01 Official
Whitepaper

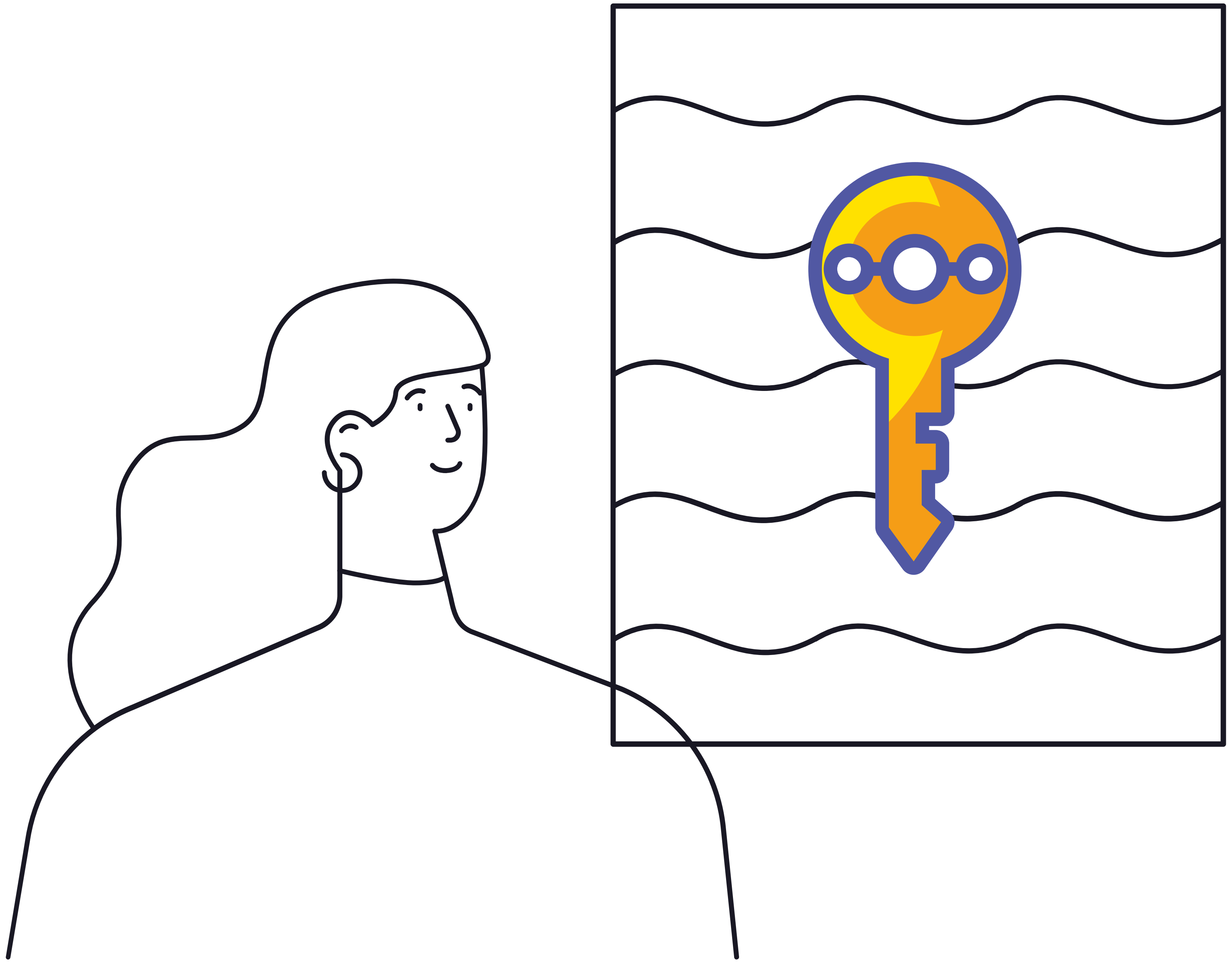
Litedoge:
a peer-to-peer cryptocurrency

by Shawn M

Similar design to Bitcoin

