WHITEPAPER

v.1.0 updated 16.11.2017

Disclaimer

This document and any other documents published in association with CryptoAlias white paper relate to a token offering (ALS token) to persons (contributors) in respect of the intended development and use of the platform by various participants. This document is not an offer of securities or a promotion, invitation or solicitation for investment. The terms of the contribution are not intended to be a financial service offering document or a prospectus. The token offering involves and relates to the development and use of experimental platform (software) and technologies that may not come to fruition or achieve the objectives specified in this project. The purchase of tokens represents a high risk to any contributor. The tokens do not represent equity, shares, units, royalties or rights to capital, profit or income in the platform or software or in the entity that issues tokens or any other company or intellectual property associated with the platform or any other public or private enterprise, corporation, foundation or other entity in any jurisdiction. The tokens are not therefore intended to represent a security or similar legal interest.

Table of contents

Intro

Cryptocurrencies are seeing an increasingly greater interest from the general public. The adoption rate is steadily rising, however they are still a long way from catching up with fiat currencies in terms of market cap, and are even further away from replacing them. The main impediments for cryptocurrencies to reach mass adoption is their difficulty of use and the security risks associated with using them, such as phishing attacks and the irreversibility of transactions.

CryptoAlias intends to facilitate and accelerate the adoption of cryptocurrencies, by making Blockchain usage simpler, easier and more secure. Our first goal is to eliminate the need of explicitly using Blockchain addresses, similarly to how domain names eliminated the need of using IPs.

On our platform, users can link their digital wallet addresses to simple, personalized and unique aliases. Instead of explicitly using a long blockchain address in a wallet when sending funds, users can start using the short and easy to remember aliases.

Whether users choose to type an alias or copy/paste a blockchain address when sending funds, before confirming the transaction they will be able to review various information about the receiver, such as status, description, last alias update time, trustworthiness of the alias/address, thus greatly reducing the probability of sending funds to a wrong recipient.

Besides solving a security issue and preventing millions of dollars to be stolen, the major benefit of CryptoAlias is its ease of use and convenience. CryptoAlias will make the blockchain technologies more friendly and secure, thus attracting many more people to this new and exciting technology. However most importantly, CryptoAlias allows users to have an identity, without having to jeopardize their privacy.

1. Context

Blockchain is a secure platform but since it is used by humans, the system might be used to exploit human error and profit from it. To be more specific: the problem we are trying to solve isn't a Blockchain problem as a technology. Until now, the blockchain has proven to be a very secure technology. What are we trying to address is the human error which is exploited by humans.

One such exploit, is the fact that Blockchain addresses are hard, if not impossible, to remember. In order to send a cryptocurrency, users have to type the receiver's address, which is a long string of random characters. When users send their coins, they cannot know for sure if they are safely sent to the desired destination. One major risk is that the users themselves can misspell the blockchain address and irreversibly send the coins to somebody else. However, as proven repeatedly, an even greater threat is that the address can be replaced by an ill-intentioned person, and the user has no chance of noticing the difference.

To better illustrate this problem, let's take a look at the CoinDash hack. It is an ICO that ended soon after it began. It abruptly halted because the Ethereum address it was using to solicit funds from its investors was altered to a fake one by a hacker. This action resulted in ether going to another source than the one desired by investors. By changing the wallet address, hackers took $7.53 million worth of Ethereum[1].

The CoinDash hack inspired us to search for a solution to prevent similar problems in the future. We identified several issues that have to be solved in the Blockchain system, as well as the features that would alleviate them. In the next chapters we will present these issues and will illustrate how CryptoAlias can solve them.

[1] https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/

2. Problems

In this chapter we present several issues related to a Blockchain wallet address and the difficulties encountered by a user when sending coins.

