www.hive.id

hive

A Decentralized Identity Management Ecosystem

Powered by Blockchain Technology and Tokenization

Executive Summary

Date Last Updated
July 09, 2018

Version
1.2

Background & Vision

The Internet was built without a standard way to identify individuals and organizations. Since the beginning of the World Wide Web, websites solved the problem by implementing user verification via passwords and usernames. Since then, the solutions haven't evolved much, yet the Web has expanded drastically since then.

An average Internet user accesses dozens of services on a daily basis. The silo-based status quo approach, where users must maintain identities for every site they interact with, has become radically obsolete. This usability disaster forms personal data honeypots for hackers. As a result the identity theft practices continue to compromise the integrity of the entire ecosystem of Internet services.

> "The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception which will cumulatively erode public trust in the Internet."
>
> *The Laws of Identity, Kim Cameron,*
> *Chief Architect of Identity for Microsoft*

Self-sovereign identity provides three elements required to solve this problem: individual control, security, and full portability. Individuals and organizations remain the sole owners and managers of their Digital Identities. Those individuals thus, serve as their own identity providers. And no 3rd party can "provide" them with another identity since it's already intrinsically theirs. Digital existence of a self-sovereign identity is independent from any organization.

A digital record that you control entirely could be a great visualization of the self-sovereign identity. You may complete it with more data on your own or ask others to do so instead.

Only you can decide how much you want to reveal and for what period of time. You can record your consent to share data with others, and facilitate that sharing. It is persistent and doesn't involve any third party. Claims made about you during the identity transactions can be self-attested or attested by a 3rd party.

To establish the identity layer of the Internet, a new, trusted infrastructure is required. The one that will enable identity owners to share their digitalized identity and verified attributes; to manage permission and to record consent.

Problems & Challenges

The ability to store and share information digitally offers so many benefits that it has become a growing trend. However, alongside the advantages of cost and convenience, a new set of concerns have developed.

Data ownership

The vast majority of Internet identities are centralized. This means that they are owned and controlled by a single entity, such as an eCommerce website or a social network.

Security

The cost to organizations to store, manage and protect huge volumes of user data is increasing in tandem with the liability. Yet, the security is never a guarantee, and users constantly fall victim to data breaches.

Trust

The real currency of digital commerce is trust. Consumers have tens or hundreds of fragments of themselves scattered across different organizations, with no ability to control, update or secure them.

User Experience

User sees yet another web site or app that demands the same details that they entered in the last 50 services they wanted to use. And then they have another username and password to remember.

We identify the following 4 problems that exist in identity management today:

- **Data ownership**
- **Security**
- **Trust**
- **User Experience**

&

In 2017, there were 16.7 million victims of identity fraud, a record high that followed a previous record the year before. The amount stolen hit $16.8 billion last year, an increase of 12% from 2016.

Account takeovers tripled in 2017 from 2016, and losses totaled $5.1 billion.

The majority of the data breaches in 2017 affected the business sector, reaching 55% of the total number of breaches, followed by medical/healthcare with 23.7% and banking/credit/financial sector with 8.5%. The business category has suffered the most breaches for the third year in a row.

53% of customers abandoned a transaction due to: 1) a lack of visible security, 2) too much information required for account setup and 3) mandatory account creation for a one-time purchase.

Hive Solution

Hive is a complete self-sovereign identity management solution that institutes a system of relationships between businesses and consumers.

It is designed to create, manage and protect the unique sovereign Digital Identities of consumers while addressing the needs of businesses at the same time: affordable KYC/AML compliance, integrated Customer Due Diligence mechanism, fraud prevention, account takeover prevention, account and promo abuse, etc.

By integrating an innovative mechanism to store identifiers, keys, pointers and proofs without relying on centralized authorities, it allows individuals and organizations to process a sequence of transactions to reliably prove their identities.

Benefits for consumers

- Full control of identity
- Least-disclosure for permissioned access
- Pseudonymity & security
- Tokenized loyalty program
- Intrinsic solution

Game-changer for businesses

- Increased conversions
- Global trust network
- Catch all vectors of fraud and abuse
- Minimized regulatory exposure
- Immutability & Transparency

Key Advantages & Unique Features

Identity verification

With Hive, users are able to build several levels of Digital Identity. Depending on business requirements across jurisdictions, different types of Identity verification may be required. Using the Legal Identity, customers can manage permissions to their personal identity information access while interacting with businesses and safely self-identify themselves on the Internet.