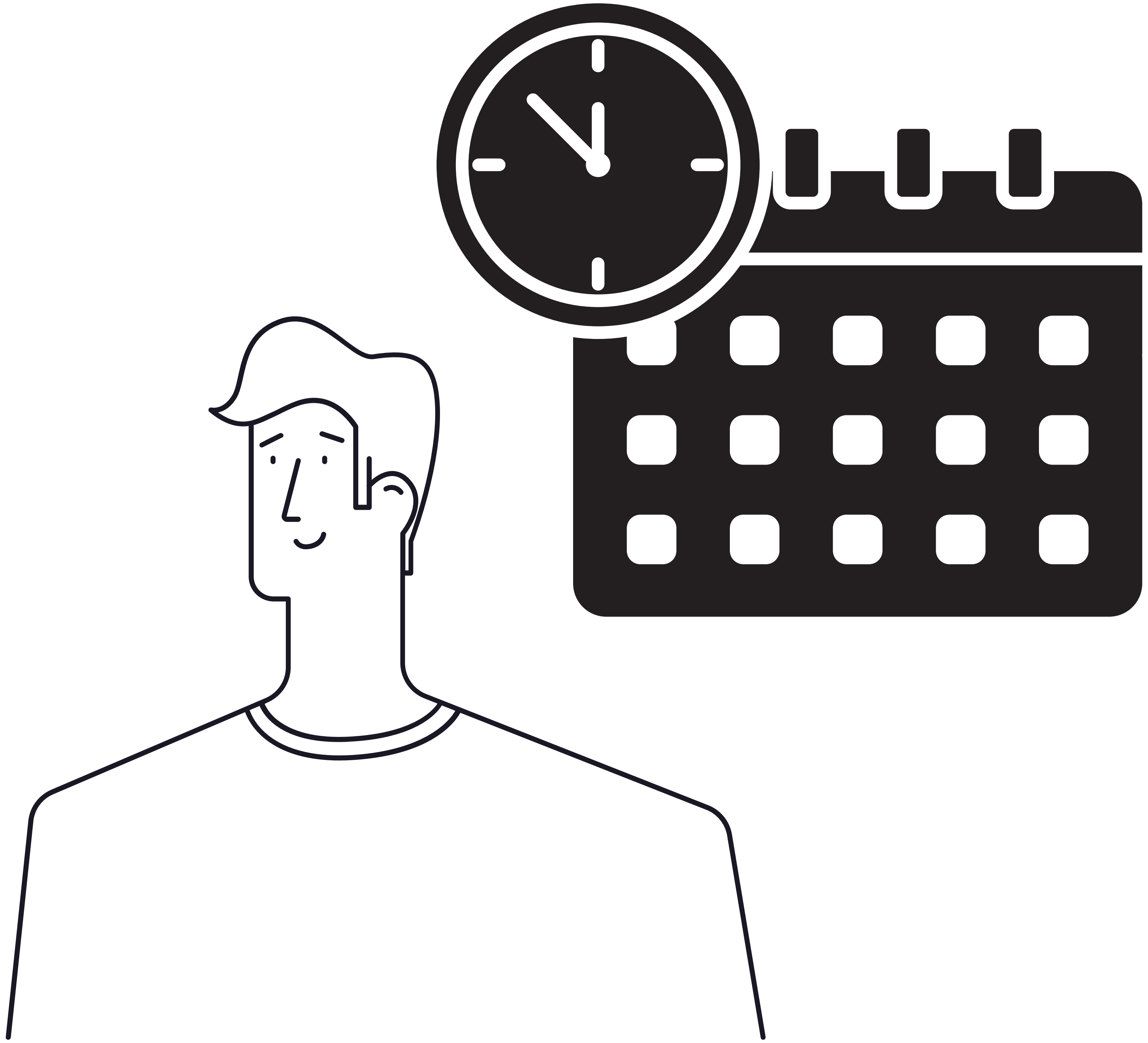
Proof of stake.
Scrypt Based.
Fast Transactions.
Low Fees.
Organised Community.

made in 2015,
no ninja launch,
no ico, no premine!



