Blockchain Identity Verification

November 24, 2017

Abstract

The ways we create and manage our identities in the increasingly digital world are broken. User credentials and sensitive data become attractive targets for hacking and theft. We experience all of the problems of fragmented and scattered identity systems - yet we do not fully receive any of the promised advantages such as increased data privacy, diffused risk or streamlined verification processes. Despite imperfections of those systems, high rates of digital penetration already led more than half of the world's population to adopt a vast variety of apps, online services and digital payment systems which require user identification. One of the core identification processes widely adopted by global businesses and organizations is KYC. Introduced in the early 2000's, KYC puts in place a policy framework for financial institutions to Know Your Customers1 before opening any account. While nowadays being a mandatory procedure in most major jurisdictions, the KYC process is often slow, painful and inefficient. Besides poor customer experience for both users and organizations, the actual cost of running a comprehensive KYC compliance program continues to rise and has negative impact on businesses. KYC is stuck in the era of branch visits and paper checks. However, while there are substantial issues with the current state of KYC, there are no real proposals to curtail the requirements. KYC is too important in the fight against money laundering, terrorist financing and fraud to rollback. The only solution is to optimize performance by improving the processes to cut costs and improve the customer experience: a decentralized, automated and transparent ID verification service based on Blockchain. KYC.LEGAL provides self-verification of personal data, verification through certified agents in under 30 minutes, digital signature, document verification and third-party verification service provision. In a nutshell, we created a tool that permits users to confirm their identity remotely with zero hassle while delivering required proof to service providers in compliance with KYC regulations. We see KYC.LEGAL and associated technologies as a future part of global identification verification standards, solving a complex problem of identity verification in a secure, protected and efficient way.

Contents

1. Legal Disclaimer

The purpose of this White Paper is to present the KYC.LEGAL project to potential token holders in connection with the proposed Token Generation Event. The information set forth below may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information to potential token holders in order for them to determine whether to undertake a thorough analysis of KYC.LEGAL token generation with the intent of acquiring them.

Nothing in this White Paper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction.

This document is not composed in accordance with laws or regulations of any jurisdiction which are designed to protect investors. Certain statements, estimates and financial information contained in this White Paper constitute forward-looking statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. This English language White Paper is the primary official source of information about the KYC Token Launch.

The information contained herein may from time to time be translated into other languages or used in the course of written or verbal communications with existing and prospective customers, partners etc. In the course of such translation or communication some of the information contained herein may be lost, corrupted, or misrepresented. The accuracy of such alternative communications cannot be guaranteed. In the event of any conflicts or inconsistencies between such translations and communications and this official English language White Paper, the provisions of this English language original document shall prevail.

2. Value Proposition

We propose KYC.LEGAL as a service that allows services to verify users and prevent fraud. Based on blockchain technology as a tool to protect and validate personal data for internet users, KYC.LEGAL provides:

• Users: Painless and fast verification process, protection of personal information through encryption and biometric data, data hosting on user's device, control over provided data, digital signature for document verification.

• Service providers / token holders: KYC compliance, reliable and secure user information, fraud prevention, ecosystem to interact with customers.

On top of that, KYC token is infused with a set of features that, if desired, allows KYC token holders for additional revenue streams creation.

3. Introduction

The promise of identification services was to create a more reliable and efficient way to verify our IDs while protecting our privacy. The hope was that the Internet would arrive with a transparent and streamlined KYC process.

In theory, a single technology would have secure access to our personal data and provide it on demand to services per our agreement. Instead of hundreds of verification processes, we would have one. Instead of days of waiting for approval, we would wait minutes. Instead of exposing our data to thousands of platforms for an indefinite period, we would keep it private and under control.

That didn't happen. Instead, the identification ecosystem that has evolved over the last decade is full of middlemen, is complex in nature and has dubious processes. We lost our privacy, our data became target for hackers, we pay never-ending fees, and suffer slow speeds. Companies

have spent billions on compliance while their experience hasn't improved a bit.
This paper will review the current state of ID verification tech focusing on KYC process. It will outline a new solution that creates a transparent and efficient Blockchain-based service for users and service providers.

3.1 ID verification market

We live in a brand new digital world. More than that, we are the grassroots of Web3, experiencing increasing power and influence of Blockchain-based technologies on our day-to day life.

According to recent MarketsandMarkets[2] report, Blockchain technology market size will be worth 2.3 billion by 2021, increasing at a compound annual growth rate (CAGR) of 61.5 percent. Within Blockchain, the digital identity market is expected to grow at the highest rate as the Blockchain would make digital identities more secure and efficient, resulting in seamless sign-ons and a reduction of identity fraud. In addition, the global Identity Management market worth is projected at $14.82 billion by 2021, up from $8.09 billion in 2016[3].

In fact, Bitcoin wallet and trading platforms are experiencing an explosive growth in their user bases. In June, Coinbase added 1M new users, demonstrating a massive increase in its user base in a relatively short period of time, and the rate of growth doesn't appear to be slowing down[4]. The number of Blockchain wallets has been growing since the creation of the Bitcoin virtual currency in 2009, numbering approximately 15 million Blockchain wallet users in September 2017[5]. And this is only the tip of the opportunity iceberg.

As the world goes digital, ID verification penetrates a vast range of service providers - from small businesses to large organizations across dozens of industries face the need to improve identification processes and provide reliable data protection. From banking ($580B in credit cards in 2016, $1656 in E-wallets in 2017)[6] to online investing ($146B in 2016)[7], from insurance services ($922,6B in 2016)[8] to gambling ($19,7B)[9], from healthcare ($9.8B in 2017)[10] to legal services ($168B in 2016)[11]. According to KYC.LEGAL research, every day 100,000 Blockchain users pass through KYC verification.

