ABC - Anti-Bureaucracy Coin

Digital Platform for decentralized Authenticity of identities, signatures and e documents, using blockchain protocols

Edilson Osorio Junior, Miriam Tomie Oshiro, Helena Suarez Margarido

OriginalMy.com

July, 2017

Draft v1.2

1. Summary

Since 2015 we have been developing a global platform in which we provide new blockchain applications focused on generating registers and strong proofs of authenticity in a decentralized manner.

Having been the 1st regtech that uses blockchain for real-world cases, our applications, which are already available to Brazilian users, promote a new way for registering identities, cost reduction for signing documents (e.g., paper dematerialisation, transport and manual authenticity recognition in traditional institutions) besides the exponential increase in efficiency and render obsolete any centralized institutions responsible for registering and certifying the authenticity of contents.

Economic Freedom Index places Brazil 140th[1] in the bureaucracy ranking, having gained a worldwide reputation for big bureaucracy that significantly prevents business development. The formal procedural bureaucracy is a profitable business in all countries with Civil Law system, which includes Latin America and much of Europe. However, the centralization of information is a global issue and allows asymmetries of information that might make people and organizations susceptible to fraud.

The key to reduce these asymmetries is the decentralized authenticity, which can be achieved by means of decentralized networks that use public blockchains to provide full transparency, access, and trust.

In this document we will present:

- The active applications, in operation and their specifications
- The new platform

- Token ABC - Anti-Bureaucracy Coin

2. Index

1. Summary 1

2. Index 2

3. Glossary 2

4. Concept 5

4.1 Information Security and blockchain-based technologies 5

4.2 The dysfunctional bureaucracy 6

4.3 Decentralized Registers and Authenticity 7

5. Current Platform: Applications and History 9

5.1 Proof of Authenticity 9

5.2 Signing of contracts - 1st version (discontinued) 9

5.3 Mudamos+ Project 10

5.4 Proof of Authenticity for Web Content 10

5.5 Blockchain ID: registration and identity management 11

5.6 Contracts Signature - 2nd version (current) 12

5.7 Sidechain 12

5.8 Multiple Blockchains 13

6. Specifications 13

6.1 Proof of Authenticity for digital documents 13

6.2 Proof of Authenticity for Web Content 15

6.3 Blockchain ID 15

6.3.1 App Registration and Preliminary Validations 15

6.3.2 Automatic search on public networks 16

6.3.3 Automatic document validation 16

6.3.4 Granting Blockchain ID 16

6.3.5 Blockchain ID Recovery 16

6.4 Signing documents and contracts 17

6.4.1 Using the Ethereum Classic blockchain 17

6.4.2 Using the Bitcoin blockchain 18

7. New Platform 19

7.1 Internationalization 19

7.2 User Experience 20

7.3 ABC Token 20

7.4 OTC OriginalMy 20

7.5 Decentralizing the Blockchain ID 21

8. Crowdsale: ABC Tokens 22

8.1 Phase 01 22

8.2 Phase 02 23

8.3 New blockchain and token swap 23

8.4 Token Sale Schedule 23

8.5 Tokens issuance and deadlines 24

8.6 ABC Token Sale terms and conditions - Phase 01 25

8.6 Legal Provisions 26

9. Team 27

10. References & Bibliography 28

10.1 References 28

10.2 Bibliography 29

3. Glossary

For this whitepaper purposes some definitions have been adopted so that words and/or capitalized terms shall have the following meanings.

- Digital Signature: a cryptographic method to validate digital documents or informations, which fully proves that the information from which it has been originated has not undergone any alteration.

- Electronic Signature: use of any electronic signature mechanism not necessarily cryptographic. It works as indication of proof, having no legal value by itself, being the equivalent of a physical signature.

- Authenticity: Indicates absolute legitimacy, veracity and/or originality of something. It is the assurance that certain information was furnished by the indicated source and has kept its integrity, i.e. it has not been modified.

- Blockchain ID: method of registration and identity management in decentralized public blockchains created by OriginalMy that allows the verification of users without the custody of documents or private and/or classified information.

- Civil Law: also known as Code Law, is the most widespread Legal System in the world. It is based on Roman law and is systematized through the codification of law. In these systems, the main source of law is the written (positive) law.

- Common Law: Legal System of Anglo-Saxon origin, it is the body of law derived from judicial decisions, rather than from statutes or constitutions (Case Law).

- CPF: Brazilian individual taxpayer registry identification, a number attributed by the Brazilian Federal Revenue (*Receita Federal* of Brazil) to individuals who are tax residents in Brazil.

- Full Faith and Credit: legal presumption (*juris tantum*) of Authenticity given to documents and certificates issued by public servants.

- ECM: Enterprise Content Management. It is a union of a processes and technologies that provide easy generation, control, storage, sharing and retrieval of documents and another contents for an organization

- Information: any sort of content that might be stored and/or transferred which is valuable to a person and/or organization.

- KYC: abbreviation of know your customer, is the process of identifying and verifying customer identities. Mandatory procedure for regulated markets participants, especially financial and capital markets, which aims to curb illegal practices such as money laundering, corruption and terrorism.

- Operação Lava Jato: ongoing investigations of crimes such as corruption, fraud, money laundering, involvement in criminal organizations, and tax evasion (among others), conducted by the Brazilian Federal Police. To date, 282 persons have been criminally charged and 107 have been convicted, including politicians, civil servants and private sector executives. The estimated loss to the public coffers amounts to USD 13.42 billion [3]

- OTC OriginalMy: over-the-counter market to be made available by OriginalMy for the purchase and sale of ABC tokens directly by the company. That will be based on secondary market values, according to rules specified in whitepaper.

- Permalink: URL that points directly to a specific post on a website with multiple posts (blog, social networks, etc).

- OriginalMy Platform: set of applications developed and made available by OriginalMy, based on the concepts of registration and Proof of Authenticity in blockchains, currently consisting of: (i) Blockchain ID, (ii) Proof of Authenticity for digital documents, (iii) proof of authenticity for web content and (iv) Digital and Electronic Signature of documents and contracts. Available at https://www.originalmy.com.

- Proof-of-Work: protocol consisting of complex cryptographic calculations used for preventing spam and mass cyber attacks. Prior to the desired action, the user shall perform a particular task in order to prove to the validator agent that self-effort was made, what is mandatory for access granting or action acceptance.

- Proof of Authenticity: proof that a particular digital document is covered by Authenticity.

- PTAX: official conversion rate of *Reais* (BRL) to US Dollars (US$) as of October 4, 2017, calculated at 3.13: 1 [4]

- Register of Authenticity: storage of Digital Signature in any media.

- Roadmap: OriginalMy development goals for the targets set forth in Phase 01 of crowdsale, as specified.

- Information Security: concerns the protection of Information in order to preserve its confidentiality, integrity, availability, authenticity and legality as defined in the ISO/IEC 27000 standard set.

- Sidechain: roughly speaking, blockchains that validate data onother blockchains without needing to modify the code of the original one. It can help on scalability, efficiency, and costs of native protocols.

- Legal Systems: legal models that aim at legal security. The manner in which the result is sought explains the functioning of different legal systems and the institutes that compose them. Currently, the prevailing traditions in the world are the Civil Law and Common Law Systems.

- Web-of-Trust: reputation system that uses encryption with levels and chaining of recommendations to enhance trust.

4. Concept

4.1 Information Security and blockchain-based technologies

The Information Security good practices govern the protection, use and access to information, as well as their availability to users, while their integrity and authenticity remain preserved, with exposure of the content according to the appropriate access control.

