



The iZAC

AN ENCRYPTED SECURE TOKEN

White Paper

Table of Contents

Introduction.....	3
Blockchain.....	4
What is Blockchain.....	4
Growth of distributed ledger technology	4
Architecture and Development.....	6
Design.....	6
.....	7
.....	7
Benefits	7
Technological motivation.....	7
iZAC Key Features	8
Consultancy.....	8
Active development	8
iZAC Affiliate Network.....	8
Blockchain explorer.....	9
iZAC wallet	9
Eco-life	9
Scalability	10
Initial distribution.....	10
Affiliate network distribution	12
.....	12
Stack unlock process	12
Stacking process.....	13
Transaction Cost	14

Introduction

A crypto-token (similar to a cryptocurrency) is a medium of exchange, making use of cryptography to secure transactions and to control the creation and distribution of additional units. Development of crypto-tokens has been actively growing alongside cryptocurrencies throughout the past decade, in today's economic climate they continue to gain acceptance through a broad range of transactional possibilities for both individuals and organisations.

Our aim is to become a stable and dependable supplier of crypto-tokens allowing the holder of an iZAC¹ token to be confident their secured assets cannot be used in any way other than for the purpose they have intended. This will ensure the distribution and value of each token is not controlled solely by the crypto miners, but by the iZAC community. Our purpose is to empower the iZAC crypto-token through an Affiliate Marketing Channel, a strategy gaining more currency with the cryptocurrency and crypto-token communities. The iZAC Community aims to inspire, be inspired, to educate, and to support its members in these endeavours.

iZAC is a crypto-token that has the nomination iZAC and has eight digits after the decimal point (for example 0.12345678 iZAC). The main scope is to create a Crypto-On- Stop-Solution for private, corporate and investment needs.

We provide a strong use case for storing and processing digital transactions in a secure and transparent way. Our system is based on the Ethereum blockchain application platform and follows the cryptocurrency standards offered by Ethereum at the deployment moment Proof-of-Work (PoW).

The Ethereum blockchain's smart contracts are used to validate and protect certain rules regarding the distribution, freezing and ownership of issued tokens. These contracts are enforced by the Ethereum network and cannot be invalidated or changed by the company or users.

Problems we all face today

Facebook, Google, Banks and your Governments are all collecting data about you. Where you shop, what you search for online, where you travel and how much you earn. All of this data is being used by direct marketing advertising. They spam you 24/7 with Email, Pop-up messages and unwanted texts. Who hasn't received the phone calls from call-centres asking for donations. Even when you share your details with trustworthy business they are constantly being hacked and your personal details shared with the world or held against you for ransom.

There is currently no way you can own your identity to control whom has access to your personal information, your medical records, your transaction history for important contractual documentation, nor a certainty that future needs will permit you to control access to your identity for proof in dealings that it was you whom conducted the transaction.

A way needs to be found that identifies you as 'you' and cannot be refuted. The way to do this must be a commonly accepted method and easily protected from theft, misuse, and proxy. Invalid transactions and contracts should be easily repudiated. At the present time, data held about you only relies upon a promise not to misuse your data and a promise that best efforts of security will prevent a breach against the safety of your information stored at providers. Numerous breaches in past years confirm that nobody can protect your information other than yourself.

The challenge is how this can be done, and this is the mission of the intelligent Zero-knowledge-proof Crypto (iZAC) technology to deliver this capability.

1 iINTELLIGENT Zero-knowledge-proof Access Crypto-token

Blockchain

What is Blockchain

A blockchain is a distributed database, which makes the creation of a digital ledger of transactions and sharing of the ledger among a distributed network of computers possible. It uses cryptography to allow each participant on the network to manipulate the ledger in a secure way without the need for a central authority. It maintains a continuously growing list of records (blocks), each containing a time stamp and a link to the previous or parent record.

iZAC is built and available on a blockchain and is accessible as a DApp (Distributed Application). The reason for using blockchain technology in the development of iZAC is to provide a decentralised infrastructure that is stable and secure for all parties involved.

The advantages for solutions built on blockchain technology are:

1. Trust less exchange

Two parties can make an exchange without the oversight or intermediation of a third party, strongly reducing, or even eliminating, counterparty risk.

2. Empowered users

Customers are in control of all their information and transactions.

3. Durability, reliability, and longevity

Thanks to the decentralised nature of the networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks.

4. Transparency and immutability

Changes to public blockchains are viewable by all parties, which creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.

