Permission Foundation Technical Whitepaper

The Permission® Marketplace

August 2019, Version 1.8

Contents

The Permission® Marketplace

Introduction

By creating ASK, the standard cryptocurrency for Permission, the company Permission.io foresees a world of e-commerce built on a model of permission versus legacy models of interruption and data exploitation. The first application of ASK will be the Permission Marketplace where members can search for products and services and be compensated in ASK for engaging with merchants. The merchants offering the highest bids will have their products displayed at the top of each product or service category. This model built upon permission and transparency leads to better ROI for merchants while building trust and transparency with their target customers.

The Problem

Over the past decade, the $4 trillion per year e-commerce market has become increasingly intrusive in an ever increasing attempt to engage users. It is based on interruption, obfuscation, and the exploitation of personal data.

Advertisers and merchants face additional challenges. The cost of engaging with users has risen dramatically over time, and we anticipate it will continue to do so under the current interruptive model. Digital advertising continues to deliver a lower ROI year after year. Reportedly, 40% of digital ad traffic is the activity of digital robots clicking on ads. Click fraud is estimated to be more than $50 billion per year, making it the second largest organized crime in the world.

This damages trust between parties and inhibits interactions. All parties involved want a more trusted and transparent environment.

The Permission.io Solution

Members will be paid for their time, data and intent to engage in commerce. Their profile data will be securely stored in a private, self-sovereign method, with the user controlling access to their data. Advertisers, merchants and others may ask permission to use that revocable data for targeting. Advertisers and merchants will be drawn to Permission.io because it delivers trusted interactions with the member. They will have access to a richer collection of first party targeting data than anywhere else. Trust is the crucial value for any seller, whether it is a multinational member product company or a local retailer. According to a 2017 Ernst & Young survey, 74% of members would boycott a brand that they no longer trust.

The Reputation Engine

Just as the blockchain enforces immutability, provenance and security, the Permission Marketplace will create transparency, honesty, and integrity. Permission.io's goal is to build trust by integrating into its system a sophisticated reputation score ("Permission Score") for members, advertisers and merchants. Good behavior is incentivized and bad behavior is penalized.

Member Reputation

The ideal behavior of the member is to search for and purchase products and services in the same way that they currently browse the Internet for specific things that interest them. To be exact, we expect their browsing and shopping behavior to not vary significantly from the current norm.

We will encourage merchants and advertisers to provide consumers with relevant product descriptions, as well as promotional and/or exclusive offers, that entitles the buyer to rewards/discounts as they move through each step of the sales funnel. In so doing, we will be able to analyze not only member responses, but also sales cycle behavior, “from search result or ad to purchase.” Using machine learning data analysis techniques, we will thus be able to identify the normal range of member patterns, both for searching for products and for the sales conversion on partner sites.

For members, the reputation engine will analyze their behavior and calculate their “Permission Score” through multiple identity points and behavioral factors. Those members who try to game the system by searching for goods or services in which they have no interest, and hence never buy, will be excluded from the more rewarding opportunities by their reputation score.

Merchant Reputation

In order to promote trust with consumers and fair competition among merchants, merchants will also be accorded a “Permission Score.” The merchant’s Permission Score is based on their behavior within the marketplace, as enforced by the established rules of the marketplace (Merchant Terms of Services), as well as consumers’ evaluation of their relationship with the merchant. Consumers will have the ability to report misleading advertising/products and deceptive practices.   Similar to the member’s reputation score, advertisers and merchants will be scored by reviews, comments and marketplace behavior that may be made available to all members of the Marketplace.

The Long Term Vision

We are working towards a fully decentralized network that hosts content and data profiles and enables commercial interactions between its members. In time, the marketplace can and will be suitable for other activities that will broaden its reach. Examples include recruiting, political campaigns, surveys, coupon strategies, club memberships, and even dating.

The Technology Imperative

Permission.io believes that the technical governance of the Permission marketplace is key to its success. The goal is to provide all participants in the market the possibility of becoming stakeholders in the operation of the Permission blockchain. The goal is decentralization of the governance of the blockchain and its network. With respect to computer resources, we have a growing need for content storage and for a growth in full nodes that implement the Permission blockchain.