The main attributes of Information Security [5], determined in the old ISO/IEC 17799 (inspired by BS 7799), which later came to be revised in a series of 27000 family standards, are:

- **Confidentiality:** ensure that access to information is made only by authorized persons;
- **Integrity:** safeguards the accuracy and completeness of information as well as its processing methods;
- **Availability:** ensure that authorized users have access to the information and corresponding assets whenever is necessary;
- **Authenticity:** guarantee that information and/or users in a communication process truly are who they claim to be; and
- **Legality (or compliance):** is the legal value granted to the information within a communication process.

Still, according to some authors, Information Security also deals with non-repudiation or irretractability, which is the attribute that assures the **impossibility of denying authorship** in a communication process.

Blockchain-based technologies typically adhere to the attributes of Information Security, as exemplified below:

1. The **top triad of information security attributes** is native to the protocols of public blockchains, whereby confidentiality is guaranteed by exposing only the data necessary to identify the transaction, having been some blockchain protocols that assures anonymity regarding transactions. The integrity of the data is guaranteed by means of consensus, mainly Proof-of-Work. The availability is made through the decentralization and distribution of the network, providing an adequate business continuity plan;

2. The **authenticity of the information** is guaranteed by means of use of digital signatures and authorization through private keys which are exclusively held by the author due to asymmetric cryptographic techniques;

3. The **legality** is verified since the aforementioned provisions o are in compliance with the law and regulatory frameworks that require the appropriate handling of both information and digital documents.

Such technologies are also inviolable and its validation mechanisms are used at all times, being verifiable in a simple way and guaranteeing the integrity of the information [6]

4.2 The dysfunctional bureaucracy

Bureaucracy might be defined in a broad sense as a system that operates according to pre-established strict rules, in order to guarantee great "*accuracy, speed, certainty, knowledge of the files, continuity, strict subordination, reduction of disagreements and reduction of material costs and people* "[7]. This concept is fundamental to understand how complex organizations such as societies, national states, and modern capitalist corporations are constituted, since strict rules establish order and control and assures efficiency in these institutions performance.

Thus, bureaucracy presupposes characteristics that, if applied to complex organizations, would result in functional categories: rationality, normatization, hierarchy, specialization and impersonality [8].

Bureaucracy might be decisive for the creation of efficient complex organizations however it might also result in a concentration of power by these organizations, leading to systemic dysfunctions and even to restricted systems with the quasi-purpose of the perpetuation of the status quo to the detriment of the public interest.

One example of the above mentioned is Brazil, where the abuse of rigid rules has led to a symbolic state of a dysfunctional bureaucracy which is inefficient in dealing with public policies and prevention of illicit acts. The main evidence for this fact is that the investigation of the largest corruption case of Brazilian history [9], called "*Operação Lava Jato*", have been conducted since 2014 without conclusion thus far.

Amidst the Brazilian institutional crisis, OriginalMy was born, with the purposes of eliminating the dysfunctional bureaucracy ingrained into culture and society, which is not only responsible for allowing corruption and money laundering, but also prevents the development of society and the exercise of free enterprise.

But it is not only Brazil that suffers from this problem. In all the countries with Civil Law system it is possible to find public and private institutions that profit from the oligopoly of the Public Faith, establishing lengthy and non-intuitive processes for access to information and verifications of Authenticity. In practice, the centralization of Proofs of Authenticity is one of the main sources for the asymmetry of information and clears the way not only for market inefficiencies, but also for the practice of fraud.

In other countries, notably Common Law countries, the centralization of Proofs of Authenticity is usually based on a person or organization that has some right concerning a Information, being eventual falsities and/or inaccuracies exemplarily punished on the basis of institutes such as fraud and ideological falsity. Given this centralization, the proof of falsehood is a *quasi* diabolical proof that not even multiple *subpoenas* can solve. Thus, in the same way that occurs in countries with Civil Law system, the consequence of the impossibility of assessing Authenticity of Information is an enormous damage to companies and society.

It turns out that the centralization of Proofs of Authenticity, whether in positivist countries or in those in which custom and usage are primary source of law, is the principal pillar that supports dysfunctional bureaucracy. More evidence lies in the fact that the most common consequences of this process (such as bribery, influence peddling and fraud) are suffered on a daily basis by people, organizations and governments from several countries.

As a result, the world has long suffered from a vicious circle because whereas the institutional imposition of a formal bureaucracy seeks to prevent illicit practices, it also encourages the centralization of verifiable information. Thus the will-capacity-opportunity triad that enables people and organizations to have the power to lie and cheat remains intact, which may lead to the conclusion that these new "layers" of imposed bureaucracy have the same defects as the current systems information management and authenticity gauging. Therefore, it is to be expected that dysfunctionality would be once again the result.

In the opposite direction technologies that use public and decentralized blockchains are in place: the incentive to participate by supporting the protocol overcomes the incentive to fraud it [10]. Moreover, decentralization itself makes it unlikely that a person or organization concentrates all the requirements needed (such as will, ability and opportunity) to defraud certain Information or to misuse it.

A decentralized form of registration and verification of Authenticity of Information may result in the distribution of the Full Faith and Credit among owners of certain Information, providing incalculable benefits to corporations and the global society.

4.3 Decentralized Registers and Authenticity

Even though the top triad of the Information Security attributes are guaranteed by the blockchain protocols, legality and data authenticity still rely on external applications to comply with legislation and various regulatory frameworks in order to provide a perfect legal act for all intents and purposes.

OriginalMy Platform thus provides decentralized Authenticity for documents and information through several public blockchains. Combined with other open protocols, it helps to create sophisticated Proof of Authenticity towards identities, expression of will (such as sign-ups, access logins and document signing) and several digital documents.

In practice, it is possible to perform acts such as the conclusion of legal business, in accordance with all legal requirements regarding verification of existence, validity and effectiveness, including unequivocal proof of identity and not merely possession of a password or private key.

An Authentic Information means an information which is proven to be authentic and has not been modified. Using a complex cryptographic algorithm on the original Information, it is possible to find a new Information that unequivocally represents the original. This new information is named cryptographic hash, represented by a string of defined length of characters (like this: *c66663acfe3611b9ed95c79aad41dc6fca83636361880 7cfd4ee7b88ef15fa34*). This hash is the Proof of Authenticity regarding that Information.

Notice that the hash does not allow to infer the original information nor reconstitute it. The Authenticity verification is only possible by re-applying the same cryptographic algorithm over the original Information. If Authentic, the same hash will be displayed. Comparing the hash of the original Information with the hash of the Verified Information, it will be possible to identify if the former has undergone modifications because, if a modification has been made, the resulting hash shall be different.

To assure that the hash of the original Information remains incorrupt, OriginalMy registers it in one or more public blockchains, which in turn store it. Once the blockchain confirms the storage, it provides a timestamp that represents the time at which it became aware of that hash. This is the Proof of Authenticity that an identical information was made available at a given time. After that confirmation, the Proof of Authenticity is automatically replicated to all the nodes that compose the network of each blockchain in which the registration was made.

Given the elementary features of public blockchains such as immutability, transparency, decentralization and data distribution, OriginalMy provides decentralized Authenticity for digital documents, without registering or making public the content of User Information in order to preserve privacy and confidentiality.

Patterns and open protocols tend to be more effective than closed standards since they are not only auditable but also dispose of several communities engaged in its development.

For this reason, OriginalMy operates with several dApps [11] (decentralized applications) that might be publicly accessed by other smart-contract systems in order to share the infrastructure and then improve processes as well as control efficiency.

