PAN AFRICAN COIN White Paper

This is a working document that is subject to review

SEPTEMBER 2020

DISCLAIMERS

No Advice

This whitepaper does not constitute any investment advice, financial advice, trading advice, or recommendation by onsokoafrica.com, its affiliates, or its respective officers, directors, managers, employees, agents, advisors, or consultants on the merits of purchasing PAC tokens nor should it be relied upon in connection with any other contract or purchasing decision.

Not a sale of a security

This whitepaper does not constitute a prospectus or financial service offering document and is not an offer to sell or solicitation of an offer to buy any security, investment products, regulated products, or financial instruments in any jurisdiction. PAC tokens are not being structured or sold as securities in onsokoafrica.com. Owners of PAC tokens are not entitled to any rights in onsokoafrica.com or any of its affiliates, including any equity, shares, units, royalties to capital, profit, returns, or income in onsokoafrica.com or any other company or intellectual property associated with onsokoafrica.com.

No Representations

No representations or warranties have been made to the recipient of this whitepaper or its advisers as to the accuracy or completeness of the information, statements, opinions, or matters (express or implied) arising out of, contained in, or derived from this whitepaper or any omission from this document or of any other written or oral information or opinions provided now or in the future to any interested party or their advisers. The PAC tokens, as envisaged in this whitepaper, are under development and are being constantly updated, including but not limited to key governance and technical features. If and when they are completed, they may differ significantly from the description set out in this whitepaper. No representation or warranty is given as to the achievement or reasonableness of any plans, future projections, or prospects and nothing in this document is or should be relied upon as a promise or representation as to the future. To the fullest extent possible, all liability for any loss or damage of whatsoever kind (whether foreseeable or not and whether or not onsokoafrica.com has been advised of the possibility of such loss or damage) which may arise from any person acting on any information and opinions contained in this whitepaper or any information which is made available in connection with any further inquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

Risk Statements

Purchasing PAC tokens involves substantial risk and may lead to loss of a substantial or entire amount of the money involved. Before purchasing PAC tokens, you should carefully assess and take into account the risks, including those listed in any other documentation. A purchaser should not purchase PAC tokens for speculative or investment purposes. Purchasers should only purchase PAC tokens if they fully understand the nature of the PAC tokens and accept the risks inherent to the

PAC tokens.

Cryptographic tokens may be subject to expropriation and/or theft; hackers or other malicious groups or organizations may attempt to interfere with our system/network in various ways, including malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing, and spoofing which may result in the loss of your cryptographic tokens or the loss of your ability to access or control your cryptographic tokens. In such an event, there may be no remedy, and holders of cryptographic tokens are not guaranteed any remedy, refund, or compensation. The uncertainty in tax legislation relating to cryptographic tokens and digital assets may expose cryptographic token holders to tax consequences associated with the use or trading of cryptographic token.

Digital assets and related products and services carry significant risks. Potential purchasers should take into account all the above and assess the nature of, and their appetite for, relevant risks independently and consult their advisers before making any decisions.

ABSTRACT

The PAC chain is a decentralized, programmable database designed to support a low-volatility cryptocurrency that will have the ability to serve as an efficient medium of exchange for billions of people in Africa. The PAC protocol allows validators to jointly maintain a database of programmable resources. These resources are owned by different user accounts authenticated by public-key cryptography and adhere to custom rules specified by the developers of these resources. Validators process transactions and interact with each other to reach consensus on the state of the database. Transactions are based on user-defined smart contracts in a new programming language called ***Move***. The platform hopes to create wealth for the continent through her four pillars namely E-Commerce, The Finance Services Platform, The Crypto-Fiat Mobile Exchange, and the PAC chain. Onsokoafrica.com is the Ultimate consumer discount hub for online shopping. For security purposes, Onsoko will hold the vast majority of funds in cold wallets to deter hacking. A few shall be held in hot wallets for liquidity purposes. Besides, there shall be a two-step authentication and whitelisting of wallet addresses for payouts to curtail the potential for loss.

EXECUTIVE SUMMARY

MISSION AND VISION

Decentralization holds the key to empowering people around the world to better safeguard their rights by accelerating the transition to adopting blockchain technology.

MISSION

To facilitate wealth creation and improve quality of life through blockchain technology.

VISION

To be the preferred crypto-fiat exchange, financial platform, and e-commerce hub in Africa.

PROBLEM STATEMENT AND OUR STRATEGY

Key Challenges in Driving OnSoko Africa Adoption

The African continent, with a total area of over thirty and half a million km^2 (30,415,875 km^2) in size, is 3 times the area of China, 10 times the area of Europe, and 4 times the area of the United States of America. The continent which has a superb climate is 60 percent arable land, 90 percent raw material reserve, 40 percent gold reserve, and 33percent diamond reserve and yet she is taunted as the poorest continent in the world. With a population of 1.3billion people, Africa can only compare to China which has a population of 1.4 billion. If well natured, by 2050 Africa alone will be able to feed a billion people.

Despite such wealth, the continent operates below capacity in an industrial sense making it the least industrialized in the world. The few available industries are starved of requisite capital to enable them to compete favorably in the global arena. It is unfortunate that Africa exports cheaply raw materials for processing before exorbitantly importing finished products from other continents.

OUR STRATEGY

Focusing on industrializing the continent, the OnSoko Africa has a model that seeks to popularize products manufactured in Africa on her e-commerce found at www.onsokoafrica.com. The company, apart from building these brands, will ensure that the manufacturers are directly linked to their customers and finance companies in a business-to-business-to-customer setup (B2B2C). An equivalent of an LPO shall unlock much-needed funding to keep production mills running. The company shall use augmented reality and social media analytics to create value for money and position the organization under cost leadership.

OnSoko Africa shall use Artificial Intelligence (AI) to complement its digital marketing. By leaving the most time-consuming and logic-based jobs to AI such as Twitter bots, image recognition, speech recognition, product recommender systems, and analytical techniques, the marketing team shall free up time to think creatively. This dichotomy shall ensure that clients are empowered to control their money anywhere anytime, safeguarding their data, and protecting their identity from compromise by any central entity.

Job Creation.

Sustainable industrial growth in an expanded market shall uplift the economic standards of the continent with increased job creation opportunities. Through a unique, multi-level marketing model, the majority of the continent's youth, under the OnSoko Africa model, will be engaged in brand building, marketing, selling, and delivering the products within and outside their home countries. Personalized content has become a major aspect of marketing and will be vital to ensure customer delight. It delivers a unique experience to customers based on their choices and preferences and is considered a better option than "one-size-fits-all" marketing. With the availability of data like purchase history, consumer behavior, and links clicked, businesses can customize their content and boost their Return on Investment. Businesses these days are leveraging the power of personalization by customizing emails based on behavior, interests, and demographics.

