iZac

Own your identity

Table of Contents

Disclaimer

PLEASE READ THE DISCLAIMER SECTION (ANNEX A) CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S).

Introduction

This whitepaper paper is the result of collaboration between skilled individuals who care deeply about individual privacy, integrity and non-repudiation of transactions carried out over the public internet containing your personal information. iZAC Coin Pty Ltd is continually seeking input from experts in the fields of personal privacy, allied health professionals, blockchain specialists, academics and business advisors.

The iZAC Token uses blockchain and advanced encryption technology to enable the concept of Zero-knowledge proofs, allowing the owner of the data to control its distribution when it matters most.

An iZAC Token enables the user to retain control over their personal information no matter whether it is medical, financial or other personal information or transaction records, with a facility to “fail safe open” in a controlled fashion to give access in case of a true emergency, or “fail safe closed” for other transaction records ensuring your privacy.
This process records transactions with this data in an auditable, transparent and secure way on iZAC Tokens’ distributed ledger.

The iZAC Token will form an eco-system for others to build or enhance their current applications thus improving their transaction security and user experience.

This iZAC Token Whitepaper 2.0 will outline the vision held by the team at iZAC Coin for the implementation of a method for the guaranteed “zero-knowledge proof” for transactions giving confidence to all transacting parties.

What is an iZAC Token

iZAC is a new concept in crypto identity management. We are embedding your personal biometrics into your token and storing it with in the iZAC Token blockchain. This revolutionary approach allows us to make very specific and personalised keys, to be used within the iZAC ecosystem.

What we are building is a crypto identification management system based on the Etherum blockchain and embedded with your DNA, fingerprint, facial detail and eye scan. This creates an unbreakable bond between the token and the registered owner, you can think of them as digital keys and locks. Both the key and the lock are combined into the same device. When you attempt to open the lock it will compare your biometrics with that recorded within token to confirm your identity.

When the iZAC Token is combined into the Ethereum blockchain with your DNA the token can be personalised to either your whole family or you as an individual.

The key to making iZAC Tokens a success lies in our ability to encourage the iZAC community to build an ecosystem of interested parties and companies to develop the "Locks". These physical or digital locks will then be encoded with the iZAC Token.

Transactional integrity and the iZAC Token

Transactions today

In our current world of transactions, we rely more on the honesty and trustworthiness of the other person whether they are an individual or a business and a not insufficient amount of luck. The same situation applies if you are transferring money between bank accounts, or your medical records are being transferred between medical professionals or hospitals.
Both of these instances and many others are vulnerable to external interference by unauthorised persons bring into doubt the authenticity of the transaction.

Transactions of tomorrow

Data security is paramount due to the increased sensitivity of data which can be deemed as personally identifying. For instance; financial legal or health records. Over the past 10 years there has been a continual increase in personal data theft due to inadequate care and attention by those who have care of your personal information.

"Your medical information is worth 10 times more than your credit card number on the black market."

Technology News, Reuters, September 24th 2014

Many have tried to overcome this issue, including governments around the world and is a source of frustration for people wishing to take advantage of the value of a 21st century economy of connected value. The most significant components of this challenge focuses on data security using the pillars of user authorisation and transaction non-repudiation.

The grail quest for true data security has always rested with the ability to with doubt identify information relating to a person without giving up the content of the information, and gaining that persons' permission, no matter of their current location.

At iZAC Coin we believe there is an answer to this problem, it uses a personal identity cryptographic token with that individuals' biometrics entered as part of the encryption string created with the token. These tokens can be single use or be a permeant fixture and are premised on the core value for securing anything, being the *Need to Know basis*.

As the holder of an iZAC Token you have the final word on who needs to know.

Use cases

By using an iZAC Token, access to secured information can be restricted to only the individual, family member(s) or appropriate others. We have described just a few interesting use cases we have considered:

Medical records

Electronic health records or e-records are used in most advanced Weston economies, these implementations use a robust but linear access control method. Currently your medical records rely upon a promise not to misuse this information and the best effort actions of well intentioned but fallible people. This has led to numerous data breaches growing in frequency and with a large personal impact. The challenge is how to solve this situation and give patients and their families peace of mind.