The decentralization of the network will guarantee that its software and its future development is not controlled by a single central authority or a cartel of interested parties. Instead, it will be determined by a globally diverse population of stakeholders, including Permission.io members, computer resource providers, developers and businesses that participate in the marketplace. We will encourage all stakeholders to become providers of storage resources and possibly to participate by running consensus nodes.

The anticipated release of Casper Protocol (PoS) to the Ethereum network would serve our path to decentralization. The Permission blockchain will first adapt a hybrid, PoA/PoS to ease the inclusion of PoS, then move completely to PoS when sufficient distribution has occurred. If Casper continues to be pushed, we have a path to decentralization via our identity management of Proof of Authority (PoA) nodes. Either way will achieve the goal of an open, public, neutral, and censorship-resistant blockchain.

Other Platform Applications

The technical details of Permission.io will be made available for developers to build complementary applications to those that Permission.io provide. Many services now offered through the Internet will, over time, become available through blockchain applications, including: every variety of social media application, every kind of data storage, email and messaging, buying and selling new and second hand goods, publishing, banking, investment, mortgages, credit checking, educational services, health services, dating, advertising and more.

Some of these may be developed on Permission.io. Others will become available through directly linking to other blockchain capabilities that currently exist or are in the process of being created. For example, existing blockchain services include: retail, mobile game playing, competitive eSports, gaming, document storage, digital asset management and financial services.

The Permission.io Blockchain

The Permission.io blockchain and its environment consists of a network of server nodes with specific functions. Before we describe it, we will explain the process that determined its design. Over the past year, we investigated a series of blockchain technologies and concluded that developing our own robust blockchain technology was critical to a successful endeavor for the following reasons:

- Scalable. The blockchain needs to be able to scale to accommodate in the region of 1 million users relatively quickly, and up to 1 billion users in the long term. This level of scalability was beyond the capability of most “off the shelf” open source blockchain technology.

- Functionality. The blockchain has to be an independent chain, designed for smart contracts and not present developer recruitment problems, as well as have a single coin for a better user experience.

- Cost. The blockchain needs to provide a low cost per transaction, which in turn means that the blockchain consensus mechanism needs to involve minimal computer power.

Permission.io Blockchain Technology Choices

After investigating alternatives, Permission.io chose a blockchain based on Ethereum with the Clique consensus mechanism, as implemented in Geth (Go Ethereum). This technology combination is publicly available for test on the Rinkeby testnet, and since the choice was made, the team has been testing its capabilities. As many readers of this paper will be unfamiliar with the technology described, we summarize it with the following words:

It is an Ethereum-based blockchain that uses a Proof of Authority (PoA) consensus mechanism.

We have adopted this combination of technology and are further developing it to suit our longer term needs. At the time of writing, it meets all of the above-listed requirements. In particular, it is capable of supporting at least 300 transactions per second (TPS) under test.

As the technology is derived from Ethereum, it will also be able to take advantage of the various Ethereum performance enhancements that are currently in progress, such as Plasma, the Raiden Network, Truebit and the various chain-sharding experiments.

The Clique “Proof of Authority” (PoA) Consensus Mechanism

This is a remarkably simple consensus mechanism that uses a central ring of nodes which compete to create new blocks. On average all are equally successful so it is as if they took turns in a round robin manner to create the next block. The decision as to which node to choose next is determined by the Clique PoA protocol. The Authority node pool can be extended to include new nodes.

A significant advantage of PoA for Permission.io is that it considerably simplifies network launch, since it will be easy to assemble a small number of honest nodes to form the initial Authority pool.

The Network Structure

As illustrated in *Figure 1*, Permission.io has the following components:

- Permission coin wallets: We will offer our own, and other third parties may also provide, such wallets.
- Full node: Full nodes hold a full copy of the Permission.io blockchain and can be operated by anybody. They could include a Permission wallet.
- Boot nodes: These are the entry points into the network for new nodes.
- API nodes: These nodes provide blockchain API access to Permission.io's internal services and third parties.
- Authority nodes: These are the "mining" nodes that create new blocks.