ONSOKO ECOSYSTEM

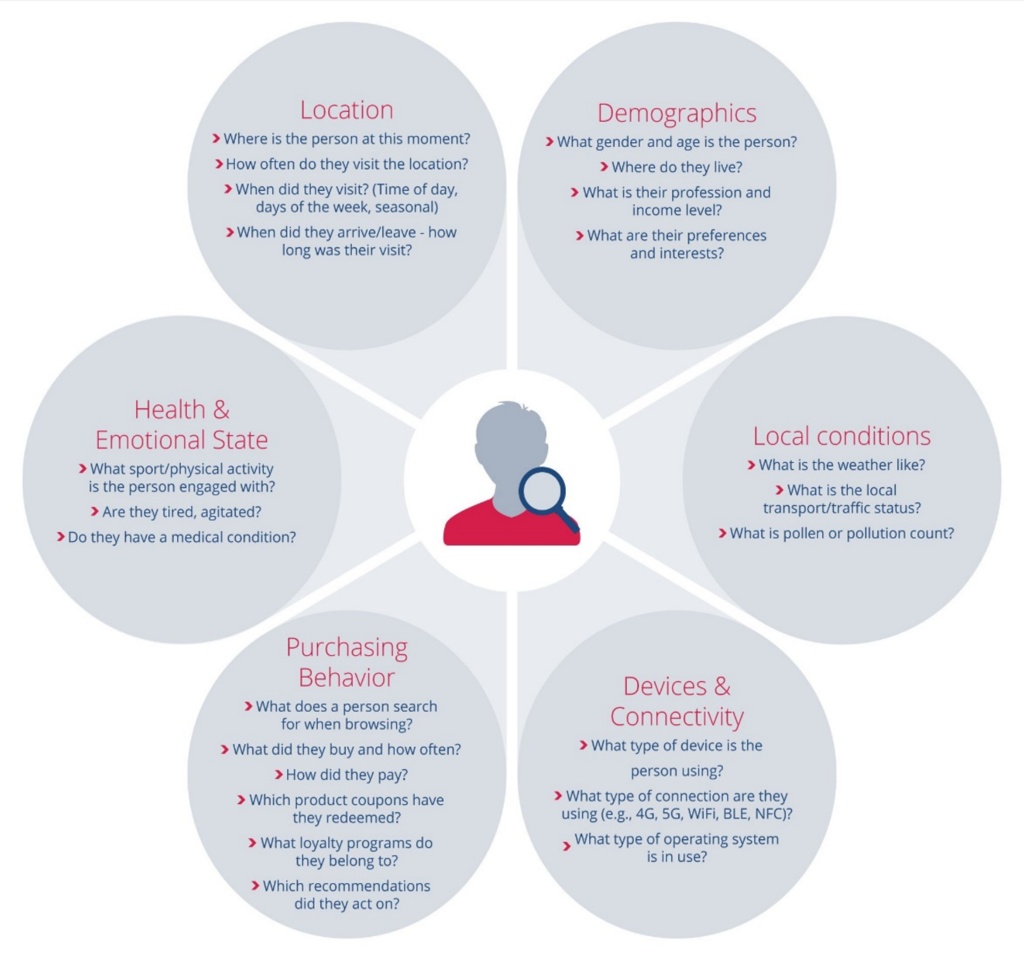
ONSOKO E-COMMERCE

OnSoko Africa is an online retail service that allows business-to-business sales as well as business-to-customer, customer-to-customer affiliate marketing. It is designed to sell a wide variety of products and services with extremely reasonable fees compared to other options. It will be possible to pay with Pac Coin or fiat directly from your wallet or card and mobile app. Pacdexchange allows buyers to pay with Pac and the merchant will receive fiat currency. OnSoko Africa is for individuals and businesses whether big or small to sell and buy anything within the law be they physical products, digital products, or services online. You will sell at ease with peace of mind. Payments can be made directly from the trading account through your Pac wallet or mobile app which will automatically convert your Pac coin to fiat or spend your fiat to get Pac coin. Clients exhibit hybrid purchasing behavior today, and this will continue; for example, more affluent consumers combine premium and value brands in their shopping mixes, while low-income consumers save up for select premium products as status symbols. Going forward, clients will increasingly move between segments, and this fluidity means that the boundaries between segments will blur. Clients are also drawn to the heightened relevance and utility that more personalized services can afford (when executed well), and expectations here will intensify. Old segmentation models based on socio-demographic parameters and past search and purchase patterns alone will prove ineffective. Instead, Onsoko made Africa Limited will take a far more sophisticated, creative approach to segmentation that is based on context rather than old-school, prescriptive, one-size-fits-all models.

Moving from a 2 D to 3 D customer perspective

The range and depth of customer data insight are widening. There will be more digital services, platforms, and devices than ever before capable of generating data insights, including social media and messaging apps, location-based services, and online and mobile payments. On the device's front, smartphones, tablets, and connected TVs will be joined by wearables, medical appliances, connected cars, and multiple embedded touch points in smart homes and cities.

These multiple sources of data, combined with the ever-improving capacity to reconcile data coming from different devices, will enable an increasingly rich view of the consumer, moving from today’s still largely two-dimensional view to one that is fully contextually relevant. OnSoko Africa understands how these multiple customer insights relate to touch points in the consumer shopping journey, such as where they viewed a product (location and device). Below, is a 360-degree contextual view of clients.



Location

- Where is the person at this moment?
- How often do they visit the location?
- When did they visit? (Time of day, days of the week, seasonal)
- When did they arrive/leave - how long was their visit?

Demographics

- What gender and age is the person?
- Where do they live?
- What is their profession and income level?
- What are their preferences and interests?

Health & Emotional State

- What sport/physical activity is the person engaged with?
- Are they tired, agitated?
- Do they have a medical condition?

Local conditions

- What is the weather like?
- What is the local transport/traffic status?
- What is pollen or pollution count?

Purchasing Behavior

- What does a person search for when browsing?
- What did they buy and how often?
- How did they pay?
- Which product coupons have they redeemed?
- What loyalty programs do they belong to?
- Which recommendations did they act on?

Devices & Connectivity

- What type of device is the person using?
- What type of connection are they using (e.g., 4G, 5G, WiFi, BLE, NFC)?
- What type of operating system is in use?

Reasonable Fees

Buyers will use the platform free of charge. Sellers on the other hand will pay commissions on the platform of anywhere between 5 percent to 10 percent depending on sales volume which is a sliding scale. The annual membership fee ranges from $ 300 to $ 500 depending on sales volume. Payment of these fees with Pac token will save considerably.