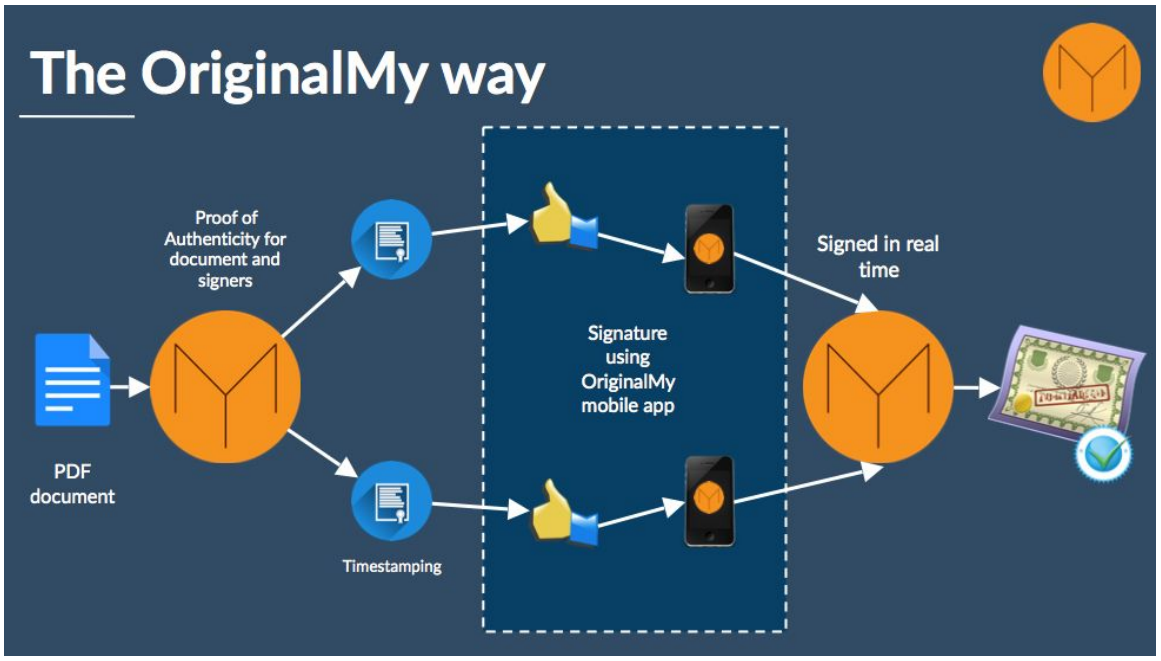


Fig.1: Example of OriginalMy Platform usage: Signing documents and contracts with identity validation

5. Current Platform: Applications and History

5.1 Proof of Authenticity

The OriginalMy Platform was released on July 18, 2015 during Bitconf III, an event that took place in Florianópolis, Brazil. At that time, the platform used to provide registration of Proof of Authenticity regarding digital documents in blockchain, dealing with digital signature and timestamp provided by Bitcoin blockchain.

5.2 Signing of contracts - 1st version (discontinued)

Right after the release, OriginalMy have verified demand for signature solutions regarding documents registered in blockchain (i.e., providing consent or agreement to the content of the documents). In analyzing the main legal challenges regarding existing Digital and/or Electronic Signature means, OriginalMy came to the conclusion that the major issue concerning digital environments is the proof that individuals expressing will are in fact the person who should do it.

On this specific topic, it is worth mentioning that both traditional technological solutions and those developed with blockchains assume that possession of a password or private key is sufficient for proving identity purposes. However, such assumption has proven to be ineffective in Authenticity ensuring, given the increasing amount of digital fraud (through hacking, malware or simple "white frauds" [12]), and regulated industries reluctance to migrate registrations and verifications to the digital environment.

Our first approach to solve this issue was also in 2015, when we developed the first version of the documents and contract signature system by means of video-testimony on which it could be applied biometric verification to detect and evaluate several control mechanisms such as speech stress level, micro facial expressions, among others.

Although this model was legally validated, it did not achieve the expected adherence because it had a significant transition cost: people traditionally sign documents but not state in video their agreement to its content.

Therefore we began to study and develop a new model of electronic signature that had the same legal consequence, but with a more friendly usability. In order to ensure that an Electronic Signature not being questioned concerning authorship, a fraud-resistant user identification layer would be required.

At the beginning of 2016 we started to develop a new model that would make it possible to prove the Authenticity of legally perfect acts, through unquestionable identification of users and at the same time to be used in signing documents and contracts reducing discomfort of video-testimony.

The described signature model has been updated to a new one, with better usability, and then was made available only for legacy browsing.

5.3 Mudamos+ Project

As soon as the protocol was redesigned, ITS-Rio (Institute of Technology and Society of Rio de Janeiro) invited us to prototype solutions that could enable the signing of Popular Initiative Projects [13].

Using the new signature identification model developed by OriginalMy, ITS-Rio was granted the Google.org Social Impact Challenge award in 2016 [14]. Thus, we developed the entire layer of identity and signatures in blockchain, based on a customized version of the protocol we had designed.

In addition, to increase security and mitigate the risk of fraud, the app makes Proof-of-Work for each signature executed (generating a single-transaction block) on the user's mobile device. This proof-of-work is based on the hashcash[16] algorithm, the same one used by Bitcoin to validate transactions and avoid fraud.

Mudamos+ already has more than 270 thousand unique registered users, 500 thousand downloads and 240 thousand signatures made using the customized engine developed by OriginalMy, with several Brazilian federal entities signaling acceptability of law projects to be signed through the app.

5.4 Proof of Authenticity for Web Content

After some demonstrations of the first applications, we were presented with the necessity of a proof of web content authenticated in blockchain, with timestamp, on an automated way. The content to be registered could come from slanderous acts committed in social networks, for instance, and its evidence would be used in court to prove that certain content was available on the Internet at some point in time.

Furthermore, we developed a plugin for the Chrome browser which collects an electronic version of a visualized content (preferably through a Permalink), generates a report in compliance with the legal requirements as it might be used as an evidence, and automatically registers the Authenticity of this report in blockchain.

5.5 Blockchain ID: registration and identity management

Method from which a customized version for the *Mudamos*+ project was derived, our method of registration and identity management ("Blockchain ID") proves that a certain user is the one who it alleges to be, as well as all verifies the acts performed by the user (authenticity of authorship).

We started the development of this protocol [17] in April of 2016, assuming lack of reliability of the current Electronic Signature models and the requirements to verify identities Authenticity, according to the regulatory framework of several countries and also using as reference several open protocols such as BitID [18].

Blockchain ID was created towards formalization of legal business by means of electronic signature of contracts and documents, without weaknesses of current Electronic Signature systems which can not assess authorship.

The method of registration and identity management developed and made available through Blockchain ID has proved to be incredibly effective, and although there are important improvements to be developed and implemented (as explained below). It is used too as a form of digital KYC, avoiding the need for passwords to access websites or to fill in registrations (sign up).

Among many differentials features regarding the proposing identity systems and KYC mechanisms based on blockchain existent so far in the market, we can list the following:

1) No cost is expected for registering identities. We believe access to the network should be free to all users who desire to have a Blockchain ID;

2) Recovery of Blockchain ID will not rely on the consent of third parties. We understand identity is a human right and, thus, its granting or recovery should not be subject to the power or interference of any third party;

3) Biometric use in order to access or perform sensitive actions ensures that the identity stored in the device may only be used by the owner of the device;

4) At no time user information are publicly exposed;

5) The solution presented by OriginalMy is the only one that provides (complex and automated) validation of the data provided by the user at the time of registration.

6) In addition, it is also the most complete solution in the market since it has the following security controls, constantly improving:

    a) Biometry;
    b) User and password;
    c) Full Attribute Record;
    d) Automated validation of registered data by means of information search in public networks, OCR and image reading;
    e) Blockchain ID stored only on device;
    f) And, in case of signature of contracts, it proves document possession.

5.6 Contracts Signature - 2nd version (current)

After finishing the identity management layer, we developed the 2nd version of the contract signing platform. First, the Bitcoin network was used and, after a significant increase in the fee value of the transaction in May 2017, it was migrated to the Ethereum platform and, subsequently, to the Ethereum Classic.

