aRIA: A Peer-to-Peer Electronic Cash System

White Paper v1.2

aRIA Developers
support@ariacurrency.com
www.ariacurrency.com

1. Introduction

aRIA - RIA is the integration of cryptocurrency's two foremost Blockchain technological achievements — Bitcoin, and proof of stake consensus.

Today, Bitcoin core continues utilizing proof of work, a consensus algorithm that is slow, open to 51% attacks, costly to mine, harmful to the environment, and resistant to scalability.There are, however, many innovations unique to Bitcoin that require preservation, such as its 21 million token supply model and proven code-base developed by many of the world's foremost software engineers and cryptographers.

By combining Bitcoin's strongest assets with a highly efficient, scalable, and flexible proof of stake consensus algorithm, aRIA introduces a new paradigm for cryptocurrency utility. aRIA does everything Bitcoin is currently able to do, while bringing new advances inblockchain technology onboard, thereby updating Bitcoin for the future.

2. Mission

The world is at a crossroads. Trust in financial institutions is at an all-time low, yet the cryptocurrency revolution kicked off by Bitcoin hasn't materialized for the masses. After years of opportunity, most cryptocurrency projects have failed everyday users by under-delivering on promises and over-complicating digital assets.

aRIA aims to pick up where Satoshi Nakamoto's vision of a bank-less, financially independent, and peer-to-peer electronic cash system left off. aRIA is simple to use, scalableto the financial uses of billions of people worldwide, secure — and most importantly, easy to adopt for existing enterprise, payment, and retail applications.

3. What is Proof of Stake?

Consensus in Bitcoin is achieved by requiring generated blocks to contain a proof that the miner which generated the block solved a computational hard task. Unfortunately the concept of the Proof-of-Work (PoW) based system tends to lean towards eventual self-destruction.

Proof-of-stake (PoS) aims to replace the way of achieving consensus in a distributed system; instead of solving the Proof-of-Work, the staker which generates a block has to provide a proof that it has access

to a certain amount of coins before being accepted by the network. Generating a block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called stake) is specified by the network through a difficulty adjustment process similar to PoW that ensuresan approximate, constant block time.

As in PoW, the block generation process will be rewarded through transaction fees and a supply model specified by the underlying protocol; which can also be seen as interest rate by common definition.The initial distribution of the currency is usually obtained through a period of PoW mining.[1]

4. Problems of Bitcoin Centralization

A popular saying is If it ain't broke, don't fix it. While many Bitcoin proponents may say that Bitcoin isn't broken, that perspective quickly goes out the window when framed in terms of the future.

Owing to its current electricity-based miner-dependent design, Bitcoin encourages the centralization of mining resources. Put simply — electricity, and the mining hardware that runs on it — are costly resources. Additionally, mining Bitcoin requires that one possess those resources, or ongoing access to them, in high supply.

5. aRIA Solves Bitcoin's Centralization Problem

The problems associated with Bitcoin's centralization are many and has been well documented in the Blockchain Community. However, aRIA solves those problems through a novel solution — namely, by replacing the Bitcoin proof of work algorithm with a Bitcoin proof of stake algorithm.

By replacing Bitcoin PoW with PoS, the four problems associated with proof of work that combine to create an unnecessarily centralized cryptocurrency disappear. aRIA is lessdependent on electricity, has a lower barrier to entry regarding hardware and is thus more accessible and easily decentralized, is eco-friendly because of its gentle use of electricity, and is more resilient to 51% attacks because of its decentralized-by-design architecture.

6. aRIA Reduces Electricity Consumption by 99%

Let's face it — the world is at a major crossroads when it comes to energy consumption. If we are designing the future of currency, and if what is at stake is creating a better way to do finance,then that way must be in line with the demands of a cleaner economy.

As such, a proof of stake consensus algorithm is the only way to go, and is the update that Bitcoin is sorely in need of. aRIA reduces Bitcoin's energy consumption by 99%, a figure that has been confirmed by the Ethereum team.