Onsoko Mobile Applications

This is an innovative application that allows both crypto trading as well as shopping on the platform. Onsoko mobile app will allow clients and advocates access all parts of the platform right from your android or iOS mobile gadget. Keep OnSoko exchange in your pocket with all the advanced tools giving you the fastest arbitrage and multi-exchange trading options available. Shop from any location and pay with Pac and enjoy discounts and offers from trading partners on our platform. These trading partners can customize their products to fit customer specifications. Super agents shall come in handy along the value chain for seamless delivery of services.

THE FINANCE SERVICES PLATFORM

The exponential rise of computational power and storage capacities, along with ever-expanding access to knowledge, are some of the key driving forces of the fourth industrial revolution. Blockchain technology is, perhaps, the single most exciting innovation with enormous implications for revolutionizing products and services, comparable to the invention of the internet. One of the immediate candidates for disruption by this technological advancement is the financial services industry, which, up to very recently, has been unhealthily rigid.

Apart from the ubiquitous functions of blockchain technology, such as the point-to-value transfers, there is one, that, up until recently, has been hugely underappreciated-the digitization of assets. The blockchain immutably records the transfer of tokens or units of ownership on a distributed ledger and thus makes the process trustless and transparent. The digitization of assets (tokenization) is doing the same to the securitization of the financial markets as what the advent of the email has done to the post office. While securitization converts an illiquid asset or group of assets into financial securities, tokenization allows for that security to be traded over a digital medium with unprecedented ease and cost efficiency.

This platform shall provide fiat loans secured by crypto assets. While there are a variety of business models, crypto lending platforms can be divided into two main camps: centralized, which are generally businesses that selectively onboard clients, manage payments and custody assets; and decentralized, which are largely protocols that automate distributions and allocations. Pan African Coin shall incorporate structured financial products customized to client risk profiles with a downside risk of zero within an agreeable locking period. The range and complexity of this platform shall be within the confines of splinternet and socially responsible investment. Pan African Coin shall be guided by both precautionary motives and transactional motives in addressing client needs but desist from any speculative component in their endevours with client funds. The financial package in this platform includes the following services: mobile-based co-operatives, peer-to-peer lending, crypto-asset loans, insurance, and remittance. The origination process is purely client based.

Crypto lending vs Traditional lending

Crypto lending is markedly different from traditional lending. It's not just the innovation in the technology powering smart contracts, or the new types of assets that can be collateralized. The sector also stands out for the flexibility and relative security of credit.

Variety and speed

First, crypto lending involves a much wider range of assets, which confers a flexibility on market participants. Few traditional finance platforms offer yields on such a wide range of assets. While it is possible to lend various types of traditional securities and submit an even broader range of assets (including real estate and art) for collateralization of a loan, the lending of crypto assets involves less paperwork, fewer intermediaries if any as well as lower (and generally more transparent) fees. Front end load is non-existent.

Users of lending platforms, both centralized and decentralized, can switch between assets with relative ease, depositing Pac coin (for instance) to take out a stablecoin loan, or using their ether stake for a Pac coin loan that enables them to fund an exchange account to buy more ether. This can be done in seconds.

Collateral

Collateral deposited for loans from these platforms is always in crypto assets, which are more liquid than many types of collateral in traditional markets. What's more, for now, most platforms insist on the collateral of over 100 percent, sometimes as much as 150 percent, to offset possible asset price volatility. Given the relative liquidity of these assets (compared to commodities), should the market turn south and the loan-to-value ratio decline, lenders could sell the collateral in the markets. This would in theory stem their potential losses (although possibly accelerate the slump). The total market capitalization of digital assets is expected to be $ 5 trillion by 2025 as a consequence of blockchain technology adoption across various industries.

Regulation

Currently, crypto lenders are not considered banks and do not need special licenses. While this may be a deterrent to many potential participants due to a lack of trust, it allows lending businesses to focus on building a strong reputation through service and selective transparency. It also allows them to keep costs down for users, as reporting requirements are low.

Benefits

Few will object to the additional income that lending could bring to crypto asset holdings. Lending services enable holders of crypto assets to supplement the capital gains potential with interest income. This, combined with the relatively attractive yields on crypto-assets compared to those on more traditional assets, could entice a broader range of investors into the crypto asset class, boosting volumes as well as strengthening liquidity and infrastructure. Another benefit is the increased facility for selling short, in which a pessimistic trader borrows an asset to sell on the market to buy it back at a lower price. The ability to short an asset is important for reliable price discovery—if those that think the price will go down don't have a way to participate in a market, the market will reflect a buyer's bias. A lively derivatives market is one way to express a negative opinion; selling short is another, and could become a more extended use case as platforms adopt features that make it almost as simple as trading futures. Perhaps the strongest benefit to the sector comes from additional liquidity. Many traders and investors deposit their crypto holdings as collateral to borrow either cash or another crypto asset, with which to increase their crypto holdings. This effectively introduces leverage into the sector but enhances liquidity through additional trading.

Risks

Among the risks posed by the growth of crypto lending services is the “over-financialization” of the market. While crypto lending shouldn’t increase a token’s supply, the emergence of layered claims on a holding, and the issuance of securities based on those claims, could blur the bearer nature of crypto assets and the rights of the original holders. Another risk, present in all centralized financial services, is that of counterparty default. Crypto lending platforms are as yet unregulated and uninsured (although many have custody insurance). The collapse of a significant lender would send ripples of doubt throughout the system, as actual ownership and eventual recovery of deposited tokens would be unclear.

With decentralized platforms, transparency can also be a risk. On-chain lending implies that others will be able to see transactions, and even if identities are masked, forensics could uncover them as well as trading strategies that could be malicious.

Smart contracts that move funds and manage investment contracts are relatively new technology. Errors can most likely be patched, but meanwhile, funds can be misdirected, and if these transactions are registered on a blockchain, the errors may be impossible (or politically very difficult) to correct. Even centralized platforms may find themselves required to improve their transparency, which will increase costs and business risk as their terms and conditions become easier to replicate. Furthermore, most of the main platforms delegate the safekeeping of their clients’ assets to reputable crypto custodians with insurance, but others may find themselves required to change their practices to ensure the protection of users’ funds.

Network security

In Proof-of-Stake (PoS) blockchains, token holders can participate in a network by “staking” holdings in exchange for a role in its governance and maintenance. The greater the number of and dispersion in stakers, the greater the network’s security. If on-chain lending offers a better financial return, users will choose that over staking privileges— this would thin the ranks of stakers, reducing a network’s security. This could even be “gamed” by an attacker, who could intentionally lure token holders away from staking rewards and take advantage of the lower security to effectively “take over” the network. Lending could also affect governance issues in other ways, such as allowing a bad actor to borrow large amounts of a staking token to attempt some kind of majority voting attack on a network. Alternatively, staking could perhaps one day offer enough yield to compete with lending platforms, which could weaken some business models and further concentrate the sector.

