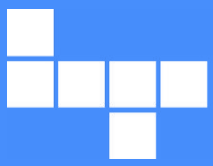


BLOCKPASS

WHITE PAPER

Identity for a Connected World

A user centric identity application for regulated industries and the Internet of Everything

WHITE PAPER

Identity for a Connected World

A user centric identity application for regulated industries
and the Internet of Everything

Version 1.3.3

LEGAL DISCLAIMER: Please read the following notice carefully as it applies to all persons reading this Whitepaper. This document was prepared by Blockpass and its affiliates who may alter and update this notice at their discretion. This document does not constitute nor imply a prospectus of any sort and it does not establish a relationship between you and Blockpass. No wording contained herein should be construed as a solicitation for investment. Accordingly, this whitepaper does not pertain in any way to an offering of securities in any jurisdiction. Rather, this whitepaper constitutes a technical description of the business purpose, function, economic and social value of the **Blockpass** platform, the creation and distribution of **PASS tokens** based on that platform, and the promotion, implementation, and adoption of an identity ecosystem serving as a conduit among humans, objects, and devices. This Whitepaper is for information purposes only. Users who intend to purchase **PASS tokens** are strongly advised to read this Whitepaper carefully and perform due diligence in their respective jurisdictions. Users that are citizens or resident of any country where purchase of similar tokens may be prohibited, or the sale itself is deemed not compliant with applicable laws and regulations are not eligible to purchase **PASS tokens** at this stage. Please note that if you are a resident of the United States you will NOT be able to purchase **PASS tokens.**

Blockpass and its affiliates shall have no liability for damages of any kind arising from the use, reference to, or reliance on this whitepaper or any of the content contained herein, even if advised of the possibility of such damages. This paper is a description of the current and planned Blockpass ecosystem, the participants designing and developing it, and the project undertaken to bring it to fruition. As such, this paper may contain predictions, estimates or other information that might be considered forward-looking. While these forward-looking statements represent Blockpass's current assessment of what the future holds, they are subject to risks and uncertainties that could cause the actual results to differ materially. Hence, the reader of this whitepaper is cautioned not to place undue reliance on these forward-looking statements, which reflect the opinions of the Blockpass team only as of the date of issuance of the paper. Please bear in mind that Blockpass does not obligate itself to revise or publicly release the results of any revisions to these forward-looking statements in light of new information or future events. Investing in new technology may involve risk and we recommend that you seek out independent financial advice before purchasing **PASS tokens.**

Contents

Executive Summary

The world is becoming more connected, and recent accelerations in the development of blockchain technologies attest to this fact. Now, quickly approaching, is Web 3.0, the next generation of the internet, where on-chain (blockchain) services will be accessible alongside their online counterparts, where profit and value centers will be shared across open networks, and where everything will be connected.

Whereas today internet-based industry is centralized, and goods and services must be obtained through a third party (e.g., Amazon, Uber, Airbnb), Web 3.0 users will be able to go online to access services that have eliminated centralized forms of organization and that operate through decentralized applications (Dapps). Over time, these Dapps, owing to shared-cost infrastructures and a growing demand among users for data security, will outcompete the centralized applications, and a new, decentralized economy will come to the fore.

To make this Web 3.0 vision fully feasible, the blockchain industry - and the blockchain networks themselves - require the support of compliance tools. The starting point for the creation of these compliance tools is a know-your-customer (KYC) solution - a method for blockchain service vendors to confirm the identity of their customers. This setup will streamline the accessing of blockchain services for users and drive down compliance costs for blockchain merchants, who are facing ever-increasing regulatory demands. In the Internet of Things, KYC is the first step, as it enables the digitally registered ownership of things.

A Self-Sovereign Identity Solution

Blockpass is an identity application for regulated services and the Internet of Things (IoT). It is positioned as a first step towards the development of a fully self-sovereign identity protocol for the Internet of Everything (IoE).

An **identity application** is a software product that allows users to establish (verify), store, and manage identities. The identities that an identity application platform can store include those of people, things, and of other objects. The current, initial, release of the Blockpass app provides an identity solution for humans. Future releases will include solutions for devices and objects.

A **self-sovereign** identity application is a platform where users can establish, store, and manage identities whilst maintaining full control over all data involved. Data collected to establish a self-sovereign identity is not stored on any central server. Instead, the data is passed to the verifier (be it a machine or a human) to view only for so long as is required to create the identity. When the verification is completed, the data is sent back to the user's own personal device.