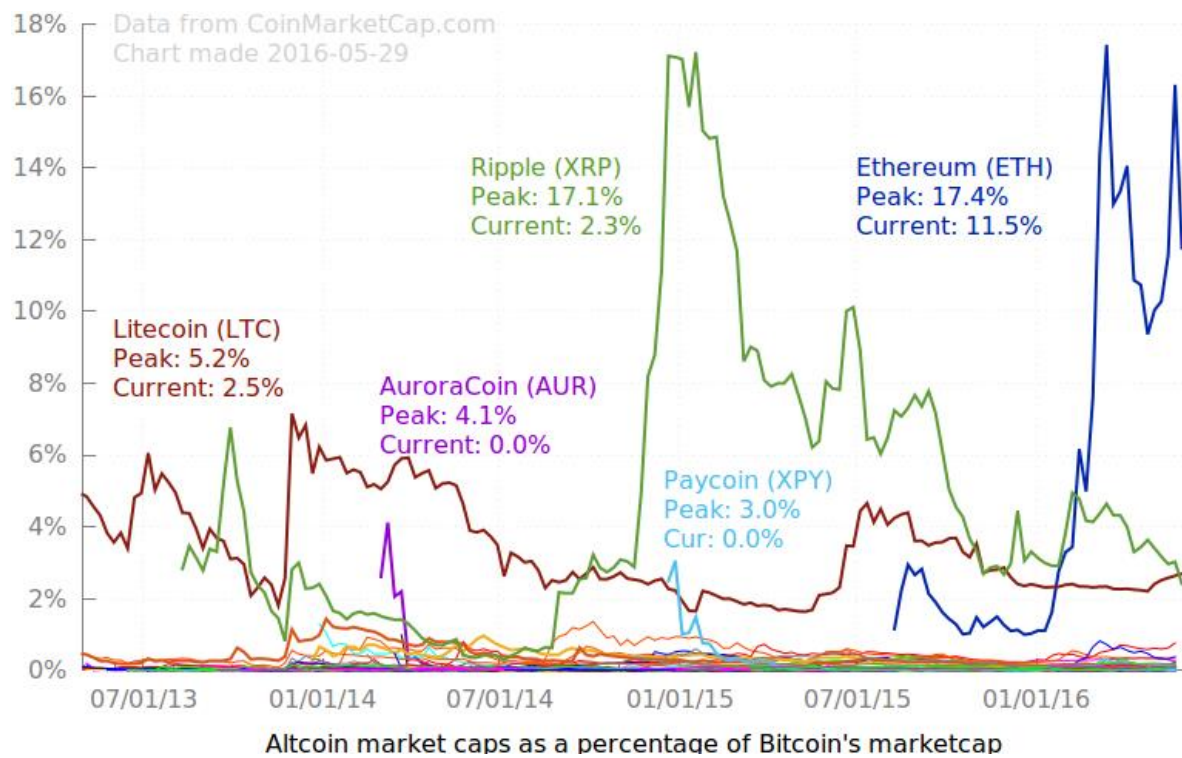
Growth of distributed ledger technology

A distributed ledger represents a consensus of replicated, shared and synchronised digital data, geographically spread across multiple sites, countries and/or institutions. The efficiency of distributed ledger derives from the immediate reflection of changes made by any participant towards all copies of the ledger. The current full potential of the distributed ledger technology is achieved when other applications are layered on top of the distributed ledger (e.g. smart contracts).

Smart contracts represent contracts whose terms are recorded in a computer language; they can be automatically processed by computer systems. It is economically viable to form these contracts, as there are low contracting, enforcement and compliance costs.

Today, the distributed ledger technology is still in its infancy and blockchain represents one of the very first implementations to make use of it. The predictions regarding its development are positive. An ever growing number of experts are predicting that blockchain technology will revolutionise the way individuals will use these emerging technologies. The world's banks (large and small), together with and government institutions and, increasingly, financial regulatory bodies, are working to implement blockchain applications to provide a more secure and trustworthy service to their customers.

As the blockchain technology becomes increasingly mainstream, an increasing number of cryptocurrencies appear each year, all of them competing for the same market. iZAC Coin Limited (company trading name) offering the iZAC isn't going to be just another digital currency; the creators have their own philosophy to create a meaningful and unique purpose for its initial core customers.



Architecture and Development

Design

The iZAC encrypted token is built on Ethereum, a blockchain-based distributed computing platform that makes use of smart contracts².

By using Ethereum as the abstract foundational layer, we can implement all the features and rules on the iZAC directly into smart contracts, which are then deployed and processed by the entire network. By using the entire Ethereum infrastructure with the purpose of validating transactions and adding new blocks to the blockchain, we minimise any possible attack on the coin.

On top of Ethereum, we build the services using Geth³ (Go-Ethereum). Geth is a multipurpose command line tool that runs a full Ethereum node implemented in Go. By installing Geth, one can take part in the Ethereum live network and mine real ether, transfer funds, create contracts and send transactions, explore block history etc. The Geth is to run on a proprietary Linux server with no RPC/ HTTP open ports. The communication, which involves the Geth, is managed through the Node.js intermediary application and the Ethereum network.

The applications connecting to the Ethereum blockchain are built on Truffle⁴. Truffle is a development environment, testing framework and asset pipeline for Ethereum. We use Ethereum Truffle for:

- built-in smart contract compilation, linking, deployment and binary management,
- configurable build pipeline with support for custom build processes, and
- network management for deploying to many public and private networks.

The communication between the Ethereum blockchain and the web-applications is managed using the Web3.js framework. Web3.js⁵ is the Ethereum compatible JavaScript API, which implements the Generic JSON RPC specification.