Pacdexchange.com

What services do **crypto exchanges provide?**

As in other financial markets, crypto exchanges provide several important functions, including:

- Trading services—the ability to buy and sell cryptocurrencies;
- Price formation—information about the consensus market value of cryptocurrencies;
- Asset storage—most crypto exchanges offer accounts or wallets typically stored in the cloud, where individuals can store their crypto assets (i.e. public and private keys to access their coins in the blockchain) to make these directly available for trading on the exchange.

As with any marketplace, crypto exchanges benefit from network externalities. As the number of traders on a crypto exchange grows, the opportunities for traders to trade on that exchange increase, and the exchange becomes more attractive to other traders.

This platform lets users trade Pac at ease with the following value propositions:

i. Deep liquidity with access to the best execution prices;
ii. Competitive fees offered with high volume accounts trading attracting concessionary rates
iii. Engaging events provided such as discounted token distributions and trading activity-driven competitions
iv. Institutional-grade infrastructure that powers high-availability, fully-resilient, and horizontally-scalable components.

Pacdexchange.com Shall deliver a suite of trading-related services for both retail and institutional users.

TOKEN DISTRIBUTION AND PLANNED USE

Overall Distribution Allocation

Pan African Coin is offering 1,000,000,000 PAC tokens to be distributed through multi-signature storage wallet allocations as follows:

i. Angel Investors have been allocated 100,000,000 PAC token representing 10percent shareholding

ii. Bounty programs offered to ICO promoters and developers stand at 100,000,000 PAC tokens

iii. Capital Reserve is allocated 100, 000, 000 PAC tokens

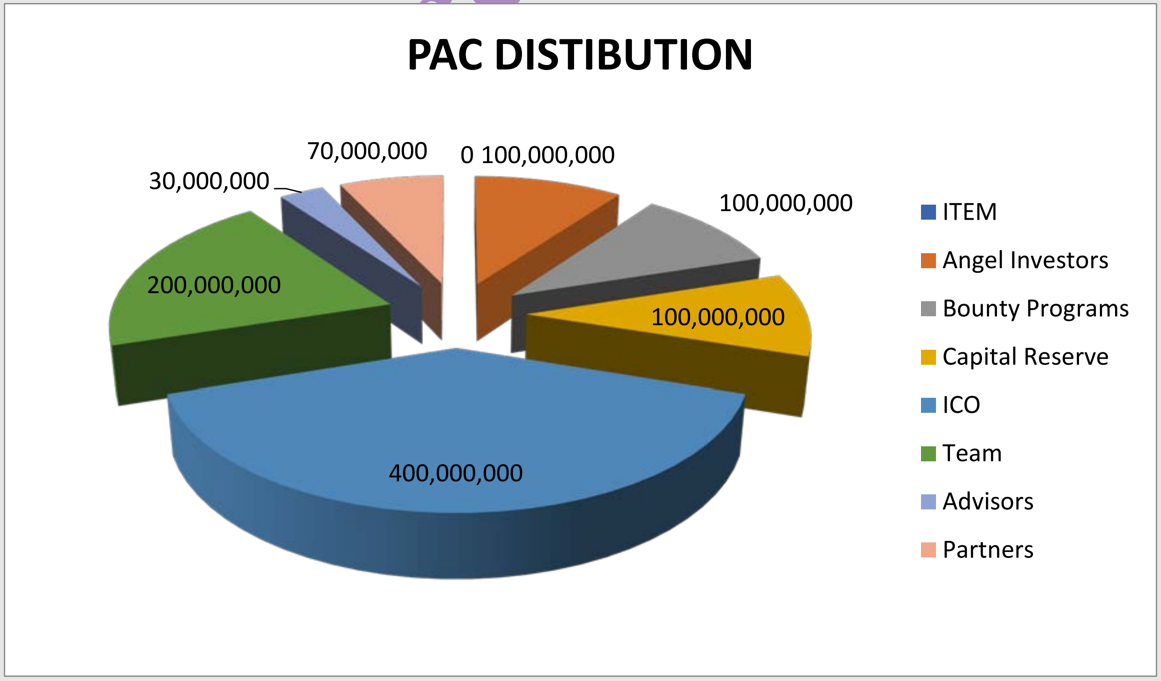
iv. Initial Coin Offering targets 400,000,000 PAC tokens

v. The team is allocated 200,000,000 PAC tokens

vi. Advisors have been allocated 30,000,000 PAC tokens

vii. Partners have been allocated 70,000,000 PAC tokens

Initial value: 1 PAC = 0.30 USD



PROJECTIONS

Africa’s population is projected to be 1.34 billion people in

The company is looking to build a community of 100,000 participants in 1year.

The community is expected to be attracted by the products in the ecosystem,

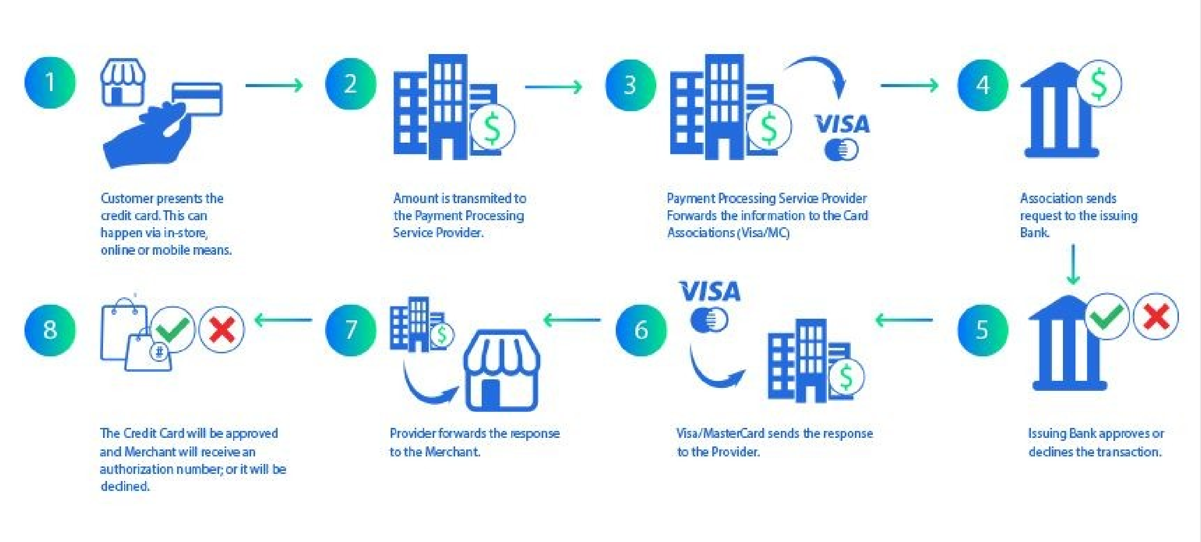
Thus;

100,000 participants transacting an average of $100 per day on the exchange will create a trade volume of 10,000,000 USD i.e. 100,000 x $100 = $10,000,000

This will translate to a demand of up to 33, 3333,333 PACS daily.