The contract signing platform was officially launched in May 2017 during the Consensus Conference in New York. Available in the Apple Store and Google Play, the application allows Brazilian users to sign up (i.e. get their Blockchain ID) and then easily sign documents mitigating any friction (such as video-testimony).

Additionally the digital document duly signed is also registered, and it is possible to verify its authenticity through the OriginalMy Platform or directly, on Ethereum Classic network.

5.7 Sidechain

Current blockchains have scale challenges, both in terms of the transactions per second rates (tx/s) and cost of transaction (fee).

The blockchain of the Bitcoin network was designed to register 7 tx/s but it actually performs only 3 tx/s while Ethereum, theoretically designed to register tens of thousands transactions per second[19] has reached its limit on 15 tx/s.

Furthermore, blockchains that count on more entropy have a very high cost to record Information, limiting its scale gains due to both transaction flow and cost.

Because of the given reasons, we are using a customized version of Decred's DCRTime project[20] for documents Registration of Authenticity, which is based on the open timestamps standard [21] to provide scaling in the digital document timestamping process.

By implementing this functionality, we got a significant improvement in transaction processing, enabling management of millions of transactions per second without loss of performance or significant increase of the costs.

We intend to study the evolution of this format also for the signing of documents and contracts, in order to allow greater gains in scale, both in processing volume and in price reduction.

In the future, once the expected implementation of contract execution is completed, the sidechain will be made available as an open source platform.

5.8 Multiple Blockchains

When it was released in 2015, OriginalMy registered the Authenticity of documents only in the blockchain of the Bitcoin network.

With the evolution of blockchain-based protocols and considering that we are agnostic about the blockchain used, OriginalMy Platform provides registering in 4 public blockchains in addition to other private ones, being the most relevant:

- Bitcoin: www.bitcoin.org
- Ethereum: www.ethereum.org
- Ethereum Classic: www.ethereumclassic.org
- Decred: www.decred.org

In this way, the Platform was designed to be very flexible, making the registering according to the needs of the clients that integrate the APIs environment.

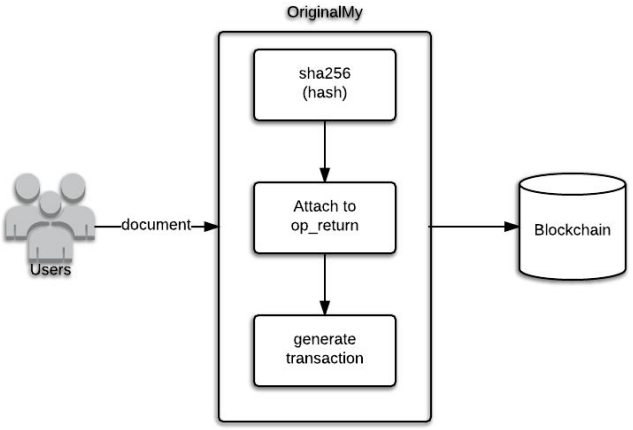
A worth point is the way OriginalMy Platform was designed and developed: it enables integrator agents to develop their products or integrations without the need of knowing details about existing blockchains.

6. Specifications

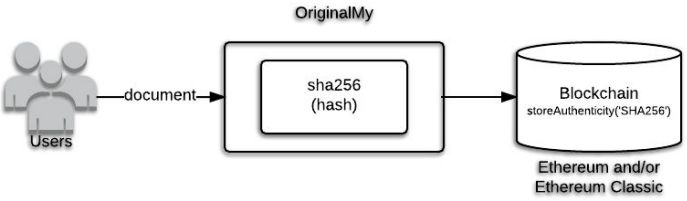
6.1 Proof of Authenticity for digital documents

Initially, the Authenticity registering was made with the document Digital Signature (SHA256 [22]) stored in the op_return field [23] of the Bitcoin network transaction. After the addition of more blockchains, this format was made according to the protocol used.

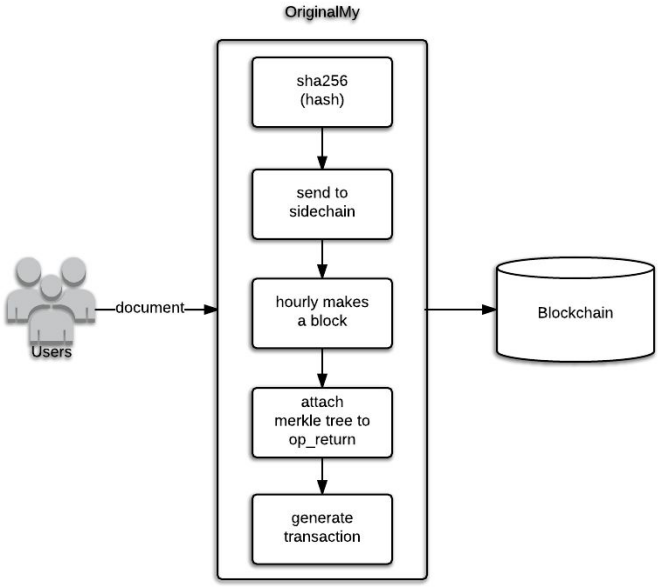
- Bitcoin: (sha256 + Brazilian legal time + OM marker) attached to the op_return



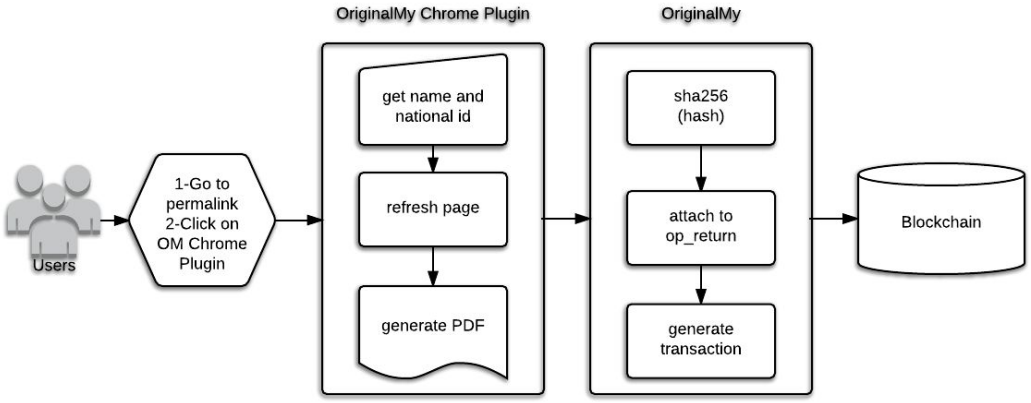
- Ethereum: https://github.com/OriginalMy/originalmy-dapp-addresses
    - Mainnet Ethereum >> Document Authenticity
- Ethereum Classic: https://github.com/OriginalMy/originalmy-dapp-addresses
    - Mainnet Ethereum Classic >> Document Authenticity



- Decred: (merkle tree + OM marker) attached to the op_return



6.2 Proof of Authenticity for Web Content



The registration process is the same for the Proof of Authenticity of digital documents in each blockchain.

6.3 Blockchain ID

At the moment the user signs up on the app, the registration goes through several automatic validations, in three steps:

6.3.1 App Registration and Preliminary Validations

1. User and password creation;
2. E-mail validation;
3. Validation of phone number and mobile device;

4. Validation of the *CPF* on public government databases;
5. User selfie photo is taken directly via app;
6. Photo of the identity document is required in order to identify both the user and the identification document number; and
7. Creation of a Blockchain ID, whose private part is stored only in the user's mobile device, without contact with others nor our systems. The public information is sent to our servers for final validation.

Our systems, employees and cooperators do not (and never will) have contact with the information used to generate or recover the Blockchain ID, being such information unique to the user.

The Blockchain ID is currently associated with the user's taxpayer registration number (*CPF)* publicly in a blockchain, allowing creation of only one per single user and enabling verification 24 hours a day, 7 days a week.

