Alsacoin: A Scalable Confidential Cryptocurrency

Christian Nyumbayire

July 20, 2019

Blockchain cryptocurrencies [11, 12, 10, 4] have guaranteed since their inception a level of safety, certainty and rapidity to financial transactions never reached before by traditional services based on trust and semi-manual accounting. In the years, blockchain technology has found application even outside finance as a tool to certify data and execute programmable contracts [6]. There has been some progress since its invention in 2008 [10], but we find that there are still some ill-solved problems: privacy and scalability.

The problem of privacy is complex: on one side we want to ensure that users don't have to reveal information about their business to anyone able to access the system records, on the other side we want to keep them accountable. So we want confidentiality about transactions but pseudonymity for identity. On the implementation side, we also want to not have to rely on untested or poorly tested assumptions. So we have to use only lightweight cryptography based on standard assumptions paying attention to not incur in big losses in performance.

At the moment there are more proposed solutions to blockchain inherent scalability issues, but we are still far from reaching the maximum capacity of 65000 transactions per second guaranteed by Visa Network. We think a good solution, even if partial, should be decentralized, without committees nor nodes with a special status and open to future improvements. It should allow to extend it without having to redesign it, an operation that can be difficult and expensive in long-running protocols.

Alsacoin is our solution to these problems in the case of simple online payments and data certification (no "smart contracts" [6]). The protocol is simple and open enough to and extended in a second time in different ways without redesigns.

To solve confidentiality, we found a good candidate in PGC [7], a cryptographic protocol for pseudonymous confidential transactions that only uses standard cryptography and is agnostic on respect of the consensus proto-

col used. PGC uses a twisted version of ElGamal [9] for homomorphic encryption, Bulletproofs [1] for zero-knowledge proofs and a scheme for digital public key signatures (we opted for Ed25519 [3]). This is lightweight cryptography based only on the Elliptic Curve Discrete Logarithm Problem.

For scalability, we used Avalanche [5], a dagchain (Directed Acyclic Graph) protocol that does not make use of blocks as in blockchains, but operates directly on the graph of transactions, and does not require any kind of mining protocol. Thanks to this protocol we can eliminate two important sources of deadlocks that would make increasing scalability hard: having to work on a single chain and having to increase the consensus latency to wait for mining or for one or more voting committees to form [4]. With 2000 nodes, Avalanche guarantees 3400 transactions per second (tps) against Bitcoin 7tps (classic blockchain) and Algorand 874tps (BFT with committees).

Although we don't require mining, we opted to keep coin production in the hand of miners. Alsacoin uses a proof-of-work algorithm similar to Hashcash [8], the same used by Bitcoin, but uses the memory-hard hashing function Balloon [2] in place of SHA256. Mining is "autistic": it does not take place in the consensus phase and for coin production. This assures us to not degrade Avalanche performance. To keep verification complexity bounded, we require coinbase transactions to take as input one or more outputs owned by the miner from chains of transactions that have as root the dagchain root, the Eve transaction.

Alsacoin with the prefixes of the International System of Units, e.g.: 10^{-9} ALSA is 1 nALSA, 10^{-6} ALSA is 1 μALSA, etc.

The name of the protocol comes from alsadf (الصدف), "shell" in Arab. Shells where one of the first means of exchange used in history [12].

References

[1] Benedikt Bünz et al. *Bulletproofs: Short Proofs for Confidential Transactions and More*. `https://crypto.stanford.edu/bulletproofs`. 2017.

[2] Dan Boneh et al. *Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks*. `https://crypto.stanford.edu/balloon`. 2016.

[3] Daniel J. Bernstein et al. *High-speed high-security signatures*. `https://ed25519.cr.yp.to/ed25519-20110926.pdf`. 2011.

[4] Shehar Bano et al. *SoK: Consensus in the Age of Blockchains*. `https://arxiv.org/abs/1711.03936`. 2017.

[5] Team Rocket et al. *Scalable and Probabilistic Leaderless BFT Consensus through Metastability*. https://arxiv.org/abs/1906.08936. 2019.

[6] Yining Hu et al. *Blockchain-based Smart Contracts — Applications and Challenges*. https://arxiv.org/abs/1810.04699. 2019.

[7] Yu Chen et al. *PGC: Pretty Good Confidential Transaction System with Accountability*. https://eprint.iacr.org/2019/319. 2019.

[8] Adam Back. *Hashcash — A Denial of Service Counter-Measure*. http://www.hashcash.org/papers/hashcash.pdf. 2002.

[9] Taher ElGamal. *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. http://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf. 1985.

[10] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. 2008.

[11] Neal Stephenson. *CRYPTONOMICON*. https://www.nealstephenson.com/cryptonomicon.html. 1999.

[12] Nick Szabo. *Shelling Out: The Origins of Money*. https://nakamotoinstitute.org/shelling-out. 2002.