The PAC CHAIN

A key prerequisite for healthy competition and innovation in financial services is the ability to rely on common infrastructure for processing transactions, maintaining accounts, and ensuring interoperability across services and organizations. By lowering barriers to entry and switching costs, the PAC protocol will enable startups and incumbents to compete on a level playing field, and experiment with new types of business models and financial applications. Blockchain technology lends itself well to address these issues because it can be used to ensure that no single entity has control over the ecosystem or can unilaterally shape its evolution to its advantage [1].



1 Customer presents the credit card. This can happen via in-store, online or mobile means.

2 Amount is transmited to the Payment Processing Service Provider.

3 Payment Processing Service Provider Forwards the information to the Card Associations (Visa/MC)

4 Association sends request to the issuing Bank.

5 Issuing Bank approves or declines the transaction.

6 Visa/MasterCard sends the response to the Provider.

7 Provider forwards the response to the Merchant.

8 The Credit Card will be approved and Merchant will receive an authorization number; or it will be declined.

Captured above is a depiction of the highly centralized payment system we are coming in to alleviate through Pac protocol. OnSoko Africa’s solution is a decentralized trust and reputation system working flawlessly together through a Pac chain based payment gateway.

The PAC protocol. The PAC chain is a cryptographically authenticated database [3, 4, 5] maintained using the PAC protocol. The database stores a ledger of programmable resources, such as PAC coins. A resource adheres to custom rules specified by its declaring module, which is also stored in the database. A resource is owned by an account that is authenticated using public key cryptography. An account could represent direct end-users of the system as well as entities, such as custodial wallets, that act on behalf of their users. An account's owner can sign transactions that operate on the resources held within the account (2).

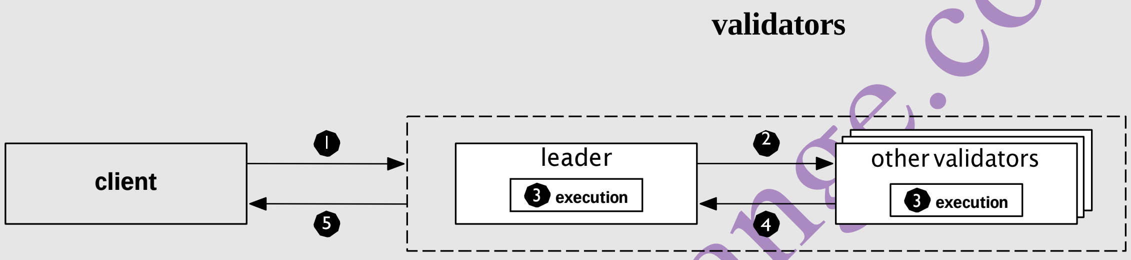


Figure 1: PAC protocol.

Figure 1 shows the two types of entities that interact using the PAC protocol: (1) validators, which maintain the database, and (2) clients, which perform queries on the database and submit transactions to modify it.

Ledger State

The ledger state represents the PAC ecosystem, including the quantity of PAC held by each user at a given version. Each validator must know the ledger state at the latest version to execute new transactions.

The PAC protocol uses an account-based data model [6] to encode the ledger state. The state is structured as a key-value store, which maps *account address* keys to *account values*. Account value in the ledger state is a collection of published ***Move*** resources which store data values and modules which store codes. The initial set of accounts and their state are specified in the genesis ledger state.

Account addresses.

The PAC protocol does not link accounts to a real-world identity. A user is free to create multiple accounts by generating multiple key-pairs. Accounts controlled by the same user have no inherent link to each other. This scheme follows the example of Bitcoin and Ethereum in that it provides pseudonymity [7] for users.

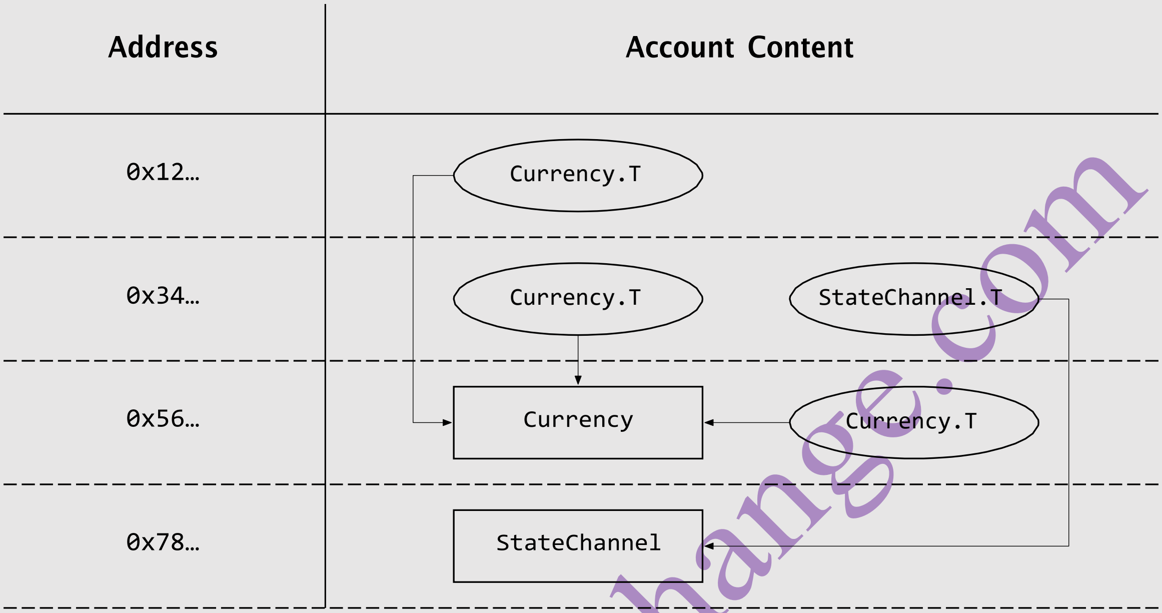


Figure 2: An example ledger state with four accounts. In this diagram, ovals represent resources and rectangles represent modules. A directed edge from a resource to a module means that the type of resource was declared by that module. The account at address 0x12 contains a Currency.Tresource declared by the Currencymodule. The code for the Currencymodule is stored at address 0x56. The account at address 0x34 contains both a Currency.Tresource and a StateChannel.T resource, which is declared by the module stored at address 0x78.

Resource values.