The communication layer between GETH and the front-end application is implemented using Node.js, which uses an event-driven, non-blocking I/O model that allows it to manage communications between the users and the iZAC token. The Node.js application is communicating with GETH through IPCs (Internal Procedure Calls). The Node.js application is sharing the same server with Geth.

Communication with the Ethereum node is done through the JSON RPC API. JSON-RPC which is a stateless, light-weight Remote Procedure Call (RPC) protocol. Primarily, this specification defines several data structures and the rules around their processing. It is transport agnostic in that the concepts can be used within the same process, over sockets and over HTTP.

The front-end application is implemented using the AngularJS framework⁶. This application is located on a different server and communicates with the Intermediate Layer using Web Sockets and a REST API.

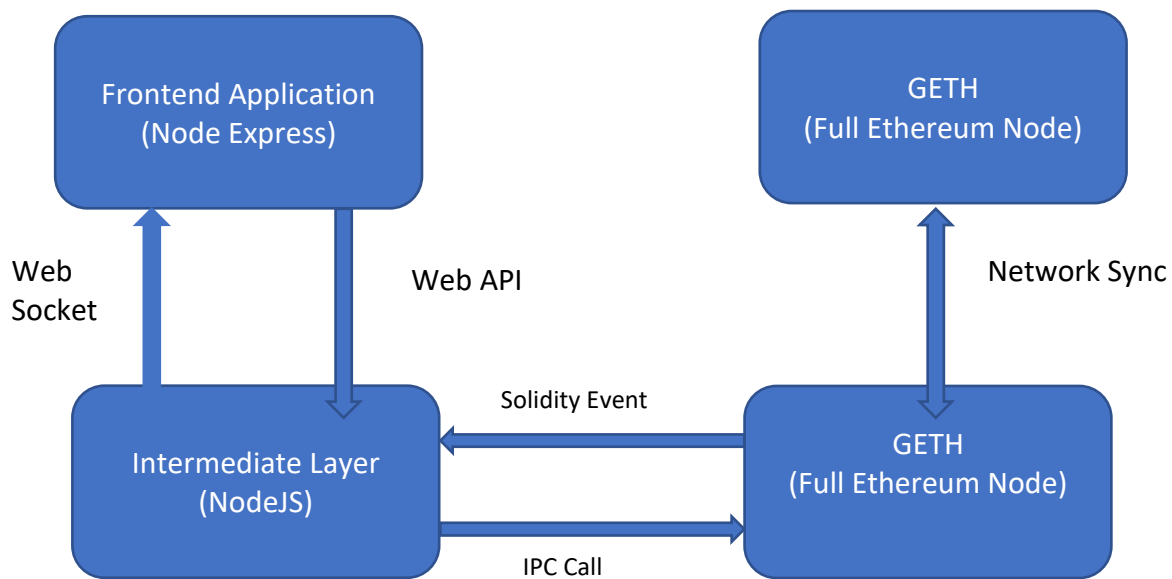
² A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts were first proposed by Nick Szabo in 1996.

³ <https://github.com/ethereum/go-ethereum>

⁴ <https://github.com/ConsenSys/truffle>

⁵ <https://github.com/ethereum/web3.js/>

⁶ <https://github.com/angular/angular-seed/wiki>



Benefits

The main benefit to investing in the iZAC is the ability to ensure the stored value held within the iZAC is forever linked to you through blockchain and encrypted bio-dynamics. This integral part of the design, gives iZAC investors the ultimate say in the distribution of wealth or any other commodities of value secured using an iZAC token. This security feature, coupled with the intrinsic advantages of a crypto-token, such as not being linked to any banking services, enables the iZAC holder/investor to use financial services for their daily transactional processes. iZAC also has an advantage of being able to offer the possibility of online and offline transactions, and an option to exchange iZACs into FIAT⁷ money, in a simplified manner.

The blockchain technology enables the user to transfer funds in a fast and easy manner, which excludes third-party actors, unlike the traditional banking systems.

Technological motivation

Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality. It provides a decentralised virtual machine, the Ethereum Virtual Machine (EVM), which can execute peer-to-peer contracts using a cryptocurrency called Ether.

We see three main approaches for building advanced applications on top of our crypto-token:

- building a new blockchain,
- using scripting on top of Bitcoin, and
- building a meta-protocol on top of Bitcoin.

Building a new blockchain allows unlimited freedom in building a feature set. Still, there is a considerable security risk with new blockchains. For example, if there aren't enough miners in the very beginning, the network is vulnerable to a 50%+1 attack⁸.

⁷ FIAT - Any money declared by a legitimate government to be legal tender.