- **Security**

  Cryptocurrencies reached a market cap of over 200 billion dollars in November 2017.[2] It is an attractive market with a big growth rate, but at the same time it is a huge attraction for hackers and mischievous people. A user without experience in the Crypto world might be unprotected when faced with scams, like in the case of CoinDash. As such, events like this draw attention to possible security issues in ICO funding and might provoke new restrictions from Governments, thus disrupting the trust and the growth of the market in general. If this problem won't be fixed, we will see an increase in frauds related to Blockchain wallets. Beside economic losses related to such hacking activities there are issues on trustworthiness. If these frauds will persist, users will get afraid about investing in ICOs and in Cryptocurrencies.

- **Complexity**

  The human brain is used to process simple and memorable elements, rather than complicated lists of random characters. Humans are good at remembering a few complex chunks of information while computers are good at remembering many simple chunks of information. It is a lot easier for a person to remember four photographs in great detail than it is to remember a list of forty-two-digit numbers; quite the opposite for a computer. The human brain is not good at remembering long lists of unrelated numbers, dozens of nonsense words, or lengthy grocery lists. From a practical perspective, this means that people are more likely to use something in a context they understand, or something that is emotionally important for them. Simply said, a Blockchain address has a complex structure and is difficult to remember. Because of its complexity people are prone to make mistakes. That is why, beside the security benefits of implementing CryptoAlias, another great advantage is simplicity (making the blockchain easier to use).

- **Standardization**

  We live in a world where every individual is unique. It's "cool" to personalize everything and to delimit ourselves from the crowd. Everyone is different and this is the beauty of our society. We live in a world of technology and have grown up surrounded by revolutionary discoveries in technology and internet. Blockchain is the new revolution and everyone will be a part of it. But Blockchain doesn't offer an identity. It doesn't offer the possibility to personalize the system. A user has a random set of characters among other millions who are part of Blockchain.

[2] https://coinmarketcap.com/

3. Solutions

CryptoAlias addresses the problems described in the previous section by allowing users to associate a blockchain address with a simple, user-friendly and unique alias. The easiest way to illustrate what CryptoAlias does is by using an example.

Bob is a web developer and accepts payments for his services on the following Ethereum address "0x7045275C5D1EDc11167ad4f5E8fE6FCD4aCD8af3". On the CryptoAlias platform, Bob associates his address with a unique personalized alias "Bob". Besides the alias, Bob also associates his address with the status "Active" and the description "Use this address to pay for website development. If you have any questions, contact me at bob@mail.com".

Jim is Bob's devoted client, who regularly sends Bob ether in exchange for his services. Instead of using Bob's blockchain address, Jim can start using the "Bob" alias instead. When Jim types either the "Bob" alias in a wallet or Bob's blockchain address, all the information about the receiver (such as alias/address, status, description) is displayed. Jim can review this information before confirming the transaction. For a quick demo of how CryptoAlias looks in practice, click **here**.

By implementing this system, CryptoAlias offers a number of advantages:

- **Identity**
  Anyone can get a personalized and unique identity on the blockchain. Initially, an identity will be any combination of numbers and letters, so users could get their name, their company's name, their favourite word, or something completely abstract as their alias.

- **Security**
  CryptoAlias prevents users from sending funds to the wrong address, as it's less likely to mistype a short and simple word than a lengthy string of random characters. If users continue to use blockchain addresses, they can use the shown aliases to confirm that they have the correct address. In addition, CryptoAlias makes it harder for attackers to trick people into sending them funds. For instance, if an ICO address is replaced, the new address will have a different alias (or none) and will thus be easier to spot. Moreover, addressing this security problem, enhances the credibility of the Blockchain system as a whole.

- **Convenience**
  CryptoAlias makes it very simple for clients to find you on the blockchain. Since aliases are short and simple, they can be typed from memory, saving the burden of finding and copy pasting a blockchain address. Moreover, aliases reduce the time spent on double checking the correctness of the long blockchain addresses.
  In addition, CryptoAlias allows the owner to change his/her wallet address, while maintaining the same alias. This change will be transparent for the clients, as they will continue to reach him/her at the same alias. However, in order to prevent malicious behaviour after an alias changes its owner, for a predefined period of time clients will be notified before sending funds to this alias and asked to carefully verify the correctness of the address. This notification will be displayed in the wallet along with all the other CryptoAlias information. As a result, the sender will be able to spot irregularities before confirming a transaction.