A resource value is a record that binds named fields to simple values such as integers or complex values such as other resources embedded inside this resource. Every resource has a type declared by a module. Resource types are nominal types [8] that consist of the name of the type and the name and address of the resource's declaring module. For example, the type of Currency.T resource in Figure 2 is 0x56.Currency.T. Here, 0x56is the address where the Currency module is stored, Currency is the name of the module, and Currency.T is the name of the resource.

To retrieve the resource 0x56.Currency.Tunder account address 0x12, a client would request

0x12/resources/0x56.Currency.T. The purpose of this design is to let modules define a predictable schema for top-level account values — that is, every account stores its 0x56.Currency.T resource under the same path. As such, each account can store at most one resource of a given type. However, this limitation is not restrictive, since programmers can define wrapper resources that organize resources in a custom way (e.g., resource TwoCoin {c1: 0x56.Currency.T, c2: 0x56.Currency.T }).

Module values. A module value, or *module*, contains ***Move*** bytecode that declares resource types and procedures. Like a resource type, a module is identified by the address of the account where the module is declared. For example, the identifier for the Currency module in Figure 2 is 0x56.Currency.

A module must be uniquely named within an account — each account can declare at most one module with a given name. For example, the account at address 0x56in Figure 2 could not declare another module named Currency. On the other hand, the account at address 0x34 could declare a module named Currency. The identifier of this module would be 0x34.Currency. Note that 0x56.Currency.T and 0x34.Currency.T are distinct and cannot be used interchangeably (2).

Transactions

Clients of the PAC chain update the ledger state by submitting transactions. At a high level, a transaction consists of a *transaction script* (written in ***Move*** bytecode) and arguments to the transaction script (e.g., a recipient account address or the number of PAC to send). A validator executes the transaction by running the script with its arguments and the current ledger state as input to produce a completely deterministic transaction output. The ledger state is not changed until the transaction is committed during consensus by agreeing on a binding commitment to the output of the transaction.

Events.

The event list is a set of effects produced by executing the transaction. ***Move*** code can trigger an event emission through an event structure. Each event is associated with a unique key, which identifies the structure through which the event was emitted, and a payload, which provides detailed information about the event. Once a transaction has been committed by the consensus protocol, events generated by the transaction are added to the agreed ledger history and provide evidence that the successful execution of a transaction resulted in a specific effect (2).

Transactions can only generate events — they cannot *read* events. This design allows transaction execution to be a function only of the current state, not historical information, such as previously generated events.

Ledger History

The ledger history stores the sequence of committed and executed transactions as well as the associated events they emitted. The purpose of the ledger history is to keep a record of how the latest ledger state was computed. There is no concept of a *block* of transactions in the ledger history. The consensus protocol batches transactions into blocks as optimization and to drive the consensus protocol. However, in the logical data model, the transactions occur in sequence without distinction as to which block contained each transaction.

Responding to client queries. Validators can use ledger history to answer client queries about previous ledger states, transactions, and outputs. For example, a client might ask about the ledger state at a specific version (e.g., "What was the balance in the account at address *x* at version 30?") or the history of events of a certain type (e.g., "What payments did the account at address *y* receive in the last 20 minutes?").

Executing Transactions

In the PAC protocol, the only way to change the blockchain state is by executing a transaction. While Move is used to define core system concepts, such as the PAC currency, users are unable to publish custom modules that declare their resource types. This approach allows the ***Move*** language and toolchain to mature — informed by the experience in implementing the core system components — before being exposed to users. The approach also defers scalability challenges in transaction execution and data storage that are inherent to a general-purpose smart contract platform.

ExecutionRequirements

Known initial state. All validators must agree on the initial, or *genesis*, ledger state of the system. Because the core components of the blockchain — such as the logic of accounts, transaction validation, validator selection, and PAC coins — are defined as ***Move*** modules, the genesis state must define these modules. The genesis state must also have sufficient instantiations of these core components so that transactions can be processed (e.g., at least one account must be able to pay fees for the first transaction; a validator set must be defined so a quorum of the set can sign the authenticator committing to the first transaction).

Deterministic. Transaction execution must be *deterministic* and *hermetic*. This means that the output of transaction execution is completely predictable and based only on the information contained within the transaction and current ledger state. Transaction execution does not have external effects (e.g., printing to the console or interacting with the network). Deterministic and hermetic execution ensures that multiple validators can agree on the state resulting from the same sequence of transactions even though transactions are executed independently by each validator. It also means that the transaction history of the blockchain can be re-executed from the genesis block onwards to produce the current ledger state.

Metered. To manage demand for compute capacity, the PAC protocol charges transaction fees, denominated in PAC coins. This follows the *gas* model popularized by Ethereum [16]. Pan African Coin takes the approach of selecting validators with sufficient capacity to meet the needs of the PAC ecosystem. The only intention of this fee is to reduce demand when the system is under a higher load than it was provisioned for (due to a denial-of-service attack). The system is designed to have low fees during normal operation when sufficient capacity is available. This approach differs from some existing blockchains, which target validators with lower capacity and thus at times have more demand to process transactions than throughput. In these systems, fees spike during periods of high demand representing a revenue source for the validators but a cost for the users.

Asset Semantics. The ledger state directly encodes digital assets with real-world value. Transaction execution must ensure that assets such as PAC coins are not duplicated, lost, or transferred without authorization. The PAC protocol uses the ***Move*** virtual machine to implement transactions and custom assets with these properties safely.

Transaction Structure

A transaction is a signed message containing the following data:

- **Sender address:** The account address of the transaction sender. The Virtual Machine reads the sequence number, authentication key, and balance from the PACAccount.Tresource stored under this address.

- **Sender public key:** The public key that corresponds to the private key used to sign the transaction. The hash of this public key must match the authentication key stored under the sender's PAC Account.T resource.
- **Program:** A ***Move*** bytecode transaction script to execute, an optional list of inputs to the script, and an optional list of ***Move*** bytecode modules to publish.
- **Gas price:** The number of PAC coins that the sender is willing to pay per unit of gas to execute this transaction.
- **Maximum gas amount:** The maximum number of gas units that the transaction is allowed to consume before halting.
- **Sequence number:** An unsigned integer that must be equal to the sequence number from the sender's PACAccount.T resource. After this transaction executes, the sequence number is incremented by one. Since only one transaction can be committed for a given sequence number, transactions cannot be replayed.

Executing Transactions

Executing a transaction proceeds through a sequence of six steps inside the Virtual Machine. Execution is separate from the update of the ledger state. First, a transaction is executed as part of an attempt to reach an agreement on its sequencing. Since the execution is hermetic, this can be done without causing external side effects. Subsequently, if an agreement is reached, its output is written to the ledger history. Executing a transaction performs the following six steps:

(1) Check signature. The signature on the transaction must match the sender's public key and the transaction data. This step is a function only of the transaction itself—it does not require reading any data from the sender's account.