Recently, increased importance of ID verification improvement powered various legislative activities in the field. The major one, called the General Data Protection Regulation (GDPR)[12] has been ratified by the European Parliament in April 2016 and will take effect in May 4 2018. Focusing on responsibility for personal data management, it enforces new obligations regarding estimation of high-risk methods of personal data proceeding (Privacy Impact Assessments), influence on users, appointment of a designated executive (Data Protection Officer), awareness during the selection of mediators taking part in data proceeding, and record of all actions of personal data proceeding.

And so we decided the time was right for KYC.LEGAL to tackle these challenges.

3.2 Market Challenges

We believe that current state-of-art ID verification solutions represent a promising opportunity: the market is clearly large and rapidly growing; ID verification became an indispensable part of almost every business and every industry; on top of that, digital identification faces multiple challenges which, if solved, will make life easier for millions of users and thousands of businesses. Let's break some of those challenges down.

For users:

- Bad user experience.
Overall experience is currently pretty annoying. Imagine, you just registered on Poloniex. You are going through registration on Kraken. You are required to submit your information all over again, attach a photo of your ID and wait - sometimes minutes, sometimes days or weeks.

- On top of that, there is an obligation to provide tons of personal data even though only part of it gets verified.
Services rely on complex personal data verification algorithms, which sometimes demand a lot of private information. However, we all would prefer to provide ser-

vices just the bare minimum. One example is adult websites that post 18+ content. Now, in order to access the website, you will be requested to provide your complete ID information or authorize through your social network profile despite the fact that only year of birth is truly required.

For service providers:

- High user verification costs.
User verification on average costs between $10 and $1500 per KYC[13], depending on the service. It also takes up to 2+ days on average and at times amounts to 6 weeks in processing.

- Inauthentic user data.
Due to increase of fraud risk, services are forced to implement complex personal data verification algorithms. Nevertheless, in most cases they fail in creating a trustworthy verification process, which leads to:

- Violation of Terms of Use, often without any consequences, which causes a financial and other distresses to business and customers.

For everyone:

- Data storage security and identification costs.
Every time we apply to join an exchange, to link our new wallet to a bank account, or to use a digital service, both parties are required to engage in the verification process over and over again, providing and requesting same data and as a matter of fact spending our efforts and time inefficiently. Storage of personal data in multiple databases is not cheap and increases risks of fraud, hacking and illegal distribution of user data.

3.3 Blockchain technology for personal identification

The diversity of middlemen and the lack of value-added to service providers and users make some sort of simplification of the present online ID verification system inevitable. The reality remains: user experience is valuable, but it hasn't been properly improved with an efficient and transparent service.

According to Customer Due Diligence[14] (CDD) Market Survey 2016 performed by Nice Actimize, Financial Services Organizations are facing an increased need to evaluate and enhance organizational CDD/KYC controls in order to address the new regulatory requirements. Top operational challenges related to current CDD/KYC are manual processes and data quality & availability, and the highest operational priorities related to CDD/KYC programs are to improve data quality, investment in new technology solutions and process automation.

Blockchain technology, utilizing a decentralized data ledger, is capable of addressing challenges of the CDD/KYC process. Decentralized data ledgers enable storage of any kind of data, including identity data. Let's take the Ethereum verification process as an example. As we know, the verification process lies on the shoulders of miners, who check every transaction for validity before putting it in a block. As a result, transactions stay in the blockchain forever, and every user has a proof of its validity. At the same time, every transaction validity must be confirmed by several independent sources before it can be considered valid.

For that matter, the main advantages of the technology as a foundation of an innovative ID verification solution are:

- Absence of centralized control. Every Blockchain user stores Data which is automatically updated with every new entry.

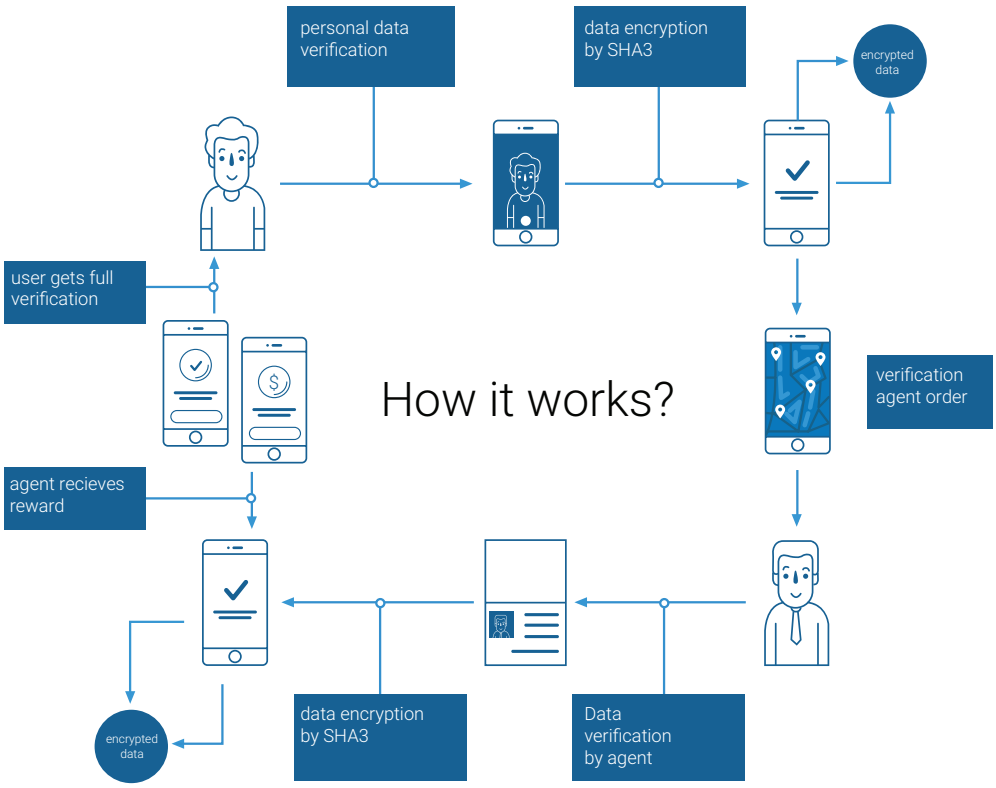
- Transparency of ongoing transactions. Every participant has access to complete information about every step of the process and its participants.