- **Information**
  Besides being associated with a unique alias, a blockchain address can also be associated with a status and a description. Statuses are predefined and vary depending on the wallet's purpose (i.e. personal wallet, company wallet, ICO wallet). For instance, in case of an ICO, the owners can choose between the Created/Started/Closed statuses. This way investors will receive precious information right when they introduce the alias/address in the wallet. The description can be used to inform clients about terms and services (for owned accounts), or to describe functionality (for contract accounts).

- **Portability**
  CryptoAlias is compatible with all blockchains. We aim to become the de facto standard for blockchain identity, similarly to how DNS is for the web. After implementing the CryptoAlias system for Ethereum, we plan to extend our platform for all major cryptocurrencies. A user will be able to use the same CryptoAlias for different cryptocurrencies, making the blockchain simpler. In other words, an alias will not be dependent on a particular platform. To exemplify, if someone owns the alias "JohnDoe", then they can reuse it across multiple blockchains (that are supported by the CryptoAlias system). On each blockchain platform they can set a separate status and description. As a result, CryptoAlias bridges the gap between different blockchains, as it brings together addresses from different blockchains under a single identity. One of the benefits is that by knowing your alias, clients can reach you on any blockchain without knowing the exact address.

- **Interoperable**
  A user will be able to use the same alias for different Blockchain platforms. However, CryptoAlias will prevent users to make transactions from an Ethereum wallet to an Alias which doesn't have an Ethereum address associated with it. The system will spot the differences and will warn the user. The same is available for all inter-platform transactions. However, in the future, if the sender wants to send funds from a different blockchain than the receiver's, then CryptoAlias will offer the option to make a conversion. For instance, if a user wants to send 10 ETC to an alias connected to an ETH wallet, CryptoAlias will let the user choose if he/she wants to make a conversion at the market rate and send the funds to the selected alias. This will save users time as they won't need an exchange to make the conversion.

- **Anonymity**
  CryptoAlias makes no concessions. Although users get an identity on the blockchain, they don't jeopardize their privacy. An alias corresponds to a wallet, not a person. Ordinarily, a person will have multiple wallets. It's up to the user to decide for each wallet if they want to choose an alias with their real identity or something totally unrelated to their persona.

4. General Rules

An alias can be any sequence of valid characters with the length between 1 and 40.

A valid character is:

- Any of the 26 letters in the English alphabet.
- Any of the 10 digits
- Any of the 4 symbols: "-" (hyphen/dash), " " (space), "." (dot),"'" (apostrophe/single quote).

To avid ambiguities, the following rules apply:

- Aliases are case insensitive. For instance, "John", "JOHN"and "joHn" are all representing the same alias.
- Letters "i" and "L" are considered the same. The main reason for this rule is that upper case "i" looks similar to lower case "L". To exemplify, if there is an alias called "internet", no one can create an alias called "Lnternet".
- Analogous to the above rule, the letter "o" and the digit "0" are considered the same.
- Symbols cannot be used at the beginning or at the end of an alias. In other words, the first character of an alias should be a number or a letter, and the last character of an alias should be a number or a letter.
- Symbols cannot be used 2 in a row. In other words, a symbol is always preceded by a letter or a number, and is always followed by a letter or a number.

In early 2018, we are considering to release aliases with the special character ":" (colon). Aliases containing colons won't be tradable or available for sale on our platform.
Instead, they will be free and will be reserved for users that authenticate through 3rd party services (i.e. Google, Facebook, Twitter).

For instance, the owner of john@gmail.com might authenticate on our platform with his Gmail account and will get for free the alias "gm:john". Or the owner of the Facebook account with the ID jim.doe might authenticate on our platform using his Facebook account and will get the alias "fb:jim.doe".

This initiative will help users to get started with CryptoAlias and has the purpose of stimulating the adoption of the platform. Users would be able to get a free alias in order to try out our platform and see its benefits.