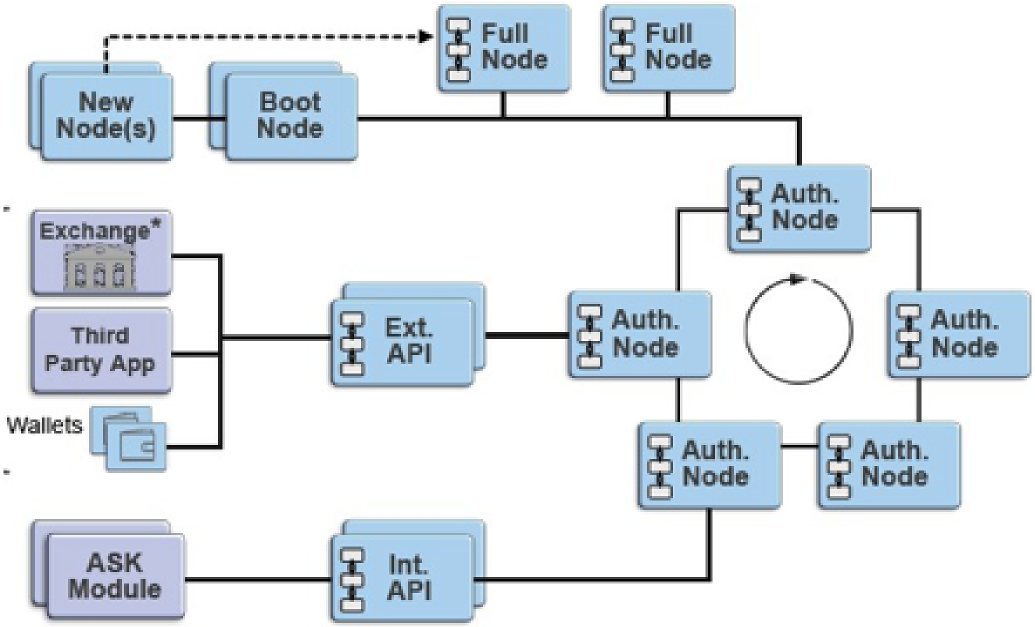

Figure 1. The Permission.io Blockchain

The Boot Node provides them with the connection information they require to connect to the blockchain network. They could be a node that wishes eventually to become an Authority node or they might become an Internal API node or an External API node or simply a Full Node. The Boot Node (in practice, a cluster of nodes for the sake of load balancing and redundancy) provides them with a list of node addresses. Although all nodes run Geth, the Boot Nodes are distinct in having fixed IP addresses which Permission.io publishes.

Public access to the network for processes that need continuous access is provided by External API nodes. This includes Permission wallets and 3rd party apps. If so, it could build an API node. The internal API nodes are for private access by Permission.io processes that need to post Permission transactions to the blockchain.

Finally, there are the Authority Nodes which share the work of adding new blocks to the blockchain as indicated by the circular arrow. At launch, Permission.io will provide most of the network nodes. However, it will be possible for other nodes to be added by third parties further decentralizing the PoA consensus.

Permission.io Blockchain Governance and Proof of Authority

The Clique PoA protocol imposes a dynamic randomized weighting scheme. It has the effect of increasing the probability of any node completing the next block when it has not completed a block for a while. The protocol divides the workload fairly evenly although also somewhat randomly between the pool of Authority nodes. As the Permission.io blockchain is based on the Ethereum blockchain, there is the concept of “gas”; gas is used to pay the transaction cost. The Authority node which completes a block is rewarded with the total of all the transaction fees paid by the transactions in the completed block.

The blockchain will comprise a small number of Authority nodes owned by Permission.io, together with other nodes owned by developers and other third parties. However, the pool of Authority nodes is not static. Aside from the fact that occasionally a node will fail and the pool will be diminished until it is restored, new nodes can be promoted into the pool and nodes can also be relegated.

Governance

Permission.io intends the blockchain to be fully decentralized and will encourage other participants to try to enter the Authority pool. The main risk to the blockchain is that some individual or group could acquire 51% control of the Authority nodes and thus post false transactions (a 51% attack).

For that reason, a fairly complex set of governance rules is being created. The plan is that a four-layer process will be implemented, consisting of Governing Nodes, Authority Nodes, Trusted Nodes and Ordinary Nodes, as illustrated in *Figure 2*.

