can set that maximum amount, since only the user can determine the trust level to be reached. In turn, the system has to broadcast these batched transactions to the Bitcoin blockchain, e.g., if the user sets the limit at €100 and if the virtual balance reaches this value, all accumulated transactions are broadcast. This approach was chosen over the Lightning network's approach [L4], since its technical complexity is lower and more importantly it also works with transaction malleability. The current Coinblesk design can be optimised further, once transaction malleability is solved in the Bitcoin network or any another crypto-currency, such as Litecoin, which does not suffer from malleability, is used. However, as mentioned above, the Coinblesk app does not follow the fully trustless approach in such cases, since the Coinblesk server requires this minimal trust up to the amount specified by the user.

All funds deposited in Coinblesk are held at a 2-of-2 multisig address, which means that even if the operator of the Coinblesk server is intentionally malicious, he will never be able to steal a user's funds. In the case of a Coinblesk server hacking and private keys being stolen, the hacking could only be successful if hackers were able to gain access to the user's private keys as well in order to steal bitcoins. Also, if the Coinblesk server disappears, clients are no longer able to spend their bitcoins. This is a major problem, because Swiss law requires customers of a payment service to be able to gain full access to their funds in any situation, and especially if the operator of a payment system should become bankrupt – or in the case of the Coinblesk service, it might be hacked. Additionally, all Coinblesk clients need to trust that the system will not disappear.

Thus, the effective solution to this problem is a "refund transaction" as time-lined in Figure 1. A refund transaction is a pre-signed, time-locked transaction, which sends all client funds to an address, exclusively controlled by that client. Therefore, a refund transaction is automatically created by the Coinblesk app as soon as a new unspent output appears in the wallet – in particular, whenever bitcoins are received or a transaction is created. The app takes all the unspent outputs and creates a single transaction sending all bitcoins to an address of a private key that is derived from the client's private seed. The client signs this transaction and returns it to the server. The server checks that the transaction is in fact time-locked, signs it, and returns the transaction fully signed back to the client. Now, the client is in possession of a valid, fully signed refund transaction that becomes valid as soon as the time-lock expires. Thus, in case the Coinblesk server suddenly disappears, a client can broadcast the refund transaction and regain control over all their bitcoins.

In conclusion, the experience with the Coinblesk design and implementation as well as experience from other applications, such as the pharmaceutical supply chain [L3, L5], provides useful information about scalability, energy efficiency, ease-of-use, and some insights into customer acceptance. These results should be widely applicable in the blockchain world.

Links:

[L1] http://www.csg.uzh.ch/csg/en/news/Bitcoins.html
[L2] http://www.csg.uzh.ch/csg/en/news/ coinbleskatCeBIT.html
[L3] http://www.csg.uzh.ch/csg/en/news/kickstart-accelerator.html
[L4] https://lightning.network/lightning-network-paper.pdf
[L5] https://modum.io/

References:

[1] T. Bocek, B. Stiller: "Smart Contracts – Blockchains in the Wings", in: C. Linnhoff-Popien, R. Schneider, M. Zaddach (Edts.): "Digital Marketplaces Unleashed", Springer, 2017.
[2] A. D. Carli: "Protocol Improvements in CoinBlesk – A Mobile Bitcoin Instant Payment Solution", Master Thesis, Univ. Zürich, Department of Informatics, Communication Systems Group, Zürich, Switzerland, April 2016.
[3] R. Voellmy: "CoinBlesk, a Mobile NFC Bitcoin Payment System", Bachelor Thesis, Univ.Zürich, Communication Systems Group, Department of Informatics, Zürich, Switzerland, August 2015.

Please contact:

Thomas Bocek, Sina Rafati, Bruno Rodrigues, Burkhard Stiller
University of Zürich, Switzerland
[bocek|rafati|rodrigues|stiller]@ifi.uzh.ch

Bitcoin Unchained

by Christopher Carr, Colin Boyd (NTNU), Xavier Boyen and Thomas Haines (QUT)

Bitcoin's distributed ledger is an innovative way of solving the double spending problem in a decentralised system. However, it causes incompressible transaction delays and incentivises consolidation of mining power. We ask, is it possible to eliminate these problems without losing the decentralised principles that Bitcoin was built on?

Over eight years have gone by since Bitcoin's deployment, and it is still going strong. While there are many explanations for its success, the innovative backbone structure – the blockchain -– which has inspired so many alternative systems, undoubtedly plays a leading role in this story.

Blockchains store the state of the transactions in the system. Users compete to form new blocks, which confirm both new and all existing transactions in the previous blocks. Those who create blocks first are rewarded with cash in the system.

Despite the blockchain innovation, there are some fundamental problems that lie in its design, which stem from the blockchain itself, and affect all similar systems.