Blockpass in its first release creates user-centric identities, integrating a KYC procedure that involves data deletion at each step of verification, and that allows data to only be stored on the user's personal device. Blockpass identities can be authenticated because a root hash, derived from a Merkle tree composed of encrypted versions of the user's data, is stored on a private blockchain, for comparison with the data stored on the user's device. Importantly, the hash data can be deleted from the private blockchain at the user's request.

The **Internet of Everything** is an all-encompassing internet of things, and will be an open network where devices and other objects are connected to one another - and to their human owners - through the gradual embedding of hardware and software. In the IoE, the identity of every 'thing' or person is essential. Blockpass was conceived as a multi-purpose identity application for establishing these identities. Blockpass' initial releases focus on human identity. Later, Know Your Device (KYD) and Know Your Object (KYO) protocols will be developed that verify 'thing' identities.

An Effective Human Identity Application for 2018

Blockpass in its current form is an effective solution for a number of key use cases.

1. KYC for regulated services, transactions (ie. the purchase of security tokens), and Dapps.

2. KYC for Blockchain merchants and service providers, seeking to follow best practices.

3. Self-sovereign identity establishment and management for blockchain users.

4. A revenue generating proposition for ID verifiers - the Proof of Verification Rewards system.

A Growing User Base of Verified Identities

Blockpass identities each are part of a rapidly growing user base of verified persons. The utility of this user base cannot be overstated. Any regulated service provider seeking to offer data security to its users will be able to find its audience among this user base. Additionally, creators of Dapps and of connected devices will be able to quickly onboard users or device owners who have already established Blockpass identities.

The growth of the Blockpass user base will be accelerated through the distribution of PASS tokens, an ERC20 standard token. PASS tokens function as discount vouchers for the Blockpass identity procedure. PASS tokens will be available for purchase from official distributors during the Initial Token Distribution Event (ITDE) from 31st May, 2018 until 30th November, 2018.

Benefits for Businesses and Individuals

Business

A comprehensive identity verification portal for quick and easy user onboarding for regulated industries.

1. **Rapid User Onboarding**

   The use of blockchain technology and smart contracts eliminates tedious KYC & AML compliance procedures by reducing sign up friction and increasing conversions.

2. **Low Cost Pre-verified Compliance**

   With shared regulatory and compliance services, it becomes possible to onboard users without expensive and duplicative identity verification of the same user multiple times across different services.

3. **New Application Potential**

   A modernized compliance protocol will enable new levels of efficiency and application possibilities for blockchain, fintech, and traditional institutions.

Individuals

A faster, safer, easier way to access regulated industries.

1. **Speedy Gateway to Compliant Services**

   Blockpass provides a secure and rapid gateway to access ICOs, exchanges, and other regulated services without the need to complete redundant compliance requirements.

2. **Own Your Own Data**

   Blockpass is a self-sovereign identity verification service that only stores a cryptographic representation of your verified identity on a blockchain whitelist. Your data is stored on your mobile device and shared only with those who you choose.

3. **Shared Identity Whitelist**

   The end of multiple KYC identity checks. Blockpass enables users to get approved and whitelisted once for near immediate access to multiple merchants and service providers.

A Digital Identity Solution For Humans

Why Start with Humans?

Ultimately, the Blockpass Identity Application will enable the creation, storage, and management of identities for any manner of 'things,' in addition to humans. Indeed, the original premise for the project was to create identities for things like solar panels, so that they might each be assigned ownership.

The Blockpass team quickly realized that the first step towards this technical feat would be to create the human identity to which the ownership of the things would be associated. Additionally, for a number of key reasons, starting with humans makes good business sense.

KYC is big business

The number of projects raising funds through Initial Coin Offerings (ICOs) and Tokenized Security Offerings (TSOs) has grown to be quite large - in 2017 alone, ICOData recorded 6 billion USD (4.8 billion euros) raised through 881 ICOs.[1] In just the first three months of 2018, 3 billion USD (2.4 billion euros) was raised.[2] Blockpass' self-sovereign identity product qualifies as applicable to KYC/AML compliance for token sales, as well as for many other regulated services. As a result, the token sale market is a major opportunity for Blockpass.

Token sale projects face increasing regulatory pressure

ICOs, and particularly TSOs, are facing increasing pressure to meet regulatory requirements, and KYC procedures have become the norm among top ICOs[3]. Of the 468 ICOs listed on ICOBench.com as of 24th March 2017, 262 required some form of KYC in order to participate.

Already, the market has begun to react to the demand. The increase of regulatory requirements, and fines incurred when they are not met, have begun to drive compliance investment across the banking, finance, and crypto industries into new and innovative Regtech, including digital identity solutions.