- Absence of middlemen. Technology allows to build interactions based on decentralized network and automation, without third-party members and delays.

Nowadays decentralized systems are globally adopted by international corporations and governments. Investing in new technology solutions and process automation, was one of the top three priorities for surveyed CDD providers.

Meanwhile, these enterprises still maintain significant staff of lawyers, notaries, regulators, bankers and other clerks to verify and approve a multitude of processes around KYC compliance. Manual processes are labor intensive, subject to human error, and lack consistency. Furthermore, an increased workload can result from the need for more people to do things manually. However, survey respondents indicated their willingness to work smarter, not harder. Blockchain provides a platform for technologies to introduce secure and automated solutions while complying with the latest regulations around KYC performance.

4. KYC.LEGAL solution



To improve performance for all parties, ID verification processes require a new platform and a unit of exchange.

The platform involves the roll-out of a set of automated services based on decentralized Blockchain technology. We divide them into two types: self-identification services and agent-required verification services.

Self-identification, or self-verification of personal data: KYC.LEGAL allows user to verify provided data through a simple code generation process to confirm the validity of entry.

Verification through certified agents: many KYC verification cases require a third party - a certified agent - to prove a user's identity. KYC.LEGAL addresses this problem by creating a global network of licensed verified agents (present in first 20 major megapolises by 2020) capable of providing verification on demand in under 30 minutes after your request, arriving wherever you are.

Additional sets of services (currently in development) include:

- **Digital signature and document verification:** verified users are empowered to verify documents and check the validity of verification of the document by other users.

- **Third-party service provision:** KYC.LEGAL ecosystem allows verified third-party companies to provide verification and digital signature services.

KYC.LEGAL offers a simple, fast, safe and low-cost authentication method while addressing the main market challenges, such as:

- **Bad user experience at high cost** (KYC.LEGAL technology converts the stuck in the past KYC process into Blockchain-based automated verification, saving money and time)

- **Inauthentic data provision leading to Terms of Use violations and frauds** (service provider can be assured of user data validity, as it is verified by authentication processes and personal identifiers as well as protected by blockchain technology that provides security and information integrity)

- Lack of control over users' personal data distribution (Blockchain-based technology enables the creation of a separate hash for each user data parameter, while storing name, age, address, insurance, and AP data separately)

- Data storage security challenges and costs (KYC.LEGAL does not host any personal data after confirming the identity of a user through cryptographic hashing. In the case of hacking KYC.LEGAL or any company using its services for user verification, personal data will not be affected as it is stored only on the user's device. Particularly relevant now, as only in 2016 about 15.4M US citizens became victims of fraud through hacking private information, losing about $16B. With KYC.LEGAL, user is responsible for security of their own data storage by fully controlling the list of data to provide).

Now, shifting to the second deliverable of the KYC.LEGAL proposal - unit of exchange. Creating a unit of exchange involves the introduction of the KYC token.

KYC token and Smart Contracts are ERC-20 compliant.

It is a token used for the decentralized ID verification referrals and for user acquisition. KYC connects service providers and users, creating a new referral-based ID verification economy and boosting user adoption for the benefit of service providers, community and KYC token holders. The token is based on Ethereum technology, an open source, blockchain-based distributed computing platform with smart contracts. These cryptographically secure smart contracts are stateful applications stored in the Ethereum blockchain, fully capable of enforcing performance.

KYC token for token holders. KYC token can be used in two ways:

First - traditional **"passive" mode** designed for any type of token holders - token holders after gaining ownership of tokens can transfer them between wallets or crypto exchanges.

Second - **"active" or "stack" mode** designed for existing and aspiring service providers. Token holder can create her Stack through a secure profile on KYC.LEGAL platform and store her tokens in there. After tokens are placed in Stack, token holder activates a referral link connected to

her Stack. Token holder can place this link on any digital resource (websites, social media, in direct emails and text messages etc.) in order to promote her Stack. Inside of her Stack, token holder can define revenue split between her and users to be verified through her referral. Price of verification falls between $10 and $50 range per user depending on location and other factors. 50% of total amount covers the service of certified agent vetted by KYC.LEGAL to complete verification. The remaining 50% is divided between token holder and user (in form of discount on service) based on split ratio defined by token holder. Users are incentivised to pick token holders providing favorable conditions. In return, token holders are incentivised to provide numerous cheap verifications rather than a few expensive ones.

Every new user verification performed utilizing a provided referral link locks the verification capability of one KYC token from the token holders' Stack for a month. In a month, this KYC token is unlocked for next verification. The maximum number of verifications performed by one KYC token amounts to 12 per year.