(2) Run prologue. The prologue authenticates the transaction sender, ensures that the sender has sufficient PAC coin to pay for the maximum number of gas units specified in the transaction, and checks that the transaction is not a replay of a previous transaction. All of these checks are implemented in ***Move*** via the prologue procedure of the PAC Account module. Gas metering is disabled during the execution of the prologue.

(3) Verify the transaction script and modules. Once the transaction prologue has completed successfully, the VM performs well-formedness checks on the transaction script and modules using the

Move bytecode verifier. Before actually running or publishing any ***Move*** code, the bytecode verifier checks crucial properties like type-safety, reference-safety (i.e., no dangling references), and *resource-safety* (i.e., resources are not duplicated, reused, or inadvertently destroyed).

(4) Publish modules. Each module in the program field of the transaction is published under the transaction sender's account. Duplicate module names are prohibited — for example, if the transaction attempts to publish a module named M to an account that already contains a module named M, the step will fail.

(5) Run transaction script. The VM binds the transaction arguments to the formal parameters of the transaction script and executes it. If this script execution completes successfully, the write operations performed by the script and the events emitted by the script are committed to the global state. If the script execution fails (due to having run out of gas or a runtime execution failure), no changes from the script are committed to the global state.

(6) Run epilogue. Finally, the VM runs the transaction epilogue to charge the user for the gas used and increment the sender's account sequence number. Like the prologue, the transaction epilogue is a procedure of the ***Move*** PAC Account module and runs with gas metering disabled. The epilogue is always run if execution advances beyond step (2), including when steps (3), (4), or (5) fail. The prologue and the epilogue work together to ensure that all transactions accepted in the ledger history are charged for gas. Transactions that do not proceed beyond step (2) are not appended to the ledger history. The fact that these transactions were considered for execution is never recorded. If a transaction advances past step (2), the prologue has ensured that the account has enough PAC coins to pay for the maximum number of gas units allowed for the transaction. Even if the transaction runs out of gas, the epilogue can charge it for this maximum amount.

The *Move* Programming Language

The key feature of ***Move*** is the ability to define custom *resource types*, which have semantics inspired by linear logic [9]. Resource types are used to encode programmable assets that behave like ordinary program values: resources can be stored in data structures, passed as arguments to procedures, and so on. However, the ***Move*** type system provides special safety guarantees for resources. A resource can never be copied, only *moved*. Besides, a resource type can only be created or destroyed by the module that declares the type. These guarantees are enforced statically by the ***Move*** VM. This allows us to represent PAC coins as a resource type in the ***Move*** language (in contrast to Ether and Bitcoin, which have a special status in their respective languages).

Authenticated Data Structures and Storage

After executing a transaction, a validator translates the changes to the logical data model into a new version of an authenticated data structure [3, 4, 5] used to represent the database. The short authenticator of this data structure is a binding commitment to a ledger history, which includes the newly executed transaction.

Like transaction execution, the generation of this data structure is deterministic. The consensus protocol uses this authenticator to agree on an ordering of transactions and their resulting execution (we discuss consensus in detail. As part of committing a block of transactions, validators collectively sign the short authenticator to the new version of the resulting database [2].

Using this collective signature, clients can trust that a database version represents the full, valid, and irreversible state of the database's ledger history. Clients can query any validator (or a third party replica of the database) to read a specific database value and verify the result using the authenticator and a short proof. Consequently, clients do not need to trust the party that executes the query for the correctness of the resulting read.

Ledger History

Most blockchains, starting with Bitcoin [10], maintain a linked list of each block of transactions agreed on by the consensus protocol with a block containing the hash of a single ancestor. This structure leads to inefficiencies for clients. For example, a client that trusts some block B and wants to verify information in an ancestor block B' needs to fetch and process all intermediate ancestors.

Accounts

At the logical level, an account is a collection of resources and modules stored under the account address. At the physical level, an account is treated as an ordered map of *access paths* to byte array values. An access path is a delimited string similar to a path in a file system.

Account Eviction and Recaching. We anticipate that as the system is used, eventually storage growth associated with accounts may become a problem. Just as gas encourages responsible use of computation resources, Pan African Coin expects that a similar rent-based mechanism may be needed for storage. The organization is assessing a wide range of approaches for a rent-based mechanism that best suits the ecosystem.

Byzantine Fault Tolerant Consensus

The consensus protocol allows a set of validators to create the logical appearance of a single database. The consensus protocol replicates submitted transactions among the validators, executes potential transactions against the current database, and then agrees on a binding commitment to the ordering of transactions and resulting execution. As a result, all validators can maintain an identical database for a given version number following the state machine replication paradigm [11].

Networking

The PAC protocol, like other decentralized systems, needs a networking substrate to enable communication between its members. Both the consensus and shared mempool protocols between validators require communication over the internet. The network layer is designed to be general-purpose and draws inspiration from the *libp2p* [12] project. It currently provides two primary interfaces: (1) Remote Procedure Calls (RPC) and (2) DirectSend, which implements fire-and-forget-style message delivery to a single receiver.

The networking system uses the same validator set management smart contract as the consensus system as a source of truth for the current validator set. This contract holds the network public key and consensus public key of each validator. A validator detects changes in the validator set by watching for changes in this smart contract. To join the inter-validator network, a validator must authenticate using a network public key in the most recent validator set defined by the contract. Bootstrapping a validator requires a list of seed peers, which first authenticate the joining validator as an eligible member of the inter-validator network and then share their state with the new peer.

Performance

The mission of the PAC protocol is to support global financial infrastructure. Performance is an integral part of meeting that need. A discussion of three components of blockchain performance is undertaken below:

1. **Throughput:** The number of transactions that the blockchain can process per second.
2. **Latency:** The time between a client submitting a transaction to the blockchain and another party seeing that the transaction was committed.
3. **Capacity:** The ability of the blockchain to store a large number of accounts.

Protocol design. Many elements of the PAC protocol are chosen partly based on performance. Pan African Coin selects elements of the protocol with parallelization and sharding in mind. The sparse Merkle tree approach to computing authenticators allows sharding the database across multiple machines (which increases capacity) or processing updates in parallel (which increases throughput). Initial transaction validation, which includes computationally expensive signature verification, can also be parallelized.

Validator selection. Like most services, the performance of the PAC chain depends on the performance of the underlying validators that operate it. There is a tradeoff between decentralization and performance. Requiring extremely well-resourced validators limits the number of entities that could perform that role. However, the presence of extremely under-resourced validators would limit the performance of the whole system [2].

Pan African Coin favors a balance of these approaches by targeting nodes that can run on commodity hardware that many entities can purchase. However, it is assumed that nodes run on server-class hardware and within well-connected data centers. The organization uses an approximate analysis to show that the system is likely able to meet the demand of 1,000 transactions per second [2].