[1] http://icodata.io/stats/2017

[2] http://icodata.io/stats/2018

[3] http://news.bitcoin.com/kyc-requirements-are-making-icos-riskier-not-safer/

The Regtech industry is growing

Medici, a financial technology market insider, estimates that the Regtech industry will reach $118.7 billion USD (96 billion euros) by 2020[4], and KYC is at the center of this growth. CEB Global found that 62% of surveyed bank executives expected to increase their KYC compliance spending, with 29% in the range of 4-10%[5].

[4] http://gomedici.com/a-report-on-global-Regtech-a-100-billion-opportunity-market-overview-analysis-of-incumbents-and-startups/

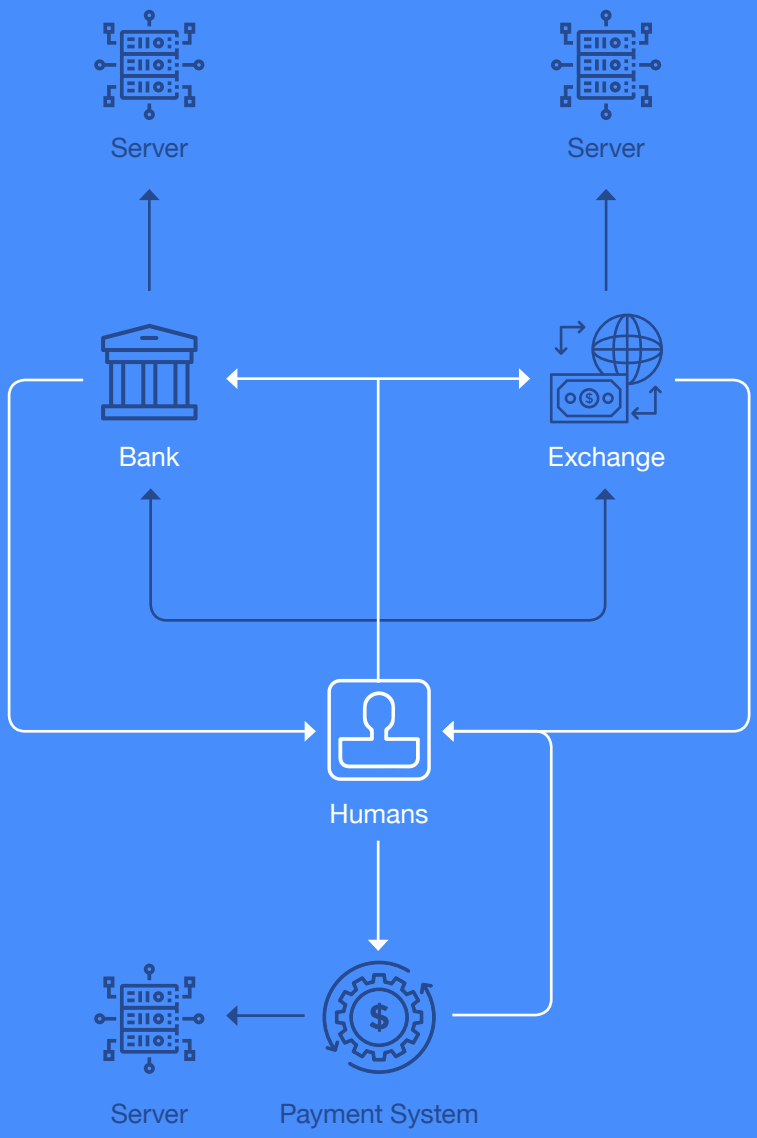
[5] http://www.fico.com/en/node/8140?file=11847

Decentralized KYC is in demand

With the rapid approach of the Web 3.0, the demand for decentralized Regtech solutions that deal with identity is significant. Usually, KYC involves storing users' personal information on company owned (or else third party) servers. Decentralized identity solutions function in a user-centric manner - by only storing personal data on users' own devices - and using Merkle trees and root hashes of that data, stored in a decentralized manner, for authentication.

Centralized KYC

User-centric and decentralized KYC



1. **Self-sovereignty is something people want:** In a study carried out by the Pew Research Center, 91% of respondents agreed that consumers have lost control over how personal information is collected and used by companies.[6] Decentralized KYC gives users full-control over their data, and this is something people want and are willing to pay for.

2. **Decentralized KYC is more cost-efficient for businesses:** Legacy KYC solutions are prohibitively expensive. In a report, Consult Hyperion estimated that a KYC check can cost 10 to 100 GBP (11 to 114 euros) per customer.[7] In the most extreme example, Thomson-Reuters found that some firms were spending up to 500 million USD (400 million euros) on KYC compliance and customer due diligence.[8] Additionally, simply by eliminating data storage costs, decentralized KYC reduces business' overhead.