Given the above, cryptocurrency exchanges, internet-providers, advertising agencies and professionals and other service providers with similar existing revenue models have a potential to obtain the highest value from becoming an "active" KYC token holder while acquiring users and developing the Blockchain ecosystem.

While creating their own revenue streams by attracting and verifying new users, "active" token holders will subsequently increase the KYC token's value providing benefits for the holders who will remain intact.

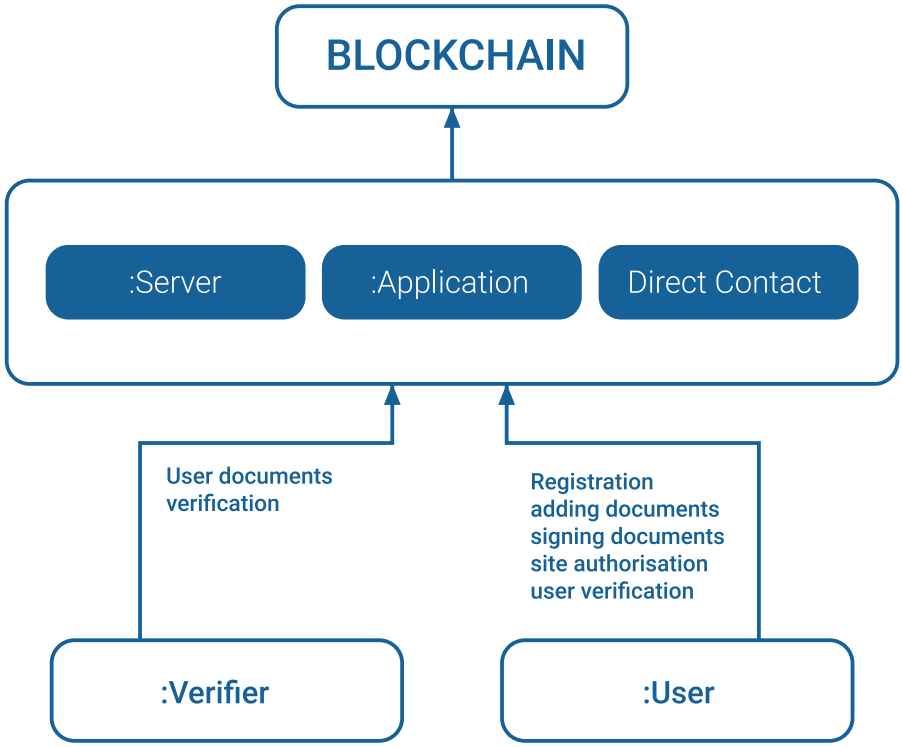
KYC token for users. After downloading the KYC.LEGAL application, users can either obtain self-verification services for a full fee or receive a discount defined by token holder by using a referral link connected to his Stack. If agent-certified verification is required, after submitting their data into the app users can activate a certified agent by simply pressing a button. The nearest agent will arrive to users' location in under 30 minutes for verification (in development, will cover first 20 global megalopolises by 2020 - for details please see our Roadmap). Hash of users' data is immediately submitted to Blockchain and user is free to provide his data to any third-party service right away. Third-party services will only receive information that user decides to provide.

In compliance with existing regulations, KYC.LEGAL conducts a thorough vetting process for agent certification and attaches a rating system to every certified agent.

4.1. Technology

Ethereum has been used for mobile payment systems, distributed exchanges, tokens pegged to commodities and fiat currencies, market clearing mechanisms, micropayment systems for distributed computing resources, commodities and securities exchanges, crowdfunding, and legal document verification. Large firms have invested in and deployed Ethereum, with JP Morgan, Deloitte, IBM, Santander Bank, Microsoft, the Luxembourg Stock Exchange, and the Royal Bank of Scotland being key early adopters.
The KYC.LEGAL technology and token are fully built on the Ethereum platform. You can see our overall structure below.

General view of the whole system:



Used as project nodes:

1. Server
2. Smart-contract based on Ethereum
3. Client mobile application
4. Agent mobile application

Blockchain base can be accessed in three different ways:

1. **Direct appeal.** Direct contact to a Smart Contract on Solidity. Our Smart Contract possesses a communication interface that can be interacted with without a server or app (e.g. to check another user or see a list of verifiers).
2. **Appeal through the server API.** Services can communicate with system users via an API in order to verify their own users through KYC. The API provides a QR-code to the service that allows you to request personal information from the service and identify it.
3. **Mobile application.** The mobile application exchanges data with the database through the server API. This is used as the primary way to interact with the system and is available to all users.

4.2. Use cases and growth opportunities

Imagine a KYC process that is efficient, cheap, reliable and takes no longer than 30 minutes. We've just created it. Now we are about to implement it (and probably conquer the world). Indeed, our solution can be applied to a whole multitude of currently painful KYC-related experiences. For example:

- Identity verification
- Crypto-exchange and ICO registrations
- Digital notarial actions (through KYC.LEGAL app and notarial digital signature)
- Digital medical services (such as obtaining medical consultations, doctor referrals, zero-fraud digital medical prescriptions to allow selling prescription drugs through online stores etc.)

- Digital insurance (instant confirmation provision for insured event occurrence, etc.)
- Banking and Investment services (such as obtaining remote loans, verifying financial transactions, remote brokerage accounts development, remote purchasing of securities etc.)
- Online Gambling (confirm your identity once instead of multiple verification processes)
- Social networks

  ... and many more.

4.3. Economics

With new digital economies booming and the volume of ID verification requests growing at unprecedented rates, KYC.LEGAL is aiming to execute its unit economics through data monetization while sacrificing our potential ID verification revenues in order to accelerate user growth. (remember? 50% to certified agent and 50% is split between token holder and user discount).