Coin age

COIN AGE IS SIMPLY DEFINED AS CURRENCY AMOUNT TIMES HOLDING PERIOD.THE CONCEPT OF COIN AGE WAS KNOWN TO NAKAMOTO AT LEAST AS EARLY AS 2010 AND USED IN BITCOIN TO HELP PRIORITIZE TRANSACTIONS, FOR EXAMPLE, ALTHOUGH IT DIDN'T PLAY MUCH OF AN CRITICAL ROLE IN BITCOIN'S SECURITY MODEL. BLOCK TIMESTAMP AND TRANSACTION TIMESTAMP RELATED PROTOCOLS ARE STRENGTHENED TO SECURE THE COMPUTATION OF COIN AGE. IN ORDER TO FACILITATE THE COMPUTATION OF COIN AGE, WE INTRODUCED A TIMESTAMP FIELD INTO EACH TRANSACTION. ADDITIONALLY, WHEN BOB SPENT THE 10 COINS HE RECEIVED FROM ALICE, WE SAY THE COIN AGE BOB ACCUMULATED WITH THESE 10 COINS HAD BEEN CONSUMED (OR DESTROYED).

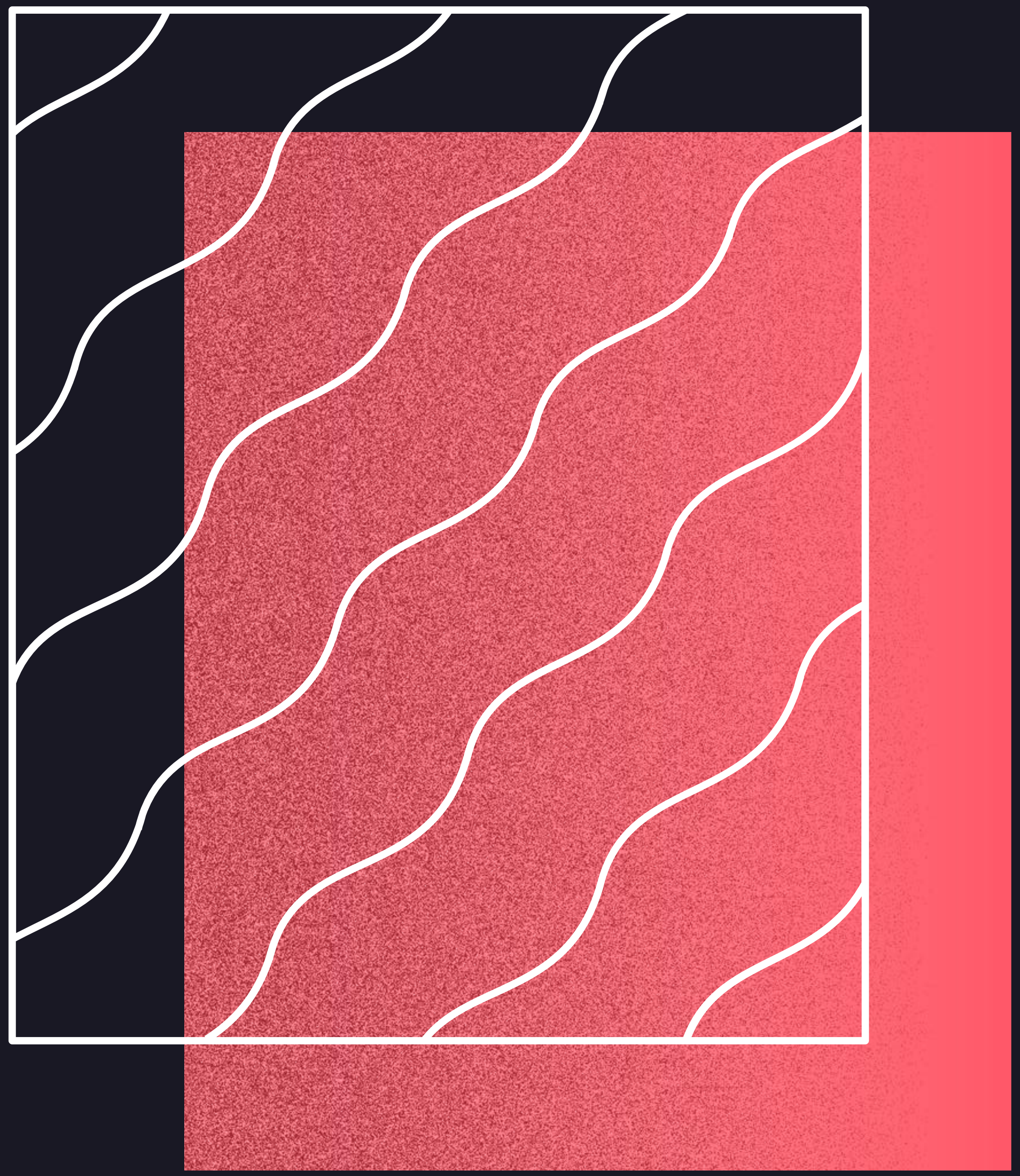


Proof-of-work helped to give birth to Nakamoto’s major breakthrough, however the nature of proof-of-work means that the crypto-currency is dependent on energy consumption, thus introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees. As the mint rate slows in Bitcoin network, eventually it could put pressure on raising transaction fees to sustain a preferred level of security. One naturally asks whether we must maintain energy consumption in order to have a decentralized crypto-currency?

Thus it is an important milestone both theoretically and technologically, to demonstrate that the security of peer-to-peer crypto-currencies does not have to depend on energy consumption. A concept termed proof-of-stake was discussed among Bitcoin circles as early as 2011. Roughly speaking, proof-of-stake means a form of proof of ownership of the currency. Coin age consumed by a transaction can be considered a form of proof-of-stake. We independently discovered the concept of proof-of-stake and the concept of coin age in October 2011, whereby we realized that proof-of-stake can indeed replace most proof-of work’s functions with careful redesign of Bitcoin’s minting and security model. This is mainly because, similar to proof-of-work, proof-of-stake cannot be easily forged. Of course, this is one of the critical requirements of monetary systems - difficulty to counterfeit. Philosophically speaking, money is a form of ‘proof-of-work’ in the past thus should be able to substitute proof-of-work all by itself

