Amolecoin Whitepaper

By: Basliel Selamu and Bekalu Temsgen (Founders)

October 24, 2019

Amolecoin

Amolecoin makes free, decentralized payments possible within seconds, allowing truly decentralized global remittance at speeds that could rival any established payments network or e-wallet. It's the cryptocurrency that's ideal for countries like Ethiopia.

Amolecoin Features

Lightning Fast Transactions take as little as 2 seconds. With no bottlenecks or fees, Amolecoin is faster than other cryptocurrencies and competitive with credit cards and Apple Pay.

Zero Fees Amolecoin transactions cost Coin Hours, a separate currency paid to Amolecoin holders for each hour they hold a coin.

Secure Built from the ground up in Golang, Amolecoin makes full use of time-tested cryptographic standards to ensure transactions can't be tampered with. Amolecoin renders useless such threats as 51% attack, reversal, duplication, and malleability.

Private Amolecoin's transaction structure was designed to seamlessly adopt the CoinJoin protocol. Once integrated, Amolecoin mixes transactions from multiple wallets to ensure they are indistinguishable from one another.

Sustainable Without the enormous computational energy requirement typical of PoW and PoS processes, Amolecoin can run on a 30-watt cell phone processor.

Supply & Distribution

Amolecoin is immutable. The total supply is capped at 100 million 1 coin for every Ethiopian, and coins cannot be created or destroyed. Distribution is an open process. As more coins reach the public, the rate of distribution will slow. This approach puts Amolecoin in the hands of users and community members instead of miners and speculators.

Our mission is to create a new more stable finical system for Ethiopia. Unowned distributable coins will go into supporting long-term network growth (e.g. subsidizing more users to build nodes). Because of this growth-oriented approach, Amolecoin does not need a large up-front fund. At the time of writing, there are 75 million undistributed Amolecoin, and they cannot be distributed until the first 25 million (25%) have been distributed. For every year after the first 25% are distributed, another 5% unlocks.

Distribution beyond the initial 25% is hard-coded into protocol and time locked so that coin distribution stays below the 5% maximum. By creating a hard-coded, time-locked distribution policy, Amolecoin ensures several things: a fair process that does not deviate from the team's original intent, a rate of distribution aligned with user growth, and the protection against inflation.

Obelisk

Obelisk is central to the entire Amolecoin infrastructure. Web-of-trust consensus changes the way we understand and use blockchain technology. It removes the need for costly mining resources, eliminates the vicious cycle of mining incentives, exponentially improves transaction speeds, and delivers greater security.

Bitcoin's Problems and the Weaknesses in Proof-of-Work

In Bitcoin's early programming, there was a fundamental miscalculation that the mining process would produce an economic incentive structure conducive to decentralization. Instead, PoW has concentrated influence among mining pools that can supply the resource intensive miners with cheap power. These same groups of influence can orchestrate widespread changes to the network (e.g. forks).

Satoshi Nakamoto himself identified mining-control as the biggest noncryptographic threat to the Bitcoin network due to the possibility of 51% attacks when more than 50 percent of the hashing power is confined to one actor.

This also implies that the operation of the network is both economically and environmentally inefficient. According to Energy Researcher Sebastiaan Deetman (2016), "If the Bitcoin network keeps expanding…it could lead to a continuous electricity consumption…[equivalent to] the total consumption of…Denmark by 2020." The continuous input of processing power required by the mining process also incurs monthly costs in the tens of millions. There is little sustainability.

The enormous mining costs can only be offset by exponential influxes of new capital and new users. However, few coins outside of Bitcoin and Ethereum have the rapport to sustain such growth.

The Centralizing Tendency of Proof-of-Stake

Although PoS algorithms tackle the security issue of 51% attacks, they are arguably even more vulnerable to centralization than PoW networks. With PoS, the size of a participant's holdings of the particular cryptocurrency (or "stake") determines their voting power for technical changes in the network. Participants also get to mine a portion equivalent to their stake regardless of processing capability.

This principle significantly increases the economic barriers to launching a 51% attack. The financial cost of acquiring the majority of a network's tokens in the open market likely exceeds the potential gain. Furthermore, if an attacker successfully becomes the majority stakeholder in the network, they will suffer most from the attack due to impact on network stability and market response.

Although it raises the barrier to human-led attacks on the network, PoS creates a centralizing impulse equal to PoW. With PoW, voting on the implementation of technical changes to the network "is divided among miners, developers, and other crucial members of the community," (Young, 2016) whereas a PoS system gives "major stakeholders…a technical ability to make any changes they like without considering the will of the community, businesses, miners and developers. This centralization of voting power and, essentially, control of the network defeats the purpose of a distributed ledger-based cryptocurrency since it contradicts its entire principle of distributing all elements within the network to avoid the presence of a central authority." (Young, 2016).