Every piece of data that KYC users will choose to provide for ID verification is of high value to service providers. Thus, KYC.LEGAL will disclose hash of data upon request of third-party providers in exchange for a small fee ($1-$2). Currently, such providers (for e.g. cryptocurrency exchanges) have to wait for 2 days for this type of user data and pay over $1 a piece.
Now, imagine a user who decides to register and open accounts on 40 cryptocurrency exchanges - every time, KYC.LEGAL is reimbursed for providing the hash of data while the actual data is securely stored under the users control.

For scale estimation, let's take our ICO example. Out of a maximum of 42,000,000 issued KYC tokens, a conservative forecast is that every 4th token will conduct at least one verification per year bringing its holder $12 on average. This gives us $100-$120M in total revenue for all token holders during year 1 - given that potentially token holders will cumulatively invest not more than the $35M max cap, it's over a 300% increase.

Another example: We estimate to acquire and verify 10,000,000 users by the end of 2018 which is just 0.3% of our potential market. However, it is 10,000,000 hashes of data that, if sold once to

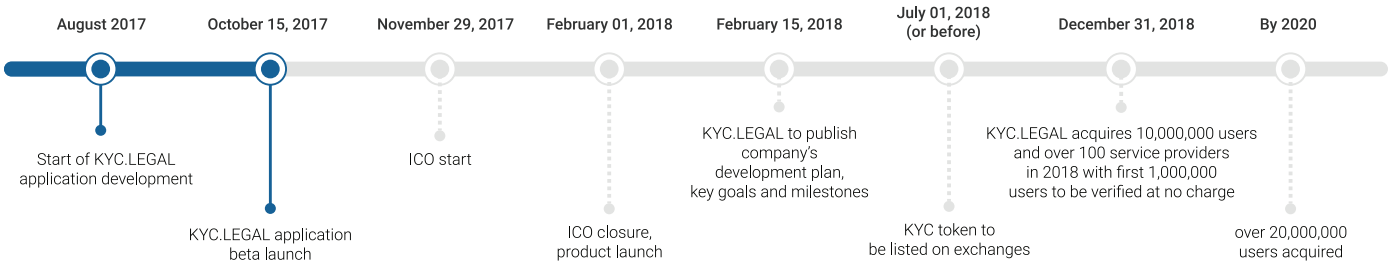
a service provider for $1 makes up $10M in revenue. 10,000,000 hashes resold multiple times to various counter-agents makes up for $150-$200M in first year revenues.

There are 100,000 Blockchain users requesting KYC verification every day. How much of that valuable data are we going to capture?

This leads us to our roadmap.

4.4. Roadmap

Our current state of technology is functional Beta. We are actively integrating with various partners and providers.



Marketing and agent acquisition efforts roadmap:

5. Business Landscape

We are standing at the grassroots of digital identification services. The current business landscape is comprised of numerous embryos of technologies and ideas, but no real working products. Among the strongest representatives of the field is Civic - a blockchain-based ecosystem that releases identity verification and protection tools. Civic's ICO in June 2017 raised $33M in tokens, which proved high interest to the digital identity services topic.

5.2. KYC.LEGAL Advantage Matrix

Present service	KYC.LEGAL service
User frustration over 2d+ of waiting time	Process completion in under 30 mins
Walled gardens	Free software, open-source infrastructure
Complex manual process	Simple automated process
Subject to human error	No humans - no errors
Security issues	No fraud / malware
Is an obligation for users and service providers - no interest in adoption	Is a single effort solution to hundreds of websites for users and a revenue opportunity for service providers - high adoption potential
Dubious	Transparent
Security Breaches	User controls, manages and protects own data
Time consuming third-party verification	Certified agents on-demand
Incapable to prevent recent Uber hackings, Equifax leak, Yahoo hacking	KYC technology capable to prevent hackings, leaks and breaches

5.3. Key Team Members

Daniil Rausov, Founder
Serial entrepreneur in the field of B2C IT-solutions with successful exits for over 10 years.
Sergei Bekrenev, Co-Founder
Founder of European Legal Service - the largest legal services company in Eastern Europe. Him and his team's global professional experience shaped KYC.LEGAL value proposition and services in compliance with current legal framework.
Nikolai Evdokimov, Strategy Director
ICO and blockchain expert, blockchain entrepreneur with numerous successful digital marketing and blockchain products. Founder of Cryptonomous, AppinTop, AdtoApp, SEOpult.ru.

6. Token Sale

KYC is an Ethereum token which authorizes the usage of all KYC app services.
Token generation means generation and exchange of KYC between ICO participants.
Tokens will be released and distributed within 7 days after the ICO closure.

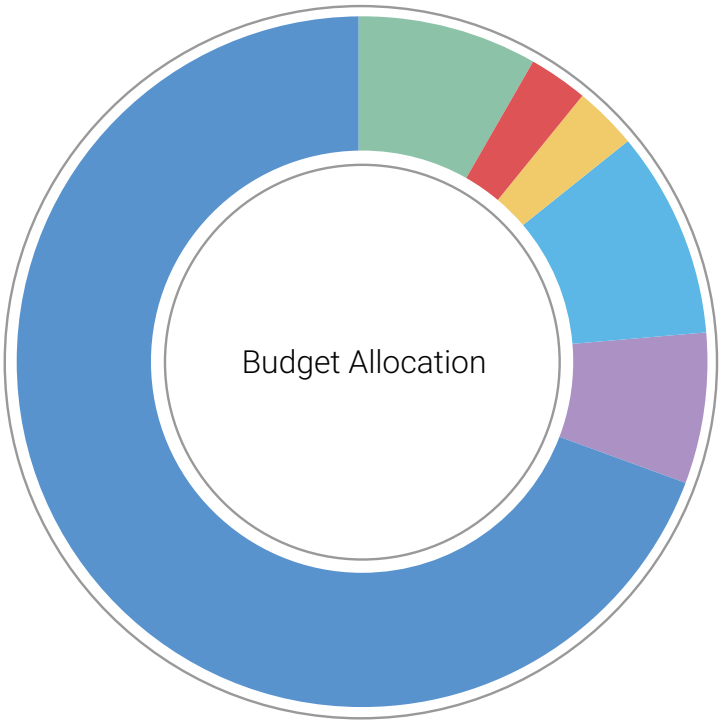
The offer is opened to the global community excluding U.S. citizens, who are prohibited by the law of their country to take part in such activities.
KYC.LEGAL is not responsible for members who violate ICO-related laws of their country of citizenship.

