TECHNICAL DOCUMENT FOR IBA COIN

ABSTRACT

An engaged, robust, active community with the means for adequate governance and decision-making processes is fundamental to the success of any decentralized, peer-to-peer cryptocurrency. The protection of personal information, especially financial data, is essential to preserve everyone's rights. It is not practical, nor historically wise, to trust centralized regulatory entities to protect an individuals' data appropriately. Additionally, without a proper system of governance, it is equally unwise to trust a cryptocurrency project or a specific blockchain with claims of being decentralized, as a single individual can hijack the network, unilaterally make a decision, or worse, lose access rending the codebase unaccessible.

Furthermore, for an emerging cryptocurrency project to thrive in a world where:

a. Energy is not taken for granted,
b. It has a solid economic model for growth without massive Quantitative Easing devaluation through inflation, and
c. It allows access to participate and earn from the global network from any low power device (e.g., mobile phone),

There must be a conscious thought into the algorithm selected (proof of work vs. proof of stake), the underlying economic system, and a means of network participation.

This is where the **IBA COIN** project comes in. The preservation of your rights and freedom, secured financial data, and privacy-protecting blockchain, can leverage greater cost efficiencies and reach wider adoption in an efficient, economically sound, and environmentally friendly manner at the protocol layer. The project does this while enhancing security and providing resistance to nefarious censorship or network exploitation of individual rights.

To solve these problems and gaps in the current cryptocurrency landscape, IBA COIN incentives every node in the network to be part of the block generation process through the implementation of a Proof of Stake consensus algorithm to decide which block will be chained next. Another layer to the network contains Masternodes, that provide Level 2 networking functionalities such as governance mechanisms. Further characteristics are:

1. Currency-flow balancing at the protocol level through novel inflationary/deflationary mechanisms incentivises decentralization and minimizes outside monetary policy involvement.
2. Staking with static block reward emission and tail end inflation enables more efficient resource allocation.
3. Low marginal costs for hardware/devices to stake and/or operate Masternodes reducing barriers to entry, allowing anyone to participate at any scale, and superior to other projects demanding wasteful energy requirements and hardware needs.

,

4. Global community-run decentralized governance allows for state-less oversight and provides direct community involvement and growth of the project.
5. Advanced Proof of Stake features such as Cold Staking (Ledger Tool for IBA COIN)

The entire IBA COIN ecosystem is akin to being a decentralized, self-organizing, virtual private on-demand network (VPN), but for money.

Proof of Stake

Through the implementation of PoS, the network has computing resources available which automatically select the node to generate the upcoming block on the chain based on delimited competition. In the case of IBA COIN, these limits are demarcated by considering the balance (UTXOs) staked by the wallet—every staking node is competing to create a valid block, very much like PoW. Nodes, however, are technically limited in the number of trials in a given time (eliminating the need for higher computing power) and the difficulty to get a valid block is inversely proportional to the amount being staked. A higher balance means a higher chance of satisfying the difficulty criteria, validating the block, and being rewarded. Staking is significantly less demanding on resources than PoW mining (i.e., Bitcoin), as there is no need to push towards ever increasing difficulty to solve algorithms necessary to mint coins, and the associated increase in computing power to solve said algorithms. PoS *is* an environmentally friendly alternative to PoW.

While the environmental factor alone already helps PoS stand out against PoW, there is another factor to be considered: maintaining a fair distribution of power across the network, which should be a high priority target of any cryptocurrency. With the expanding difficulty of PoW mining that necessitates more powerful devices (aka rigs) that cost more to run, the ability for people to feasibly operate such devices becomes more exclusive. Real life barriers to the average person in PoW operations include costs of hardware, electricity consumption spent on computing, and further consumption on cooling. Inevitably, this results in a great deal of power held by smaller groups of miners, of which even fewer will be able to remain competitive, not only leading to a monopoly in rewards, but in control over networks. IBA COIN use of PoS over PoW presents a far lower economic and resource dependent barrier for adoption and global use. Furthermore, setting up a PoW mining device requires more technical/advanced knowledge than setting up a staking node, which opens up a space for wider adoption and involvement of non-technical users.

