Company Oriented Blockchain

Weinberghöhe 27,

6300 Zug, Svizzera

October 9, 2019 - v.3.0

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

This page has been intentionally left blank.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Abstract

TakaMaka solves the problems of Governance of both the public and distributed Blockchain, and the execution of Smart Contracts, with particular attention to enterprise environments.

TakaMaka introduces an innovative Proof Of Stake solution, which allows a high degree of transaction reliability under normal working conditions (1,000,000 Tx/h). In this context, the verification process and the Blockchain algorithm permit the realisation of a self-financing network and the creation of a digital currency for the organization of the Blockchain reward system, which evolves and not influenced by foreign actors.

We have the ability to accurately estimate the number of operations and the amount of resources needed for the execution of Smart Contracts, provide accurate and non-variable estimates for constant gas operations and parameterize for those where the size of the data varies. The idea behind this structure is to enable budget planners and writers of intelligent contracts to know and plan the costs with a high degree of accuracy.

TakaMaka is a free, open source third generation Blockchain, with a high degree of security and reliability, high performance, with Smart Contract execution and entirely developed in JAVA.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Index

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Introduction

The Blockchain, as is well known, is a distributed ledger designed to provide an immutable and reliable record among a number of unreliable actors; the most well-known case, thanks to Bitcoin, the Blockchain allows the transfer of control from one user to another of a digital value, safeguarding its integrity and privacy.

The Ethereum ERC20 protocol, has allowed the creation and development of a wide variety of projects and structures utilizing tokenized resources, which have allowed the creation of the first bridge from a centralized business model to a disintermediate one, between the real world and that of the Blockchain.

Since the increase in popularity of the Blockchain, countless of other projects have taken off. The most common projects have been developed either by simply copying and forking the Bitcoin algorithm, or by exploiting the Ethereum protocol. In other cases, by creating their own solutions based on a Blockchain, a consent algorithm, a programmability and a token.

The Idea Behind TakaMaka

However, neither Bitcoin nor Ethereum, nor other more famous projects have been developed through exploiting the full potential, programming simplicity and design comfort, of a widely known, high level, object-based, language, such as Java, designed to be as independent as possible from the hardware platform of execution.

TakaMaka is a protocol similar to Ethereum, but faster and safer. It designed to be used in Java, with a usability and familiarity of the code, which makes the approach friendly to most who, with new ideas and projects, want to develop on Blockchain.

This eliminates unpleasant "bottlenecks" which, without the specific programming skills, slows down the approach of individuals to the Blockchain. Moreover it reduces the gap between the lunch of the project , staff training and overall costs of start-up, which significantly affect and often dissuade from starting a new business model.

The ability to customize and tokenize your idea, the construction of Smart Contracts with a fixed and predefined cost, integration with third-party (and non-third-party) Oracles, the ability to use two coins (one stable and one not), offers business oriented TakaMaka programmers, developers and start-ups fast and direct access to the world of Blockchain.

The consent protocol PoS (Proof of Stake) allows access first of all, to the network for investors, supporters of NODES and stakeholder bettors, and furthermore a constant reward, which indirectly allows users to utilize a fast and secure network which is easy to program and which trades in a stable way at up to 1,000,000 Tx / h and beyond.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

TakaMaka

TakaMaka is a company oriented Blockchain that bases its core on the most widespread and extensively used verifiable programming language: Java!

Java is a responsible language, with intrinsic characteristics of portability, reliability and verifiability, which we decided to use as a single code for the management and programming of the entire infrastructure of our Blockchain. From the NODE, to Smart Contracts, to programming, the only thing you need to know is Java.

The main strengths of our Blockchain, can be identified as: Full stack java, which does not require special development environments, Smart Contract Java, a high performance Blockchain, branded tokens that require native tokens to work, but which hide their use from the end user.

In addition to the Blockchain technology we have developed a native cryptocurrency that presents itself as both, a stable coin and as a variable coin that follows the trend of the mining market, necessary for the TakaMaka network..

Why Java

For more than 20 years, Java has been one of the preferred programming languages and despite its age it remains by far the most widely used language. It is mainly for this reason that we decided to use it as a base and the only code for the entire Blockchain infrastructure.

To date:

97% of corporate desktop computers use Java.

89% of desktop computers (or laptops) in the United States use Java.

9 million Java developers worldwide.

Developers' preferred option.

3 billion mobile phones use Java.

5 billion Java cards in use.

125 million TV devices use Java.

5 of the top 5 original equipment manufacturers provides Java ME.

Thanks to this choice, which we believe to be strategic and which represents the core of the TakaMaka project, it was possible to apply all the tools for Bug reporting and those for

forecasting the results of execution during the development of Blockchain software, which currently form part of our Blockchain.

The TakaMaka Algorithm

The TakaMaka algorithm is a crucial part of the infrastructure it supports. Furthermore it uses a new demonstration of the PoS (Proof of Stake) algorithm, which determines how individual NODES reach consensus on the network.