Ethereum's well-documented move away from PoW and over to PoS was hastened in part because of the team's discovery that PoS represents a drastic reduction of electricity dependency. Under the proof of stake algorithm, Ethereum developers plan to reduce blockchain energy consumption by at least 99% [13], leaving those still using PoW algorithms to wonder why.

By reducing the need for electricity, the playing field for network validation becomes much more even. Without having to worry about a cheap electricity source, network validators on the aRIA network can simply use the energy source from wherever they are. The electricity needed by lightweight hardware for PoS validating is such that only minimal electricity is needed. The amount of electricity it takes to run a laptop is enough — but what's more is that in a PoS network, validators, referred to as stakers, can delegate the task of staking to a staking pool. This means that individual stakers can validate the network without having to actually run hardware themselves — all the while their stake is still in their wallet as usual, thereby circumventing the centralization of mining pools, too.

7. aRIA Makes Staking Easy

Proof of work networks require miners with access to cheap electricity and expensive hardware mining rigs. aRIA, on the other hand, eliminates the need for a mining rig because proof of stake networks are lightweight and don't place excessive hardware demands on stakers.

Whereas miners are required to solve complex algorithmic equations and thus need increasingly better hardware miners, stakers are only required to create consensus around each transaction, and are rewarded for their effort according to their stake.

This reduces the materials threshold for would-be participants and makes it possible for true decentralization to occur. Stakers can use normal hardware, such as a laptop or desktop computer, or they can delegate their stake to a mining pool while retaining their staked aRIA coins in their wallet.

Reducing the burden on network participants is a key aRIA design goal. The lower the strain and demand on stakers, the higher the rate of participation, and the more decentralized and flexible the network becomes. If the paradigm for participation requires an actor to have immense resources, then we will only see a repetition of the hoarding of resources already present in the world.

So, the question we must ask ourselves is — should blockchain be for the 1%? Or is blockchain an attempt to go in the other direction and widen the scope of participation? Fundamentally, we believe in the latter, and have designed aRIA to encourage mass participation.

8. aRIA Is Environmentally Friendly

The future is in our hands. Anyone and everyone who has a stake in the future also owes it to themselves to participate only in networks who understand the ramifications of using environmentally disastrous technologies such as PoW.

As such, the aRIA team is committed to finding better ways to do blockchain, beginning with making Bitcoin green. For years, the profits made on Bitcoin speculation were the only green things about it. However, now that there is an update to the network which integrates proof of stake, investors, speculators, and network participants alike can all rejoice in the fact that this is a form of digital currency that reduces blockchain's impact on the world.

Additionally, proof of stake is elegantly simple in its architecture. Rather than requiring unfathomably complex machinery for solving an increasingly difficult algorithm, all that is required of stakers is skin in the game — a stake of the network's token that is put up for validation. Owing to the simplicity of proof of stake, there is less that can go wrong versus more complex systems, and much less required in terms of resources that strain the environment.

9. aRIA Is More Secure Against 51% Attacks

Security is the top concern amongst cryptocurrency advocates, investors, speculators, and network participants. Who wants to lose everything because of a flaw in the system?

Bitcoin has just such a flaw — it is called centralization. Mining creates a paradigm of centralization that raises the specter of a 51% attack. If such an attack were to occur, the entire network, and its billion of dollars in value, would be jeopardized. It's safe to say that in such a circumstance, the Bitcoin network would be finished.

aRIA, by transitioning the entire updated Bitcoin codebase to proof of stake, avoids the possibility of a 51% attack with its elegantly simple design. Whereas an attacker needs to control 51% of the network hashrate for Bitcoin, if an attacker made an attempt on aRIA, they would need to control at least 50% of the network's token supply.

This difference is very important to recognize. Hashrate can be consolidated by creating common interests for the heads of major mining cartels. However, tokens can't be consolidated by the same effort, since they are distributed across a wider cast of actors who have varying interests, aims, and network values. The effort required to sway token holders into selling or contributing

their stake would be incalculably difficult, bordering on impossible, and so remains outside the scope of threats to aRIA.