6.3.2 Automatic search on public networks

After the creation of an account and Blockchain ID, the system searches government public databases for CPF number validation purposes, by means of comparison of the data previously provided with those publicly verifiable.

6.3.3 Automatic document validation

After validation of the CPF number, other data and Information on public networks, the system automatically sends to OriginalMy validation team the Information that requires manual validation. If any type of inconsistency is detected, the registration is blocked. The user may only use Blockchain ID after providing valid information.

6.3.4 Granting Blockchain ID

Blockchain ID is created using asymmetric key cryptography based on blockchain technology.

Blockchain identities are publicly stored in blockchain:

- Ethereum Classic: https://github.com/OriginalMy/originalmy-dapp-addresses
    - Mainnet Ethereum Classic >> CPF IDs and wallets repository

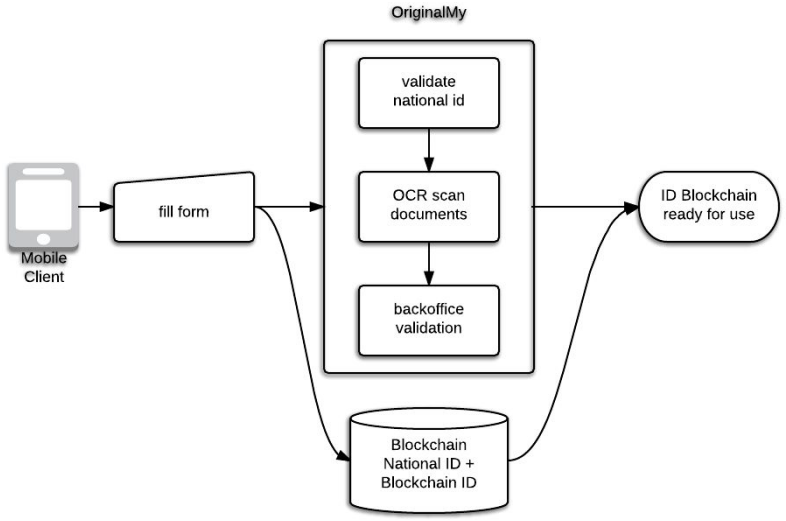
6.3.5 Blockchain ID Recovery

In case of phone device exchange, reinstallation of the app or login to a new device, the system will request data validation.

After that, the system will provide an opportunity to recover the previous Blockchain ID. It will require a set of 12 words (provided at the time of Blockchain ID creation) which will enable the recovery of Blockchain ID.

However, if the user does not have the words or misses several times, the system will automatically process the creation of a new Blockchain ID, as it would be done in the initial registration process.

The new Blockchain ID will succeed the old one and will be linked to the user both in his new device as publicly registered in blockchain. Thus, any history of signed contracts and registered documents will remain intact.



6.4 Signing documents and contracts

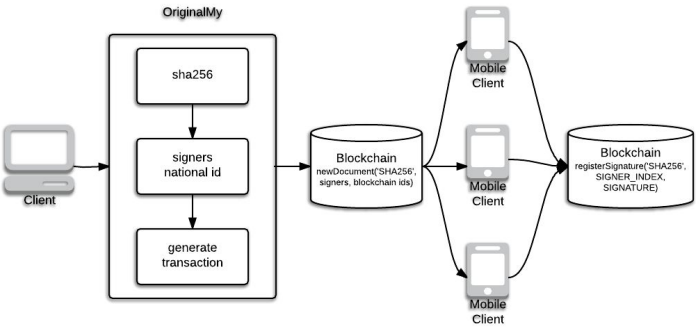
Contracts were initially signed by using the blockchain of the Bitcoin network and then migrated to Ethereum Classic because of cost and performance.

In this sense, the Ethereum Classic network, besides being cheaper, has a faster transaction rate: while in the Bitcoin network it takes 10 minutes for a document to appear in the user's subscription application for signing purposes, by using Ethereum Classic the same result can be reached within 15 seconds.

6.4.1 Using the Ethereum Classic blockchain

After having identity validated in our system, the user can use it to perform actions on a digital environment, from logging on another platforms that use OriginalMy ID services without needing to fulfill a new application (sign up) and login to websites (sign in) without exposing passwords, to online signing legally accepted, binding and enforceable documents.

Signing documents is carried out through the mobile app OriginalMy (Android and iOS), proving the authorship and document proof of possession at the signing time.



After all signatories have signed the document, the smart-contract changes the flag from *checkCompleted* to *True*. Any other third-party smart-contracts that are monitoring the signing process can automatically continue their processes from this point.

6.4.2 Using the Bitcoin blockchain

Although not currently used for cost reasons, this protocol was developed prior to migration to other blockchains and may eventually be reconsidered.

If this is the case, the process will follow the flow below:

Register:

1. On the OriginalMy site the original contract is provided and the *CPFs* of the signatories are listed.
2. Creating 1 transaction with the information:
    a. System generates a wallet address to identify the contract (contract address)
    b. Register on op_return: [sha256 + wallet of contract + OM marker]
    c. Search in the smart-contract of IDs (IdRepo) by the Blockchain ID of the listed *CPFs;*
    d. Generated wallet addresses with CPF in hash160: [sig; CPF] Generated wallet address with Brazilian legal time in hash160: [t; timestamp]
    e. Sent dust to register *CPFs* and legal time.

Validation:
Verify contract address and find interactions with Blockchain User ID.

This interaction will only occur if the user provides document Signature using the mobile app, proving the authorship and performing the proof of possession of the document at the signing time.
Example of contract record transaction:
https://blockchain.info/pt/tx/523e63ad8a1cd928e7a5292f7145af3596bb11475750b466319e74d77003ef24

Explanation:
tx: 523e63ad8a1cd928e7a5292f7145af3596bb11475750b466319e74d77003ef24

- 1HyuB5rM3ZpP1cHqTCJLGs65usNkzDZiUU: blockchainID of signatory 1
- 1BXEycBEfCqYgPGebhkLBwKrp4VpbiHszV: nationalID of signatory 1 (hash160 hex encoded)
- 1KaRgqmRSLwYFfeyHgpQaSnLsK3bVwpUqc: blockchainID of signatory 2
- 1BXEycBDsSGSGmWqgd6KrQN4Hu8RKTDCCa: nationalID of signatory 2 (hash160 hex encoded)
- 1BbaJGRHWCfX18bFKqyTSHGEm8QS7MBXAx: legal time (hash160 hex encoded)

op_return
- sha256: 971bbbc7e67522ec7df3fd523bf9d83899f376d0b3c66d5a2776420b178a84743
- wallet of contract: 15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR
- marker OM: ORIGMY

Example of transactions of signature for this contract:
https://blockchain.info/address/15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR

- wallet of contract: 15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR

Verify if *1HyuB5rM3ZpP1cHqTCJLGs65usNkzDZiUU* and *1KaRgqmRSLwYFfeyHgpQaSnLsK3bVwpUqc* had interactions with this contract address. This means that both have signed the document.

7. New Platform

The present crowdsale aims to start a new phase in the development of the OriginalMy Platform. The new platform will bring global solutions for identity, documents and signatures registrations in a digital environment, as well as trigger the process of complete decentralization of the Blockchain ID.

Once Phase 01 of the crowdsale is successful (see item 8), a new, specific and decentralized blockchain for optimized Authenticity registrations will be designed. Such protocol shall take into consideration digital identification mechanisms, including the ones adopted in some applications already developed by OriginalMy.

It is important to emphasize that the process of decentralization of Proofs of Authenticity, besides being a technological challenge, involves dealing with traditional institutions, both public and private, that exist for the sole purpose of centralizing information. Because of that, we chose a gradual process of network creation and gradual decentralization, and the ABC tokens offer was similarly divided into two stages.