5. Technology

The CryptoAlias technology can be split into two categories:

- **The decentralized technology** that runs independently without the team's involvement.
- **The centralized technology** that is managed by the CryptoAlias team

1.1. The decentralized technology

CryptoAlias is a decentralized application built on Ethereum. Once deployed, the system will be able to run independently without the team's involvement. All the data used by CryptoAlias is public and accessible to everyone on the blockchain. The most important entities in our system are:

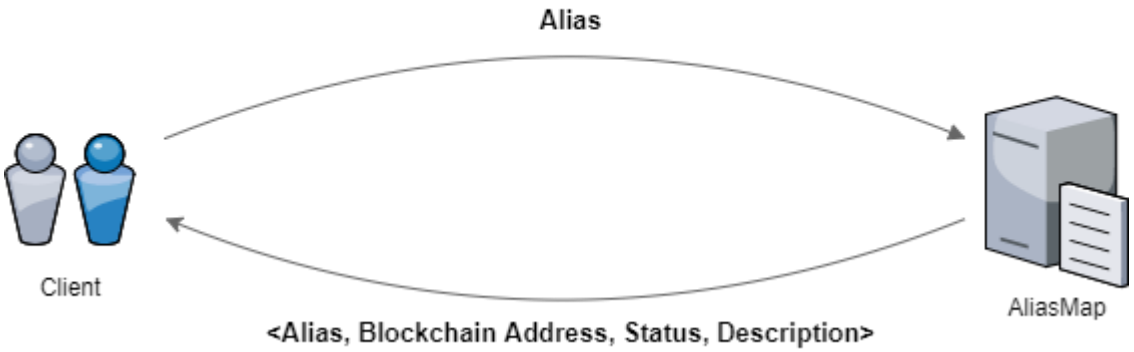
- The mapping between aliases and blockchain addresses (called AliasMap)
- The mapping between blockchain addresses and aliases (called AddrMap)
- The alias price table (called AliasPrice)

The architecture of our storage structures is strongly correlated with how people will use the platform. We foresee two main stages in the way people will use CryptoAlias:

- Initially, being used to the old ways, people will continue to copy/paste a blockchain address into a wallet when sending funds. In this scenario, CryptoAlias will have more of a security and information role, since users will look for the alias in order to confirm the correctitude of the pasted address, and since users will get relevant information through the status and the description fields.
  At this stage, the most common operation performed in our system would be querying by blockchain address (retrieving the alias, the status and the description using the blockchain address).
- In time, getting more used to the presence of the Alias and getting accustomed to the aliases of a certain vendors/recipients, users will start typing the alias directly into the wallet instead of typing the blockchain address. The main reason for this shift would be the ease and simplicity of typing in an Alias, rather than finding a blockchain address and copy/pasting it.
  At this stage, the most common operation performed in our system would be querying by Alias (retrieving the blockchain address, the status and the description using the Alias). As a result, planning for the long term, we designed the "query by Alias" operation to be the one performed most efficiently.

Next, we'll present a quick overview of each of the main entities specified earlier.

- **AliasMap**



There will be one AliasMap entity for each blockchain supported by CryptoAlias. For instance, when the system is launched there will be an AliasMap entity for Ethereum and an AliasMap entity for Bitcoin.