Staking pools, while beneficial for delegating stake and lessening the technical knowledge required by individual stakers, have been accused as possible sources of centralization within the proof of stake ecosystem. However, because staking pools don't require the physical warehousing of tokens being staked and are merely delegates of stake, don't possess the tokens in a saleable format. Again, this reduces risk of 51% network attacks for not only aRIA, but all proof of stake networks.

10. aRIA Architecture

At its core, aRIA uses the same updated codebase as Bitcoin. The significant difference, however, is the consensus algorithm. aRIA uses proof of stake, rather than proof of work,for consensus building.

It is important to note that aRIA is not a Bitcoin chain fork. Instead, it is anoriginal implementation of the Bitcoin codebase with several performance and consensus upgrades that make aRIA a superior choice for financial applications such as payments — allowing to vastly improve network scalability.

11. Staking Prerequisites

Staking is the process of holding funds in a cryptocurrency wallet to support the operations of a blockchain network. Essentially, it consists of locking cryptocurrencies to receive rewards.

The following prerequisites apply to staking RIAs:

- The coins to be staked need to be matured; this means that the unspent outputs (UTXOs in short) need to have a depth in the main chain of at least the 500 blocks (which is the coinbase/coinstake maturity)

- The coins to be staked need to be in compatible address/transaction types (please check accordingly; at the time of writing this paper only P2PK and P2PKH are supported).

- Supported Addresses:
    - Address starting with uppercase "A"
    - Address starting with "aria"
- Unsupported Addresses:
    - Address starting with lowercase "a"

12. Block Structure

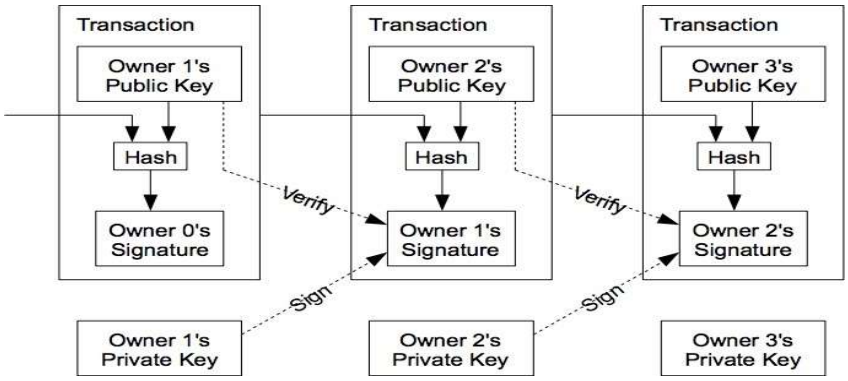
aRIA uses PoS V3 as consensus algorithm. The blocks must abide by these rules:

- Must have exactly 1 staking transaction
- The staking transaction must be the second transaction in the block
- The coinbase transaction must have 0 output value and a single empty vout
- The block timestamp must have it's bottom 4 bits set to 0 (referred to as a "mask" in the source code). This effectively means the blocktime can only be represented in 16 second intervals, decreasing it's granularity
- The block's kernel hash must meet the weighted difficulty for PoS
- The block hash must be signed by the public key in the staking transaction's second vout. The signature data is placed in the block (but is not included in the formal block hash)

- The signature stored in the block must be "LowS", which means consisting only of a single piece of data and must be as compressed as possible (no extra leading 0s in the data, or otheropcodes)
- Most other rules for standard PoW blocks apply (valid merkle hash, valid transactions, timestamp is within time drift allowance, etc)

13. Transactions

Like Bitcoin, aRIA transactions function on the basis of public and private key signatures wherein a public key is verified, and a private key is signed by the sender.



In non-proof of stake blockchain networks, double spends are discouraged by the lack of incentive for staking every fork. However, proof of stake networks like aRIA do incentivize staking every fork. Does this mean there is a higher chance of double spend transactions in PoS systems? The answer is no.