Education verification

Online and offline educational institutions can become Vendors to verify existing credentials of their students and provide digital certificates, diplomas, etc. attested on the Hive blockchain. We believe that the access to the technologies that makes credentials portable and immutable will impact the evolution of the educational systems around the world.

Employment screening

To complete their Digital Identity, users will be able to verify their work experience, store employment references, and request employment screening services (including background checks, driving records, drug & health checks, etc.) from Vendors to add corresponding attestations to their profiles. Additionally, Hive will introduce a feature, which will allow users with verified credentials to endorse each other.

Identity protection

To protect the established Digital Identity, an Identity protection service will be available on the Hive Marketplace. Hive Identity Protection will be providing the following services (subject to availability in certain countries):

- Address change verification
- Dark web monitoring
- Credit Monitoring
- Data breach notifications
- Annual credit reports & scores
- Insurance protection package
- 24/7 customer support

Key Advantages & Unique Features

Hive Fraud prevention & Machine learning

One of the core pains that Hive is solving for businesses is the Customer Due Diligence process, which introduces the internal scoring system to rate the accounts on the Network. Fraud is a scalable programmable operation on the Internet and we believe that it could be tamed only with the improvement of the Identity layer. All of the businesses on the Hive Network are able to flag users that have abused their protocols. Hive users are able to create only one account on the Network. Thus they have only one reputation bar. This approach helps to prevent the scaling of fraudulent activities. Furthermore, businesses can share user-generated events such as Create Content (comment, listing, message, post, profile, review), Chargeback, Login, Logout, and others with Hive Fraud Prevention for further Machine Learning analysis, to identify unusual behavioral patterns and notify the businesses about the potential threats. Hive is a single intelligent solution for different types of fraud.

Account takeover and abuse

Promo and referral abuse

User reputation and scoring

Technology: How do you combine Identity and Blockchain?

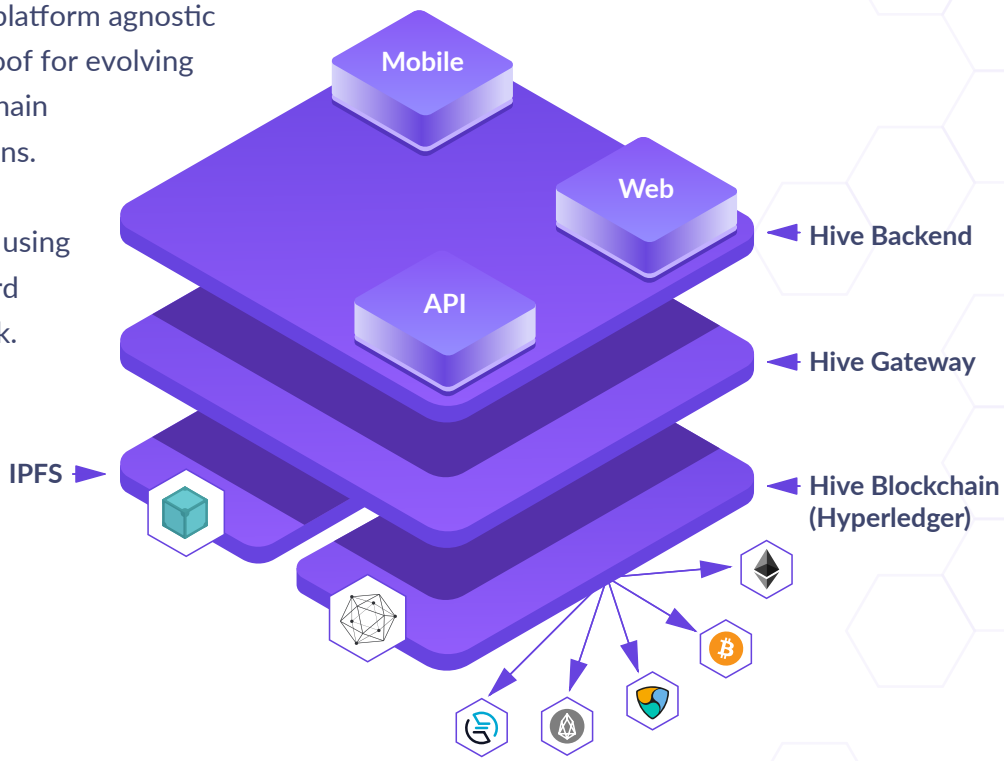
Hive provides a digital identity management ecosystem, which individuals can access by downloading the Hive Vault, setting up their digital identity on their device and verifying their identity claims to become a Hive user. Once fully verified, the attestations to this data are written by Hive to the blockchain, which can then be used by recipients of the data to verify authenticity and ownership.