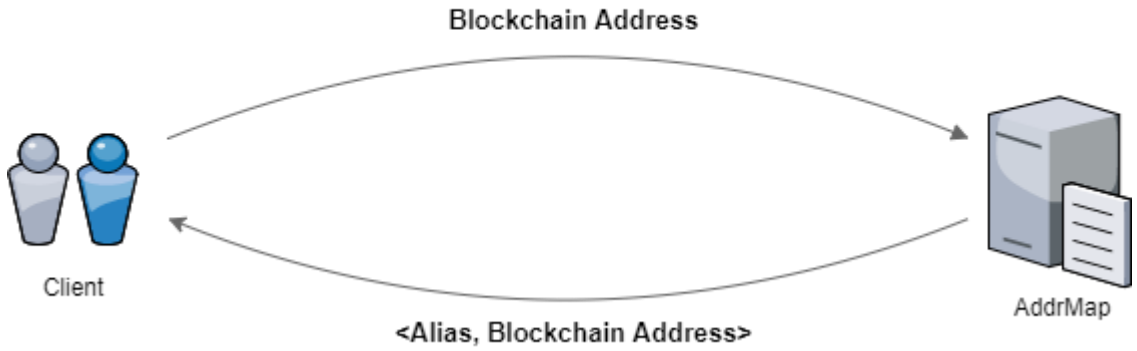
The AliasMap entity has 4 main fields: “Alias”, “Blockchain Address”, “Status” and “Description”. There will be other additional fields containing metadata as well (i.e. the last update time) but we exclude those here as they are irrelevant when explaining how the system works and just add complexity for the readers.

Since look-up will be the most common operation, the “Alias” column will be indexed using a hash-based partitioning. Let’s call the *“usage rate of the aliases of length N”* the number of used aliases of length N divided by the total possible number of aliases of length N (40^N in our case). The usage rate of shorter aliases will be much larger than the usage rate of longer aliases, as a result the hash function is designed to uniformly distribute aliases of the same length, which in turn will lead to all used aliases being uniformly distributed.
Because of the large number of possible Aliases, hash collisions are bound to happen. In other words, two different aliases may have the same hash and will thus be mapped to the same bucket. We address this by storing the Aliases inside a bucket using a balanced tree structure.
As a result, in the worst case scenario, the look-up time will be of the order $O(1) + O(\log K) = O(\log K)$, where K is the average number of aliases in a bucket.

Only one type of “Get” operation is allowed for this entity: querying by alias. Querying by the other fields is not supported.
The “Update status” and “Update description” operations are as efficient as the “Get” operation since they are based on it to find the record, and then the actual update is performed in O(1).

The “Create” (associate an alias with an address), “Delete” (remove the link between an alias and an address) and “Update address” operations are also based on the “Get” operation to find the record. However, in addition, each of these operations need to update the tree structure. Updating the tree structure will on average take O(logK) time. But since these operations will be performed much less frequently compared to the “GET”, they won’t affect the performance of the system.

- **AddrMap**



Similarly to AliasMap, there will be an AddrMap entity for each blockchain supported by our system.

AddrMap is essentially an index that for a provided blockchain address, returns its Alias. The data in AddrMap is a duplicate of the data from AliasMap, however the time benefits (faster loading times) of having this additional index outweigh the additional storage costs.

As mentioned earlier in this chapter, in the long term we expect that queries by Alias will happen much more often than queries by blockchain address. That’s why queries by alias can be performed in a single operation (a single query in the AliasMap table), while queries by blockchain address are performed in 2 operations (first Alias is retrieved from the AddrMap index, then the data is retrieved form the AliasMap entity).

- **AliasPrice**
  AliasPrice entity will contains only records of Aliases that are up for sale. Unlike the previous two entities, there will be one global AliasPrice entity as opposed to one for each blockchain.

Any modification of the data in the CryptoAlias system can be performed only through the CryptoAlias decentralized contracts. Some examples of supported actions are:

- Buying an alias
- Putting an alias up for sale
- Associating an address with an alias
- Updating the address/status/description of an alias
- Enabling/disabling an alias

Each call will perform its own set of validations before any modifications to the data are made. The most common validations are checking if the caller is the owner of the alias, the owner of the blockchain address, and checking if the caller has enough ALS to perform the action.

Although the decentralized application can run without the team's involvement, the main contract will contain an owner address field (owned by the CryptoAlias team) that will allow us to perform some special actions. These special actions will include the ability to introduce new aliases and the ability to enable aliases for new blockchains.

It's important to note, that owner won't be able to interfere in any way with existing aliases or change the existing state of the system. As a result, in the very unlikely scenario that the owner address gets compromised, an attacker won't be able to do any harm to existing users.