What this means is; as you are sitting the specialists' office and you can provide them the access they need to the appropriate areas of your health records but keep private those of which they have no need to know. In the case of an emergency the ability of the token to allow emergency medical practitioners access, this is known as Failing Open and thus providing emergency access as required but backed with accountability but the iZAC blockchain.

Financial affairs management

Access to your banking or trading accounts have been a matter of keeping account details and passwords available, the more available they are the more vulnerable they are to being misused by nefarious actors.

In the 1920s' Swiss banks set up numbered accounts so persecuted persons across Europe could secure their personal finances. These had one fatal floor, if the account holder was no longer able to provide the number no one else could access the account. Using modern technology these and other such accounts can be secured in a way never before by using an iZAC Token with the option of adding family members as required.

Legal documents such as Last Will, and Testaments can be secured in a similar way where your solicitor is the secondary person nominated on the token.

Autonomous vehicles; ride sharing application

You book your car via the registered application, it arrives to your location provided by the positioning system in the app. You open the door and get in, the car recognises you by the biometrics sample it took from the handle when you opened it.

As you get in the seats have adjusted to your height, your fav radio station is selected and the car has started off to your destination. However, there is no steering wheel or peddles, this is the latest high-tech driverless car. With iZAC Token the car it setup with your personal settings and you can relax, watch a movie, chat with friends or do your office work as the car takes care of all the driving.

As you are driving into the city the driverless cars communicate with each other, they can advise you of potential delays like traffic jams, the weather and advise the use of the fast lane. In the future, the fast is a user pay system and restricts the number of road users on them to ensure efficiently. So if your running late for a meeting or to the Russian Ballet you might opt in to paying the increased fee. Or if your enjoying the ride you choose the slow lane option, where the highway rewards you with additional iZAC Tokens.
In these days our cars don't charge you money, but use the trading system built into the crypto token ecosystems. You accumulate credits with the car company to be charged later or used to upgrade your journey to the fast lane.

Securing the iZAC ecosystem

As the controlling entity the directors of iZAC Coin have taken the security of the ecosystem very seriously. Each director has at least 15 years of working within government and banking environments. We bring to the table an understanding of how to create a secure environment both for the individuals and companies to operate with a high level of confidence.

iZAC Coin and its product the iZAC token, have embraced the newly developed Cryptocurrency Security Standard (CCSS)1. As this is a new and still developing standard the directors have decided to incorporate additional measures to ensure as complete a security coverage as possible by using existing tried and tested standards. These include:

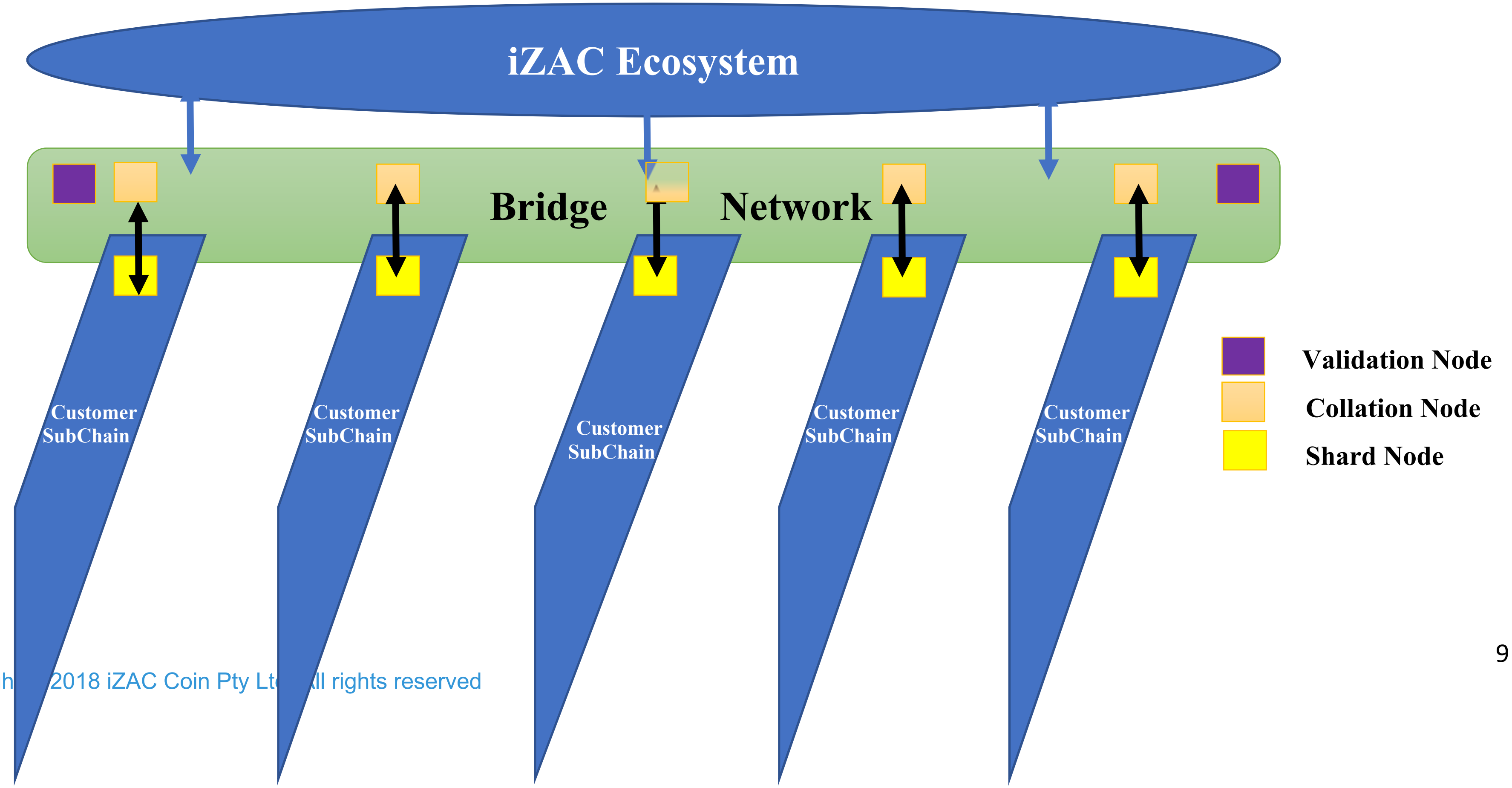
- Open Web Application Security Project (OWASP)[2] ; for secure coding and testing practices;
- Sherwood Applied Business Security Architecture (SABSA)[3] ; for identifying and mitigating business related risks and overall secure enterprise architecture.
- National Institute of Standards and Technology (NIST); for risk management[4], cybersecurity controls[5]; mitigations and guidance.
- Information Security Standard (ISO/IEC)27001[6]; system certification and accreditation
- Information Security Standard (ISO/IEC)31000[7]; risk management
- Australian Signals Directorates' (ASD) publication; Information Security Manual.

[1] https://cryptoconsortium.org/standards/CCSS
[2] https://www.owasp.org/index.php/Main_Page
[3] https://sabsa.org
[4] https://csrc.nist.gov/Projects/Risk-Management/Security-Assessment
[5] https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview/Security-Controls
[6] http://www.iso27001security.com/html/27001.html
[7] https://www.iso.org/iso-31000-risk-management.html

By using the appropriate tools provided by these well known and trusted frameworks, iZAC Coin seeks to show a higher level of probity in the efforts to make the iZAC ecosystem a trusted platform on which to conduct business. Similar controls and requirements will be required of any business partners and suppliers to the ecosystem to further reduce the element of risk from third party sources.