Every new node will start out as an Ordinary Node, and will run on the test network for 6 months before there is any possibility of it being promoted. For an Ordinary Node to become a Governing Node, it has to be promoted through the ranks by the layers above, using the following procedure:

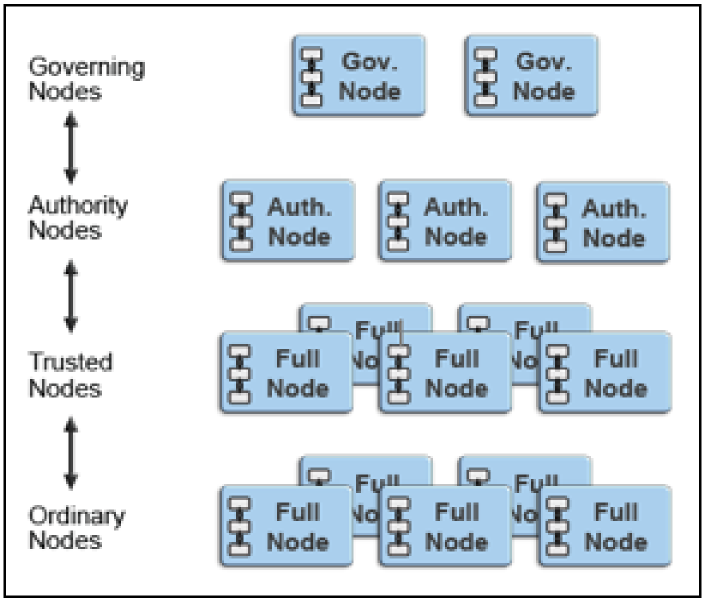

Figure 2. Permission.io Blockchain Governance

All hierarchically superior nodes, including Trusted Nodes, vote for or against the promotion of an Ordinary Node to a Trusted Node. A Trusted Node can only be promoted to become an Authority Node if the Authority Nodes and Governing Nodes vote for its status elevation. When it becomes an Authority node, it can participate in forming blocks on the blockchain. Nodes can be relegated by vote or can simply drop out. Nodes will be automatically relegated if they fail to meet the reliability, availability and performance requirements of the blockchain. Voting occurs between the 30,000 block epochs.

Permission.io's goal is to encourage its members to configure Ordinary Nodes on a global basis. In time, members will take control of the governance of what will have become a widely decentralized blockchain network.

Storage Nodes

The purpose of Storage Nodes is to store the data, both profile data and content, to serve up to members who wish to access it and to content providers who wish to upload it. The Storage Nodes are required to meet reliability and performance criteria, but aside from that there are no specific requirements. We will encourage all content providers to run Storage Nodes either individually or collaboratively.

Distributed data storage will be managed through smart contracts that are stored on the blockchain. This will provide a public audit trail of all data storage activity and all associated Permission coin payments associated with it. Our current intention, as we have already noted, is to implement IPFS for data storage. Using Permission.io's data algebra technology (discussed within the Data Algebra and Permission section) we will implement a metadata layer to provide a more comprehensive directory of the distributed data resource.

Because of the structure of IPFS, the stored data will automatically be secure, versioned and backed up. It will also be efficiently located within the network, providing a peer-to-peer access capability to its users.

Permission.io Security

There are two aspects of security to describe here. The first is the management of keys and the second is ensuring that members are real people and that no person can acquire more than one membership of the network.