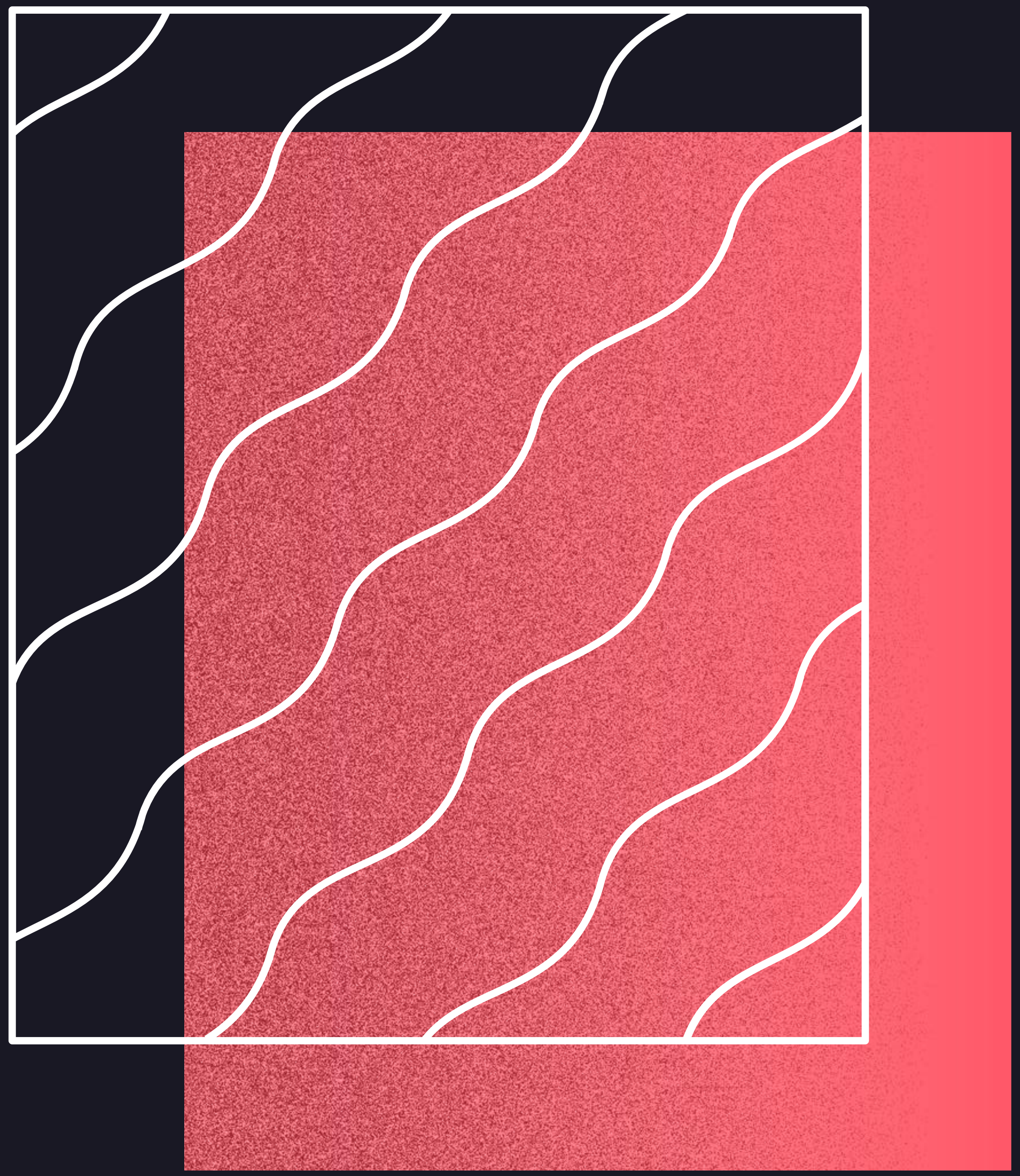
Figure: Structure of Proof-of-Stake (Coinstake) Transaction generating a block for the network and minting for proof-of-stake. The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-ofwork blocks. However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved. The hash target that stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (in contrast to Bitcoin's proof-of-work target which is a fixed target value applying to every node). Thus the more coin age consumed in the kernel, the easier meeting the hash target protocol. For example, if Bob has a wallet-output which accumulated 100 coin-years and expects it to generate a kernel in 2 days, then Alice can roughly expect her 200 coin-year wallet-output to generate a kernel in 1 day. In our design both proof-of-work hash target and proof-of-stake hash target are adjusted continuously rather than Bitcoin's two-week adjustment interval, to avoid sudden jump in network generation rate. Minting based on Proof-of-Stake A new minting process is introduced for proof-of stake blocks in addition to Bitcoin's proof-of-work minting. Proof-of-stake block mints coins based on the consumed coin age in the coinstake transaction. In a pure proof-of-stake system initial minting can be seeded completely in genesis block via a process similar to stock market initial public offer (IPO).