7.1 Internationalization

The first goal to be achieved once the crowdsale results successful is the internationalization of the OriginalMy Platform. In order to do so, substantial changes will be made to allow registration in Blockchain ID by users from other countries, according to the Roadmap herein.

7.2 User Experience

We are aware that blockchain-based applications need to solve real problems without significant friction or transaction and/or transition costs. Thus, one of the main goals will be to make substantial improvements in the navigability of applications that are already available on the website and through mobile applications.

7.3 ABC Token

All features made available through the OriginalMy Platform shall only be accessible through the ABC token (see Roadmap for implementation). In this sense, the ABC token will entitle the use of every application available in the OriginalMy Platform and the access to specific network incentive programs. Users will be able to purchase ABC tokens from crowdsale participants (secondary market) or directly from OriginalMy, according to certain rules (OTC OriginalMy).

7.4 OTC OriginalMy

In order to make the universal use of the OriginalMy Platform possible, in we intend to create our own over-the-counter market, through which ABC tokens will be sold directly to those who wish to use our services. The price for use, which for purposes of mere reference is currently set at R$ 5.20 (US$ 1.66) for retail, may vary according to the volume, services and the blockchains used.

Once the OTC is available, OriginalMy shall make its best efforts set its minimum sale price above the secondary market price. Currently, we estimate that the price of the ABC token sold through OTC will be at least 20% (twenty percent) higher than the weighted average price, to be accrued by considering the volume of tokens traded in the 30 previous days in relevant secondary market that registers the higher volume of ABC token negotiations:

$$OTC\ Sale$$

$$min.\ Price = 1,2 \times \frac{\sum_{i=1}^{n}(pi \times xi)}{\sum_{i=1}^{n} pi}$$

At where:
p = volume of ABC Token trading in the most liquid secondary market in the last 30 days; and

x = ABC Token trading price in the most liquid secondary market in the last 30 days

Moreover, according to OriginalMy's discretion, an ABC tokens repurchase program may be released. Shall that be the case, OriginalMy shall make its best efforts to offer to pay a maximum price, lower than the average secondary market price one. Currently, we estimate that the highest price for ABC tokens to be repurchased shall be of 80% (eighty percent) of the weighted average price, to be accrued by considering according the volume of ABC tokens traded in the 30 prior days in relevant secondary market that registers the higher ABC token trading volume:

$$max.\ Price = 0,8 \times \frac{\sum_{i=1}^{n}(pi \times xi)}{\sum_{i=1}^{n} pi}$$

OTC Purchase

At where:
p = volume of ABC Token trading in the most liquid secondary market in the last 30 days; and
x = ABC Token trading price in the most liquid secondary market in the last 30 days

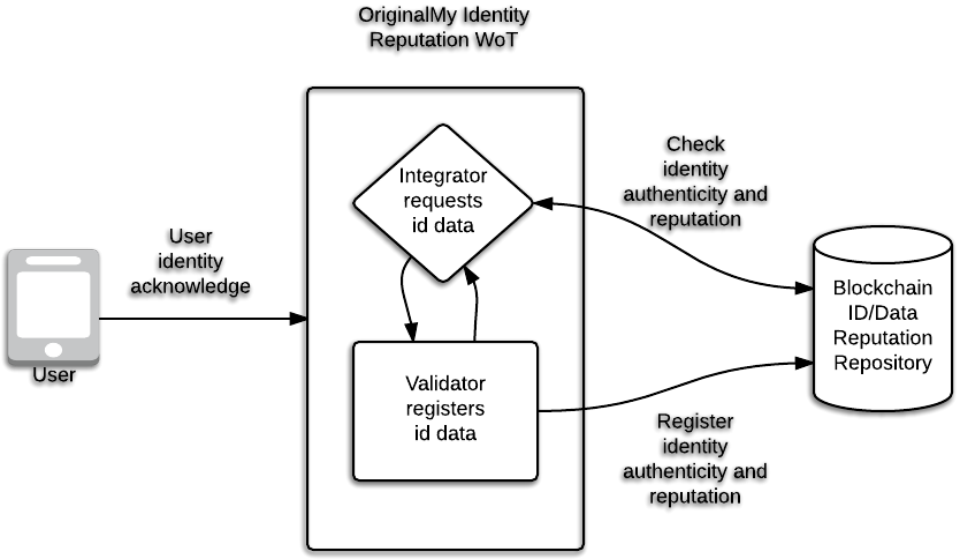
We reserve the right to change the rules herein in a timely manner if it is necessary for the proper conduct and development of our business, at our own discretion. If this is the case, we shall seek to balance any rules' changes to the interests of the ABC token holders. Any modifications shall be broadly disclosed through our official communication channels.

7.5 Decentralizing the Blockchain ID

The Blockchain ID solution can bring countless benefits to companies in many industries and to society, through applications both developed by OriginalMy and by third parties. For this to be possible, one of the key measures will be decentralizing the process of creating and validating identities and attributes in blockchain, thus encouraging the creation of substantial network effect and incentives for a massive adoption of such platform.

Using Web-of-Trust resources associated with decentralized blockchain Authenticity, it will be possible to access the consistency and reputation of each attribute that are pegged to user's identity.

In this sense, OriginalMy will be responsible for providing the architecture and design of such new protocol, planning it the step-by-step in order to safely decentralizing the Blockchain ID, to create and actively contribute for such new decentralized network creation, through a specific incentives' system that encourages and rewards users' IDs and attributes registration, validation and revalidation ("Proof-of-Authenticity").



8. Crowdsale: ABC Tokens

The token sale process has been splitted into 2 different phases, given that it is the first utility token crowdsale held in Brazil and one of the first in the world that aims to tokenize the entire economy of a technology platform, already developed and in production.

Thus, as a cautionary measure taken due to the respect we have for those who shall participate in this process, we found it feasible and recommendable to divide the tokens sale into two different stages, aiming for a gradual process of decentralization and the organic creation of a decentralized network.

8.1 Phase 01

Phase 01 of the ABC tokens sale is raising funds for the platform internationalization, including multiple countries' ID public database research and validation, and significant improvements in user experience (items 6.1 and 6.2). For this, the minimum crowdsale overall contribution must reach at least USD 1,000,000.

Furthermore, should additional resources be available, it will be possible to expand the platform to more countries, to implement the complete tokenization of OriginalMy Platform and the OTC OriginalMy (items 6.3 and 6.4). In order to do so, the crowdsale contribution must reach at least USD 3,000,000.

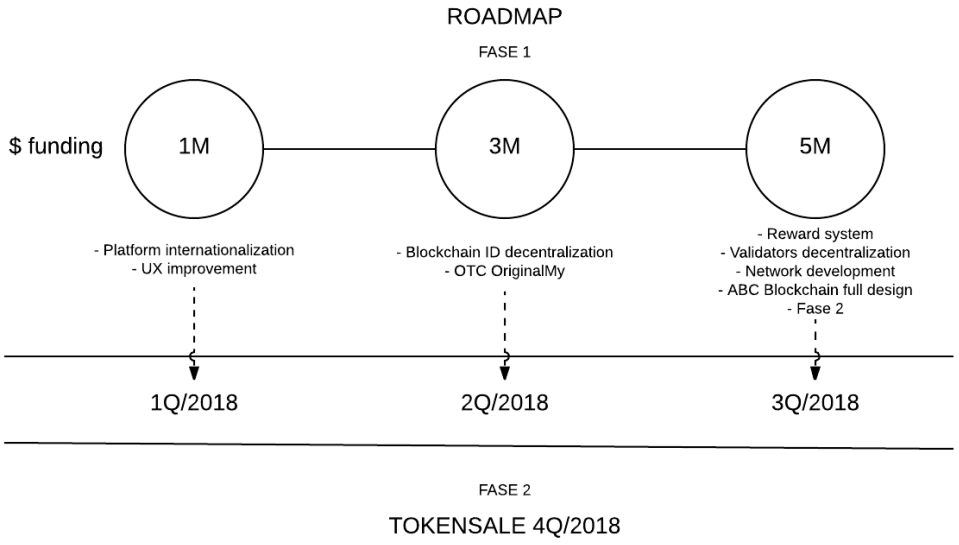
Finally, should the overall contributions reach the hard cap amount (USD 5,000,000), it will be possible to decentralize data validators, create a reward system for them and users, promote a global network and prototype a new blockchain specific to deal with Authenticity (item 6.5). That will help to speed up the new protocol creation before Phase 02 starts.