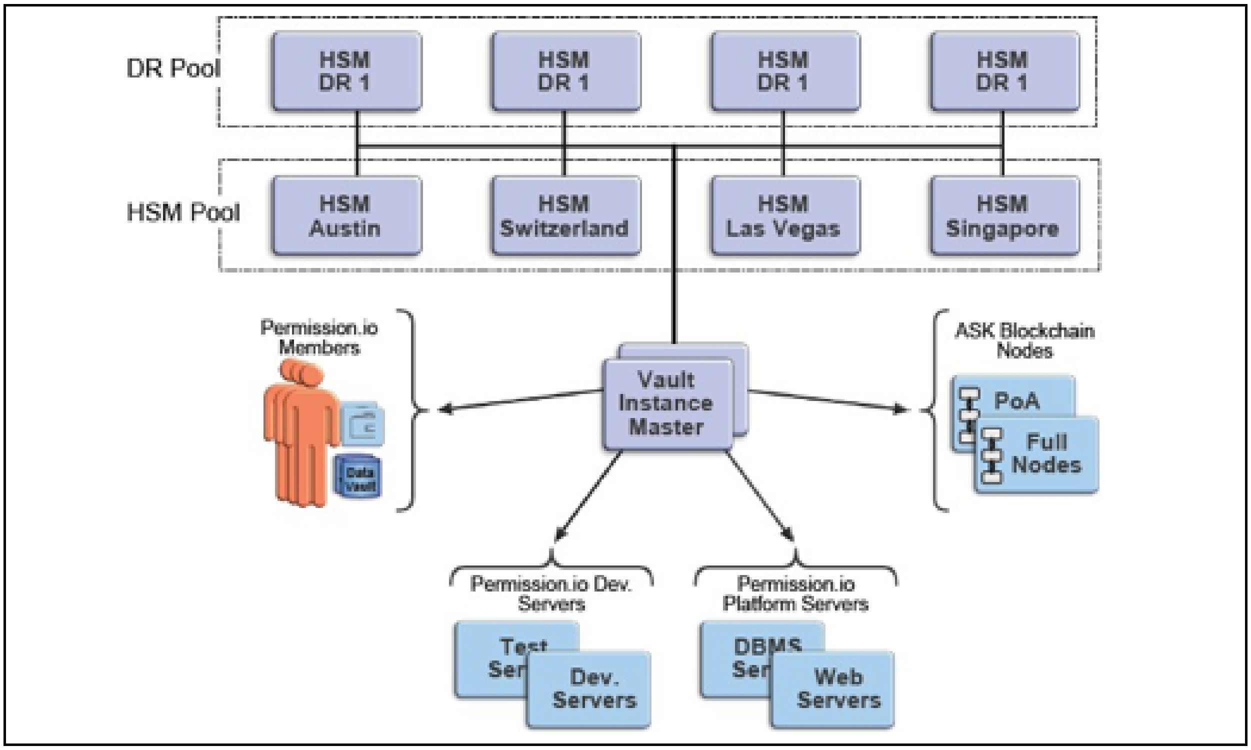

Figure 3. Permission.io Key Management

Key Management

Given that Permission.io needs to be able to support millions if not hundreds of millions of members, there is a requirement for a highly scalable key management system. Members will be provided with a key (a public and private key pair) when they register. The private key they are allocated will be used for access to their wallet and the data stored in their data vault.

The proposed solution is illustrated in *Figure 3*. Permission.io will be using open source technology to manage all keys and passwords. This will be backed by a pool of Hardware Security Module (HSM) servers, backed by a disaster recovery pool. The HSM servers will be located in different regions, providing secure high availability and redundancy.

As indicated in the diagram, there will be a cluster of redundant Vault Instance Masters interacting with members to provide keys for secrets. Similar key management architecture will be used for all other services involved in accessing, developing or running Permission.io. The primary function on this proposed architecture is for managing keys in a zero trust environment with zero knowledge of the stored secrets.

Identity Management

From both a security and business perspective, it is vitally important that every member is a genuine person and cannot be a software robot and that no one is able to establish more than one identity. Our solution to this problem can be thought of as a "Wheel of Trust," as illustrated below.