Technical Bit

iZAC Shards



The Mattiuzzo Model

The iZAC Token are built on a foundation of main chain and subchains. The iZAC Coin blockchain, beginning with the iZAC Token Genesis Block provides functions for transaction management, subchain management, smart contract management, security control and customer account controls.

ZK-SNARKs and Zero-knowledge proofs

Zk-SNARKs, a zero-knowledge succinct non-interactive argument of knowledge. Sounds impressive but the fundamental idea is zero-knowledge.

Zero-knowledge proofs aren't new, they were in invented by researchers from MIT back in the 1980s. The basic idea is they allow someone to prove a claim to someone else without conveying any information. We hope to make it workable by fusing Zk-SNARKs with the blockchain and linking this to an individual via their biometrics.

This will change the digital world forever! You will no longer fear the loss of your identity and amongst other things, making the aftermath of identity theft a much less painful as proof and trust will be much easier to establish than it is today.

Transaction management

A total of 400 million iZAC Tokens Have been created in the genesis block creation event. The tokens are assigned to holders in accordance with the established program and the smart contracts. Through the iZAC ecosystem accounts will be created via nodes and recorded on the iZAC Token. All transactions are recorded to a block, linked to the previous block, forming the blockchain of the iZAC Token. The iZAC blockchain is the public ledger of the iZAC Token with all transactions stored in nodes dispersed throughout the iZAC networked ecosystem to ensure safety and reliability of transactional data.

Subchain management

The major function of the Mattiuzzo model is the management of subchains. As subchains can only be created by an iZAC Token account holder, it is necessary to hold iZAC Tokens. The creator of a subchain can customise the details and functions of these subchains and specific information within these subchain tokens. This custom information forms the data structure describing the subchain, which is recorded in the block in similar fashion to the of the current period by the accounting nodes in a way similar to the parent iZAC Token forming a transaction record. This allows the subchain to be used as a separate blockchain, recording the transactions of the subchain tokens.

All transactions are recorded in the blockchain of the iZAC Token allowing the subchains to run independently of each other. Nodes running on the iZAC Token only need to communicate data to conduct consensus and validation of iZAC Token transaction blocks. This enables a daily update to occur and gives maximum flexibility and scalability for each subchain. Each subchain will be responsible for their own data validation, comparing the biometrics of their own subscribers.
Note: the size of the iZAC genesis chain will not appreciably increase as only the subchain description information will stored.

Smart contract

The iZAC Token uses smart contract technology developed by Ethereum. iZAC Tokens will be applied in the final token creation to include details such as subchain creation contracts, equity distribution and security features. The iZAC Token blockchain technology defines two types of account concepts:

1. The general account storing the tokens;
2. The smart contract account storing smart contract procedures.

When a transaction is sent to the smartc ontract account address, the corresponding smart contract will be triggered and implemented. The output performed by the customised operations, make transaction requests, modify the account status and execute code as needed.

Subchain functional features

During its creation, a subchain can be customised to support all or a subset of the functional features of the parent iZAC blockchain, allowing for greater flexibility and customisation. The supported customised features include subchain token transactions, subchain token and iZAC blockchain token transactions, cross subchain token transactions, smart contracts, aliases, account control, instant messaging and data storage.

Block Structure

The trading ledgers of the iZAC Token are stored in iZAC Token blocks which are series connected forming the iZAC Token blockchain and subchains. These blockchains are stored in many nodes on the iZAC ecosystem network, making the transaction records open, safe, decentralised and traceable.

Each block is made of up to 255 transaction records. Each transaction contains identification information contained within the header. The information contained in each block as follows:

- Block depth and timestamp
- Block identity
- Block account ID and public Key
- The identity of the previous block and the hash value
- The total number of tokens for the transactions contained in the block and byte fee
- Transaction information contained in the block
- Block payload length and payload hash value
- The general signature of the block
- Accumulated coinage difficulty of the block

PoST Consensus Mechanism

The iZAC Token blockchain conducts block consensus and validation based on the Proof of Stake & Trust (PoST) consensus mechanism. PoST is an innovative updated version based on the Proof of Stake (PoS) consensus mechanism.