TakaMaka is a fully fledged cryptographically secure PoS with a new chain selection rule, which allows new and offline participants to join the Blockchain through bootstraps, using only the reliable copy of the genesis and client block, without this happening through further advice input, such as checkpoints, or assumptions about past availability (knowledge of the entire chain history).

In this way TakaMaka allows access to the Blockchain through the execution of bootstrap from genesis.

Advantages of Bootstrap from genesis

In the Bootstrap phase, i.e. loading initial instructions, clients select the correct chain because it executes the bootstrap process from genesis.

Thanks to bootstraps, a NODE will remember its most recent successful peer connections, so that, if it is restarted, it can quickly re-establish connections with its former peer network, always opting for the right chain.

Anyone can join the correct chain safely, by simply executing and using the information from the genesis block, without the need to join the secure chain through blocks which are constantly online and/or through "reliable checkpoints".

The Bootstrap from genesis is an important feature of PoW environments, particularly bitcoins, and also represents an advantage in terms of security over PoS environments.

TakaMaka integrates PoW and PoS in a new hybrid security concept, which allows this chain to remain almost immune even from long range attacks, perpetrated by malicious actors.

In TakaMaka's PoS there is the so-called block reward. In fact there is no prize for those who insert the right block in the Blockchain, as no new crypto currency units are created with the creation of each block. But in essence, validators are rewarded differently, earning "only" a commission for validated transactions.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Malicious Attacks on the TakaMaka Chain

Let's assume that a new participant in the network is trying to find "the right story", but has no information about the protocol. In a complex and distributed network, there are always parts that we call "honest parts" that provide a correct Blockchain, and "dishonest or opposing parts" that provide an alternative.

In POW (Proof of Work) you can check that the main chain (managed by honest parties) has the most blocks and therefore the "opposition" chain will be substantially shorter (allowing new parties to connect to the correct Blockchain), in TakaMaka's Proof of Stake the only information that new participants have to understand which is the honest part, is the genesis block, which is the only true information to access the reliable chain and to verify whether you are actually looking at the honest Blockchain.

When you are dealing with two forked chains created in recent history, to be able to understand and choose the correct Blockchain, the rule of the heaviest chain is applied. In this case, the concept of a heavy chain represents the overall stake that has been "bet" on that version of the story.

Thanks to the concept of Blockchain from genesis, extensively reworked and developed by us since the most famous version Cardano Ouroboros[3], we have built and optimized a secure and incontrovertible consensus algorithm which is economic and democratic and resistant to long-range attacks, typical of the Stake's protocol.

Prevent an Attack

What happens if the fork is larger than a certain number N of blocks?

The solution is to go back to the time when the chain diverges and to isolate a certain region of blocks. Within a certain time interval, it is necessary to check which of the 2 chains is denser. The correct chain will always be the densest one within that time interval.

If the majority of the parties follow the protocol, in a sufficiently large segment, the corresponding chain will always be the densest (especially after the occurrence of a fork).

TakaMaka is designed so that contradictory Blockchains, shortly after the fork, show a less dense block distribution.

This rule is used to determine which is the correct Blockchain to connect to, implemented with great effect by the algorithm, to improve the principle of the longest chain.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Algorithm Specifications

While in the Proof of Work, miners invest the computing power to compete, be chosen, undermine the next block and win a prize in doing so, in the Proof of Stake, it is the stakeholder who forms the next block.

The main advantages of our Proof of Stake algorithm are mainly energy efficiency and security. Moreover the ease and accessibility of the network encourages users to set up and maintain NODES.

Although stakes act as an economic incentive to dissuade the validation or creation of fraudulent transactions, the TakaMaka protocol is independent of both the maximum network delay and the minimum and/or maximum level of stakes availability. Furthermore it has been developed to address an arbitrary number of problems affecting the NODES such as: network problems, operating system restarts or updates, transaction problems and validation of Smart Contracts or network interface and system clock errors which may not be completely operation related but perhaps actively engaged in maintaining the Network.

The TakaMaka algorithm is effectively a POS, but with features comparable to the Proof of Work, built on a 30-second partitioning grid called SLOT.

Only 1 block produced by the miner can correspond To each SLOT [30 sec], which can be filled up to a maximum of 10,000 transactions, which then links it to the data of the previous EPOCHs (time period consisting of 24000 contiguous slots).

We know that in PoS, one of the main aspects of vulnerability is time related. With that in mind, the only two possible solutions are either making time safe, or finding a way not to rely on time.

Timing attack in PoS

Let's say that we are in the condition in which the miner A has 1000 coins and the miner B 10,000. In a situation so extreme, it is evident that the miner B has a 10x advantage over A in the generation of blocks.