THE MAIN LDOGE KERNEL



// LiteDoge kernel protocol
// coinstake must meet hash target according to the protocol:
// kernel (input 0) must meet the formula
// hash(nStakeModifier + txPrev.block.nTime + txPrev.nTime + txPrev.vout.hash + txPrev.vout.n + nTime) < bnTarget * nWeight
// this ensures that the chance of getting a coinstake is proportional to the
// amount of coins one owns.
// The reason this hash is chosen is the following:
// nStakeModifier: scrambles computation to make it very difficult to precompute
// future proof-of-stake
// txPrev.block.nTime: prevent nodes from guessing a good timestamp to
// generate transaction for future advantage
// txPrev.nTime: slightly scrambles computation
// txPrev.vout.hash: hash of txPrev, to reduce the chance of node

THE MAIN LDOGE KERNEL



// generating coinstake at the same
time
// txPrev.vout.n: output number of txPrev, to
reduce the chance of nodes
// generating coinstake at the same time
// nTime: current timestamp
// block/tx hash should not be used here as they
can be generated in vast
// quantities so as to generate blocks faster,
degrading the system back into
// a proof-of-work situation.

ENERGY EFFICIENCY

When the proof-of-work mint rate approaches zero, there is less and less incentive to mint proof-of-work blocks. Under this long term scenario, energy consumption in the network may drop to very low levels as disinterested miners stop mining proof-of-work blocks. The Bitcoin network faces such risk unless transaction volume/fee rises to high enough levels to sustain the energy consumption. Under our design even if energy consumption approaches zero the network is still protected by proof-of-stake. We call a crypto-currency long-term energy-efficient if energy consumption on proof-of-wor

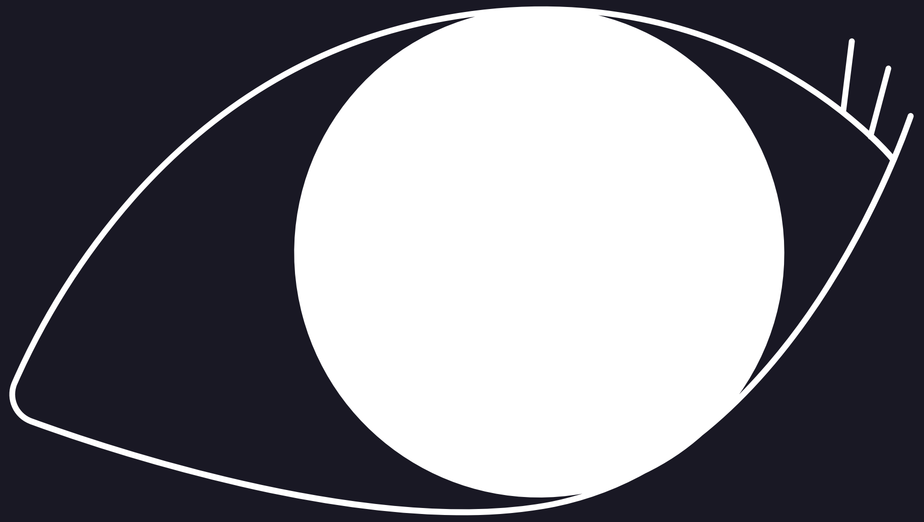
REFERENCES

Babaioff M. et al. (2011): On Bitcoin and red balloons. Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf) https://university.peercoin.net/#/9-peercoin-proof-of□stake-consensus https://blackcoin.org/blackcoin-pos-protocol-v2-whit epaper.pdf

ACKNOWLEDGEMENT

We would like to thank Satoshi Nakamoto and Bitcoin developers whose brilliant pioneering work opened our minds and made a project like this possible, along with the developers of peercoin, blackcoin, and novacoin. We thank you.