The above scenario is commonly referred to as the “nothing at stake” problem — but it incorrectly makes several drastic assumptions which are, in reality, nearly impossible. The most egregious of those assumptions is that every staker will stake every fork, when the possibility of amassing enough support per fork, no matter how far fetched, is nearly zero.

Because an attacker (or group of attackers) would need to incentivize stakers en masse to support a damaging fork, the logistics and cost of doing so are prohibitive.

In Bitcoin’s proof of work algorithm paradigm, that isn’t the case. Mining cartels aren’t holding delegated coins, nor are they simply representing the interests of others. They possess unjustifiably large amounts of hashrate, making it possible for a double spend attack to occur should any of those heads of interest collaborate.

Therefore, aRIA transactions are secure against double spend attacks while retaining the basic Bitcoin transaction infrastructure that users know and enjoy.

14. Mutualized Proof of Stake (MPoS) Consensus

Proof of stake consensus algorithms take on many forms. There are delegated proof of stake systems such as those used by EOS, and BFT PoS systems such as Cosmos. In the case of the former, dPoS adds undue complications to an already elegantly simple premise held by PoSnetworks. Additionally, dPoS algorithms introduce the possibility of increased network centralization, and don’t create enough cost for an attacker.

To further prevent the possibility of an attacker disrupting the aRIA blockchain, Mutualized Proof of Stake consensus function has been implemented. In a nutshell, MPoS creates an impossibly high cost barrier for malicious actors — one that is, theoretically, impassable.

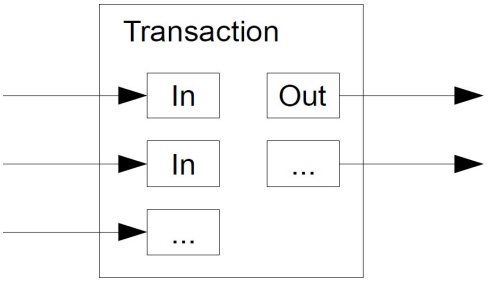
MPoS Explained

a. Prevent malicious miners from attacking the network for free by constructing expensive to validate blocks and then receiving all of the fees back to themselves through the mining process.
b. Help to make it more difficult and expensive for an attacker to DoS the network.
c. When a staker mines a block, he/she receives only a small portion of the PoS reward fees. The rest of the reward and fees are shared with 9 other people.
d. When a staker mines a block, his/her stake script (staketx.vout[0]) is registered to receive a share of the reward, lasting 10 blocks, 100 blocks from when the block was mined.
e. Thus, every block there will be 10 reward recipients. The creator of the block, and 9 "mutual stakers".
f. After 9 blocks of shared rewards, the staker's script will be removed and another will be added to replace it.
g. If a stake script has mined more than 1 block in a 10 block period, then there can be a case where he/she receives 2x the share. However, once the earliest stake script instance exceeds 110 blocks from its mined block, it is dropped and the reward drops to normal. Identical stake scripts should not be combined into a single UTXO – the rewards should be duplicated.

Under MPoS, attackers can't spam the aRIA network with fees. Instead, network participants all share the fees, instead of the totality of fees going to a single block creator — as is normally the case. With fee sharing in place, and an ongoing rotation of stakers, the substance behind a spam attack vanishes. Additionally, because the MPoS algorithm has already been deployed at scale within our test network, its success under widespread use has already been proven.

15. Stake Aggregation

In order to eliminate practices such as transaction flooding whereby a staker can gain an advantage by staking with a high number of transactions (fan-out), aRIA combines several inputs when creatingthe staking transaction (fan-in), trying to create a bigger stake for the block. To counter the unwanted effects of this input reduction mechanism which could lead to having really large transaction outputs, if the stake is above a certain threshold it will also be split into several outputs.