The traditional PoS is a distributed consensus algorithm, which is an upgraded version of the Bitcoin Proof of Work (PoW) consensus algorithm. In the PoW consensus algorithm, the nodes involved in the consensus need to continue trying to solve the problem of cryptography, to confirm the transaction, then write into the block and get tokens as a reward. In most cases, this reward comes from the unallocated tokens, hence the process is termed mining. As mining becomes more and more difficult due to the “mineral resources” reducing, a lot of computing resources are wasted. In the blockchain network based on the PoS consensus algorithm, in most cases, all the tokens are issued at the very beginning, the block is then successfully created and written into the accounting nodes of the blockchain; the accounting reward is buy the byte fee, paid by the transaction initiation node, so the consensus mechanism is vividly called coinage. The more tokens held by each of the modes involved in the consensus process and the longer the time these tokens are held the greater the opportunity to successfully complete the block creation and writing process there is. This mechanism greatly reduces the operational difficulty of accounting, saves valuable compute resources and at the same time provides a mechanism of selecting “good” accounting nodes to strengthen the security of the blockchain.

iZAC Coin will use an innovative node reputation evaluation system which permits a node reputation mechanism to adjust the difficulty based on PoS and highlight the importance of reputation designed in the PoST consensus mechanism. This consensus mechanism brings two positive effects:

- Keeping a good credit record to cultivate a healthy business ecology;
- Provides an upgraded selection mechanism to choose more honest “high quality” nodes improving the security of the blockchain.

Additional consensus mechanisms

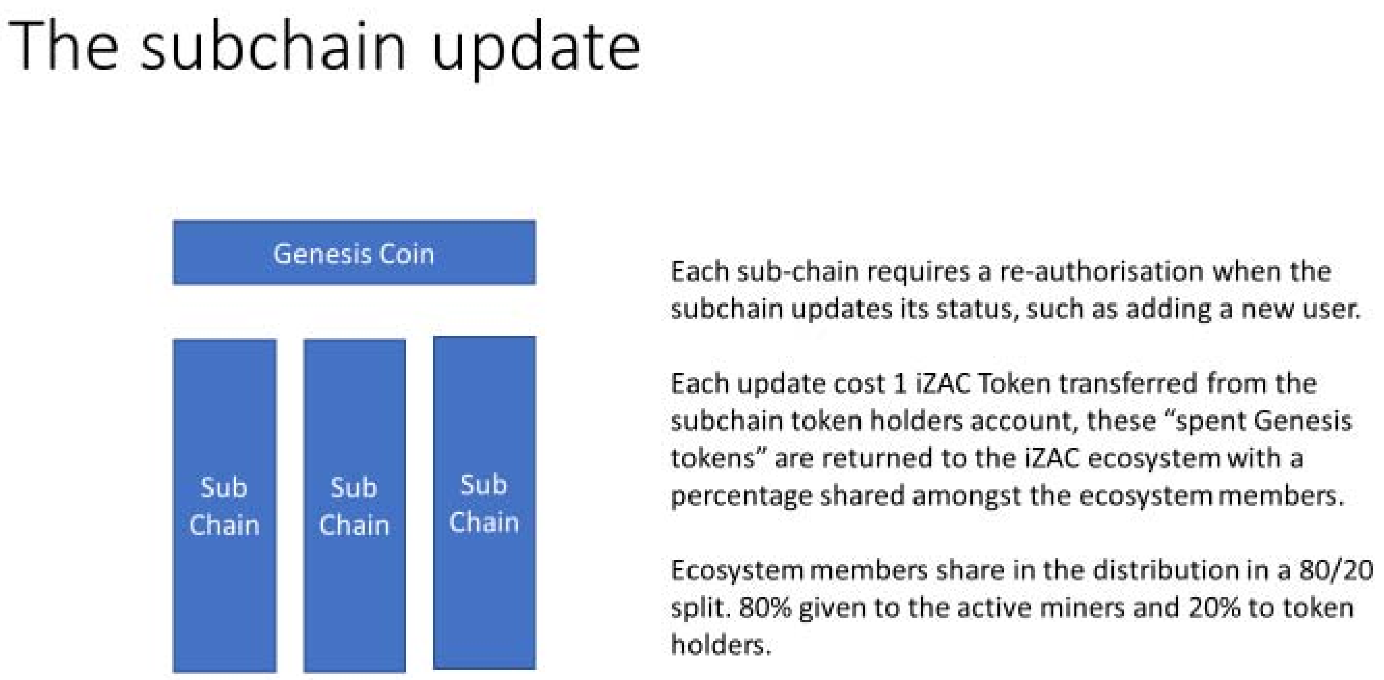
The flexible structure of the iZAC Token blockchain determines that the subchains can choose PoS, PoST or other consensus mechanisms to achieve the optimal application effect in different application scenarios.
By issuing different subchains, iZAC Token connects different types of nodes to apply to various scenarios. Due to the diversity of each subchain there is an ever-increasing need for many nodes online at the same time to meet different application requirements.