3. **Decentralization fosters a better user experience:** Centralized data storage means that a KYC check likely only applies to a single onboarding process. Decentralized data storage enables the possibility of a universal identity wallet. With the Blockpass Identity application, the user keeps all their digital KYC in a single place - on their personal device - which they have at their fingertips at any time. Once the user's credentials have been verified and signed, they may re-use them quickly and simply with any number of services. When a user joins a new regulated service, if their Blockpass Identity application is configured, they can prove their identity extremely quickly.

4. **Web 3.0 developers demand decentralized KYC for their products:** Current online identity services cannot support the burgeoning development of Dapps and crypto-assets. KYC solutions that operate off-chain cannot reconcile users' digital identities with decentralized applications. Blockchain Dapps currently lack Regtech solutions that would enable compliant and secure services. For Dapps to reach their full potential - to be compatible with regulated transactions - they require a method to verify user identities.

5. **Crypto-asset transactions require onchain KYC:** Security tokens, which are currently being issued as 'meta' tokens on Ethereum, Neo, and other networks, require KYC of the issuer, sender, and receiver of the asset. Transactions of the assets should be irreversible from a legal and non-technical point of view, which is only possible by proving that the counterparty actually signed a transfer with Blockpass.

[6] http://www.adweek.com/digital/study-pew-public-perceptions-privacy/

[7] http://miteksystems.co.uk/blog/numbers-speak-themselves-true-cost-aml-and-kyc-compliance-banks-and-payments-firms

[8] http://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

The Blockpass Human Identity Solution

Blockpass manifests itself as a user-centric and self-sovereign identity application for regulated services and the Internet of Things. Blockpass offers a next-generation, effective identity creation and storage protocol.

Blockpass is built with self-sovereignty in mind: Blockpass starts from the premise that users need to hold and control their own identifying data - not third parties. So, in Blockpass, online identity data belongs to, and is entirely controlled by, the user. Blockpass does not retain any user data, nor is any raw user data stored on any blockchain or third party server. Users choose what credentials they want to have verified and signed (such as a proof of address or a government-issued piece of ID), decide where that data is stored (such as on their device or in the cloud), and control who may see it. Authentication data, stored on Merkle trees whose root hashes are stored on private blockchains, can be deleted at the user's request.

Blockpass digital identities have a high degree of utility: As an owner of a Blockpass verified identity, you gain access to a growing ecosystem of Web 3.0 service providers that have chosen to accept Blockpass identities as KYC. For businesses, Blockpass can be seen as a shared KYC platform, where a pool of pre-verified users is shared between businesses thus reducing the cost and time of onboarding new customers.

Blockpass digital identities are underpinned by their reusability: With a Blockpass Identity application, the user keeps all their digital KYC in a single place, which they have at their fingertips at any time. Once the user's credentials have been verified and signed, they may re-use them quickly and simply with any number of services. When a user joins a new regulated service, if their Blockpass Identity application is configured, they can prove their identity extremely quickly.

Blockpass offers an onchain identity solution that is easy to combine with other decentralized technologies or processes: Blockpass offers an onchain, immediately available, verified digital identity. For a transaction to be compliant in regulators' eyes, both transacting parties need to prove the transaction was personally authenticated. With Blockpass, users can transparently sign transactions and dapp accounts with their compliant digital identity, meaning that buyers and sellers will be able to safely and compliantly complete transactions and that dapps will seamlessly meet the basic verification requirements for the services they provide. Furthermore, this setup enables the generation of multi-signature smart contracts that require personal authentication with the Blockpass tool.

The Blockpass Suite of Products

The Blockpass human identity application is supported by several additional software products. In sum total, Blockpass consists of the following:

1. **The Blockpass Identity User Application**
2. **Blockpass Certificates**
3. **The Blockpass Automated Verification System**
4. **Blockpass ID Keys**
5. **The Blockpass KYC Admin Platform**

User Application

The user application is Blockpass' consumer-oriented front end.
In the most basic sense, the Blockpass user application is a portal through which users can manage those digital signatures which constitute a Blockpass identity.

From the app, users are able to create a new account (profile), submit documents for verification, submit their digital identity to service providers to pass KYC, log in to Blockpass-enabled services, sign crypto-asset transactions, and access third-party Dapps. Users, having full control over their Blockpass identities, use the application as a personal dashboard for identity management.

