Notefile for the future predictions of the Bitcoin/Blockchain TA Project (WS 18/19)

Those are just some collected thoughts I came accross while reading the paper (Note the different headings...) - We should definitely talk about those together once more.

Disk Space

The author of Bitcoin already noticed, that this will someday be a huge issue, because, in order to sustain the chain of trust, and chain of custody, the whole blockchain has to be stored across every participating node. In order to somewhat compensate this, the specification allows for old transactions to be removed from the network, without losing the integrity. This is done so using Merkle Trees (See <1> chapter seven and references for more information)

Still, the chain will grow, block headers must be saved in order to preserve integrity (About 80 bytes per block) which may become a problem iff the technology sets foot. A possible solution attempt would be to cut of parts of the blockchain, and only use archived strips in order to keep verifying the integrity of the chain. Those archived versions would need to be stored at multiple locations, so instead of a central authority we would have again a decentralized version, just with less nodes, therefore requireing less space. (E.g. each state stores its copy of the archived blockchain)

It is also possible to check the integrity of a transaction without running a full-blown network node, by just obtaining a copy of all the block headers from the bitcoin network. He/She can then verify, that the transaction was accepted by a (hopefully trustworthy) node, and confirm this by seeing, that all further nodes were also accepted by the network.

Privacy

Currently we trust authorities to keep our bank information in secret. Without trust into a central authority, we only have the network, and furthermore, we have to make each and every transaction publicly available for the whole contraption to work. Privacy is gone!

The paper states that, in order to reclaim the privacy one would have to break the chain of information at another place, and since every participant is identified by his public key, we could anonymize the public keys, in order to preserve privacy. (See figure 1)

The problem, in a large scale, is, that once a public key can be linked to a real identity (i.e. a person or an organization/government) you could essentially follow the chain of custody up to its root and know every transaction taking, as well as have the currency balance of said identity. On the one hand this might add transparency into the transactions of governments, on the otherhand, if used on the public, would essentially lay the foundation for financial mass surveilance.

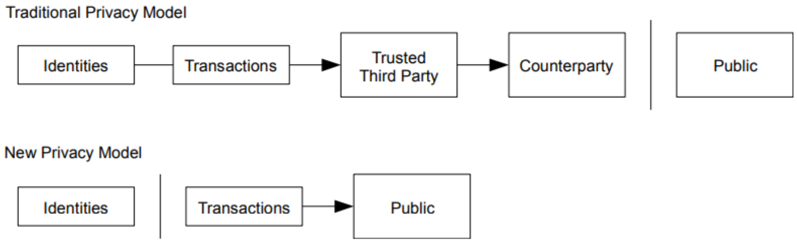

Figure 1: Standard vs. Bitcoin privacy models

Power

The proof of work costs a lot of computational resources. Currently that results in prices for Graphical Processing units rising, as well as opening a market for blockchain-specific mining ASICs (Application-specific integrated circuit) - It is, however also a problem for the power grid. Already the bitcoin network alone costs around 53.29TWh a year. <1 as of Nov 27, 2018> Iff used on a global scale, those numbers will rise, and we need to find ways to circumvent the large power-consumption.

Digital Grid

We discussed that we would just assume that the foundations for our scenarios would be given at time, but I just wanted to mention that iff one of our non-trivial scenarios happens, it has to be clear, that all participating parties need a stable connection to the currency network, which for simplycity shall be the internet, in some form. (Be it global players and governments, or actually every person inhabiting the planet!)