all can, in principle, perform all actions, though some actions are *very* resource heavy
- **But not particularly well designed P2P**
 - (ignoring mining, which is often *grotesquely* energy inefficient, and which because of economy of scale has become *quite* centralised with giant mining server farms wherever in the world electricity is cheap)
 - every peer stores all the state (currently 185 GB for Bitcoin)
 - every peer performs all the smart contracts
 - if they defer these actions to other, more capable peers, how is this different from trusting a central authority?

The Blockchain & the Internet of Things

- **The blockchain**
- **Blockchains for the Internet of Things**

So, what use might it be?

- Well...
- **Use cases**
 - decentralised architecture for IoT (sounds good, but why build it on blockchains?)
 - micropayment infrastructure for microservices (performing sensor readings, doing calculations, storing data)
 - direct access to manufacturing equipment
 - energy trading (from one home to another)
 - logistics tracking (containers from origin to destination)
- **Many, if not all of these can be solved today using common PKI (public-key infrastructure) methods**
 - far more scalable, and based on proper computer science, software engineering, and mathematics rather than white papers and press releases

So, is it a good idea?

- **At this point, it seems as a grossly inefficient solution searching for a problem**
- **Having an immutable, public accessible record is a great idea for *some* use cases**
 - not everything should be public *or* immutable—and other methods can be used to ensure immutability, if desired
- **There are already, rock solid, cryptographic methods to do secure transactions with strangers**
 - PKI for many purposes—a cryptographically signed transaction is also immutable
 - Secure Multiparty Computations for the truly cautious ones
- **Hype and speculation are not evidence of usefulness**
 - *actual* useful work is proof of usefulness