One of the possible ways in which a miner / validator could compromise the chain of a PoS is to perform a "Timing Attack", using UXTO which are fragments of "currency" recognized by the entire network, present in the Blockchain and never spent.

If, for example, as soon as the mining time is over, a malevolent actor immediately tries to mine a new block, creating a concept of virtual time, he would get the maximum profit even on a fake chain.

So, if the main chain always moves with an average of 1 block per second but the secret/fraudulent chain moves with an average of 0.8 blocks per second (exponentially distributed), then it is possible that the secret chain gets about two blocks, while in the same time the main chain gets only one.

In PoS an attack has a significant chance of working, with only the need for the attacker to have a high amount of Stake and to perform a very consistent number (compared to all other NODES) of bets, "out of synch"..

Why the Attack on TakaMaka doesn't Work

The TakaMaka algorithm brilliantly solves both aspects.

TakaMaka has made time safe, allowing all processes not to be attackable and making them completely robust.

In fact, the prerequisite to run TakaMaka is to have a reliable source of time. If you want to become a NODE of the network, the only thing you have to do, in addition to having a compatible hardware infrastructure is to ensure reliable timing (atomic clock, to an accuracy of 1 sec).

In addition to ensuring a safe time, to be accepted as a delegate, you must ensure a value of stakes within a range, minimum and maximum, which is defined by the algorithm of TakaMaka. The range ensures that you have a minimum value to be able to become a delegated miner, but limited to prevent you from assuming a predominant role in the network.

Therefore, to become a reliable actor of the Network, the TakaMaka algorithm inserts two important concepts that delimit the perimeter for possible malicious attacks. The first is the amount of stake controlled and/or the possibility of an accumulation over time, and the second is the need for an atomic clock that sets the correct time to ensure that the action of block mining is constant and bound to time.

In this Blockchain, the time is marked by a main loop with a frequency of 30 seconds. Instantly on the 15 and 45 seconds of each minute, a signal is produced that advances the state of the world.

The Role of the Miners

You will understand, therefore, that the role of the miners is strategic, not only to keep the Blockchain active, but also to establish a reward that can satisfy both the NODES and the token owners, creating a virtuous process closely related to an economic incentive and able to satisfy everyone.

MINING: delegate mining

The mining structure of TakaMaka is defined through the concept of the delegate miner.

With the term delegate miner, we refer to figures of the network, closer to elected miner, that are a well-defined group of (elected) miners who contribute to the maintenance of the Network.

If I own some Coin, but I don't want to take charge of building a hardware infrastructure and start to mine, I can delegate my vote to a mining NODE. A mining NODE can become such only if it gets to own a level of stakes that falls within the parameters defined by the algorithm of TakaMaka.

The election of the NODES delegated to mine takes place once every eight days and , on that occasion, stakeholders will only need to focus on a NODE, loading it with stakes, and electing it as an effective miner. The reason behind it is that those interested in investing in the network, but without specific technical expertise and / or computer skills, can collaborate in the growth and maintenance of the network by simply betting on a NODE.

Furthermore the NODES, through a minimum investment, can decide to start an infrastructure that generates profits, which come not only from mining, but also from the bets coming from the investors themselves.

Stakeholders are in effect network inspectors because they can evaluate the overall performance of the NODES on which they have bet and possibly modify their choice to reward those with better performance.

Behaviour of the NODES

The TakaMaka public chain allows you to verify and control not only the transactions, but the behavior of the NODES themselves, offering a real-time overview of the best Miners to bet on, to get the most out of the network.

The VRF algorithm (Verified Random Function)

Verified Random Function is the TakaMaka algorithm that calculates the distribution of slots between NODES, for a given epoch.

The algorithm guarantees that a defined number of SLOTs is assigned to each NODE, corresponding to the stake quota for a given EPOCH. These SLOTs are never necessarily continuous, but reflect the value of total bets on a single NODE and the amount betted by the individual, which may vary over time.

In this sense, if the NODES owner does not perform properly, it becomes irreparably unattractive and encourages gamblers to change their bets and bet on other actors in the network, effectively excluding it from the network.

The bettors' interest then shifts to other NODES, more efficient and performing better, encouraging the network itself to give its best.

If the NODE is not mining the network, it can use the resources to vote for the execution of a Smart Contract. The basic idea behind the execution of Smart Contracts, according to the TakaMaka algorithm, is to ensure that they are approved only when they receive a number of Tx-bases necessary to cover 50%+1 of the stake.

As soon as the contract is uploaded, i.e. included in the Blockchain, a start occurs at which point the NODES receiving the copy of the block, vote to determine the result.

Only the NODES that vote first are rewarded, while those that "submit" late are considered, to all intents and purposes, slow NODES and receive no compensation. The idea is to create a virtuous competition in which the best performing NODE is rewarded and wins, triggering a proactive process of competition with economic incentives.