Two major problems which are inherent to almost all blockchain models are:

1. Consolidation of power: Users are incentivised to form into groups to maximise their expected reward over time. Cartels formed in this manner are commonly referred to as mining pools.
2. Incompressible delays: All transactions have a delay before they can be considered confirmed within the system. In Bitcoin itself, this is exacerbated by block size restrictions, a source of heated debate within the community. Recently, almost all blocks have been full to capacity of transactions, and as of the time of writing have fees for posting transactions over 10 USD.

Previously, there has been a line of inquiry that looks at alternative ways of designing proofs-of-work to avoid mining pools. Miller, Kosba, Katz and Shi [1] create a proof-of-work system that allows for any pool member to cheat and reap all the rewards for themselves. Importantly, they show that a cheater can do this without any way of being caught, thus removing the incentive for mining pool formation. Lewenberg, Somplinsky and Zohar [2] design a system that allows for collections of transactions to be confirmed in such a way that overlapping blocks can be counted along with the transactions contained within them.

Our motivation stems from simultaneously addressing these two fundamental problems of consolidation of power and incompressible delays. In a joint research effort, which is a collaboration between the Norwegian University of Science and Technology [L1] and Queensland University of Technology [L2], we ask: "What happens if we remove blocks altogether?" Instead of collecting multiple transactions together, whenever you wish to create a transaction you simply reference two recent, existing transactions.

Once blocks are removed, we need a way of securing transactions against double spending. To achieve this, we look to the incentive mechanisms, and use these to promote the desired characteristics. We incentivise the collection of recent previous transactions by increasing the reward for doing so. This can also be thought of as a form of small blocks, but removing the enforced confirmation delay.

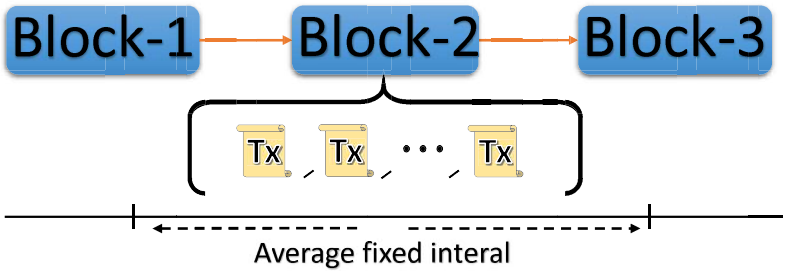

Figure 1: Blockchain model: Transactions (Tx) are collected together over some fixed average time interval and grouped into blocks, confirming the full group of transactions.

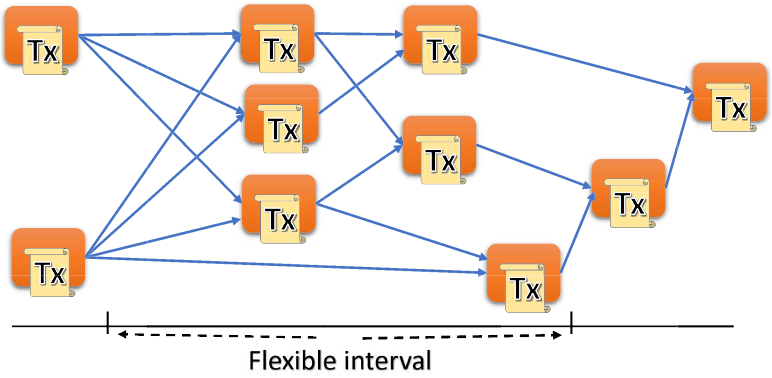

Figure 2: Blockchain free model: Transactions (Tx) are collected indivudually over a flexible time period and confirm previous transactions.

To highlight these aspects, Figure 1 shows a standard blockchain model, where transactions are collected together and formed into a block. Contrast this with Figure 2, which shows the block-less model, where transactions confirm only two previous transactions.

So far, we have developed a blockchain free system [3], and demonstrated the security of the system under the assumption of a majority of rational users. We show that the incentive mechanisms we put in place encourage transactions to finally group together at the head of the chain, where all previous transactions are confirmed from the leading transaction - a property we call convergence.

We believe this novel approach represents a large step forwards in tackling these highlighted blockchain problems. Our focus now is on addressing implementation decisions. The challenge is to select appropriate parameters that do not undermine the theoretical underpinnings. Our hope is that by designing and implementing a system in this way, we can get closer to the true ideal of a decentralised digital cash system.

Links:

[L1] http://www.ntnu.edu/iik/nacl-lab

[L2] https://kwz.me/Xd

References:

[1] A. Miller, et al: "Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions", ACM Conference on Computer and Communications Security 2015: 680-691.

[2] Y. Lewenberg, Y. Sompolinsky, A. Zohar: "Inclusive Block Chain Protocols", Financial Cryptography 2015: 528-547.

[3] X. Boyen, C. Carr, T. Haines: "Blockchain-Free Cryptocurrencies: A Framework for Truly Decentralised Fast Transactions", IACR Cryptology ePrint Archive 2016: 871 (2016).

Please contact:

Christopher Carr, NTNU, Norway
ccarr@ntnu.no