16. aRIA Payments

Of the many use cases prevalent for cryptocurrencies, the largest and most in demand is still payments. The world is slowly but surely transitioning to a paperless reality in which digital payments powered by similarly digital currencies are king — not cash.

Bitcoin cleared the way for this reality, but has stumbled in several major categories.

1. Bitcoin can not scale to the needs of millions — or billions — of worldwide users.
2. Bitcoin can't be easily integrated into existing payment rails and point of sale devices.
3. Bitcoin confirmations take far too long, making it inefficient for real time payments.

While some solutions, such as the Lightning Network, have been proposed and worked on, they are as yet missing from the space and have adoption issues of their own.

aRIA has several advantages in the payments space. It is designed expressly for integration with existing payment systems, networks, and point of sale devices for a seamless cashto crypto experience. This transition is aided by wise design factors.

1. The small block size of Bitcoin systems is a scaling liability. Proof of stake blockchains such as aRIA reduce block times to handle more transactions per second, making them fast enough to handle the speed of real time business.
2. Block finality in aRIA is improved over Bitcoin which creates a major advantage for retailers and retail users as payments are settled nearly instantly and with finality.
3. Whereas proof of work scaling solutions take network activity off the main-chain and onto side-chains, aRIA high throughput capabilities mean scaling is handled on the same chain — without having to rely on third party solutions.

17. aRIA Coin Supply

aRIA is not meant to compete with Bitcoin. Instead, it is meant to replace Bitcoin owing to its superior consensus algorithm, easily facilitated payments, and vastly reduced power consumption requirements.

Given these design goals, it is important to adhere strictly to the Bitcoin fundamentals, as aRIA pushes for a strict adherence to Satoshi Nakamoto's original vision of a cashless, bankless, and third-party free financial experience.

Maximum Coin Supply — 10 million aRIA (8 decimals)

18. aRIA Block time

The aRIA block time-spacing is set at 1 minute, making it not only more than 10 times faster than Bitcoin, but also able to handle more than 3 times the number of transactions. The block difficulty is calculated using an algorithm that relies on exponential adjustments, and the difficulty is adjusted at every block. Using this algorithm makes block times more predictable and less prone to big spikes.

19. aRIA Block Rewards

The aRIA emission rate is different from Bitcoin, with the key difference being that tokens are minted by stakers;

The rewards for the blocks are split the following way:

Block 1 has a reward of 500000 RIA (pre-mine)

Blocks 2 to 27,142,858 have a reward of 0.35 RIA

The block from 0 to 1 is a proof of work block, whereas block 1 contains premine coins which will be used by the developers; these funds will be allocated for initial Exchange funding, continued development, staking nodes, Web/Mobile Wallet user staking and maintenance of aRIA.

Apart from under-the-hood differences pertaining to consensus making and a vastly improved performance, the look and feel of aRIA is strikingly similar to Bitcoin, and will make the transition for Bitcoin users simple.

Proof of stake offers rewards to stakers according to stake size. Just as with Bitcoin proof of work mining, where rewards go to the miner who solves the block (known as block rewards), aRIA rewards also go to the staker, but split into 10 equal rewards (using the MPOS algorithm); the chance of minting a block is proportionate to the stake size, meaning, the higher the stake, the higher the chance is for the staker to mint a block before anyone else.

aRIA collects fees from transactions and uses the fee amounts to reward stakers for the activity of securing/validating the network.

Proof of work mining requires tireless commitment, expenditure of energy, high startup capital for investing hardware, and technical knowledge. aRIA, on the other hand, can be staked in the background of other tasks, giving you the opportunity to earn passive income as a staker.

20. Conclusion

In short, aRIA Currency is the next generation of blockchain and cryptocurrency from an overall efficiency standpoint. We have designed aRIA to be the fastest and lowest transaction cost available in the world. With the help of potential investors, aRIA will have vending machines to purchase/sell coins (replace global wire transfers), apps for retail transactions and even the opportunity to replace whole countries fiat money altogether. Yes, we have big plans for aRIA. There truly is no other coin like it available today.