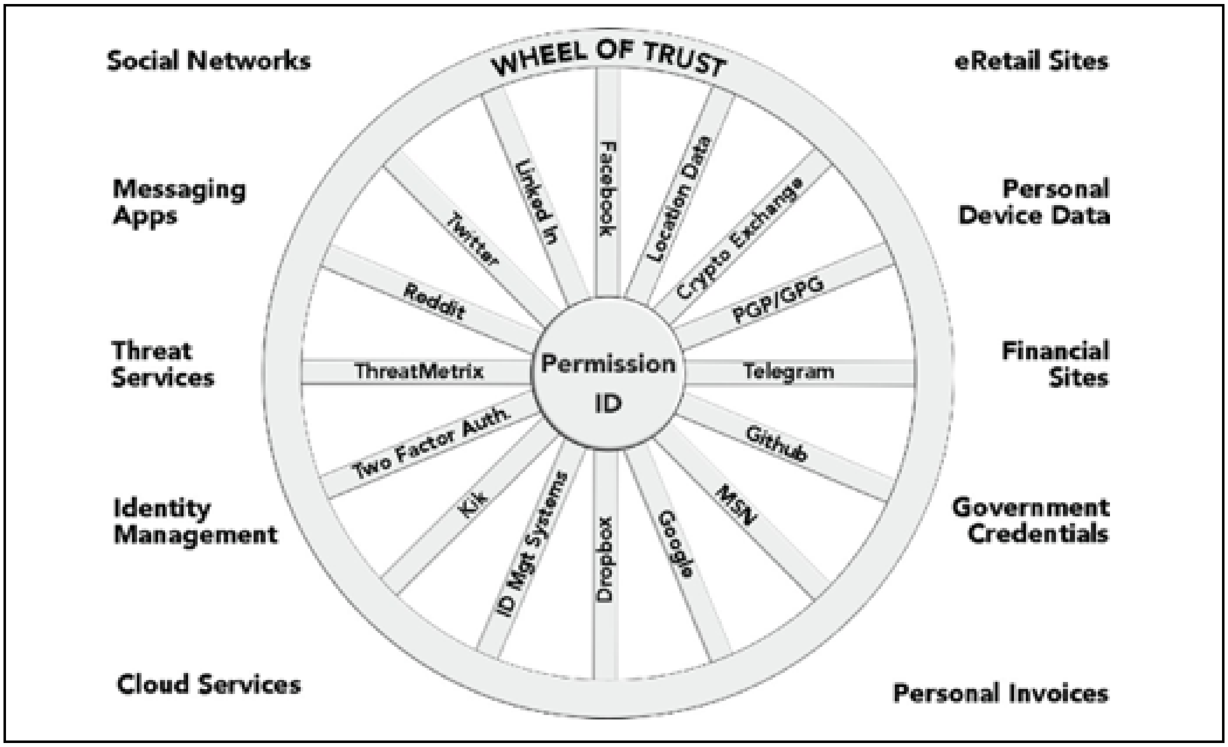

Figure 4. Permission.io Wheel of Trust

The reality is that most people already have a fairly large set of declared identity information on social networks, messaging apps, cloud services, eRetail sites and so on. While it is possible to set up fake accounts in a handful of sites, most people are unlikely to go to the trouble of setting up a large number of fake IDs. Each such set of identity details, including the two factor authentication that Permission.io implements, can be thought of as one spoke in a wheel of trust that attests to the reality of the identity's owner.

Permission.io will use such data, where members provide it, to help validate a member's Permission ID and compute their "Permission Score." We will be able to assign a probability as to whether a given member is real and we will be able to limit a member's capability and ability to earn until a believable set of identity data has been uploaded.

We can, and in many instances will, assist the identity validation process by using the services of third-parties, such as ThreatMetrix, a company that when provided with basic details can attest to a high level of probability whether an identity is valid. However, the principle is still a wheel of Trust and ThreatMetrix is still only one spoke, if a very important one, in respect of speed and convenience.

And in situations where third-party services like ThreatMetrix are unable to offer an assessment, we predict the Wheel of Trust will still provide us with a high level of certainty of identity.

Security, Manageability and Storage

Members gain access to Permission.io via OIDC compatible login credentials and use of multi-factor authentication (MFA) to ensure that only they can access their data. Their data is stored within an encrypted storage object using AES-256 encryption, in flight and at rest, that is controlled by the user. When any user data is made available to advertisers and merchants for targeting, it is stripped of all identifying data and exposed only as an anonymized, aggregated data set. All data activity is logged and auditable by the member.

No one, including Permission.io, will have access to the data held in the encrypted storage object unless they are granted permission by its owner. The owner may confer specific data access items and grant such access in the context of specific personal or business interactions. The platform software is designed to involve the minimal exposure of data and to make it uneconomic for any business to attempt to aggregate such data.

As we evolve, the innovative and comprehensive IPFS (the so called InterPlanetary File System) could be an ideal file system layer for storing data. This is a good fit within our algebraic approach to metadata (alternative approaches will be catered to as needed, e.g., where data is stored on other ledgers). The following points about IPFS are worth noting:

- Every file can be found by human readable names via the decentralized IPNS naming system.

- Each IPFS file and all blocks it contains are given a cryptographic hash (unique fingerprint).

- IPFS removes duplications (across the network) and tracks version history.

- Each network node stores only files it is interested in along with indexing information that can be used by the algebraic metadata catalog (to figure out what is stored where).

- When looking up files, it asks the network to find nodes storing the content behind a unique hash.

