Distributed Consensus Technologies in Cryptocurrency Applications

Francisco Rivera, Sathvik Palakurty

Florida State University Young Scholar's Program 2014

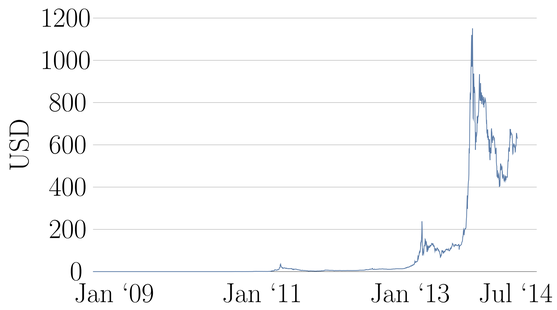
CryptoWerks.com

Distributed Consensus

Today, most services are provided by centralized institutions (eg. a bank). However, using a centralized authority requires *trust*. With the innovative ideas implemented in the Bitcoin network, distributed institutions that do not require trust become feasible to implement.

Bitcoin

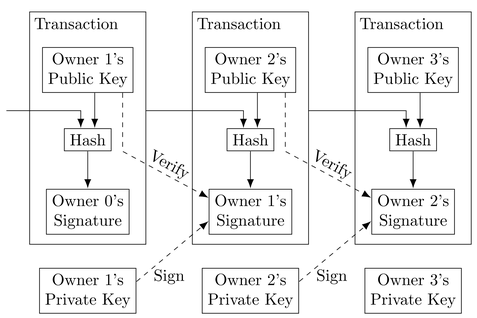
Figure 1: Market Price of BTC [1]



Two **crucial** ideas:

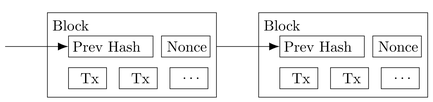
- The Transaction Chain (defines ownership)

Figure 2: Bitcoin's Transaction Chain [3]



- The Blockchain (timestamps transactions)

Figure 3: Bitcoin's Blockchain [3]



SHA 256

A well-known cryptographic hash used in Bitcoin for proof of work (miners search for nonce to make digest less than some difficulty value):

- SHA256(message) = digest $\in \{0,1\}^{256}$
- Digest is not unique to one message on which there are no size restrictions
- Cannot recover *any* information about message from digest

Scrypt

A more complex cryptographic hash used in other cryptocurrencies:

- Requires more memory and time to hash a message
- Discourages participation from ASICs (a type of specialized hardware) in mining

ECDS

Given a public key and a private key, Elliptic Curve Digital Signatures provide cryptographic evidence which can be confirmed only with the public key that the message has been "signed" by someone with the private key. However, confirming the signature does not reveal the private key. In Bitcoin:

- The message is a transaction request
- The public/private key pair is a *wallet*

zk-SNARK

A zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) lets a computationally bounded worker node prove to another node it has correctly executed certain computational tasks without having the other node execute these tasks in their full complexity to check. This technology is important to the idea of NDCoin.

Other Cryptocurrencies

Hundreds of other crypto-currencies have developed, and although Bitcoin accounts for more than 90% of the market capitalization of 400 cryptocurrencies indexed by Coin Market Cap [2], some currencies present innovative ideas that are worth exploring.

Exploring Gridcoin

- The Bitcoin network "wastes" a tremendous amount of computation power on hashing.
- BOINC (Berkeley Open Infrastructure for Network Computing) looks for volunteer computation power to run distributed research projects.
- Gridcoin incorporates participation in BOINC projects as part of mining
- Reward of mining a block depends on contribution to BOINC with respect to a network average.

What Gridcoin is Not

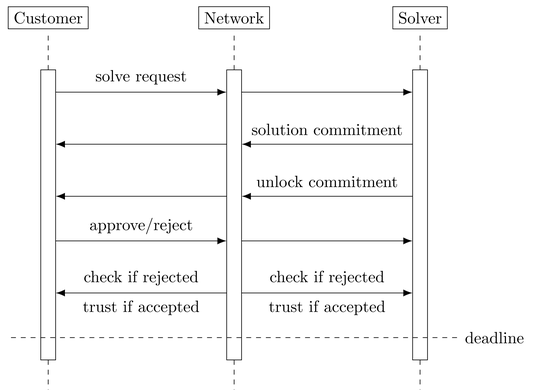
Gridcoin is innovative in using proof of work for a purpose, but it does **not** represent an effective way to hire distributed computation:

- BOINC projects must be whitelisted by a central authority to be considered legitimate for mining.
- Monetary reward comes from new Gridcoins, no way to pay for a project and attract worker nodes to it.
- No cryptographic guarantees to correctness of computation results.

NDCoin [4]

We consider a new cryptocurrency with the ability to submit to the network an incomplete transaction request. Any node can specify the destination of the funds before a deadline if it proves to the network it was the first node to successfully execute a nondeterministic algorithm that accompanies the transaction.

Figure 4: NDCoin Sequence Diagram



References

[1] Blockchain.info.
Market Price, July 5th, 2014.

[2] Coin Market Cap.
"Crypto-Currency Market Capitalizations.".
coinmarketcap.com, July 9th, 2014 11:37PM.

[3] Satoshi Nakamoto.
Bitcoin: A peer-to-peer electronic cash system.
Bitcoin.org, 2009.

[4] Dr. Mike Frank and David Mondrus.
Introducing NDCoin.
ndcoin.org, 2014.

Acknowledgements

We would like to thank Dr. Mike Frank, our research sponsor, and the rest of the Cryptowerks team for letting us be a part of this promising and exciting project!