Masternodes

The IBA COIN network is two-tiered. The staking tier is the first, in which all IBA COIN holders can participate through staking their IBA COIN; the second is the Masternode tier. Masternodes are a set of incentivised nodes within the IBA COIN network responsible for the handling of particular specialised tasks. The IBA COIN Masternode network has its roots from the cryptocurrency Dash, with a significant restructuring to a Proof of Stake consensus algorithm. As such, these nodes are an integral part of the IBA COIN digital ecosystem, and necessary to network functionality.

The Masternode network fulfils a range of functions independent of staking nodes. These distinct functions are limited to Masternodes, and cannot be completed by a standard staking node. These responsibilities are distributed across the Masternode network, and no single Masternode has power or authority in excess of others on the network.

Masternode Roles

For each Masternode, three different "roles" are defined. Each role is represented by a private/public keypair.

1. Owner: Must be unique on the network. Can update the other two roles, and the Masternode payout address.
2. Operator: Must be unique on the network. The operator key is saved in the ibacoin.conf of the remote node, and it is used to sign Masternode-related P2P messages (e.g. budget finalizations, or Masternode winners in the compatibility code). It can also be used to update the Masternode IP-address, or the operator payout address (if the Masternode is configured to allow a percentage of the reward to be paid to the operator).
3. Voting: Doesn't have to be unique (multiple Masternodes can share the same voting key). It is
   used to cast budget votes.

The same keypair can be used for all three roles (at least for now, the operator key will be changed to a BLS key soon), but they must be different from the key of the collateral address.

New Transaction Type

Here in IBA COIN COIN we introduce four new transaction types, each identifying a particular transaction payload, with its own validation rules:

- PROREG (*provider-register*): this is the main special transaction. Used for the registration of a new Masternode, setting all of its properties (such as the keys for each role). It creates the Masternode collateral, as one of its outputs, or it references a 10000 IBA unspent output on chain (in which case, it must include a signature with its keys, as proof of ownership).
- PROUPSERV (*provider-update-service*): sent by the mn operator to update the properties related to the service (IP address, operator payout address).
- PROUPREG (*provider-update-registrar*): sent by the mn owner to update the operator key, the voting key, or the payout address.
- PROUPREV (*provider-update-revoke*): sent by the mn operator to revoke the service, and put the
  mn in PoSe-banned state (e.g. in case of compromised keys). The Masternode can be "revived" later, by sending a ProUpReg tx, which sets a new operator key, and then a ProUpServ tx (signed with the new key), which sets the new IP address for the Masternode.

Masternode Voting on Budget Allocation

As a Decentralised Autonomous Organization (DAO), IBA COIN operates and abides by its own community self-governance. No single entity, nor a small collection of aligned entities, possess the ability to dictate the direction in which IBA COIN grows. This organic approach to governance is intended to draw the most value from members of the IBA COIN community, who themselves act in their own collective best interest. One of the means through which this form of governance is obtained is through Masternode voting on monthly budget allocations. Currently, Masternode operators are granted the ability to vote on proposals made by community members with the intention of bettering IBA COIN, or circumstances for it, in some way. With well 1000 Masternodes—which require a substantial investment into IBA COIN to operate— currently in operation, this approach greatly

divides power, allowing for no absolute authority within the community.

Stakenodes

In principal, PoS has the same function as PoW, to reach consensus on the blockchain. However, as noted earlier, it's much less resource intensive, thus it has become the chosen method of consensus for IBA COIN and many others projects. Using the Proof of Stake model requires the users to invest in a node by *staking* (placing on) their coins/IBA on a node (core IBA COIN wallet). In return for staking users are rewarded a set amount of coins in return. Stakenodes or Validators are responsible for the same thing as miners in proof-of-work: ordering transactions and creating new blocks so that all nodes can agree on the state of the network.

Proof-of-stake and Stakenodes comes with a number of improvements to the proof-of-work system:

- Better energy efficiency – you don't need to use lots of energy mining blocks lower barriers to entry.
- Reduced hardware requirements – you don't need expensive or specialized hardware to stand a chance of creating new blocks .
- Stronger immunity to centralization – proof-of-stake leads to more nodes in the network.

To run a Stakenode, users must simply be running the latest IBA COIN core wallet (on a device that will support its operation - laptop, desktop, raspberry pi, etc) AND have at least 1 IBA in their wallet AND have the wallet unlocked for staking.