NODE Types

The protocol foresees that there are two types of NODES, the first called main NODE and the other called Overflow NODE.

The main NODE is, to all intents and purposes, a virtual NODE. Moreover it is a catalyst for the mining activities of the NODES it organizes, which are in fact the Overflow NODES.

The latter, while they are directly and strictly engaged in validating transactions, confirming smart contracts and collecting Stakeholder bets, they leave the main NODES the task of exposing their public key, useful to aggregate the NODES and the activities of the Overflow under a single operational management element.

It is the Overflow NODES that accept the bets of the betters and then process the transactions as miners of the network, but it is the main NODE that organizes the ordinary activities and extraordinary maintenance of the pool of NODES that are running.

If a NODE or a group of Overflow NODES goes into maintenance, suffers an attack or simply a failure, it is the conductor, ie the main NODE, which reorganizes the Pool of Overflow Miners , ensuring the operational continuity of the entire Pool.

Each Overflow NODE can be created by a main NODE, but it can also "create itself". However, to be a reliable NODE and give functional guarantees and continuity, once operational, the most logical choice is that it requests to be placed in a mining pool, being authorized by a main NODE, the role of which is like the orchestra conductor of the pool.

The Overflow makes a request and is usually accepted, through an operation of automatic registration and a small fee, with the main NODE, which, for the entire EPOCH period, administers and manages it as an element of its Pool with the aim of obtaining and optimizing the maximum profitability.

The main NODE, simply put, is a virtual public address that allows for redistribution during a possible disaster over a number of servers (overflow NODES) instead of leaving the problem at a single source.

Competition between NODES

There is no substantial competition between the NODES of the Network to determine who becomes a miner, as is the case for example in the most famous and energetic PoW Blockchain. In TakaMaka's PoS, miners compete exclusively on the efficiency by which the NODE creates a block, rather than on the number of transactions it manages to include in it.

A fast NODE is the one which most quickly manages to vote on the goodness of making a call to the smart contract. The maximum number of active NODES for each EPOCH is 400. This allows sufficient redundancy within the network to guarantee the impossibility of a significant overload of the protocol and keeps its functional efficiency stable.

Mining reward

The reward fee for each Miner, in a SLOT, is set at 1 Green Token, implying a total reward of 24,000 Green Tokens for each EPOCH.

years for coin issuance	100,00
days in a year	365,00
hours in a day	24,00
minutes in an hour	60,00
ticks per minute	2,00
	105.120.000,00

If I am not a manager of a NODE, but a StakeHolder betting on a miner, my prize will be equal to 80% of the final reward, distributed according to the size of the bet of each single better.

The miner is not paid if he submits late (a rule of Universal Time). When a block in a SLOT is not added to the chain, that SLOT turns out empty and therefore the MINER does not receive any compensation for this missed operation.

An empty block will contain only COINBASE and no fees, while the transactions that are not included within 10 minutes of their subscription, will be discarded exactly as laid down by the TakaMaka algorithm.

COINBASE are the transactions that create the coins to give as a reward to the NODE that mined a block, even if the block is empty.

COIN

Through the Blockchain, TakaMaka allows the simultaneous management of two coins, one called Green Coin, the other called Red Coin. The first coin is standard, necessary for

the operation of the PoS and to ensure the longevity of the Blockchain, while the second one has a fixed-cost, enabling value transfers and payment of transaction costs.

In this sense we can provide precise estimates for constant gas operations and parameterized for those where the size of the data varies.

The basic idea of this structure is to allow those who plan the budget or write smart contracts to know the costs with a high degree of accuracy.

The following points state some of the advantages and uses of the Coins on the network:

Green coin

- Used to pay the transaction fees
- It is generated in the NODES as a result of mining
- It is used to calculate the weight of the chain
- allows the individuals to bet on a NODE in order to turn it from a replica NODE to a mining NODE
- used in the calculation of the PoS
- Divisible to 18 decimal places.

Red coin

- Used to pay the transaction fees
- created once within block Zero

Why the Need for Two Coins?

All current PoS implementations and major variants are based on the exclusive use of a single chain token for job quantification and control management.

Particularly in the early stages, this leads to an unnatural scarcity of the token due to the fact that whoever owns it has control of the chain and is not willing to sell it so as not lose that control. This situation of scarcity leads to a difficulty for those who operate on the network, to obtain the tokens necessary for the payment of the operations conducted on the network.

Moreover, in a chain initially launched by a single subject or consortium, another consequence is that the control of the entire network remains in the hands of the subject who generated it, and who could favour the onset of anomalous behaviour and nullify the decentralized nature of the network.

If the subject or consortium mentioned above significantly transfers more than 70% of the system token, it would be able to preserve the decentralized nature of the network but would progressively lose the ability to operate on it.

In order to prevent the occurrence of these problems, which are particularly serious during the bootstrap phase, it was decided to introduce an additional enabling token.