- **Bandwidth**: assuming that each transaction requires 5 KB of traffic — including the cost of receiving the transaction via the mempool, rebroadcasting it, receiving blocks from the leader, and replicating to clients — then validators require a 40 Mbps internet connection to support 1,000 transactions per second. Access to such bandwidth is widely available.
- **CPU**: Signature verification is a significant computational cost associated with a payment transaction. Pac protocol is designed to allow parallel verification of transaction signatures. Modern signature schemes support over 1,000 verifications per second over a commodity CPU.
- **Disk**: Servers with 16 TB of SSD storage are available from major server vendors. Since the current state is the only piece of information the validator needs to use to process a transaction, we

estimate that if accounts are approximately 4 KB (inclusive of all forms of overhead), then this allows validators to store 4 billion accounts. The organization anticipates that developments in disk storage, scaling validators to multiple shards, and economic incentives will allow the system to remain accessible to commodity systems.

Historical data may grow beyond the amount that can be handled by an individual server. Validators are free to discard historical data not needed to process new transactions; however, this data may be of interest to clients who wish to query events from past transactions. Since the validators sign a binding commitment to this data, clients are free to use any system to access data without having to trust the system that delivers it. Pan African Coin expects this type of reading traffic to be easy to scale through parallelism.

Implementing PAC Ecosystem Policies with Move

The PAC chain is a unique system that balances the stability of traditional financial networks with the openness offered by systems governed by crypto-economic means. The PAC protocol is designed to support the PAC ecosystem in implementing novel economic and governance policies. The protocol specifies a flexible framework that is parametric in key system components such as the native currency, validator management, and transaction validation. The following section discusses how PAC Blockchain uses the ***Move*** programming language to customize these components.

PAC Coin

Many cryptocurrencies are not backed by real-world assets. As a result, investment and speculation have been primary use cases. Investors often acquire these currencies under the assumption that they will substantially appreciate and can later be sold at a higher price. Fluctuations in the beliefs about the long-term value of these currencies have caused corresponding fluctuations in price, which sometimes yield massive swings in value.

To drive widespread adoption, PAC is designed to be a currency where any user will know that the value of a PAC today will be close to its value tomorrow and in the future. The reserve is the key mechanism for achieving value preservation. Through the reserve, each coin is fully backed with a set of stable and liquid assets. With the presence of a competitive group of liquidity providers that interface with the reserve, users can have confidence that any coin they hold can be sold for fiat currency at a narrow spread above or below the value of the underlying assets. This gives the coin intrinsic value from the start and helps protect against the speculative swings that are experienced by existing cryptocurrencies [2].

The reserve assets are a collection of low-volatility assets, including cash and government securities from stable and reputable central banks. As the value of PAC is effectively linked to a basket of fiat currencies, from any specific currency, there will be fluctuations in the value of PAC. The makeup of the reserve is designed to mitigate the likelihood and severity of these fluctuations, particularly in the negative direction. To that end, the basket has been structured with capital preservation and liquidity in mind.

Validator Management and Governance

The consensus algorithm relies on the validator-set management ***Move*** module to maintain the current set of validators and manage the allocation of votes among the validators. This contract is responsible for maintaining a validator set in which at most f votes out of $3f + 1$ total votes are controlled by Byzantine validators.

Initially, the PAC Blockchain only grants votes to *Founding Members*, entities that: (1) meet a set of predefined Founding Member eligibility criteria [13] and (2) commit a certain amount into the project. These rules help to ensure the security requirements of having a safe and live validator set. Using the Founding Member eligibility criteria ensures that the Founding Members are organizations with established reputations, making it unlikely that they would act maliciously, and suggesting that they will apply diligence in defending their validator against outside attacks.

Move makes it possible to encode the rules for validator management and governance as a module. Similarly, ***Move*** allows the staking of coins by wrapping them in a resource that prevents access to the underlying asset. The staked resources can be used to compute the voting rights of the validators. The contract can configure the interval at which changes take effect, to reduce the churn of validator set.

Validator Security and Incentives

In the initial setting, using Founding Members as validators, Pan African Coin believes that the institutional reputation and financial incentives of each validator are sufficient to ensure that Byzantine validators control no more than f votes [2]. In the future, however, an open system where representation is based on coin ownership will require a substantially different market design. In appreciating governance and equilibrium structure of block chain, the organization understands the pivotal role of stake holding and consumer confidence in wallets and other delegates. In the process, new market trade-offs between the PAC approach (proof of stake) and more established approaches such as proof of work (mining) are designed.

Move allows flexibility in the definition of the relevant incentive schemes such as gas pricing or staking. For example, *stake slashing*, a commonly discussed mechanism, could be implemented in ***Move*** by locking stake for a while and automatically punishing validators if they violate the rules of the PACBFT algorithm in a way that affects safety.

REFERENCES

[1] C. Catalini and J. S. Gans (2016). “Some simple economics of the blockchain,” *WP No. 22952, National Bureau of Economic Research.*

[2] The Libra Association (2020). The Libra Blockchain

[3] P. T. Devanbu *et al.* (*2000*) “Authentic third-party data publication,” in *Data and Application Security, Development and Directions, IFIP TC11/ WG11.3 Fourteenth Annual Working Conference on Database Security, Schoorl, The Netherlands, August 21-23,* pp. 101–112.

[4] M. Naor and K. Nissim, (2000). “Certificate revocation and certificate update,” *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, pp. 561–570,

[5] R. Tamassia, (*2003)* “Authenticated data structures,” in *Algorithms - ESA 2003, 11th Annual European Symposium, Budapest, Hungary,* pp. 2–5.

[6] G. Wood, (2016). “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” http://gavwood. com/paper.pdf,.

[7] A. Pfitzmann and M. Köhntopp, (2001) “Anonymity, unobservability, and pseudonymity—a proposal for terminology,” in *Designing privacy enhancing technologies*, , pp. 1–9.

[8] B. C. Pierce, (2002). “Types and programming languages.” MIT Press, , ch. 19.

[9] J. Girard, (1998). “Light linear logic,” *Inf. Comput.*, vol. 143, no. 2, pp. 175–204,

[10] S. Nakamoto, (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf.

[11] F. B. Schneider, “Implementing fault-tolerant services using the state machine approach: A tutorial,” *ACM Computing Surveys (CSUR)*, pp. 299–319, 1990.

[12] “The libp2pproject,” https://libp2p.io/.

[13] The PAC Association, “Becoming a Founding Member,” 2019.

[14] C. Catalini, R. Jagadeesan, and S. D. Kominers, “Market design for a blockchain-based financial system,” *SSRN Working Paper No. 3396834*, 2019.