Environment	**iOS app** **Android app**
Features	**Interfaces with the following:** Fingerprint scanner Front-facing camera Rear camera
Customer Scenarios	Establishment of Identity application Submission of information/documentation Identity backup Identity recovery
Entry	Fingerprint or face scan Password
Data Collected	Data for entry into user's Identity application Digital identification
Data Storage	Local

Creating and Storing a User-Centric Identity

The current set-up of the Blockpass user application offers user-centric identities. This means a central server still is maintained, but the user has full control over the storage of the final identity product. Subsequent releases of the application will allow for an identity that is more self-sovereign.

Step 1: Profile setup part 1 (email verification):

The user is asked to enter their email address. The app sends the email address to the server, which generates an email validation code, which in turn is sent to the email address. The app asks the user to insert the validation code. Currently, profile email addresses are stored on the server, as they may be used for identity backup and recovery. In future release, users will be able to opt-out of this backup and recovery service.

Step 2: Profile setup part 2 (Password, UserPubKey, UserPrivKey):

The user is asked to choose a password. The app then generates a private and public key pair - the UserKey - which consists of the UserPubKey and the UserPrivKey. The app encrypts the UserPrivKey with the provided password. The server creates an association between the email address and the UserPubKey. This association is stored on the server database in the current release.

Step 3: Profile setup part 3 (TouchID/FaceID):

After password selection, the user is prompted to enable TouchID or FaceID, depending on the device type.

Step 4: Identity Creation (USERID generation):

The USERID is the “code” by which a Blockpass identity can be recognized by a service provider or other entity to which an identity is submitted. When the USERID is generated by the server, it is truncated to 20 bytes, then sent to the blockchain.

Step 5: KYC Verifications: At the users’ volition, he or she may submit their own personal information and Privately Identifiable Documents (PID). The more information submitted, the higher the level of KYC achieved by the users. Additionally, the user may enhance their profile by including certificates (see below), provided by verification experts and service providers.

The verification information that is currently accepted by the Blockpass app includes:

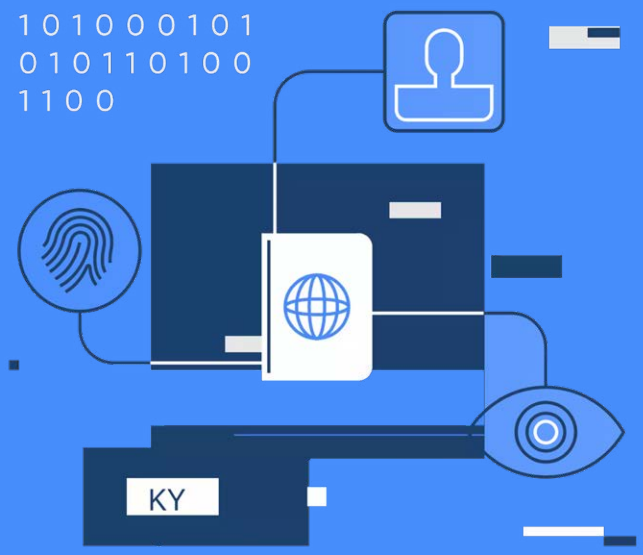
- First name
- Family name
- Full address
- Phone number
- Date of birth
- Passport scan or photo
- User selfie holding ID
- Proof of address scan or photo
- Certificates (currently, third party certificates are accepted from Onfido, Complyadvantage, and Blockpass partner service providers - the Proof of Verification Rewards system).

Every single piece of information submitted within the Blockpass user application is hashed, creating a Merkle tree. The root hash of this Merkle tree is stored on a private blockchain. When the user needs to use their Blockpass identity to access a service, the service can re-create the hash of each piece of raw data, rebuild the Merkle tree, and get the root hash. This hash can then be compared against the root hash stored on the blockchain in order to prove that the data has not been tampered with. Importantly, the user has the ability to.

Blockpass handles data encoding using JSON-LD, which allows for the serialization of data using a language-independent data format based around interoperability and openness.

Build Your User-Centric Identity

1. **Set up a profile with three-factor authentication**
2. **Enter your:**
   - Name
   - Address
   - Phone Number
   - Date of Birth
   - Passport Scan
   - Proof of Address
3. **Take a selfie holding your passport**
4. **Select to send information to verifier**
5. **Accept or decline verification certificate**
6. **Select a service provider from within the app, or scan a QR code on the service's website**



Using the Blockpass Identity to Access Services

Within the application, services can be found in the “Services” menu. Services that are listed on the app are listed according to the amount of KYC that is required for user onboarding. Services for which the user has provided enough information to onboard are listed first, while ones for which the user must provide more information are listed later.