# of tokens to be released:	35 million KYC
# of tokens to be issued:	42 million KYC
KYC token price	1 USD
at the time of ICO:	
Accepted forms of payment:	ETH, BTC, FIAT, etc.
ICO starts:	November 29, 2017
ICO ends:	March 01, 2018 or Token sold-out

6.2. Token Distribution

KYC.LEGAL releases 35M KYC tokens at a value of $1 per token during the ICO timeframe with a max cap of $35M. The KYC.LEGAL team additionally issues 20% of the released amount - 15% to be withheld by the KYC.LEGAL team and 5% to cover ICO operational costs. The total amount of tokens issued is 42M.

6.3. Budget Allocation

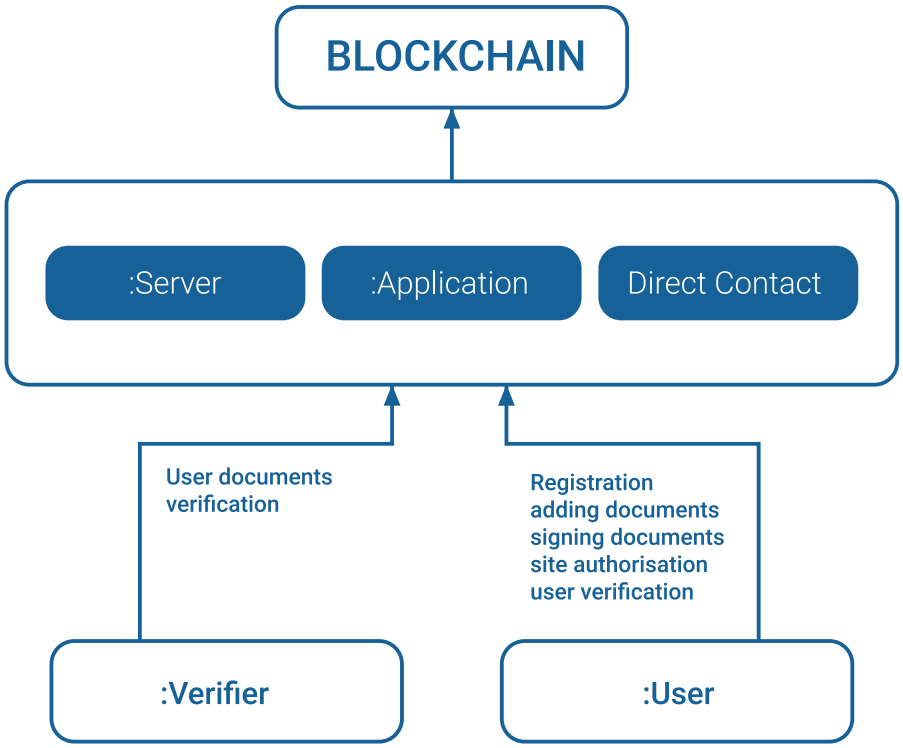


- $2.5M - discounts for partnering funds
- $3.5M - referral payments
- $1M - team salaries and overhead costs
- $1M - technology advertising
- $3M - marketing efforts and monthly Road Show participation
- $25M - financing of the free validation service provision for the first 1,000,000 of users ($25 per certified agent, the remaining half is expected to be covered by active token holders in exchange for promotion of their Stacks and services).

7. APPENDIX

Tech specs of the project

General view of the whole system:



Server

The server has an API for the mobile application and a Blockchain Ethereum database.

API consists of methods that are accessed by mobile application to enter information onto blockchain and to receive it.

Data that is transmitted while the application is interacting with the server:

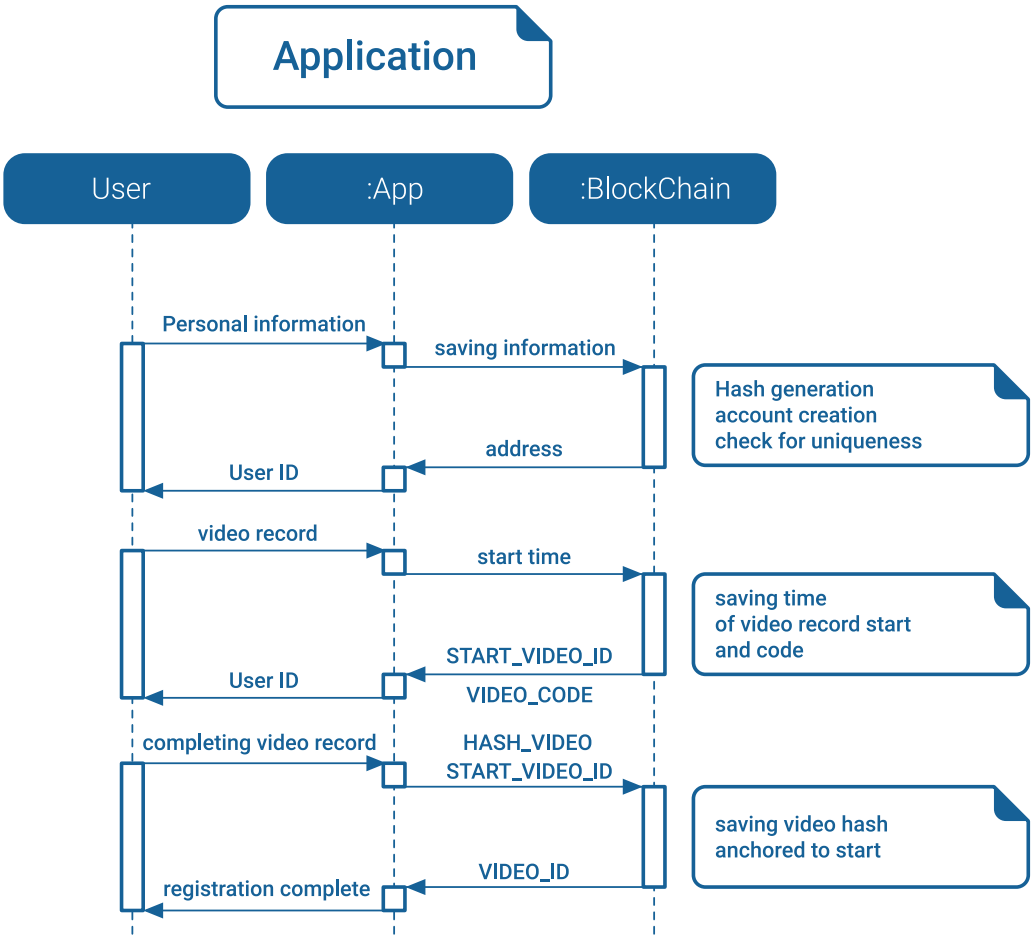
1. Registration data
2. Personal data, provided by user
3. Video to confirm the data entry
4. Data to perform user authorization in third-party services

Third-party authorization process through the KYC Legal system

1. The user clicks the “Register” button on the site.
2. The site requests data from the server. Gets the code and QR the image with the code.
3. The user scans the QR code with the application.
4. The application requests the required fields from the server, providing the code in the query.
5. Gets the list.
6. The user confirms the required fields.
7. The application sends the fields to the server, confirming the user’s agreement.
8. The user clicks the “Done” button on the site.
9. The site queries the server for the field values. Gets the key/value pairs.
10. If the site is satisfied with the data, it uses the code for authorizing.

Mobile app

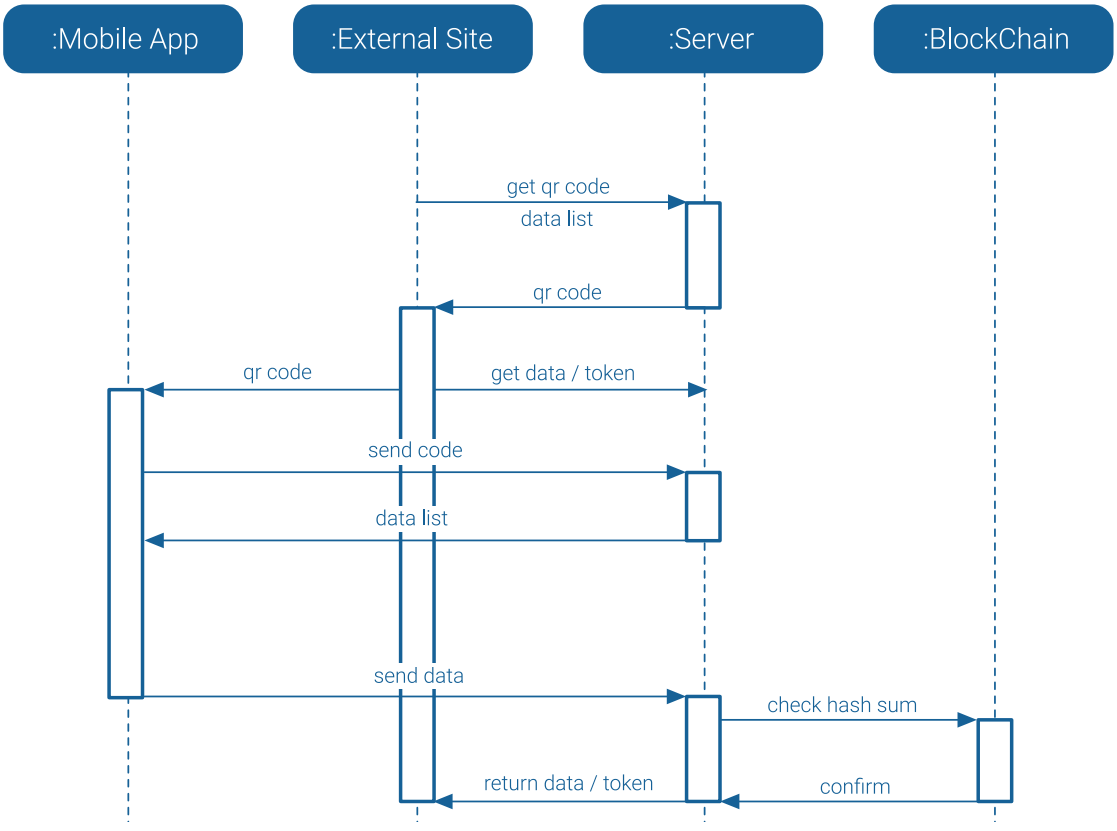
User registration in KYC app



1. The user downloads the KYC app from AppStore or Google Play.
2. Undergoes signing in steps: enter in suitable fields name, surname, sex, age.
3. Adds passport data.
4. The accuracy of the video is confirmed by the following algorithm: The user begins recording, at this point a unique code is generated and stored in the blockchain and sent to the user. This code should be pronounced while recording video.
5. Hash of video data is sent to blockchain and stored in the contract.
6. The user's identity is confirmed by an authorized agent, verifier. Verifier is not assigned manually for every user, but is defined by the administrator as a legal entity or an individual who has been granted the right to verify different users. The verifiers list will be available to the user through the mobile application, and the user will be able to choose through which verifier validates.