1.2. The centralized technology

The centralized technology represents software created and managed by the CryptoAlias team, which runs on top of the decentralized technology. As a result, this software is governed and limited by the rules of the decentralized system and can in no way bypass it. The main objective of the centralized technology is to make it easier for users/clients to interact with the CryptoAlias system.

The main components of the centralized system are the CryptoAlias web app, the CryptoAlias API and the CryptoAlias browser plugins.

- **The CryptoAlias Web App**
  First of all, the web app will allow users to easily view any information from the CryptoAlias system, without having to interact with the blockchain directly. However, most importantly, the web app will allow users to authenticate and easily manage their Aliases.
  The authentication process will happen anonymously, without users having to give up their identity or having to compromise their private keys. To register, a user will simply provide their public key (address). After providing the address, the user will receive a random number which will represent an Ether amount[3] (equivalent to an amount between $0.1 and $5). In a limited time frame, the user will be asked to send that amount to a CryptoAlias owned contract. The contract will immediately send back to the user the received amount,

[3] We use Ether as an example, as it makes it easier to read and understand. However, all the details are applicable to other cryptocurrencies as well.

so the only expense paid by the user will be the transaction fee. This way, users will be able to anonymously prove their identity.
Alternatively, for more tech savvy users, there will be the option to call a contract function (instead of sending ETH to a contract address) in order to prove their identity. This option however won't be available on all blockchains.
Once logged in, users will be able to manage their aliases, trade aliases, set statuses and descriptions.

- **The CryptoAlias API**
  The CryptoAlias API is a public API that will allow third parties to query data from the CryptoAlias system. It is mainly intended to be used by wallets with whom we'll create partnerships. Using the API, wallets will be able to get the alias, blockchain address, status and description for any alias or blockchain address.

- **The CryptoAlias browser plugins**
  In the long term, we plan to have partnerships and integrations will all major wallets. However, until that happens, we will offer browser plugins (one for each major browser), that will allow users to use CryptoAlias with unintegrated wallets as well.
  When activated, the plugin will intercept when the user types in an alias or a blockchain address (only for inputs of type text), will load all the related info in the background (such as alias, blockchain address, status, description) and then will display it to the user.
  The user will be able to activate/deactivate the plugin any time or can set the plugin to be automatically active only for certain websites.
  Users will also have the option to disable the interception, so that any query of the CryptoAlias system will be initiated only by the user (with a click) and not the plugin.

Needless to say, the centralized technology will always be subject to continuous improvement with a strong commitment to feedback from our users.

6. Market Size and Investment Potential

In this section, we'll describe clearer the financial aspects of our project. We'll talk about market size, future growth potential and our expenditure projections.

The tremendous potential of our project comes from the vast number of situations in which it can be implemented. The data that we use for this section is only a conservative and very narrow estimation of the value we believe this project can bring.

Given the functionality of our app (assigning an alias to a blockchain address) we consider any entity holding a blockchain address a potential customer. Our typical user is a blockchain enthusiast that is not comfortable with the complex and hard way of sending and/ or receiving coins. The data that we use to approximate our potential market size at the time of writing is the average number of transactions, the number of wallets and the approximate number of users that use the blockchain technology.

The first set of data that we use is the number of blockchain wallet users. We do it for the two major pairs of cryptocurrencies – Bitcoin and Ethereum. According to data from blockchain[4] info, as of 24.10.2017 there were 17000000 Bitcoin wallet users. This number represents a 60% raise only for this year to date. The growth is even more impressive if we talk about Ethereum – the second major cryptocurrency. According to Etherscan, there are 9500000 accounts as of October 2017[5]. This number represents a 800% growth from the same period of the 2016.

Another relevant set of data is the number of transactions that are made on these two currencies. For bitcoin, according to blockchain.info there are an aprox. 345000 transactions/ day. On ethereum network, the average number of daily transactions is 400000.