FINANCIAL DATA PROTECTION

IBA COIN COIN uses zk-SNARKs based financial data protection protocol on a Proof of Stake blockchain in 2021, with mainnet activation live on August 30th, 2021. This protocol was given the name SHIELD.

IBA COIN implementation of SHIELD also represents anonymity to its users without individuals having to "mint" or create a different token to participate. Instead, through the simplicity of selecting a "shielded" address, a user can send or receive IBA with the confidence that all data and financial records remain protected and anonymous. SHIELD provides complete privacy for your transactions, preserving the transaction details' invisibility from the sender to the receiver, the amount of the transaction, and balances.

SHIELD further provides the end-user with a robust and fast transaction experience. The lightweight *proofs* are as small as 144 bytes and can be generated in seconds, even on a low-powered computing device like a Raspberry Pi. Users can enjoy fast and secure/shielded transactions across the network that take less than 500 milliseconds to generate and 1/100ths of a second to verify.

As many projects have experienced (especially when requiring large denomination pools of "private coins"), the adoption and use are often small when privacy is opt-in. This puts the actual privacy of those who use the protocols in jeopardy as it makes it easier to identify those users and their funds. With SHIELD, anonymity through its shielded addresses is offered by default. However, the ability to operate in an unshielded manner (transparent) entirely remains, allowing end-users to work with exchanges.

Introduction to Zero-Knowledge Cryptography and zk-SNARKs

Zero-Knowledge proof is a cryptographic method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying (or unknowingly leaking) any information apart from one simple statement: that the statement being made is indeed true. A Zero-Knowledge protocol thus allows you to do something REALLY impressive, to prove that you know something without revealing what that something is.

Put another way, let's say you have knowledge of something, but can't share it with a second party outright due to security concerns. However, without verifying knowledge, how does this second party know that you know what you know. That's the very definition of "zero knowledge," no ("zero") information about the secret is revealed, but the second party (or any other party that needs to validate) is convinced (in full) that you know the information/data/details (that secret).

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKS) is a non-interactive zero-knowledge proof (ZKP) that can be verified without any interaction with the prover. The Sapling Protocol, makes use of zk-SNARKs proofs to allow both shielded and unshielded transactions on the blockchain.

Sapling / zk-SNARKS (Groth16)

To start, zk-SNARK or, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, refers to a method of proof construction where an individual has the ability to prove possession of certain information (e.g., private key) without having to reveal that information to another party anonymously and thus not have any interaction. So, zk-SNARKS are a way to perform a "zero-knowledge" transaction
– a proof that allows two parties to prove that a statement between a prover and verifier is true, nothing more. Sapling is an advanced privacy-enabling protocol developed by the Electric Coin Company, creator of Zcash, that combines all of the above technical aspects, along with a new cryptographic construction, standardizing a fully functional Decentralized Anonymous Payment (DAP) scheme leveraged on a novel form of zero-knowledge cryptography called the Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKS). Sapling adds new highly usable types of transactions to the standard UTXO-based blockchain that enables the preservation of invisibility of transactional (meta) data while allowing the generation of zk-SNARKs proofs as small as 144 bytes within a matter of seconds on a low powered home computer. Thanks to this massive performance improvement in Sapling, private transactions become actually practical with <1 second (~500ms) needed to execute a private transaction. On the receiving side, it should take the recipient <1 second (~10 ms) to verify that transaction. These times place a private transaction into the realms of acceptable when it comes to large scale transaction and verification times for global commerce.

Sapling Keys

With Sapling, an individual generates what is called a "spending key," allowing them to perform a payment (what is the equivalent of having a secret/private key) and a "viewing key," which allows any individual who holds this key to see the payments received or emitted. This viewing key can be thought of then as a public "statement." For example, it can be shared with an escrow attorney/account, regulator, etc. for compliance purposes. However, you need not share the spending (or private key) to share the information.

Now, let’s say you want to receive a payment. You can generate an address from that viewing key and relay that to the individual sending funds. What is really nice about Sapling addresses is that they are diversified. With a single viewing key you can create, or derive, a brand new address which in no way correlates to the previous one. How does this help maintain privacy? By having uncorrelated receiving addresses, an individual is thus prevented from potentially leaking identifiable information. If you use a static address, it would be possible for an entity to uncover the identity of the person being paid