⁸ 50%+1 attack – refers to an attack on a blockchain –by a group of miners controlling more than 50% of the network's mining hashrate, or computing power. This type of attack is currently hypothetical in nature.

iZAC Key Features

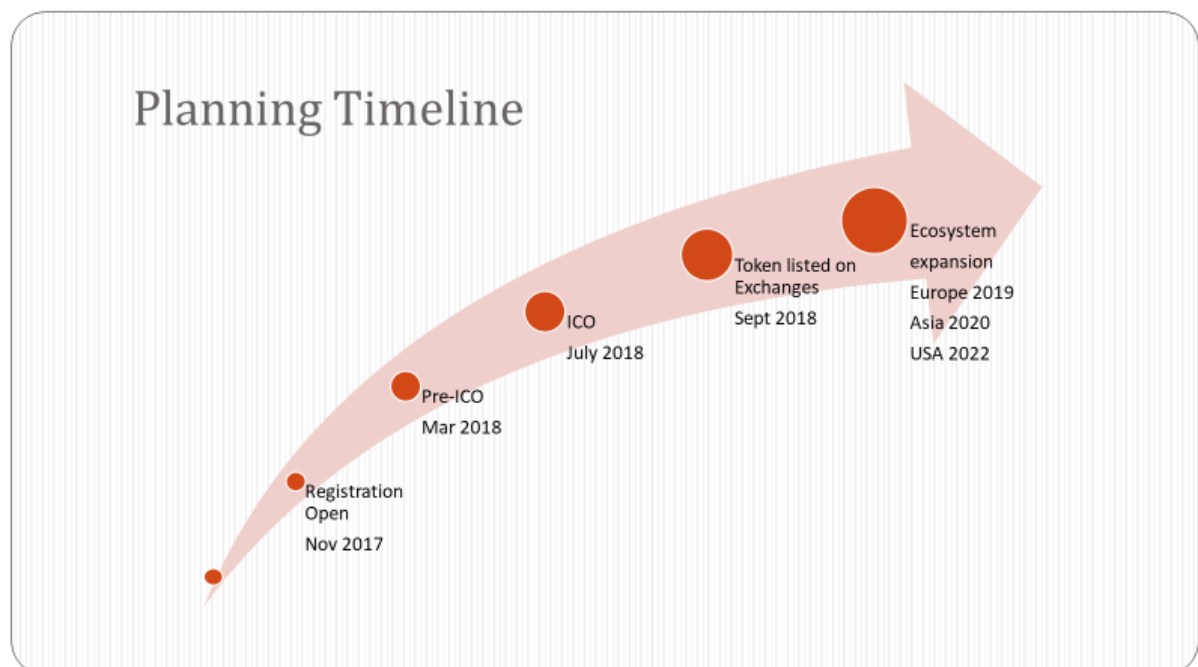
Consultancy

The team behind the iZAC is an innovative start-up company with a technology company based in Australia. Most of the application development is implemented in Europe with experienced consultants and experts located worldwide.

Our purpose is to provide a comprehensive eco-system built around the iZAC token featuring multi-platform wallets, integration with exchanges. This philosophy will be carried in to future applications as the technology matures.

Active development

The COSS (Crypto-One-Stop-Solution) encompasses all features available in a digital economical system based on the cryptocurrency. The system unifies all transactional aspects that are usually managed using FIAT money and offers solutions for exchanges, payrolls, wallets, acquisitions and transactions.



iZAC Affiliate Network

The majority of the iZAC tokens will be distributed via affiliate systems, where members will be awarded with tokens for bringing merchants on board to accept the iZAC for payments.

All awarded tokens will follow a programmed release contract in which each payment will be processed to the member's wallet over a period of 25 weeks, in weekly instalments of 4% of the total iZACs they are entitled to receive.

The total supply of iZACs will be divided into equally sized stacks, and a new stack can only become available for distribution when a minimum of 80% of the previous stack has been scheduled for transfer to its affiliate members. This is done to prevent any pump and dump strategy and/or potential flooding of the market.

Additionally, the distribution plan involves a monitored best-case scenario which limits the control of the release volume. When the best-case scenario is reached, no new stacks will be released in the current week, even if the previous stack is already more than 80% consumed.

Blockchain explorer

A blockchain explorer is to be developed based on the Ethereum Explorer⁹ code. It will allow any customer to view the balance of an iZAC wallet. The application will be accessible without authentication and will provide network statistical data such as:

- the total amount of iZACs in circulation at a given time (non-frozen tokens in wallets),
- the transactional volume available for differing periods of time (last, hour, 24 hours, 7 days, one month),
- the number of blocks, wallets, and
- the token price on various exchanges.

The iZAC explorer will be designed to offer the REST API for integration with third party systems, allowing them to display real-time information for the iZAC network. The documentation for the API will be published on appropriate forums once complete.

iZAC wallet

The iZAC Wallet is being designed as a cross-platform wallet, enabling users to store multiple cryptocurrencies and crypto-tokens (ETH and Bitcoin currently) along with their iZAC token.

For the iZAC, the wallet will provide the following functionalities:

- generate a new address on the blockchain network,
- view iZAC balance and an ability to perform send and imports with other wallets (using address and private-key, plus an export to paper wallet), and
- secure a wallet with a password and encrypted biographical information. An option to further secure this using geographical location software is actively under investigation.

Eco-life

As the system continues to develop, we predict that, based on the expected number of application users, there will be a balance between the supply and demand for the iZAC, which will ultimately lead to an increase in its value.