This enabling token allows those who have initialized the network to transfer the entire control of the network without losing the ability to operate within it.

Green Token “TKG”

The green token is not directly exchangeable with the red token and is generated directly by the mining activity on the TakaMaka chain. The payment of the mining activity premium is always paid with the green token. Furthermore this can also be used to pay transactions, create and manage Smart Contracts and get a reward from the mining activities.

But what would happen if the token in question fluctuated its value as a result of speculative actions or due to an increase in mining factors, such as an increase in the number of stakeholders?

It is clear that the cost for the base and blob transactions, or the management (creation and launch) of Smart Contracts, would have costs that increase even temporarily. To summarize, the network would behave as the most emblazoned Ethereum for example, without the guarantee of certain costs.

While on the Holder side the possibility of an appreciation in the portfolio of the Green tokens, would allow a significant economic advantage, precisely by exchanging these on some Exchange.

Red Token “TKR”

The Red token has the same purpose as the Green token, to pay fees, activate transactions and Smart Contracts. It is, however, in no way involved in mining and unlike the Green token is stable, in the sense that its value never changes and is always guaranteed by AiliA SA.

The Red tokens are generated once in the zero block, and there is no counterpart value for them, as the company AiliA SA has established sale and repurchase prices that are stable at the net spread cost.

TakaMaka's stable Red token allows the safe management of the infrastructure and the use of all the tools of the network. It pays the fees to bettors who bet on a mining NODE, but always guarantees the certainty of costs.

Being stable, it is not subject to market fluctuations, changes in mining activity or speculative effects. In this sense the Red token guarantees the stability and certainty of the management costs of both transactions and Smart Contracts.

This is why with TakaMaka it is possible to accurately estimate the number of transactions and the amount of resources to be used for the execution of Smart Contracts, providing exact and non-variable estimates for constant gas transactions and parameterizing for those where the size of the data varies.

Both Tokens are Utility, but while the Red Token can only be purchased on the AiliA marketplace, the Green Token can be purchased on the forthcoming Exchanges.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Governance

Takamaka implements a self-consistent structure in which the collective participation of the actors involved (or not) makes them honest, pushing them to improve the protocol, introducing upgrade and bug fixes.

TakaMaka pushes the collective interest to "survival", avoiding self-destructive tendencies which are not aligned with the intrinsic value of the chain.

Exactly 5,000,000 TKG (Green Coin) are made available by the company to reward those who suggest improvement, provided they contact the team through bug@takamaka.io and adhere to the Responsible Disclosure.

By applying this controlled and ethically correct model for reporting security vulnerability, anyone can contribute to raising the level of protection of TakaMaka services, helping the company to detect and take corrective actions to avoid damage and / or disruptions.

Coin Economics

Takamaka decided to introduce two coins, TKG (Green Coin) and TKR (Red Coin). The reason behind this choice is that, even if those who have deployed the network decide to transfer their entire stock of TKG, they could still continue to operate on it utilizing the TKR. Moreover this would not cause price manipulations.

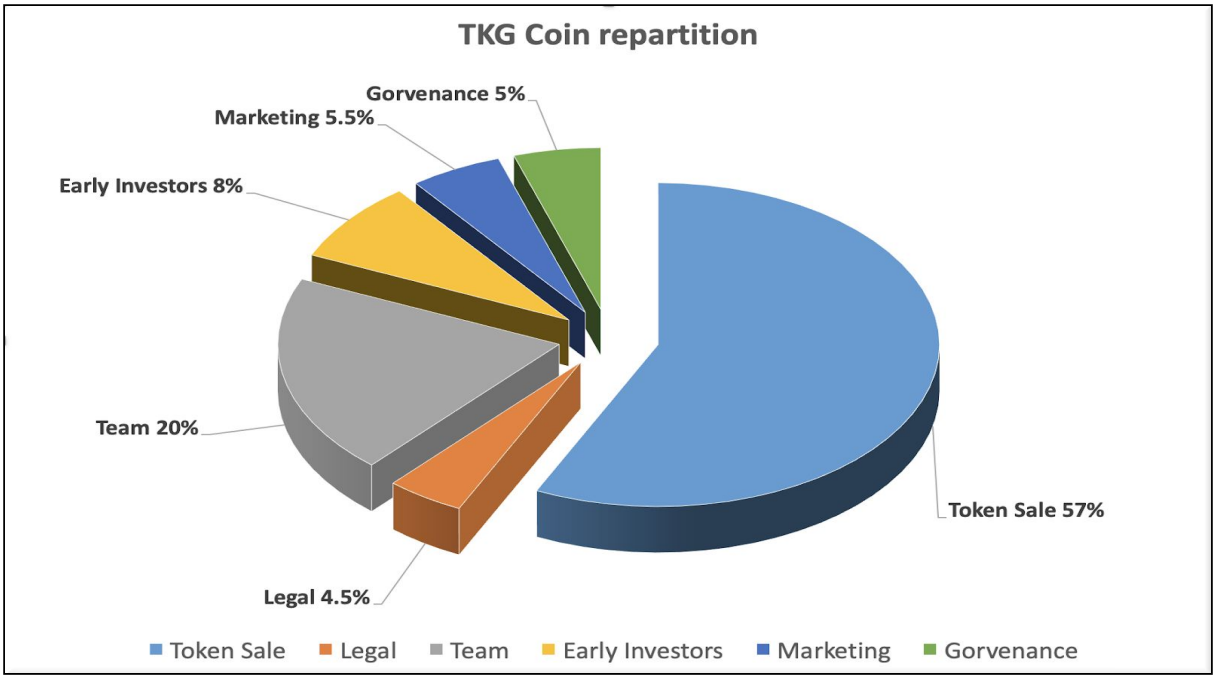
The TKG (Green Coin) is never exchangeable with the TKR (Red Coin) but it could be initially purchased from the Takamaka website and subsequently from Exchanges. Furthermore it is the coin generated from the mining activities and used to rewards the StakeHolders.