8.2 Phase 02

The Phase 02 of the ABC tokens crowdsale is expected to happen after complete execution of the Roadmap and will raise funds for the complete development of a new protocol for decentralized ID and attributes registration and verification, from people and organizations, which shall contemplate a new open-source blockchain.

A blockchain dedicated to such purposes could promote scalable low cost registration, which are much limited in the current blockchains.

The crowdsale conditions shall be disclosed in due course and the ABC tokens to be offered at such stage will be issued along with all ABS tokens and reserved for such opportunity.



8.3 New blockchain and token swap

Once the all the phases of the ABS token sale are successfully complete, a new open-source protocol will be developed for decentralized processing of authenticity registering, which will rely on a specific blockchain, with own mining system and incentives (see item 7.5).

In this case, OriginalMy will establish a program to replace the ABC tokens previously issued and by that time used to access the OriginalMy Platform, as well as a reasonable and widely reported schedule for exchanging them for tokens to be issued by the new protocol, at a 1:1 ratio.

The replacement of the ABC tokens issued by using the Ethereum platform by the new tokens will be done using Atomic Swap[24] or similar technology .

8.4 Token Sale Schedule

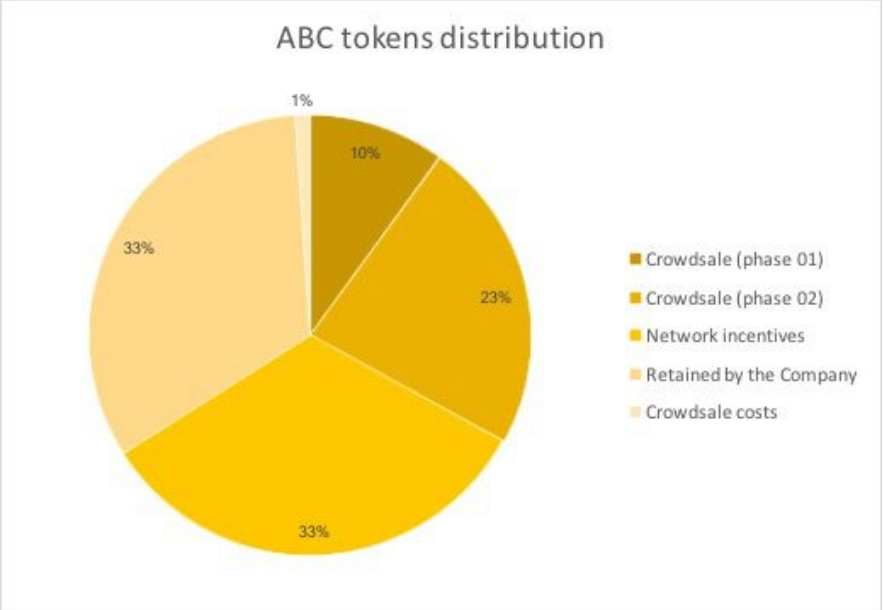
The Phase 01 Token Sale will follow a pre-established schedule with Key Dates that will guide the whole process.

It is expected to end after the sale of all the available ABC tokens for this phase or when the deadline is reached, whichever comes first.

The Key Dates for Phase 01 of the token sale are:

8.5 Tokens issuance and deadlines

- Total of Tokens: 200,000,000 (two hundred million) tokens will be issued, to be distributed as follows:
    - 33% will be made available for the Token Sale (Phase 01: 10%, Phase 02: 23%);
    - 33% remain in the company's possession;
    - 33% will be used for network development;
    - 1% will be used for crowdsale expenses.



- Tokens granted to the Team (with or without vesting): **no** tokens will be distributed nor granted as any type of compensation to the Team during Phase 01. Such policy may be revised when Phase 2 takes place, what will be opportunely disclosed.

- ICO Launch: on October 7, 2017 the exclusive ICO website will be launched. It will contain the whitepaper and other documents of the project, as well as token sale information. Prospective crowdsale participants can register as of such to receive updates on the token sale.

- Pre-Sale: the ABC Tokens pre-sale will be carried out between October 20th and 27th, 2017. The purchase of ABC tokens during such period will enable the buyer to acquire a greater number of tokens in relation to the maximum possible purchase to be made available after opening the token sale.

- Crowdsale: the ABC token sale is expected to take place between October 30th and November 30th, 2017.

- ABC tokens distribution: our expectation is that ABC tokens distribution will take place approximately one month after the end of the token sale.

8.6 ABC Token Sale terms and conditions - Phase 01

For the token sale to take place in an organized manner and as a way to allow the engagement and participation of as many people as as possible, some rules must be observed:

- Official channel: the token sale shall take place **exclusively** in https://originalmy.com/ico, where ABC tokens will be purchased, as long as crowdsale rules are observed. OriginalMy shall not be deemed responsible for any offer, purchase and/or sale occurred or that is by any means negotiated outside the aforementioned website.

- ABC Tokens: the ABC tokens will be issued by using the Ethereum platform, in ERC20 format. There will be issued the total of 200 million ABC tokens.

- Tokens availability: the total ABC tokens made available through crowdsale phases will correspond to 33% of the overall ABC tokens issued. In that sense, 20 million, (10% of the total ABC tokens) will be available for sale on this opportunity (phase 01), at the cost of of $ 0.25 each token.

- ABC Token Batches: ABC Tokens made available for sale in Phase 01 will be separated into batches, to be announced at the time of opening of sales.

- Limit of participation: the ABC token purchase in this phase 1 is limited to one (1) batch of tokens per participant. Once the purchase is completed, it will not be possible for the same person to make a new acquisition of ABC tokens in this crowdsale phase.

- Payment method: the ABC tokens purchase can only be paid with Bitcoin (BTC) or Ether (ETH). No other means of payment are accepted.

- Payment addresses: Bitcoin and Ethereum payment addresses will only be provided by the time of payment, exclusively through the crowdsale site. OriginalMy will not provide payment addresses by any other means, nor will it authorize others to do so on its behalf. Therefore, OriginalMy shall not be deemed responsible for any payments made to Bitcoin or Ethereum addresses other than those made available on the official crowdsale website.

- Payment confirmation: the payment for the ABC Tokens will only be considered as confirmed after a minimum of 6 confirmations by the Bitcoin network or 30 confirmations by the Ethereum network. Once the transaction is confirmed, OriginalMy will send an email notification informing the success of the participation in the crowdsale.

- Divergences in paid amount: payments received in amounts different than the due cost to acquire the ABC Tokens placed order will be refunded to the address informed by the participant. Shall divergence in the paid amount occur, the purchase order shall be deemed incomplete and will be canceled.

- Payment deadline: once the purchase order of the ABC Tokens has been placed, the payment must be made by the participant within 30 minutes thereafter to the Bitcoin or Ethereum address disclosed at such opportunity. In case the payment is not confirmed before the deadline, the correspondent ABC token purchase order will be canceled.

- Minimum contribution amount: the crowdsale will be canceled and all purchases will be refunded if the sale of tokens does not reach a minimum of US $ 1,000,000.00;

- Refunds: In the case of an event that results in payment refund, as per herein stated, such amount will be reimbursed to the provided refund address. Mining fees charged in the event of such refunds will be deducted from the amount originally deposited, in which case the net amount will deposited.