Conclusion

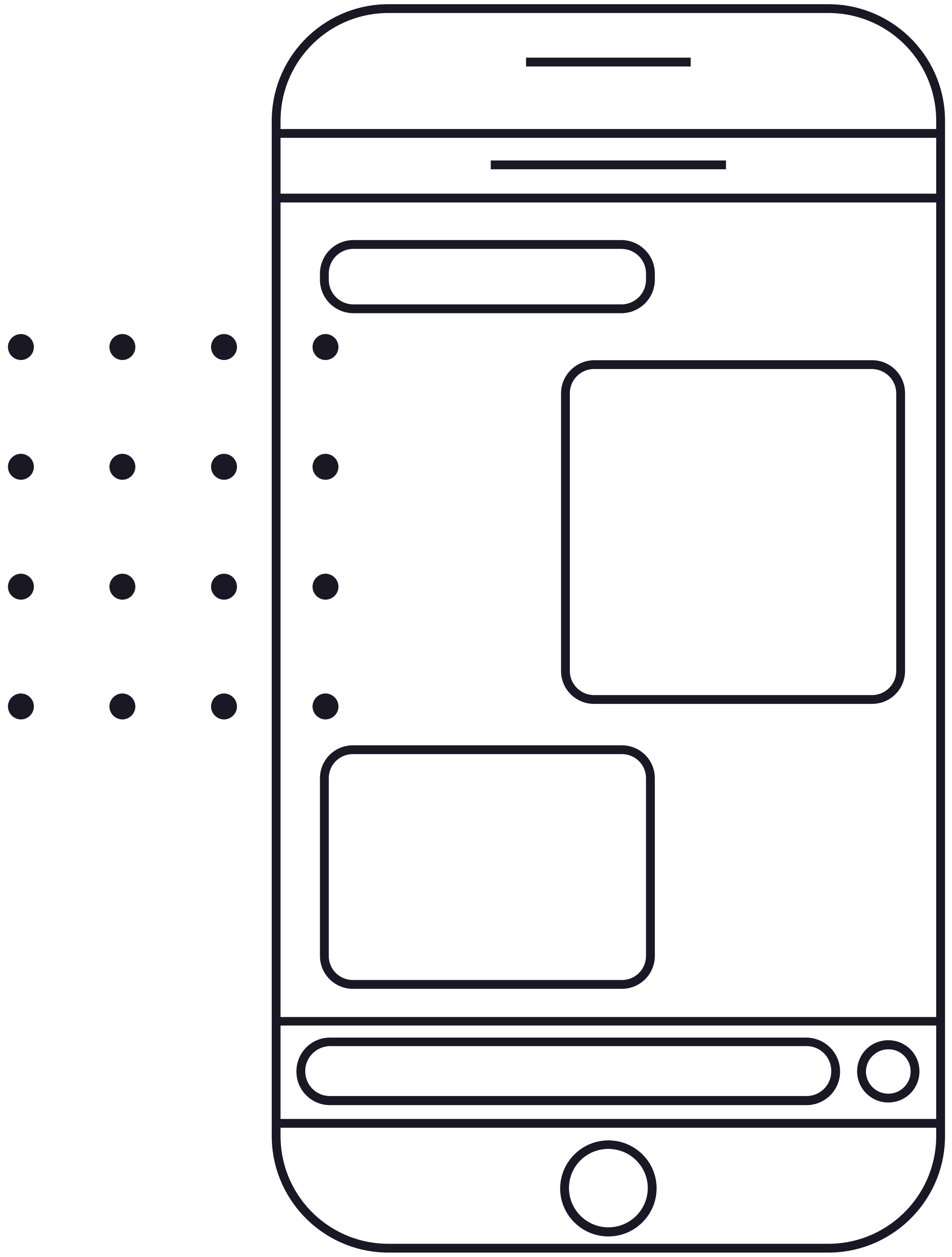


UPON VALIDATION OF OUR DESIGN IN THE MARKET, WE EXPECT PROOF-OF-STAKE DESIGNS TO BECOME A POTENTIALLY MORE COMPETITIVE FORM OF PEER-TO-PEER CRYPTO-CURRENCY TO PROOF-OF-WORK DESIGNS DUE TO THE ELIMINATION OF DEPENDENCY ON ENERGY CONSUMPTION, THEREBY ACHIEVING LOWER INFLATION/LOWER TRANSACTION FEES AT COMPARABLE NETWORK SECURITY LEVELS.

JOIN THE LDOGE COMMUNITY!

Interested in knowing more about ldoge?
Get in touch through our social pages!

Litedoge aka LDOGE (@LiteDoge2018) / Twitter
https://litedogeofficial.org/
https://discord.gg/W9jKduHN3e



THANK YOU