The TKR (Reed Coin) is generated in the block “Zero” with a stable and guaranteed value. It is not subjected to market fluctuation and/or speculation. In this sense, the TKR guarantees the stability and certainty of the management costs on the network for both transactions and smart contracts.

.

Thanks to the introduction of this mechanism, in Takamaka it is possible to accurately and precisely estimate the cost of transactions and the amount of resources needed for the execution of Smart Contracts. Furthermore Takamaka provides precise and non-variable estimates for operations at constant gas costs and parametrize all those in which the data size varies.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io



The TKG created in the block "Zero" are 99,000,000 (Ninety Nine Million), while 105,120,000 (One Hundred Five Million One Hundred Twenty Thousand) will be released in a 100-year timeframe as COINBASE, one TKG per Block.

The TKR will only be generated in the block "Genesis" in a value equal to 100,000,000,000 (One Hundred Billion) and purchasable directly on the Takamaka website.

Smart Contract

As is well known, Smart Contracts are sequences of rules and customized functions, activated by sending command transactions. Moreover they are subject to general chain rules, can never be deleted, are unstoppable and have a cost.

The idea behind TakaMaka is to allow those who plan the budget and those who write smart contracts, to know the actual costs of expenditure in advance with a high degree of accuracy.

The algorithm is able to accurately predict a fixed cost for their execution which allows both the number of operations and the total resources used in running Smart Contracts on the Blockchain to be established with precision.

The Smart Contracts are entirely written in Java. The class/jar file contains the necessary command lines, which will be sent to the network for their execution.

They are easily integrated with Oracles, both centralized and decentralized, through external calls that come directly from APIs (Application Programming Interfaces) of the applications.

The Oracles, or Gateways, are nothing more than links between the Blockchain (and therefore the smart contracts) and the real world and have the sole purpose of passing information to the smart contracts, at the exact moment in which some real world conditions occur.

Further Consideration

Smart Contracts (SC) are nothing more than programs written on the Blockchain that are tamper-proof and deterministic, that is they are executed automatically when all the conditions of the (contract) are met; they are the future of all digital and many non-digital agreements, they are tamper-proof, irreversible and unstoppable and, in principle, always very effective.

However, since Smart Contracts are deterministic (i.e. defined by the availability of the conditions required to activate actions in the contract) it is necessary to have 100% reliable data, so that these are performed with the utmost transparency and accuracy.

These can also be implemented, executed and authorized to transfer money.

In fact, these contracts are usually divided into Smart Contracts that contain money, but do not have code (external property accounts) and those that, instead, contain code (intelligent contracts).

While the former are typically controlled by an external agent (a portfolio, a human, for example) the latter are generally controlled by their code.

TakaMaka implements both alternatives within the same code, through a language that, in effect, looks like an Object based programming code, as it is created from Java.

Additional Strengths

We then analyzed the behavior of TakaMaka, offering a functional overview of the algorithm, language and infrastructure, and highlighting in particular usability, ease of writing and readability of the code. Those are the dominant strengths of the project.

TakaMaka, however, focuses on other points as well, just like a project that wants to focus on market leadership.

Let's have a look at some of them:

- **Speed of transactions:** the Blockchain of TakaMaka is a chain calibrated on a defined volume of 1.000.000 [Tx] /h estimated transactions, thanks to all the characteristics previously described.