iZAC Token Revenue

As mentioned earlier, in the iZAC ecosystem, the core parent chain is referred to as the iZAC Token which is the token used for circulation and or payment. The total number of iZAC Tokens is 400M iZAC (400 Million Tokens), released in stages, all tokens are created in the initial genesis event and stored in the genesis wallet.
Distribution via smart contracts include:

Stage 1 includes 100M tokens sold through the ICO process.
Stage 2 including advancements issued to primary holders only (token holders)
Stage 3 additional advancements released only to subchain subscribers

Additional tokens can be created via a subchain from the Genesis Block.



The subchain update

Genesis Coin

Sub Chain

Sub Chain

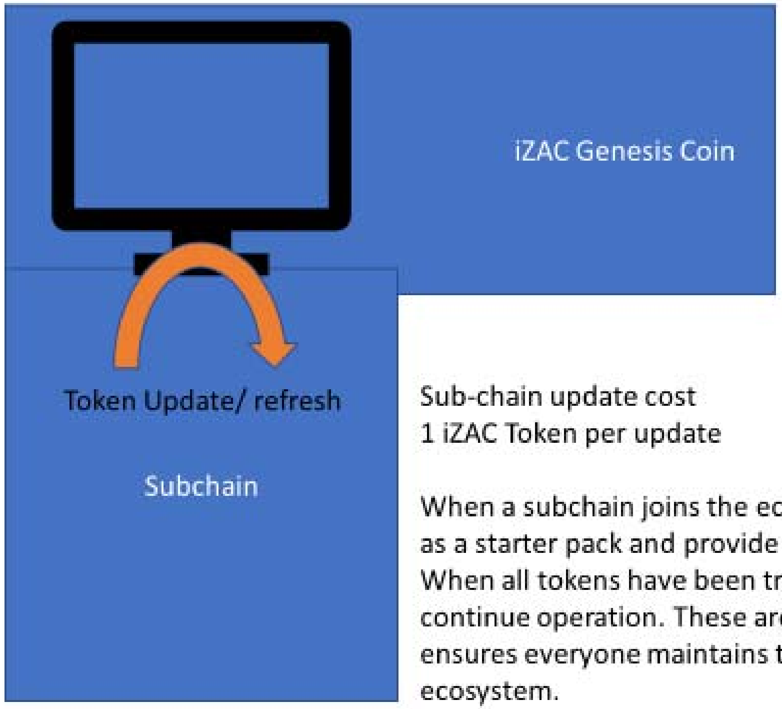
Sub Chain

Each sub-chain requires a re-authorisation when the subchain updates its status, such as adding a new user.

Each update cost 1 iZAC Token transferred from the subchain token holders account, these “spent Genesis tokens” are returned to the iZAC ecosystem with a percentage shared amongst the ecosystem members.

Ecosystem members share in the distribution in a 80/20 split. 80% given to the active miners and 20% to token holders.