Alternatively, services can be accessed through the use of a QR code. Upon scanning a code, Blockpass prompts the user to submit the necessary profile information to access that service.

Service providers may perform additional verification checks before onboarding the user. In some cases, the service provider can issue certificates that the user can add to their profile.

Blockpass Identity Backup and Recovery

It is possible for Blockpass users to backup their identity. As Blockpass is a user-centric solution, the backup process can only be initiated manually - at the request of the user. Backups contain all user-generated content, certificates, and the local key. The backup manifests itself as a binary file, which is encrypted with a password. In version one of the Blockpass user app, users may send the backup file to their email. Other destinations will be integrated in future releases. When a user wishes to recover their identity, they essentially“port”it into the app that is downloaded to their app by connecting the email address that holds the backup file and entering a pin.

Certificates

Certificates can be issued by Blockpass, third-party verifiers (which may be automated or human) and merchants (the Proof of Verification Rewards system). From the user's perspective, they represent a profile enhancement and are necessary to meet particular KYC requirements.

The certificate is signed by a notary, or some other human identity professional, who ensures that user credentials are genuine. Signed with the notaries' private keys, certificates are unalterable and thus represent the credentials signed.

The Blockpass Certificate Standard

A Blockpass certificate includes the following information:

- All data that had been submitted by the user to the certificate issuer.
- A free text field where the issuer defines the terms of the certificate.
- Dates of issuance and expiration.
- Digital signature of the issuer.

Receiving a certificate

When a user chooses to submit data for verification, meeting certain requirements, an issuer can push a certificate (via the admin platform) to the Blockpass app on the user's device. When this occurs, the user receives a push notification. The user must review the certificate content before it can be added to their profile. The user has the option to reject certificates.

Blockpass ID Keys

Facilitation of App Authentications

Blockpass ID keys are cryptographic keys signed by a Blockpass user, and which can be used to onboard into third-party Dapps and services. Like certificates, users can add public or private ID keys to their Blockpass profile. When a service requires a public key, the user can decide to share their public key. If a user wishes to sign a transaction from a multi-signature wallet, they utilize one of their private keys.

Verification of Blockchain Transactions

Blockpass and its official wallet partner, Infinito, are working to develop a multi-signature feature that will allow Infinito users to generate a multi-signature wallet by using an 'asset' key from within the Infinito wallet and a private ID key from the Blockpass Identity application.

The multi-signature wallet would then be submitted for whitelisting in the token security smart contract, where transactions would require user authentication via an ID key.

This countersignatory function is necessary to enable real-value transfer on-chain. For example, a security token smart contract would require the user who purchases the token to be from a whitelisted asset address. Whitelisted asset protocols require only that the asset address is in the whitelist - but this is not sufficient. It must be proven that the owner of the asset actually signed the transaction to move or dispose of the asset (i.e. addresses with the countersignatory function of the BP identity application).

Blockpass KYC Automated Verification System

KYC Automated Verification is a product that allows users to use Blockpass for verification with a suite of partner-automated verifiers. Data is sent to the verification services, certificates are generated and then deleted from Blockpass, and a request is sent to the automated verification agents to delete their copies.

Blockpass KYC Admin Platform

The Blockpass KYC Admin Platform is the dashboard for e-notaries and other identity verification professionals to sign credentials, and for service providers to see the progress of KYC onboarding for new users.

Environment	**Cloud / Desktop**
Features	Two-factor (verifiers provided with a PIN code)
Verifiers (Examples)	e-Notaries Lawyers Professionals in the verification of human identity Service providers such as ICOs, exchanges, and any other merchant
Customer Scenarios	Interpret and filter machine-verified data, reduce false-positive results produced by machines Investigate positive AML reports; eliminate false positives Generate certificates for verification work that has been undertaken - certificates can be transferred to users for review and for inclusion in the identity vault, if users so choose
Data Collected	KYC case data only resides on the device as long as the verifier is logged on Case data is deleted and returned to the user's device at the end of a verification session

Roadmap

Timeframe	Event	Activities
April 2018	Release Phase 1 Blockpass Identity application	**Mobile application for Android and iOS** Basic UX/UI Verification workflow External certificate Backup and recovery **Minimum viable product (MVP) of Blockpass Automated Verification** API Blockpass KYC admin tool Third-party verifier integration Developer portal Blockparser **Blockpass Connect demo application**
Summer 2018	Release Phase 2 Blockpass ID keys	**Mobile application for Android and iOS** Improved UX/UI Integrated messaging system **Blockpass Automated verification** Integrated messaging system Signed certificate generation UX/UI improvement Whitelisting smart contracts **APIs and tool documentation to initiate open-sourcing procedure** **ID keys (Identity application enables the generation of blockchain-based keys for access to dapps)**
End 2018	Release Phase 3	Third-party dapps Mobile application white-labeling services Consolidation of tools Open source