- **Smart contract:** There are special transactions in the blocks called Smart Contracts. Smart Contracts are sequences of rules and custom program functions, which are activated by sending command transactions. They are subject to the general rules of the chain and therefore cannot perform cancellations. Moreover, each operation has a cost, cannot create money from scratch, are unstoppable, independent of hardware and automatically portable. Thanks to the TakaMaka algorithm it is possible to estimate both the number of operations and the amount of total resources to be used to perform a Smart Contract on the Blockchain very precisely. Following the creation stage of a java file, the TakaMaka framework is incorporated, which introduces the methods for accessing the Blockchain. The class/jar file contains the Smart Contract, which will be sent to the network for execution. The life cycle of TakaMaka faithfully reflects the standard life cycle of java applications.
- **Security:** TakaMaka focuses on the code and feedback with the utmost attention to security. While the team checks the code for bugs and security defects, it also ensures the implementation of patches with rapid response, delegating the stress testing phase to an external team. The reason behind this is the continuous search for client-side bugs. The Java analysis tools are the same as those used in TakaMaka. Being a critical software, the development effort needs to be totally directed to verification and testing to obtain a significant reduction in final problems, primarily related to the modeling of smart contracts.
- **Case of use and adoption:** the technology is definitely one of the most important aspects of the Blockchain. However, what would be the point of technology if it were used only for speculative purposes, rather than for real use? This is one of the reasons why TakaMaka stands out from other projects. TakaMaka is confronting numerous cases of use and in partnership with listed companies is activating implementations on its network in order to guide these enterprises to the integration of centralized production processes on a decentralized Blockchain
- **User friendly:** if the main requirement is to work in an infrastructure that can easily allow anyone to become operational immediately, TakaMaka is the answer. Often training is the main problem of working with new technologies. TakaMaka overcomes this entry barrier by using development patterns and established technology. In addition, the company has the creation of an extensive library of specific documentation in the pipeline, with practical examples and step-by-step guides so that those who choose to work with TakaMaka, feel confident in the quality and validity of what is developed.

CASES OF USE

We talked about the decentralized and scalable aspect of the TakaMaka Blockchain for business, the ease of programming, the presence of two coins and the mining process, but what are the cases of real use ?

Obviously they are not only those related to transfers and speed of transactions. TakaMaka offers incredible and effective solutions for different cases of practical use such as:

- Timestamping
- Trusted DNS
- CA Authority
- Trusted Ticketing
- Budget Management

Trusted ticketing

In order to operate on the Blockchain you must have a set of keys, usually referred to as wallets. With an ad-hoc contract, it is possible to associate one or more web addresses, sample identifiers or documents, to each key in order to create unalterable shared public registers. An object of this type can be used to create delivery registers, DNS systems, delivery notes...

In the case of a delivery register, all the daily operations such as the management of proxies, delivery and collection signatures and the presence of timestamps for taking charge, once correlated with the inalterability properties of the Blockchain, guarantee the non-repudiation of the tracking system.

When operating in critical sectors, it is normal to find contracts that in compliance with SLAs, that set the minimum required quality level of service, provide penalties in case of failure to meet response times or resolutions. One of the weak points of traditional ticketing systems is the "location" of the management system itself.

If they are located on the customer's premises, they may alter the register or not apply suitable data storage policies. If they are placed at the supplier's premises, the same objections can be raised, even in bad faith, by the customer. If they are present at both the supplier's and client's premises, misalignments may arise that would be difficult to reconcile.

By combining these systems with identity and resource management and timestamping of the Blockchain , it is possible to ensure the integrity of the records regardless of their location without the involvement of a third party entity as a guarantee.

This is also made possible by multi-signature contracts that execute only if all or most of the signatory individuals approve the operation. What we have seen so far is only a small part of the possible applications developed on Blockchains.

In many cases, these are existing applications in need of an additional level of guarantee.

Marketplace

The Serena company is a Marketplace within which contracts of sale of commodities are negotiated and exchanges of proprietary cryptographic currency (SerenaCoin) and Stablecoin are executed . The platform represents to all intents and purposes a Marketplace and dex.

The trading takes place within a high-performance Blockchain, regulated by intelligent contracts, to which access is possible after a registration and provision of KYC/AML.

Each participant has access to the platform, where he checks and controls the trading prices, analyzes the trend of commodities to buy and searches for the best selling and buying prices.

Historical data and statistical and predictive shares are integrated elements in the platform, collected and managed by oracles with external APIs, which become information that the company sells.

Trading within the Marketplace is done with smart contracts that automate the actions of sale and purchase, carrying out the transfer of currency and the closing of a contract. All payments are made with the Stablecoin defined in the platform.

Control on the production chain

The supply chain control is implemented in companies which require to keep a stable levels of outgoing pollutants generated from the metal production and processing machines, the melting furnace chimney and all the working environments. In this sense, the company intends to start specific and continuous monitoring on various environmental matrices.

Takamaka's solution consists of two main components: measurement and detection. The measurement part is entirely developed with a light Hardware, while the detection section provides the integration with the Blockchain.

The data is collected through a self-powered display, which exhibits a QR code identical to the one written on a server, located in a remote position, according to the Multi Factor Authentication logic (2 Factor Authentication).