Miners



Miners must download the Mining app and hold a minimum number of iZAC Genesis Tokens to participate in mining activities.

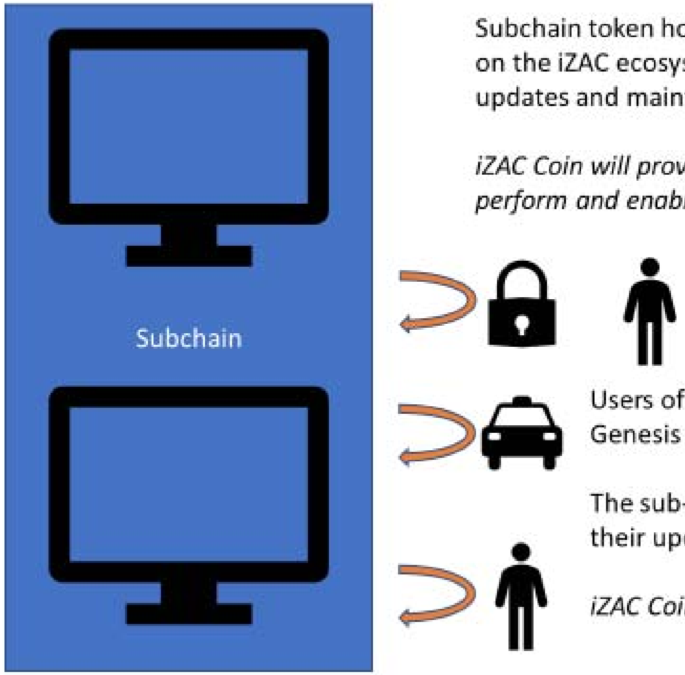
Minimum spec for mining servers:

- Must be a holder of at least 100,000 iZAC Tokens
- Graphics Card NVIDIA GeForce GTX
- 8G RAM or more
- Install the mining software only from the iZAC website
- Follow the miners configuration guide

Sub-chain update cost
1 iZAC Token per update

When a subchain joins the ecosystem iZAC Coin will transfer 1000 iZAC Tokens as a starter pack and provide a locked in 25% discount on future purchases. When all tokens have been transferred additional token will be required to continue operation. These are offered at a 25% discount to market rate. This ensures everyone maintains their subchain operations and the security of the ecosystem.

Subchains



Subchain token holders will require an annual fee to maintain their blockchain on the iZAC ecosystem. This enables the subchain to be able to perform daily updates and maintain status with the iZAC Token miners

iZAC Coin will provide assistance to setup your initial mining partner and perform and enable the distribution to all miners within the ecosystem.

Users of the sub-chain do not require any interaction with the iZAC Genesis tokens, after the user initial registration update.

The sub-chain will require Biometric enabled locks to be setup and their update remains the responsibility of the subchain owners.

iZAC Coin can provide consulting servicers to assist if required.

ANNEX A

The information set out in this document may not be exhaustive and does not imply any elements of a contractual relationship. While we make every effort to ensure that any material in this whitepaper is accurate and up to date, such as products, services, technical architecture, token distribution, company timelines - such material could be subject to change without notice and in no way constitutes a binding agreement or the provision of professional advice.

iZAC Coin does not guarantee, nor accepts any legal liability whatsoever arising from or connected to, the accuracy, re-liability, currency, or completeness of any material contained in this whitepaper. Potential iZAC Token holders should seek independent professional advice prior to relying on, or entering into any commitment or transaction based on, material published in this whitepaper, which material is purely published for the purpose of reference alone. iZAC Tokens will not be intended to constitute securities in any jurisdiction.

This whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. iZAC Coin does not provide any opinion on any advice to purchase, sell, or otherwise transact with iZAC Tokens and the fact of presentation of this whitepaper shall not form the basis of, or be relied upon in connection with, any contract or investment decision. No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of iZAC Tokens, and no cryptocurrency or other form of payment is to be accepted on the basis of this whitepaper.