The Solution: Obelisk – Distributed Consensus Algorithm

To tackle this centralization problem, Amolecoin uses a distributed consensus algorithm, Obelisk. Obelisk distributes influence over the network according to a web-of-trust. Instead of miners, the web consists of nodes (e.g. computers, DIY nodes, etc.) and each node subscribes to a list of trusted nodes. Nodes with more subscribers hold more influence in the network.

Each node is assigned a personal blockchain that acts as a "public broadcasting channel," where its every action is publicly recorded and visible. As all consensus decisions and communication occur through the personal blockchains of each node, the community can easily audit nodes for cheating or collusion— without compromising privacy. The nodes are addressed by their cryptographic public key and a node's IP address is only known to the nodes it is directly connected to. Furthermore, there are no fixed ports and no known plain text in wire format.

The public record left by each node's personal blockchain allows the network to react to defections by severing connections with less trustworthy or malicious nodes. Under the same principle, if the community feels that power within the network is too concentrated (or not concentrated enough), the community is able to shift the balance of power by collectively changing their trust relationships.

The accountability of nodes to the community and 3rd party audits as well as the transparency of consensus strengthens collective decision-making, and introduces a highly democratic and decentralizing element to the network.

Obelisk’s Consensus Solutions

High scalability and low energy consumption

The consensus algorithm was designed to be a scalable and computationally inexpensive alternative to PoW, enabling both the algorithm and block-making to run on budget hardware. Centralization becomes more difficult when more people have access.

Robust defense against coordinated attacks

Obelisk can withstand a large-scale coordinated attack by a well-organized network of malicious nodes. The algorithm is non-iterative, converges fast, can run on a sparse network with only nearest-neighbor connectivity (e.g. on a mesh network), and works well in the presence of cycles in the connectivity graph (i.e. DAG-type connectivity is not required).

Protecting against the “51-percent Attack”

Web-of-trust consensus prevents the development of centralized power. Amolecoin does not rely on mining incentives, and therefore is not susceptible to the same PoW/PoS vulnerabilities. In the unlikelihood that enough resources have been pooled to disrupt the network, it will have little effect on network users. The intruder would still need the private key of someone in the transaction chain to do any damage. There is no transaction malleability in Amolecoin. In addition, the public record on each node, including intruders, ensure its swift severance from the network upon detection.

Hidden IP addresses

The nodes are addressed by their cryptographic public key. A node’s IP address is only known by the nodes it is directly connected to.

Independence of clock synchronization

The Algorithm does not use “wall clock” (i.e. calendar date/time). Instead, block sequence numbers extracted from validated consensus and blockchain related messages are used to calculate a node’s internal time. This can be informally called “block clock.”

Two type of nodes exist: Consensus and Block-Making

A Consensus Node receives its input from one or more Block-Making nodes. The algorithms are separate for each, but they both operate on the same data-structures. Both type of nodes always performs authorship verification and fraud detection of incoming data. Fraudulent or invalid messages are detected, dropped, and never propagated— peer nodes engaged in suspicious activities are severed, and their public keys are banned.

Coin Hours

Amolecoin transactions do not incur fees. Transaction fees, similar to block rewards that incentivize miners to drive up fees at the cost of the network, only create monetary incentives with adverse effects by eliminating transaction fees.

Instead, Amolecoin transactions cost Coin Hours— not Amolecoin. To earn Coin Hours, users simply hold Amolecoin in order to participate in the ecosystem of Web 3.0. For each Amolecoin held by an address per hour, its owner nets 1 Coin Hour. Therefore, holding1000 Amolecoin for1 hour generates 1000 Coin Hours.

Beyond transaction fees, Coin Hours increase transaction privacy within the Amolecoin CoinJoin infrastructure by acting as collateral for mixing. This prevents participants from backing out of or slowing down CoinJoin transactions.

To prevent inflation and support fair use, only a maximum 100 million Coin Hours are produced each hour. Each transaction will burn 50% of the accumulated Coin Hours attached to the coin outputs being spent by the transaction, rounded up. This creates scarcity and limits the number of Coin Hours in circulation to an equilibrium value.

Appendix

A Distributed Consensus Algorithm for Cryptocurrency Networks

by user johnstuartmill and an anonymous user

Amolecoin
Amole.cc