The Hive Vault stores all user's personally identifiable information (PII) securely on the device using high-level encryption based on hierarchical deterministic keys generated, provisioned and controlled by the users themselves. Hive will not handle the storage of PII in any way, the data is only stored on the user's device.

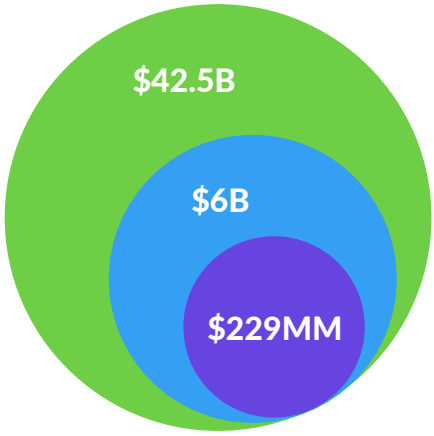
Hive is built using a hybrid blockchain model - a "private permissioned" ledger which periodically anchors to public ledgers - which can deliver the best of both worlds: public access with trusted governance. The first blockchain stores proofs of verified claims and controls access to identity records and is built using Hyperledger Fabric.

The second blockchain can be any public blockchain, to which the verified claims are periodically anchored to ensure data integrity (Ethereum, Bitcoin, EOS, NEM, etc.). In general, the solution is built in a blockchain platform agnostic manner, to future proof for evolving and emerging blockchain technology innovations.

Tokenization is done using ERC20 token standard on Ethereum network.



Market & Strategy



- **TAM – $42.5B (2023 – $88B)**

  Identity Management – $20B (2023 – $30B, CAGR – 8.45%)

  Identity Verification – $13B (2023 – $40B, CAGR – 25%)

  Identity Protection – $6B (2023 – $12B, CAGR – 15%)

  Employment Screening – $3.5B (2023 – $6B, CAGR – 11.45%)