The area operator, once he is advised on the need to carry out a survey, he interrupts the normal working procedures and heads towards the pressure gauge for the detection.

Subsequently, the area operator activates the QR code reader on his mobile phone and frames the display. The app detects the QR code and takes a picture. The sequence that the QR code exposes is not predictable therefore the photo, exactly as it is, is sent to the agency, for control and storage, and to the Blockchain.

A time stamp is applied to the photo and, thanks to the Blockchain TakaMaka, the entry history of the data is certified (the photo in this case). Furthermore, the photo is associated with the date (the hour, the minute and second) in which this data was sent/received.

When the photo is sent to TakaMaka, it results in a transaction made on the Blockchain.

A copy remains on the operator's mobile phone, one goes to the certifying company and one goes to the servers of the company interested in verifying the data control.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Team

The Takamaka team is made up of a wide mix of collaborators that range from engineers, mathematician and cryptographer, to developers of structural and architectural solutions of the Blockchain:

Nicola Fausto Spoto (research consultant): lecturer in Software analysis and verification at the Computer Science Department of the University of Verona. It mainly deals with research, in software analysis and verification on an international level. In particular, he is specialized in code written in object languages, aimed at inferring properties of correctness and security of the analyzed code.

Fausto has obtained an MSc and a PHD in Computer Science at the University of Verona and has published various scientific publications and participated in academic conferences in his field of specialization.

Giovanni Antino (blockchain developer): he specialized in the development of protocols and solutions on blockchain technology. Giovanni has also gained extensive experience in the management and development of server infrastructures for large companies in the Healthcare sector.

Giovanni holds a BSc in Computer Science at the University of Verona and also works as a Bcademy lecturer.

Francesco Pasetto (blockchain developer): he is specialized in the development of solutions and applications on blockchain technology. Francesco has a long and varied experience in software and web development, security analysis and system consulting gained working for both medium-sized companies and large corporations in the Healthcare sector.

Francesco is an expert in various programming languages and has developed his first 3D graphics engine at the age of 17.

Fabio Tagliaferro (blockchain development support): he specialized in developing solutions based on blockchain technology and cybersecurity.

Fabio holds a BSc in Computer Science from the University of Verona and is a member of Blockchain Education Network Italy and an Algorand Ambassador.

Mario Carlini (investors relations): he launched and managed companies from the early 90s, mainly dealing with international trade between China and Europe, where he was

able to learn techniques and new dynamics of economic and technological flows. In 2017 he acquired AiliA SA, a Swiss company, based in the canton of Zug, focusing on IT services and innovation processes, and then in the areas of Blockchain and AI technological transformation.

Since 2017 he is one of the founding members of TakaMaka.io.

Andrea Belvedere (developers community relations): specialized in consulting on Blockchain-based environments and solutions. From 2016 he is dealing with dissemination, networking, analysis and construction of business models on Blockchain, for various companies and ICOs.

In 2016 he founded bitconio.net, the Italian reference portal on the blockchain world.

Federico Tai (Advisor): is specialized in product management and strategic development of large digital platforms, holding various positions of responsibility in companies engaged in digital innovation such as Amazon and Amadeus. Federico has extensive international experience working in Italy, France, Germany and Luxembourg.

Federico obtained a BSc and a MSc in Aerospace Engineering at the Politecnico di Milano.

Davide Cordioli (Advisor): after graduating, he specialized in commodities trading and market research, gaining experience in England, Japan and China.

Davide has a BSc in International business at Regents University in London and also speaks fluent English, Japanese and Chinese.

AiliA SA

The project was set up and developed following a first and in-depth study carried out by Mario Carlini, current CEO of AiliA SA, on the functioning of public Blockchains. Mario identified this technology, the new frontier, as the technological paradigm that will involve millions of people and will play a major role in the way new and existing companies do business.

Having assessed the impossibility of obtaining a solution that solved the "Scalability Trilemma", he decides to develop a public, democratic and ecological blockchain and relies on the skills and knowledge of a team of experienced engineers.

Mario acquires the Switzerland based company AiliA SA at the beginning of 2017, and, in October of the same year, start the Takamaka project.

He entrusts part of the project, the cryptographic components, to the Universities of Verona and Trento, delegating the subsequent levels of development to the engineers

Giovanni Antino and Francesco Pasetto, to whom he entrusts the realization of the consensus algorithm, the Networking between nodes and the encryption.

The company is currently based in Switzerland, in the canton of Zug, and is active in the field of " IT services" and innovation processes in the fields of Blockchain and AI technological transformation.

AiliA SA
Weinberghöhe, 27
6300 Zug, Svizzera
mail: info@takamaka.io

Why Takamaka

Takamaka is a valley in French Réunion island, where a network of waterfalls converge into a river. This is similar to Takamaka smart contracts, that is, distinct objects that collaborate over a shared global storage in the blockchain.