Team

Adam Vaziri

CEO

Adam is a blockchain lawyer who has spent half a decade working on blockchain policies and assisting blockchain companies in getting licensed and becoming compliant. He is a serial blockchain entrepreneur, having founded or co-founded several successful blockchain businesses, including Diacle (2013), Bitlegal.io (2014), Chain of Things (2016), and QRC (2017), and is impassioned to build a better, smarter economy in the Web 3.0.

Hans Lombardo

CMO

Hans is a successful entrepreneur and enthusiastic evangelist of blockchain technologies, speaking at blockchain and fintech events globally. He is a co-founder of Chain of Things, a Hong Kong-based startup integrating blockchain and IoT devices, and the founder of AllCoinsNews and Chain-Finance. In 2012, he sold his previous company, a data collection and analytics research firm focused on mainland Chinese high-technology industries. He is an internet industry veteran. During the internet boom, Hans managed the APAC operations of the internet.com E-Business media network and provided due diligence support for the internet.com Venture Capital Fund in Asia, investing in a number of internet startups in Greater China.

Thomas Leiritz
CTO

Thomas is a business and technical expert with 17+ years of experience and expertise in customer-based solutions and full-stack leadership, with a lifelong passion for technology. Thomas leads the 20 person blockchain team that is developing the Blockpass application. He has a wealth of experience in building applications and Dapps for the IoT, Regtech, and Fintech.

Conor Colwell
Director of Special Projects

Conor has shot feature documentaries in war zones, developed commercial projects for the likes of Coca-Cola and BMW Designworks, and helped a startup grow to 40 people. Conor has helped start a number of companies, from craft beer imports to powdered superfood. He is now focused on leveraging decentralized - blockchain - technologies for positive environmental, humanitarian, and exploration-related applications.

Toan Hoang
Technical Team Leader

Toan has worked in a number of different capacities as a technical leader and has explored development in everything from gaming to Regtech. A blockchain early adopter, he looks to explore how the technology can be used to make large positive impacts in today's society. Toan is well-experienced in the development of decentralized technologies, having participated in a wide variety of projects at IBL.

Corporate Structure

Blockpass operations are facilitated by two entities: Blockpass IDN Limited provides the Identity application and KYC Verification service. Blockpass IDN is the founder of the Blockpass Foundation, which is the issuer of the PASS token and is located in the Isle of Man.

Description of Blockpass IDN

Name	**BLOCKPASS IDN LIMITED**
Incorporation number	2566786
Incorporation date	15th August 2017
Public registry record	https://drive.google.com/drive/u/0/folders/1s98WWDjendq-BYF8HE6LUKIJ7FAIuREk
Registration with Hong Kong	
Registered Agent	ILS SECRETARIES LIMITED, Suite 1701-02 17/F, FWD Financial Centre, 308 Des Vouex Road Central, Hong Kong

Description of Foundation

Name	**BLOCKPASS FOUNDATION**
Incorporation number	000139M
Incorporation date	22nd September 2017
Public registry record	https://services.gov.im/ded/services/companiesregistry/viewcompany.iom?Id=453650
Registration with Isle of Man Financial Services Authority	https://www.iomfsa.im/registers/designated-business/?Id=46 28th February 2018
Registered Agent	CORPORATE OPTIONS LIMITED THIRD FLOOR, 10-12 PROSPECT HILL, DOUGLAS, IM1 1EJ, Isle of Man

The Pass Token

The Blockpass Foundation will issue the PASS token. PASS tokens can be used to obtain a discount on Blockpass verification services.

PASS tokens are so-called ‘KYC tokens’. This means that in order to transfer a token to another party, the token holder must undergo a Blockpass KYC check.

PASS Token Technical Description

Network	**Ethereum**
Standard	ERC20 + KYC
Functions	Transfer requires user to download Blockpass Application and register KYC with Blockpass Foundation. Once KYC reviewed then user ‘whitelisted’ in token smart contract then data about user removed by Blockpass Foundation.

