Lava Whitepaper/Light Paper 2.0

Lava Team

Lavacoreteam@protonmail.com
https://lava.money/
May 20, 2020

Lava is money with strong store of value, medium of exchange and privacy properties. It is forked from Zcoin. Its privacy is based on Zcoin's Sigma and Lelantus technology, based on Zcoin developer Aram Jivanyan's Lelantus paper (https://lelantus.io/ and https://zcoin.io/). Eventually Lava will evolve into a more differentiated cryptocurrency.

After launch we plan on migrating to LPOS (Lease Proof of Stake explained: https://www.binance.vision/blockchain/leased-proof-of-stake-consensus-explained). Governance features will be developed. If Avalanche proves itself to be a superior consensus mechanism after being deployed on other projects like AVA (https://www.avalabs.org/), then we can possibly work towards implementing it on Lava. (Avalanche whitepaper: https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRV

GV). More research must be done on how to implement it properly. We are considering doing weekly, monthly and quarterly progress updates.

Lava technical specifics and strategy

Lava is forked from Zcoin. The total supply is 1,000,000,000 (1 billion) Lava. It's Inflation is very low, about 10 times slower than bitcoin. Inflation starts at 11.5% the first year and decreases about 1% each year. When implemented, Avalanche will allow for 1 second transactions, high scalability (thousands of transactions per second) and double spend resistance. We have an idea of how to implement it but need the budget and competent programmers to develop it for production grade software. There is no halving as in bitcoin instead the total supply will be mined in about 70 years and should be sustained by transaction fees by then. It uses the Sigma privacy protocol from Zcoin and eventually will have Lelantus implemented. 10% of the total supply will go toward giveaways, bounties, seed fund and expenses. The block time is 2 minutes and the block reward is 50 Lava per block. 70% of the block reward goes to the Lava DAO and 30% goes to stakers. Since inflation is 10 times slower, the 70% Dev reward is equivalent to a 7% dev block reward on bitcoin. The Lava treasury will not stake, except for testing and initial block processing. The Lava team will release quarterly reports detailing expenses. We will develop governance features and eventually we would like to remove the "replace by fee" anti-feature we inherited from Bitcoin and Zcoin. Replace by fee is an attack vector that allows double spending of unconfirmed transactions. Segwit is also disabled. Increasing the POS rewards is not necessary since it is essentially like a stock split, one gets more coins but each coin is worth less, with a small value transfer from non stakers to stakers. High POS rewards provide no value to the network. We will look into Zcoin's Elysium/Exodus and other alternatives like SLP, colored coins, etc to provide tokenization as long as they don't interfere with the goal of global money.

Proof of work versus proof of stake

The following explains the rationale behind the implementation of Proof of Stake in Lava and rejection of Proof of Work. Many misconceptions surround Bitcoin's Proof of work mechanism, for example, it has been said that "Bitcoin is protected by the laws of mathematics, and it can never be attacked nor hacked". This is completely false. Proof of work and Nakamoto Consensus rely on faulty game theory that no one would attack the network because it is more profitable to participate honestly than to attack. Despite this claim, we have empirical evidence that this is false. Many other projects using POW such as Bitcoin Gold have been 51% attacked by double spending (https://qz.com/1287701/bitcoin-golds-51-attack-is-every-cryptocurrencys-nightmare-scenario/). At the time of writing, we estimate the cost to 51% attack Bitcoin to be about $500,000 an hour plus an investment in ASIC miners. Emin Gun Sirer estimates this cost to be around 2-3% of its market capitalization. (You can hear more about Avalanche and Nakamoto consensus here: https://www.youtube.com/watch?v=mxshHaCAZpA). We predict that after the initial attack, panic will cause the price to drop, making the attack cheaper and cheaper. This happens in a loop or "death spiral" until it costs merely thousands of dollars per hour to 51% attack. A total cost of 3 - 7 billion dollars to protect the legacy fiat system and maintain their monopoly on money issuance is an extremely small price to pay. Additionally, an attacker can short Bitcoin with leverage to recover the costs. No miner is going to risk their capital protecting the chain by mining at a loss and trying to "out hash" an attacker.

Despite this, Proof of work is claimed to be a more attractive and decentralized way of distributing coins. Instead, massive centralized ASIC, GPU farms or botnets mine most of the coins and sell them at exchanges. End-users do not mine coins, they cannot compete, not even with CPU and Anti-ASIC mining algorithms. Therefore POW doesn't really distribute coins in a decentralized manner, it is simply an extremely expensive and wasteful way to obtain and sell coins on exchanges. A much better way would be to allow those precious resources to go towards those who contribute to the network, such as developers, stakers, adoption teams, etc. Volunteer development and POW cryptocurrencies cannot compete with POS and DAOs that can use

the inflation to increase its network effect and utility instead of wasting it on heat or power. They are at a significant competitive disadvantage. Lack of funding can also cause project capture by third parties. Additionally it should be noted that there is a window of opportunity for smaller grassroots projects to use these funding models before huge companies like Facebook launch their own cryptocurrencies.

POW leaks value out of the system. POW cryptocurrencies are terrible stores of value and the forced selling of coins by miners causes even more volatility. All the coin emission is wasted on generating heat with no security nor coin distribution benefits. Many POS cryptocurrencies try to trick investors by using the term ROI (return on investment). Coin inflation rate is not equal to return on investment. No value is added nor subtracted from the network by stakers receiving the coin emission, the real ROI from coin emission alone is zero (excluding all other variables such as coins not staked). However, if a cryptocurrency increases its network effect or its utility then value is added. If some users do not stake their coins then some value is transferred from non-stakers to stakers via inflation.

No Masternodes

There are no masternodes in Lava. Cryptocurrencies with high collateral masternodes create an artificial barrier of entry that end-users cannot acquire and it creates two classes of users, those who can afford a masternode and the rest who can't. This reduces the network effect because those who are not receiving the benefits of coin emission are less incentivized to spread adoption and contribute to the network. Masternodes also reduce the security of the network because less coin holders can participate in staking. We want users to be passionate and to incentivize decentralized development. There still are natural barriers to entry such as having the proper hardware and connectivity to process users' transactions and secure the network.

Governance and Self-funding

We plan to implement governance features similar to the Dash DAO. Having a treasury gives a cryptocurrency a significant advantage and much higher security. Although rare, an exploit in the code may exist and can cause extreme inflation as seen in Bitcoin twice. A cryptocurrency needs a full time staff to be able to detect and repair these exploits to minimize losses. Amaury Sechet, creator of Bitcoin Cash and lead developer of Bitcoin ABC client, explains that even if no exploits are found for years, a cryptocurrency still needs full time developers to be ready to fix any potential exploits at a moment's notice. (Hear his excellent explanation here: https://youtu.be/6ywIL17ityk?t=118). This is even truer for privacy cryptocurrencies that may have more attack vectors due to their complex minting or privacy mathematical proofs that only very specialized cryptographers can handle.

Lava team, compensation, and seed fund

The Lava team are anonymous due to uncertain regulation for privacy coins, and for personal privacy reasons. The executive team will receive $15,000 a month + 15% of the treasury as performance bonus and incentive. 5% of the total supply will go to the seed fund investors and founders who are also anonymous.