The iZAC has all the prerequisites to be a viable replacement for FIAT money, allowing millions of unbanked individuals to gain access to easier ways to make payment for special occasion or everyday items, while providing them the same opportunities as banked persons, backed by the latest in encryption and security technology. This is the defining feature that will allow this token to be reused continuously, thus forming a transactional eco-system.

⁹ <https://github.com/etherparty/explorer>



Through the provided facilities, the iZAC investor will have access to online and offline transactions for goods and service. This will help overcome current challenges in industries like:

- Gaming: Online gaming is a rapidly expanding industry with a high acceptance of technology. To date many passionate gamers have found it difficult to upload funds to the various gaming platforms. We envisage a solution by using the iZAC and its supporting platform,
- Real Estate: A great number of real estate developers are searching for simplified ways to accept payments for property, particularly when international transactions are involved. The iZAC represents a secure and viable alternative with the potential to create increased revenues for the developers,
- eCommerce/Merchant Platforms: These represent one of the greatest tools to gain community feedback. With an increased number of merchants accepting the iZAC, the greater the overall demand will be, resulting in its increased value,
- Wealth Protection: Using enhanced biosecurity techniques to support the cryptographic protections, this will ensure that the holder's wealth goes only where the holder intends,

Scalability

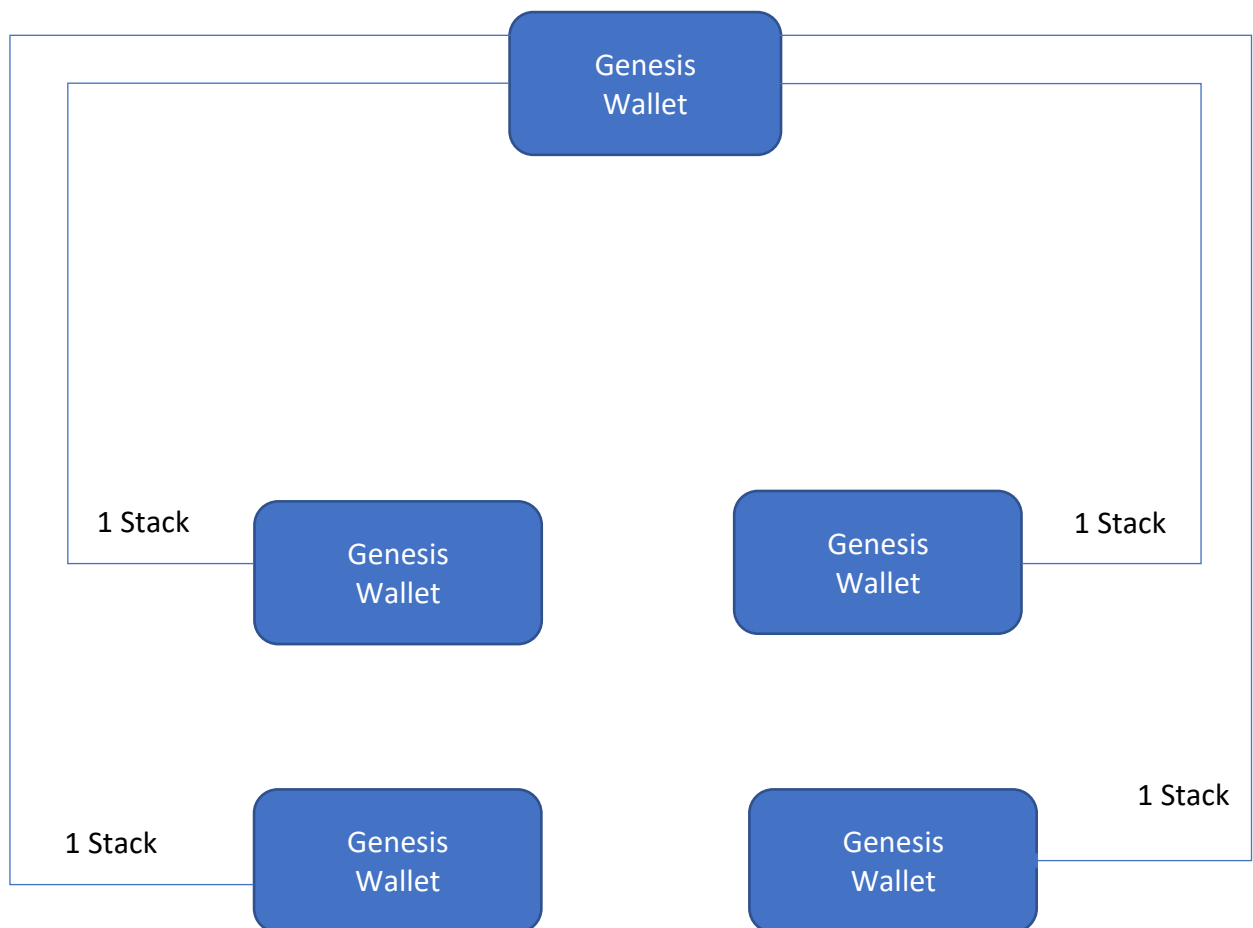
Being a crypto-token that uses a distributed ledger technology, the ecosystem supporting the iZAC is scalable. Its growth is controlled by the amount of iZAC tokens in circulation at a point in time and the number of transactions/reuses of tokens taking place in that given time.