The Permission Coin ("ASK")

There will be 100 billion Permission coins at network launch and that number will never increase. The allocation of ASK at the time of network launch is illustrated in *Figure 5* below. The percentages shown are approximate, reflecting intentions and commitments rather than actual holdings.

The allocations are as follows:

- 20% of the supply is budgeted for building the audience.
- 20% is budgeted to SAFT participants, employees, suppliers, and strategic partners.
- 60% is controlled by the Permission Foundation.

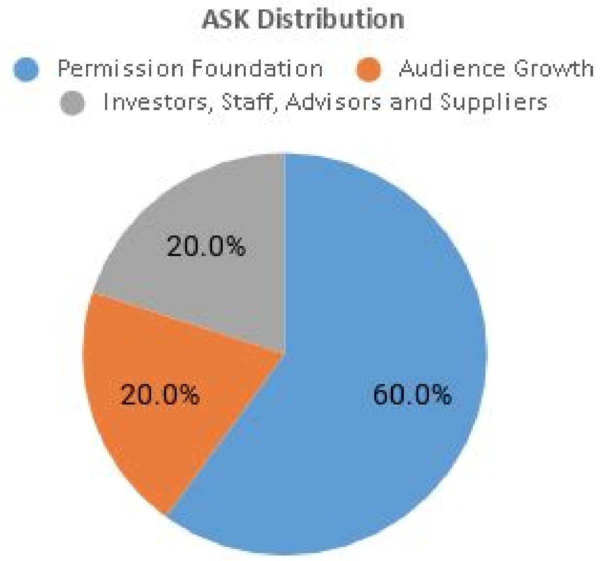

Figure 5. ASK Allocation as of July 2018

Data Algebra and Permission.io

Permission.io (previously known as Algebraix Data Corp) is the creator of data algebra, an entirely new field of mathematics. It has spent eight years developing it, proving its power to drive high performance data retrieval in many software contexts and to scale out over very large volumes of data. We believe data algebra is capable of defining and manipulating all possible data structures at any known scale.

Software based on data algebra will play a significant role in the implementation of Permission.io and will be critical to its success. The platform requires a highly versatile metadata directory (or data catalog), which will ultimately need to cater to very large volumes of data distributed across multiple blockchains and stored in a wide variety of data structures.

Design work has concluded that the personal data any given Permission.io member may choose to store will include flat files, structured database data, data objects, complex data relationships graphs and semantic metadata structures (ontologies). The data itself will be encrypted and self-defining, in the sense of knowing its origin, its lineage, its ownership and the usage permissions it can grant.

Query Acceleration

The unique capability that data algebra can provide the metadata management will be complemented by its effectiveness in other important areas of data management and network performance. Specifically, it will accelerate processing speeds significantly using its proven query acceleration capabilities and it will enable data volumes across Permission.io to scale far beyond the petabyte level. Ultimately, the software will need to accommodate hundreds of millions of data records and their frequent individual usage. Data algebra will be key to delivering acceptable performance, irrespective of scale, while ensuring the economic use of resources.

Permission.io has been issued 9 patents by the USPTO that relate to the use of data algebra in data management and database applications. In particular, several specific techniques have been developed to accelerate the performance of queries accessing files or databases.

Most of these techniques work by monitoring query activity and identifying opportunities for data reuse— they enable the precise mathematical caching of results. They have proved to be effective for queries serving BI, analytics and ETL workloads, and for RDF database workloads—often accelerating performance by one or two orders of magnitude.

Aside from query acceleration, data algebra can be usefully employed in monitoring and managing a large data resource. By monitoring all data usage within a given data environment, it can optimize data storage structures and data location in ways that will reduce access times and minimize resource usage (CPU, RAM, etc.).

Open Sourcing of Data Algebra Code

Data algebra will be an integral part of Permission.io software and an inherent part of the blockchain implementation. As we believe that the benefits data algebra confers need to be available to the whole developer community, source code will be made available on an open source basis. We intend to create an independent open source project that involves extensive use of data algebra.