Of course, this numbers would be irrelevant without a proper adoption rate. Given the functional similarities that our project has with the DNS technology, we tend to transfer the same adoption rate that this service has. The history of DNS begins with the ARPANET project in 1969. The ARPANET (**Advanced Research Projects Agency Network[6]**) was the foundation for what we know call Internet. By the beginning of the 1980's, ARPANET network has grown so much that it was almost impossible to manage the old way. So, a solution was found: *„What is needed is a distributed database that performs the same function, and hence avoids the problems caused by a centralized database."[7].*

We expect that in the near future our project (or a project that solves the same problem) will be adopted by 100% of the blockchain users. The purpose of the example from the history of DNS adoption was to show how much time did it take before the community felt the need to address this issue, found a solution and adopted it.

Market Volume = Number of target customers x Penetration Rate

Market Volume = (17000000 + 950000)*100% = **26.500.000**

[4] https://blockchain.info/charts/my-wallet-n-users
[5] https://etherscan.io/chart/address
[6] https://en.wikipedia.org/wiki/ARPANET
[7] https://tools.ietf.org/html/rfc882

This rough estimation refers to our alias functionality. We expect that as we add new features, our market volume will raise exponentially (based on the high rise of the number of target customers, though penetration rate will naturally be lower).

Investment potential

There are a few arguments that we think need to be taken in consideration by our potential investors.

- Investors have 2 ways of capitalizing with CryptoAlias: by trading ALS on exchanges and by using tokens on our platform for trading aliases. Early adopters will have the advantage of buying Aliases at very low prices. For instance, an investor can acquire the "Google" alias with 5 ALS when the platform opens, and resell it at a much higher price in the future.
- Every time that we add support for a new blockchain on our platform, the number of potential clients (users who would like to acquire an Alias) will grow. However, the number of Aliases is finite and as a result the supply is limited. Having a limited supply and a continuously growing demand, will ensure that Alias prices are steadily rising.
- Low rate of adoption of the blockchain technology
  Decentralized solutions based on blockchain technology have already proved to greatly increase the benefits of the users and decrease to almost 0 the cost of transactions in various fields (every field where some kind of middlemanship is involved). We can already see that the rate of adoption is strongly increasing on a day to day basis. All this being said, the rate of adoption of blockchain is still small compared to other disruptive technologies (internet, smartphones). This can be only of value for us. As of this moment, the costs of entering an emerging market is still low compared to the value that is brings. Given the fact that our solution is dependent on the size of the blockchain market, our market value will grow at a rate comparable to the size of the blockchain market.
- Need to make the crypto world more „user – friendly"
  Perhaps one of the greatest impediments for a high adoption rate for the crypto – world is the lack of simple solutions when it comes to entering this field. It takes a lot of time to understand how one – even if the person is interested – can make the first steps in this field. Crypto world needs more structure and more clarity.

Expenditure data

The money raised during the ICO will be used to develop, implement, market and add other valuable features to CryptoAlias. The amount raised will be split as follows:

- Partnerships 10%
- Team 10%
- Operations 8%
  This section includes all the supporting costs needed to develop such a project. It includes lease, legal advice, administrative costs, HR, equipment procurement etc.

- Business development 12%
  This section includes the costs needed for increasing the number of users that we have. It will consist of a business strategy and sales team. Actions might consist but are not limited to suggesting other functionalities, contacting and growing our partners network etc.
- App and API development 40%
  This section includes the costs needed for software development and maintaining the development team.
- Marketing 20%
  This section includes the costs needed to have a professional team of marketers. Their role will be to assure a steadily growing audience and number of leads. The role of the marketing team will also include assuring an open, continuous and clear communication with our audience.

7. Future

In this chapter we describe some of our plans for the future of the CryptoAlias platform. We present some potential directions that the project can take once the first phase is finished. Please note that the features presented here are provisional at the moment. As time goes by and we acquire new insights and feedback from the community, the direction of the CryptoAlias development might change.