The total token supply is 10.000.000.000 iZAC (10 billion tokens). The tokens are issued in stacks of 100.000.000 (100 million tokens). In total, there will be 100 stacks in 4 releases.

These tokens are distributed to iZAC platform members by using an Affiliate Marketing Platform and a set of rules deployed on the Ethereum blockchain utilising smart contracts.

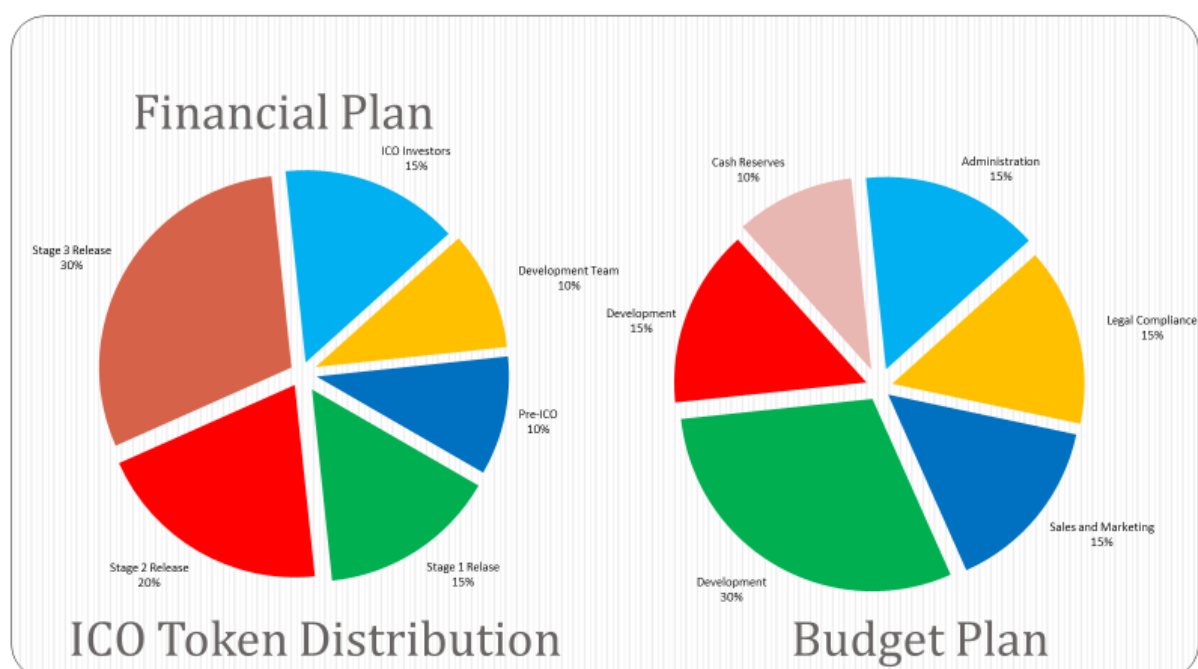
Initial distribution

The Genesis Wallet (or Master Wallet) will hold all the initial 100 stacks. During the publication of the smart-contract to the Ethereum network, the initial distribution plan will occur.



The Genesis; or Master Wallet will transfer a total number of four stacks to several special wallets:

- one block will be sent to the Stakeholder Wallet, which is locked for three years so as not to flood the market,
- one block will be released to an Investor Wallet, and
- one block will be sent to the Stacking wallet to ensure enough funds to provide the users which have deposits with their interest payments.



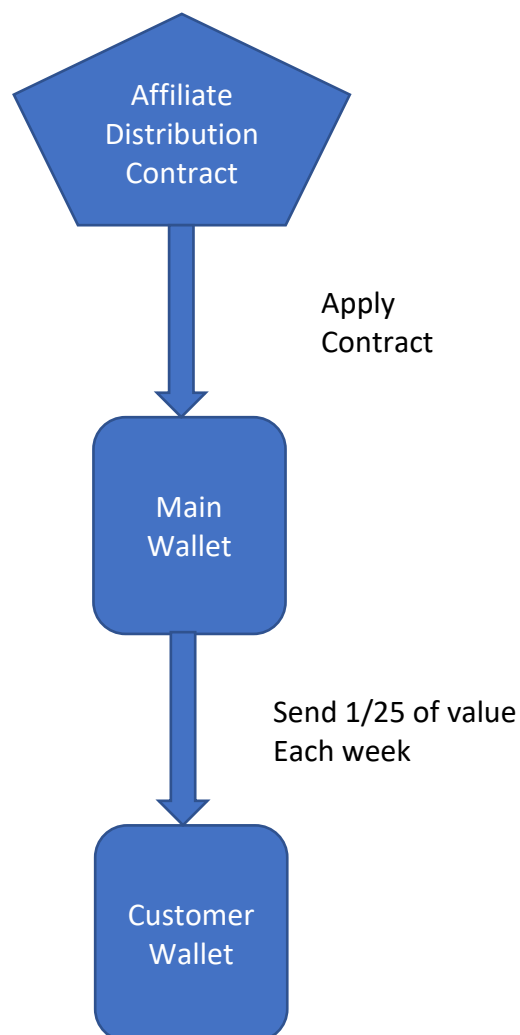
Affiliate network distribution

The iZAC is to be distributed through an affiliate network using the rules that are written in the Ethereum contracts. This distribution plan is detailed below:

- payment scheduled transactions are signed using the Main Wallet key which is controlled by the Affiliate Network Distribution company. The only transaction that the Main Wallet can do is to add scheduled payments. Normal transfers from this wallet are not possible (wallet is permanently locked),

- packages will be distributed to a user over a period of 25 weeks starting from the date his wallet was added to the affiliate network distribution schedule. The user can then receive their iZACs,

- after a scheduled payment has been committed, there is no method to stop it, delay it, or to change the receiver.



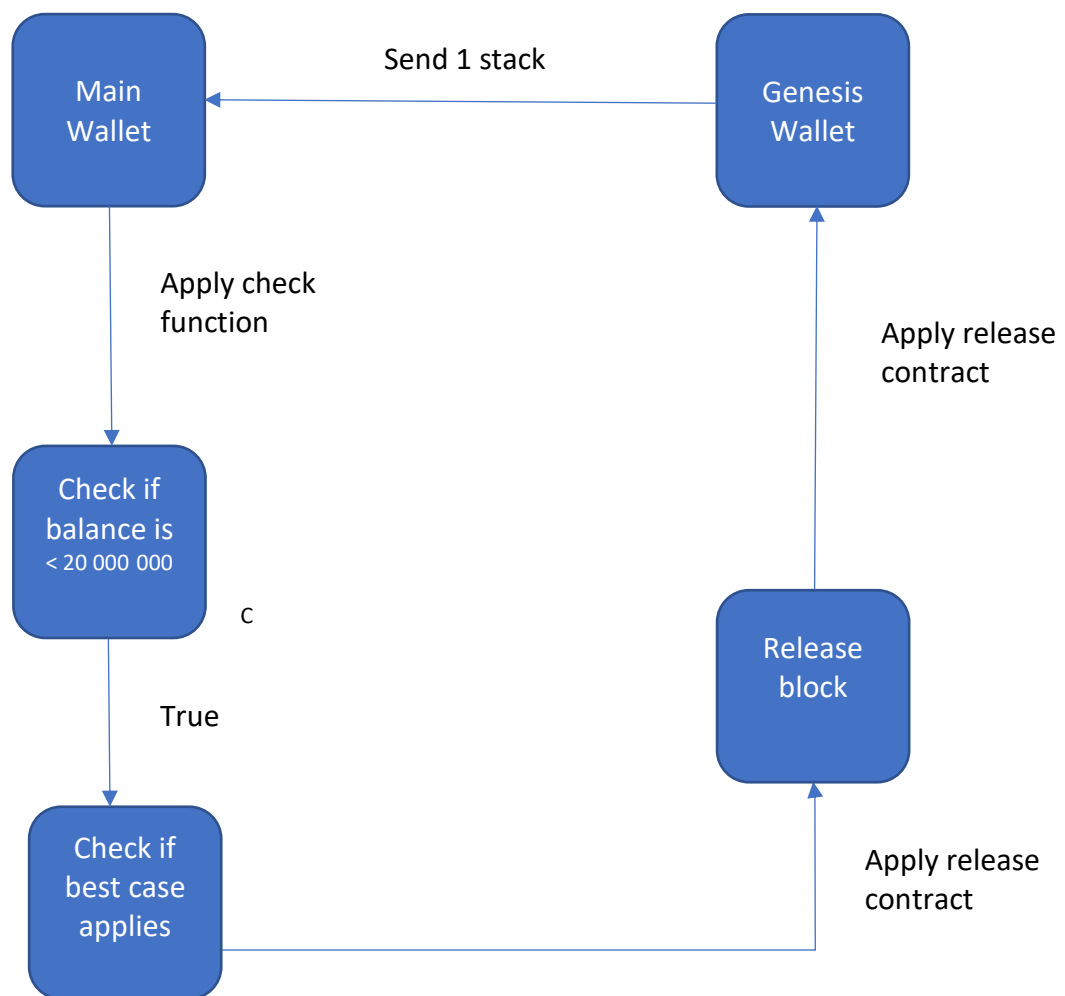
Stack unlock process

The iZAC network is composed of 100 stacks of 100.000.000 iZACs each. At the beginning of the contract, the Genesis Wallet contains 100 stacks, of which four are transferred to certain other special wallets.

As the Affiliate Network Distribution evolves over time and the Main Wallet balance is consumed, more stacks are released from the Genesis Wallet to the Main Wallet.