Token Acquisition

PASS tokens can be acquired in the following ways:

- Initial Distribution Event (six months in 2018, through official distributors)
- Second and Third Distribution Event (2019, 2020)
- Purchase of PASS tokens from secondary markets, such as cryptocurrency or token exchanges
- Airdrop (this method is intended as a means of popularizing the Blockpass app)

Participation Requirements

PASS tokens will only be available from official distributors during the TDE. To be eligible to purchase PASS tokens, users will need to approach an official distributor for purchase. Once the user has PASS tokens in their wallet, they will need to download Blockpass and register with Blockpass IDN Ltd. Unless this step is carried out, the user will be unable to transfer the token to someone else.

Role of Blockpass IDN Ltd. and the Blockpass Foundation

The role of Blockpass IDN is to sell the tokens to Official Distributors, who then resell PASS tokens to their customers. All distributions of PASS tokens occur from distributors to users.

Blockpass Foundation is the appointed protocol administrator of the Blockpass protocol. Blockpass IDN Ltd. is responsible for receiving verification data from users registering with Blockpass IDN Ltd. so they can transfer their tokens, and for Blockpass IDN Ltd. to verify the profiles of the users, add the users to the PASS whitelist, and then delete the data from the Blockpass server. The Blockpass Foundation will retain data about merchants and distributors of PASS.

Rights

PASS tokens do not entitle the holder to any rights in Blockpass IDN Ltd. nor in the Blockpass Foundation. There is no participation interest in Blockpass for token holders.

Token Distribution Events

Initial Token Distribution Event - 31st May to 30th November

All tokens are purchasable from official distributors to be posted on the blockpass.org website. Official distributors are blockchain service providers that have entered into official partnership with Blockpass.

Starting 31st May 2018 and ending 30th November 2018, official distributors will be able to sell and transfer PASS tokens to their customers. The retail price for all customers will be 0.10 Euro.

From 31st May 2018 onwards, any exchange may list PASS, and the tokens will be freely tradeable.

Token Allocation Roadmap

Total supply: 1,000,000,000 PASS tokens

Initial Token Distribution Event: 31st May 2018 to 30th November 2018.

- Hardcap: 250,000,000 PASS tokens
- Softcap: 60,000,000 PASS tokens
- Retail price per PASS: 0.10 Euro
- Following the Event, tokens will continue to be available from official distributors. Price may vary between 0.10 and 0.40 Euro per token.

Second Token Distribution Event: 31st May 2019 to 30th November 2019

- Hardcap: 100,000,000 PASS tokens
- Locked currently

Third Token Distribution Event: 31st May 2020 to 30th November 2020

- Hardcap: 50,000,000 PASS tokens
- Locked currently

Advisor Allocation: 50,000,000 PASS tokens, to be unlocked on 31st May 2019

Founder Allocation: 200,000,000 PASS tokens, to be unlocked on 31st May 2021

Other Allocations of Pass Tokens

Proof of Verification Rewards (POVR) system: 180,000,000 PASS tokens

Blockpass approved merchants that reverify Blockpass approved identities can sell identity certificates to Blockpass IDN in exchange for PASS tokens.

Grants for Identity Startups and Research: 40,000,000 PASS tokens

Airdrops: 90,000,000 PASS tokens

Treasury and Market Making: 40,000,000 PASS tokens

Glossary

Acronym	Definition
AML	Anti-Money Laundering
Dapp	Decentralized Application
GDPR	General Data Protection Regulation: European Union regulations on the handling of customer data
ICO	Initial Coin Offering
IDN	Identity Network
IoE	Internet of Everything
IoT	Internet of Things
JSON-LD	JavaScript Object Notation for Linked Data
KYC	Know Your Customer: Procedure used to identify users as part of an onboarding process of customers for an online or on-chain regulated merchant
ID-Keys	Tools that can be used to attach human identities to transactions or to access dapps
KYD	Know Your Device: Procedures that will be the next step towards a decentralized IoT. Creates for a device an “identity” that can be attached to a human one
KYO	Know You Object: A broader term than KYD, KYO is a procedure used to create identities for objects so that other identities may interact or own them
PASS	PASS Token: Can be used to obtain a discount on the verification services provided by Blockpass
PEP	Politically Exposed Person

PID	Privately Identifiable Document
Regtech	Regulatory technology: Proposes technological solutions that streamline compliance for individuals, businesses, and governments
TDE	Token distribution event
TSO	Tokenized security offering
Web 3.0	The next generation of the web, featuring a greater level of connectivity for web applications, things, and devices. While the web 2.0 is dependent on privately owned servers, web 3.0 will be made possible by distributed data storage

WHITE PAPER

Identity for a Connected World

Version 1.3.2

A user centric identity application for regulated industries
and the Internet of Everything

blockpass.org