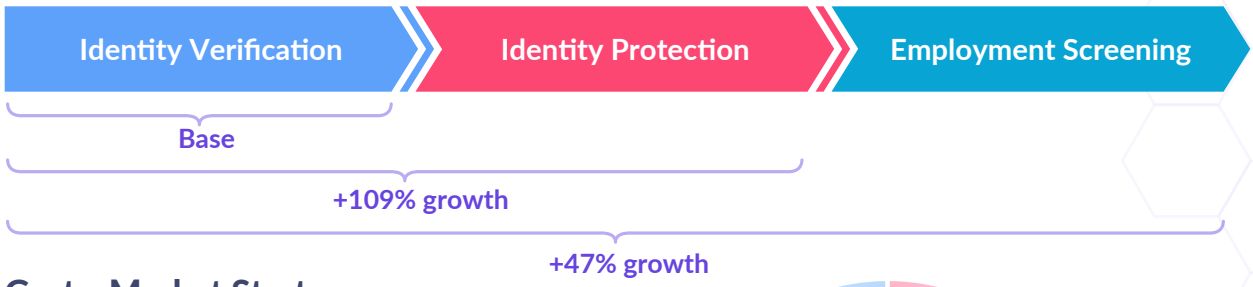
- **SAM – $6B**

- **SOM – $229MM within 3 years, $603 MM within 5 years**

  Year 1 – $29MM Year 2 – $111MM Year 3 – $229MM

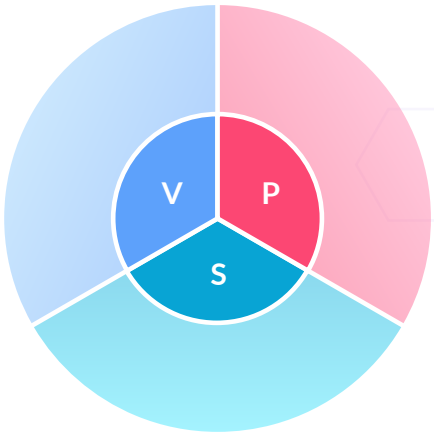
  Year 4 – $402MM Year 5 – $603MM

Key Value Proposition



Go-to-Market Strategy

- Leverage existing and develop new strategic partnerships to launch and grow Identity verification vertical
- Use rewards to create strong incentive for users and service providers to join and stay on the platform
- Upsell existing users to Identity protection and Employment screening products
- Keep scaling Identity verification and develop new strategic partnerships to scale Identity protection and Employment screening verticals



Transaction Volume

3 years – $229 MM

5 years – $603 MM

Token Volume

Fixed – $25MM

Token Generation Event (TGE)

Name
Hive ID (HID)

Total Supply
700 000 000 (no new tokens will ever be created)

Token Value
1 HID = 0.10 USD

Soft Cap
$5 000 000

Hard Cap
$25 000 000

Unsold Tokens
All unsold tokens will be burned

Major Exchanges Listing
Q4 2018

Bonus for Large Purchasers
Purchasers who commit to purchase tokens during the Token Sale in the amount equal or greater than 500,000 HID, will be eligible for a bonus. All such bonuses will be discussed individually with each potential buyer.

Use of funds

- **15%** Research & Development
- **5%** Admin & Operations
- **10%** Reserve
- **7.5%** Legal & Compliance
- **45%** Sales & Marketing
- **10%** International Expansion
- **7.5%** Acquisitions & Partnerships

Token Distribution

- **10%** Team
- **5%** Advisors and Bounty
- **20%** Reserve
- **65%** Sale and Incentives

Roadmap

Q3 2017

[Process] Idea inception and market analysis

Q4 2017

[Process] Blockchain scalability problem research

[Process] Development of the platform core started

Q1 2018

[Process] Prototype release

[Process] Incorporation in Delaware, USA

[Process] Seed round: $350 000 raised

Q2 2018

[Process] Alpha release

[Process] Blockchain technology finalization and integration

Q3 2018

[Process] Beta release

[Process] Public app release (iOS, Android)

[Process] Patent filing in other countries

[Industry] Auth plugins for popular platforms and frameworks (Shopify, Wordpress, Passport.js)

Q4 2018

[Process] Multi-language support

[Process] Employment verification and screening

[Process] Education & professional qualifications verification

[Industry] Recruiting software integration (Lever, Greenhouse, TriNet, ZipRecruiter)

Q1 2019

[Geo] Expansion to Canada

[Process] Developer community establishment

[Industry] Vending machines & specialty ATMs

Q2 2019

[Geo] Expansion to Asia

[Process] 3rd party developer SDK release

[Industry] 3rd party auth solutions integration (Auth0, Okta, Duo Security)

Q3 2019

[Geo] Expansion to Europe

[Industry] Corporate market solution (MFA, SSO, AD)

[Industry] Dedicated FinTech solutions

Q4 2019

[Process] 3rd party app marketplace launch

[Industry] Machine-to-machine auth integration (IoT devices)

Team & Partners

Kostiantyn Shterental
Co-Founder and CEO

Yuriy Znatokov
Co-Founder and CTO

Kyrylo Sopot
VP of Business Development, LATAM

Yevgen Yurash
VP of Business Development, APAC

Alena Yudina
VP of Business Development, EMEA

Ivan Arabadzhy
Senior UI/UX Designer

Sergei Poznanski
Lead Backend Architect

Artem Mirchenko
Lead Frontend & Mobile Developer

Sergey Zenkov
Senior Blockchain Developer

Alexander Ivanov
Chief R&D Officer

Advisors

Gary Baiton
Growth Hacking

Ismail Malik
Blockchain R&D, Strategist

Colin Breeze
Senior Counsel

Andrey Verbitsky
Token Architect

Strategic partners

JUMIO · GoodHire. · HYPERLEDGER · THE LINUX FOUNDATION · ENQ ENECUUM · Intercoin · POPCHEST

TGE Partners

SOLUTIONS · CRYPTO LAWYERS CORPORATION · modern token · ICO bazaar crypto market insight