- **Identity certainty (IC)**
  In order to offer some kind of certainty about an alias, we will introduce a measure called "Identity Certainty". IC will depend on many factors, such as the last alias update time (the greater the better), the number of transactions received on the alias, the total value of the funds received on the alias since the last update, and any other historic data and community feedback about the account. In other words, IC will represent the trustworthiness of an alias. The IC score for an alias will be displayed to the sender along all the other information, before a transaction is confirmed.
  For instance, if an alias received over 1000 transactions, worth over $1 million, and has an activity of more than a year, it will have a very high IC score. As a result, the sender will be certain that he/she is sending the funds to the right address and that his money is safe.

- **Identity outsourcing**
  Since an alias represents a user's identity on the blockchain, in future we might allow users to authenticate on other decentralized platforms using their CryptoAlias identity. This would be similar to how users can currently authenticate on many websites using their Google/Facebook accounts.
  The services that will accept CryptoAlias authentications, will be able to choose the minimum IC that an alias need to have in order to be eligible to authenticate on their platform.
  In addition, aliases could be used for relations with banks, government institutions or other entities that require a more thorough background check.

- **In-wallet Exchange**
  After implementing CryptoAlias on several Blockchain platforms, we want to make CryptoAlias interoperable across them. Specifically, if a user is sending his/her Ethereum Classic to an alias linked to an Ethereum wallet, CryptoAlias will notify the user about this. The system will give him/her a choice between 2 options: either abort the transaction because it is a different Blockchain platform, or the user will have the possibility to send the funds to a different wallet with the option to exchange them automatically at the market price. Consequently, this system will act as an in-wallet exchange and the user wouldn't be required to use some third party Crypto exchanges before sending a cryptocurrency to a desired alias. In order to execute this transaction, CryptoAlias will integrate its system with several exchanges.

- **Peer-to-Peer Messenger**
  In order to further increase the security of the transactions, we intend to develop an integrated messenger to facilitate communication between the receiver and the sender of the funds. The messenger will be encrypted and nobody will be able to see the communication between 2 users. The communication between 2 users can begin just after the consent of the participants in the conversation. By implementing this feature, the users will be even more confident before sending their cryptocurrencies. They will be able to chat with the alias who receives the funds before sending them.

- **3D-Security for Blockchain**
  The 3D-Security concept was originally developed by CA Technologies and is now used by Visa and MasterCard. We intend to use the same approach to secure blockchain transactions. The protocol will address several security issues, including phishing attacks and theft of wallet credentials. The user will be able to choose the desired level of security between several options, including password based security, two-factor authentication and biometric security.

- **Bid system**
  In the initial version, sellers will be able to create a sell offer only for a specific price (chosen by them) and buyers will be able to buy only aliases that were put up for sale.
  In the future, we plan to add more complex logic. Owners will be able to sell their aliases to the community and get the highest price possible through a bidding system. At the same time, if a buyer is interested in a specific alias that is not up for sale, he/she will be able to make an offer to the owner in order to buy it.

8. Conclusion

In this paper we explained the essence of CryptoAlias – replacing the bulky and complicated Blockchain wallet addresses with short and easy to use aliases. We identified several problems in the Blockchain ecosystem and illustrated how CryptoAlias can solve them. The crypto world might seem very complicated, overwhelming, and insecure for the average consumer. We intend to bring more clarity and security to the system, ultimately making it more appealing to the masses.

We have proved the technical applicability of the project and sketched our vision. Beside the main functionality, we still see a lot of room for improvement. As a result, we plan to take the project further and have provided a number of future directions we intend to take (Identity outsourcing, In-wallet Exchange, 3D-Security, P2P messenger). All these projects will further increase the security of the Blockchain, while at the same time increasing the value for the CryptoAlias users and investors.

Beside the benefits that CryptoAlias brings to the Blockchain, our idea is also a viable option for investors. We are targeting a market with an exponential growth rate and a great capacity of adoption, thus making it very likely for our project to bring a high return on investment.

With your help, we can reach all Blockchain users and bring everyone the benefits of having a personalized and memorable alias for their Blockchain address. As Cryptocurrency enthusiasts ourselves, we believe that CryptoAlias can disrupt the Blockchain industry and lead it through a remarkable transformation.