8.6 Legal Provisions

a) Legal overview on OriginalMy Applications

The applications offered through the OriginalMy Platform were developed in accordance with the Principle of Legality applicable to individuals and based on the dictates of Brazilian legislation (in particular, Law of Public Registries [Law 6.015/73], Digital Procedures' Law [Law 11.419/06], legislations on digital signatures [Provisional Measure 2200-2/01 and Law 12.682/12], KYC and Anti-Money Laundering guidelines and policies issued by the Brazilian

Financial Activities Control Council (COAF), the Brazilian Central Bank (BACEN) and the Brazilian Securities Commission (CVM). It also considers foreign legal rules (especially in EU Directive 2015/849, Financial Action Task Force (FATF), as well as foreign guidelines and regulations on KYC/AML and CTF.

b) Legal overview on ABC Tokens

ABC Tokens represent a license to use products and/or applications to be made available at OriginalMy Platform, in accordance with terms and conditions to be opportunely disclosed.

Accordingly, the ABC tokens do not have, by definition nor by purpose, the scope of representing any type of investment with the expectation of profit. Thus, sure tokens are not to be considered not treated as securities, as they do not confer to their owners any type of earnings expectations through the distribution of any amounts and/or dividends nor do they confer current or future political or economic rights on OriginalMy to the token holders.

9. Team

OriginalMy team is formed by experienced and outstanding professionals, successful in their respective expertise areas.

Edilson Osório Junior - Founder & CEO

Computer Scientist, data processing technician, professor and information security and infrastructure specialist, with 25 years in the area. Graduated in Copyright at Harvard Law School. Blockchain reference in Brazil and Latin America, has trained hundreds of developers and brought the subject to the Brazilian Market. Speaker at public and private events, including international ones, on blockchain and the disruption brought by OriginalMy.
https://www.linkedin.com/in/osoriojr

Miriam Tomie Oshiro - Co-founder & CFO

Chemical and chemical engineer specialist in engineering process, started her career in 2002 at the Chemical Engineer Department of USP, in the scientific research area focused on environment, and then worked for multinational companies at the environment, plastic, precious metals and heavy machinery field. Was also operations director at Daruni Healthcare for 4 years.
https://www.linkedin.com/in/miriam-tomie-oshiro-6a4b9223

Renato Martins da Silva - CTO

Developer (FIAP), working as such since 2001.

Worked for larges document management companies in Brazil and on processing/document classification projects for the government.
https://www.linkedin.com/in/renatomartinsdev

Helena Suarez Margarido - Legal & Compliance

Lawyer (PUC-SP), also studied in the US and Europe (LLM - University of Illinois and UCP Lisbon). Blockchain & Cryptocurrencies specialist for over 5 years. Teacher and speaker, in Brazil and abroad, counts on than 15 years experience (GP Investments, PwC and Itaú). Founder of SuM Law, Inversa Publicações writer and Bitcoin Brasil Institute co-founder.

https://www.linkedin.com/in/helenamargarido

Rafael Matos Araújo - Developer

Mechanical Engineer (PUC Minas). Worked for 5 years in the Industrial Engineering sector for large Brazilian companies, such as Vale do Rio Doce and Petrobrás.
https://www.linkedin.com/in/rafamatosaraujo

Renato Novaes de Abreu Neto - Developer

Self-taught and technology enthusiastic. Focused on web programming. Experience with Chatbots and Web Crawler Processing.
https://www.linkedin.com/mynetwork

Fernando Henrique Corrêa - Developer

Started his career developing on open-source softwares in 2004. Previous works include developing softwares for nightclubs, pubs and restaurants. Worked for Mandic (pioneer on internet services in Brazil). Has also worked as a member of UOL (most recognized news website in Brazil) using DevOps focused on development environment infrastructure.
https://www.linkedin.com/in/fernando-henrique-corrêa-98b55920

10. References & Bibliography

10.1 References

[1] 2017 Index of Economic Freedon: http://www.heritage.org/index/country/brazil (acessado em Out/2017)
[2] Ministério Público Federal: http://www.mpf.mp.br/para-o-cidadao/caso-lava-jato/atuacao-na-1a-instancia/parana/resultado (acessado em 04/10/2017)
[3] G1: http://g1.globo.com/pr/parana/noticia/2015/11/pf-estima-que-prejuizo-da-petrobras-com-corrupcao-pode-ser-de-r-42-bi.html (acessado em 04/10/2017)

[4] Banco Central do Brasil:
http://www4.bcb.gov.br/pec/taxas/port/ptaxnpesq.asp?id=txcotacao (acessado em 04/10/2017)
[5] RIBEIRO, Mario Sergio - Pós Graduação Lato-Sensu em Gestão de Segurança da Informação no Instituto de Pesquisas Elétricas e Nucleares da USP (IPEN) - 2003
[6] Orange Book, cap. 5 e 6. - Padrões de Segurança do Departamento da Defesa dos EUA: Critérios para a avaliação de sistemas computacionais confiáveis.
[7] WEBER, Max. "O que é a Burocracia?", ed. Conselho Federal de Administração, p. 37
[8] OLIVEIRA, Gercina Alves de; "A Burocracia Weberiana e a Administração Federal Brasileira", 1970, R.A.P, Rio de Janeiro, p. 54
[9] YouTube: https://www.youtube.com/watch?v=gHK9HhzaPog
[10] Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto, Satoshi, cap 6: Incentives https://bitcoin.org/bitcoin.pdf (acessado em 02/10/2017)
[11] Ethereum Homestead:
http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html (acessado em 21/07/2017)
[12] Caracterizada pelo "empréstimo" de Informação ou qualquer dado próprio para utilização por terceiro, geralmente pessoa com vínculo familiar ou de confiança. Ex: utilização de cartão de crédito de um pai por seu filho, sem conhecimento ou consentimento do primeiro.
[13] Câmara dos Deputados: http://www2.camara.leg.br/participacao/sugira-um-projeto (acessado em 04/10/2017)
[14] Google Impact Challenge | Brazil:
https://desafiosocial.withgoogle.com/brazil2016/charity/its-rio
[15] Mudamos: http://mudamos.org
[16] Hashcash: http://www.hashcash.org
[17] Github: https://github.com/OriginalMy/OrigMyID
[18] Github: https://github.com/bitid/bitid
[19] Ethereum Blog: https://blog.ethereum.org/2014/10/21/scalability-part-2-hypercubes/
[20] Github: https://github.com/decred/dcrtime
[21] Open Timestamps: https://opentimestamps.org
[22] Wikipedia: https://en.wikipedia.org/wiki/SHA-2 (acessado em 21/07/2017)
[23] Bitcoinwiki: https://en.bitcoin.it/wiki/OP_RETURN (acessado em 21/07/2017)
[24] Github: https://github.com/decred/atomicswap

10.2 Bibliography

[A] Anti-Sybil Mechanism against Bogus Identities in Social Networks:
http://ijartet.com/papers/issue2/V01I020925.pdf (acessado em 04/10/2017)

[B] Verifying Program Executions Succinctly and in Zero Knowledge:
https://eprint.iacr.org/2013/507.pdf (acessado em 06/10/2017)

[C] Enigma: Decentralized Computation Platform with Guaranteed Privacy
https://www.enigma.co/enigma_full.pdf (acessado em 06/10/2017)

[D] Hawk: The Blockchain Model of Cryptography and Privacy-Preserving ...
https://eprint.iacr.org/2015/675.pdf (acessado em 06/10/2017)

[E] Pseudonym Parties:
An Offline Foundation for Online Accountability:
http://www.brynosaurus.com/log/2007/0327-PseudonymParties.pdf (acessado em 06/10/2017)