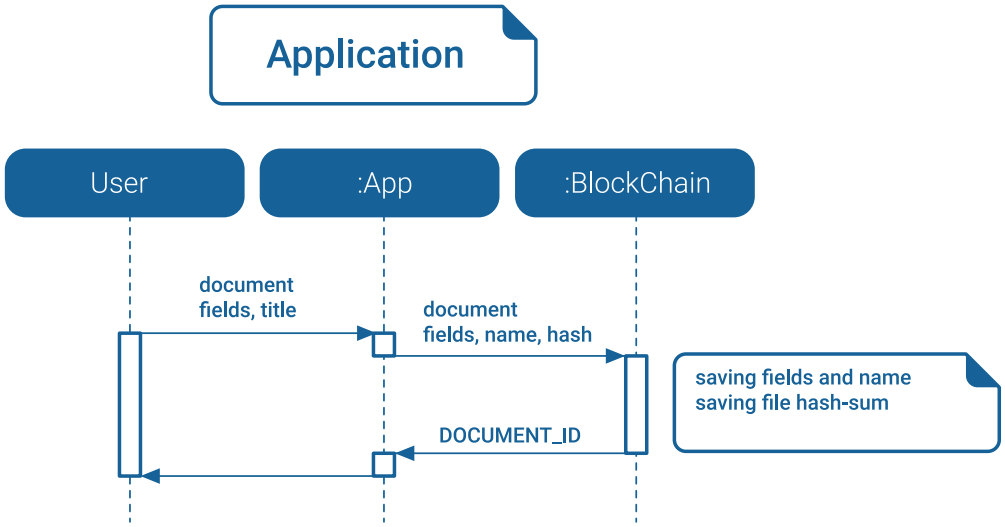
After that the KYC.Legal user is provided with his personal identifier (ID), which can be used for his personal data confirmation at the request of other users.

Authorization in third-party services with KYC Legal



Loading documents into the system

User fills in the fields and loads the file, then the data is sent to the server.



8. REFERENCES

[1] Anti-Money Laundering Countering the Financiang of Terrorism: How to Conduct proper Customer Due Diligence (October 2017) Link: https://aml-cft.net/conduct-proper-customer-due-diligence-cdd/

[2] Markets and Markets: Blockchain Market by Provider, Application (Payments, Exchanges, Smart Contracts, Documentation, Digital Identity, Clearing and Settlement), Organization Size, Vertical, and Region - Global Forecast to 2021 (October 2016, TC 4638) Link: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html

[3] Markets and Markets: Identity & Access Management Market by Component (Provisioning, Directory Services, Password Management, S SO, and Audit, Compliance, and Governance), Organization Size, Deployment Type, Vertical (BFSI, Telecom & IT), and Region - Global Forecast to 2021 (February 2017, TC 3138) Link: https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html

[4] Cointelegraph: Bitcoin User Base Surges, Coinbase Adds 1 Mln Users in 1 Month (June 2017) Link: https://cointelegraph.com/news/bitcoin-user-base-surges-coinbase-adds-1-mln-users-in-1-month

[5] Statista: Number of bitcoin wallet users worldwide from Q1 2014 to Q3 2017 Link: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[6] Worldpay: Your Global guide to alternative payments, Edition 2 Link: http://offers.worldpayglobal.com/rs/worldpay/images/worldpay-alternative-payments-2nd-edition-report.pdf?mkt_tok=3RkMMJWWfF9wsRonuqvPZKXonjHpfsX67u0vWqCxlMI%2F0ER3fOvrPUfGjI4ATspqI%2BSLDwEYGJlv6SgFQrXFMapv27gFXhc%3D

[7] KPMG: Global Insights from regional Alternative Finance Studies Link: https://home.kpmg.com/content/dam/kpmg/uk/pdf/2016/10/global-alternative-finance-report-web.pdf

[8] OECD Insurance statistics 2017 Link: http://www.oecd-ilibrary.org/oecd-insurance-statistics-2016_5jg1f8vrl7zt.pdf

[9] H2 Gambling Capital: Global Gambling Market Analysis (December 2016) Link: http://h2gc.com

[10] Statista: e-Health Market Outlook 2017 Link: https://www.statista.com/outlook/312/100/ehealth/worldwide#

[11] Statista: e-Legal Market Outlook 2017 Link: https://www.statista.com/topics/2137/legal-services-industry-in-the-us/

[12] European Commission: Guidelines on Data Protection Officers Link: http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

[13] Thomson Reuters: KYC surveys 2016 Link: https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[14] Nice Actimize: Customer Due Diligence Market Survey Link: https://www.niceactimize.com/Lists/WhitePapers/AML_CDDMarketSurvey_ResultsWhitePaper.pdf

If this document is delivered in another language than English and doubts arise concerning the translation, the English text shall prevail.