There are two rules for releasing stacks from the Genesis Wallet to the Main Wallet:

- the balance of Main Wallet is less than 1/20th of a full stack (less than 20 000 000 iZACs). Even if the Main Wallet balance is less than 1/20th, “the best scenario” could still halt the stack release trigger.
- the “best scenario” states that the total scheduled distribution added in the current week should be more than 20 million iZACs plus 10 million multiplied by the number of complete weeks which have passed since the creation of the contract.



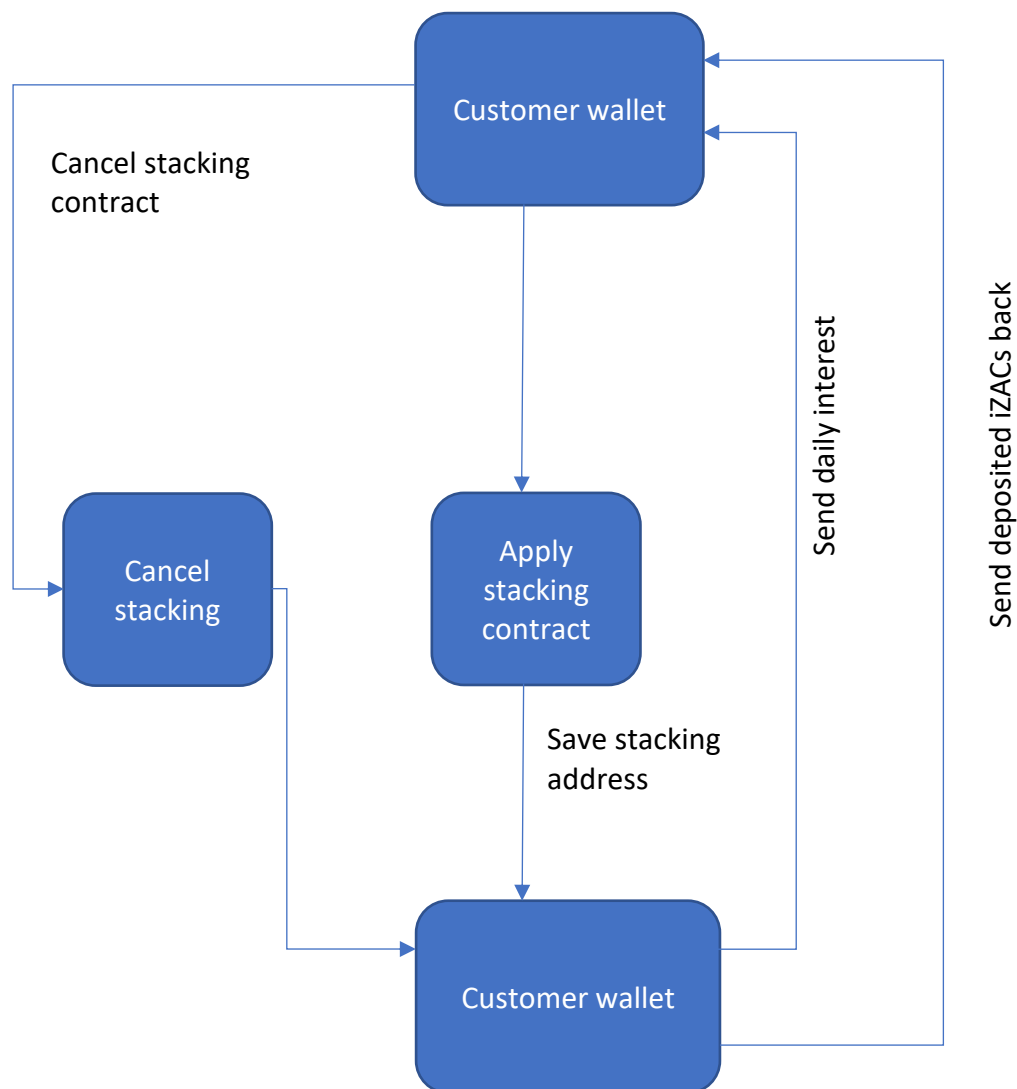
Stacking process

The users of the iZAC crypto-token can opt for stacking. Depending on the value of their deposits, they will get a variable interest payment. Fixed deposits are set for three/six/nine months and the interest is paid daily.

If an iZAC client opts for a fixed deposit, they will be required to send their iZACs to the staking wallet¹⁰. The Staking Wallet is financed during the Genesis with an amount of 100 million iZACs. The wallet is re-financed each time its amount drops under 10% of the initial value.

¹⁰ A smart wallet which sets the amount of interest automatically (based on the iZAC amount).

If the individual decides to withdraw their money before the agreed deadline, they will receive a pro-rata amount made up of the original amount minus the interest amount they have already received.



Transaction Cost

When using the Ethereum blockchain, every contract and transaction which changes the network's state (for which a new block needs to be mined) needs Gas¹¹ to be executed by the system. Gas is the internal pricing for running a transaction/contract using Ethereum (ETH). Simply, it represents the cost of getting your Ethereum message/transaction executed as quickly as possible. As every transaction published into the blockchain imposes an operating overhead to download and verify it on the network, there is some need for a regulatory mechanism to prevent abuse.

¹¹ measures how much "work" an action or set of actions takes to perform