Readers who wish to explore data algebra in greater depth can download the free eBook, The Algebra of Data, A Foundation for the Data Economy (by Professor Gary Sherman, PhD, and Robin Bloor PhD) at https://permission.io/get-book/ It is also available as a paperback on Amazon.com

Product Roadmap

For Q2 2019

- ASK Launch
- Permission.io Blockchain (LiveNet)
- Open Source (Blockchain)
- Integration with Hardware Wallets (e.g. Trezor, Ledger)

For Q3 2019

- Member, Merchant and Advertiser Reputation Algorithm
- Partnership with affiliate programs
- Partnership with ecommerce platforms
- Merchant portal (Internal)
- Ability to run Permission node (3rd Party)

For Q4 2019

- Product Search Optimization
- Keyword Bidding System
- Integration with ID Management Systems
- Enhanced Personal Datasets
- Federated Consensus
- Permission Blockchain Governance Policy and System
- Merchant Portal (External)
- Enhanced Reporting & Analytics

For Q1 2020 - Q2 2020

- Encrypted Communication
- Integration with Decentralized Identity Systems
- Permission Browser Plugin
- Targeted Personal Dataset Query
- Enhanced Reputation Algorithm

For Q3 2020 - Q4 2020

- Decentralize the Blockchain
- Self-serve Merchant Portal
- Query Optimization with Data Algebra
- Developer API/SDK
- Two-Sided Marketplace

Permission.io Executive Team

Charles Silver, Chief Executive Officer

Charles Silver has been building companies and creating liquidity events for shareholders for nearly 30 years. In the dot com era he founded RealAge, which was the leader in using data to connect brands with consumers on a permission basis. The company was very successfully sold for 9 figures to the Hearst Corporation. Prior to RealAge, Mr. Silver founded and built the Oil Dispatch franchise in Michigan. It grew to be the largest independent quick-oil-change operator in the state and was successfully sold to Jiffy Lube.

Mr. Silver is also co-founder and serves on the Board of Reality Shares Inc. (dba Blockforce Capital), the parent company of Reality Shares Advisors, a SEC registered investment adviser with 7 publicly traded ETFs. The firm launched the first blockchain ETF (BLCN) in partnership with Nasdaq and also manages two cryptocurrency hedge funds.

Andy Shah, Chief Technology Officer

Andy Shah is a technology executive with more than 20 years of experience in engineering, emerging technologies, product development and business strategy. Most recently he was CTO of an Austin, TX based company where he built a cloud-based advertising platform connecting consumers and advertisers.

Andy served as AVP of Software & Technology for Westell Inc (NYSE:WSTL) where he innovated and helped build the patented permission-based platform that securely protects, shares and synchronizes end users' personal data. Under his guidance, the Company completed $80M of acquisitions. Andy was Director of Engineering & Project Management for Sears Holding Corp (NYSE:SHLD) where he built and optimized an ecommerce marketplace. At Cleversafe Inc, he was instrumental in building a platform that was later sold to IBM for $1.3 Billion. Prior to Cleversafe, he held various technical roles as a Solution Architect, Software Architect and Software Engineer at Motorola Inc (NYSE:MSI). Andy has a Masters Degree in Computer Science and Chemical Engineering from the Illinois Institute of Technology and holds several patents.

Steven Wilkinson, CISSP, CBP - Chief Information Security Officer and Data Protection Officer

Steven Wilkinson is a certified cryptocurrency, blockchain, identity and information security professional. He brings more than 20 years of experience in technology leadership, IT and security consulting to Permission.io. While building solutions for value transfer across the Internet, Steven discovered Bitcoin in early 2011 and quickly became a miner and evangelist. Since then, he has been leading and advising on a variety of different blockchain and security projects in the digital asset space.

In 2013, Steven founded the Bitcoin consulting firm, Austin Bitcoin, which was one of the first BitPay merchant integration partners. He also serves on the Board of Directors for the Texas Bitcoin Association and is the co-founder and Vice President of the Texas Bitcoin Conference.

Steven holds a Certified Information Systems Security Professional (CISSP) certification and a Certified Bitcoin Professional (CBP) certification.

Matt Erhart, VP of Finance & Compliance

Matt Erhart is a seasoned regulatory compliance professional with nearly a decade of experience in highly regulated industries, including brokerage and exchange markets, asset management, banking and consumer lending. Most recently he worked for Blockforce Capital where he served as the Chief Compliance Officer for Reality Shares Advisors, an SEC registered investment advisor managing approximately $300 million in assets.

Matt began his regulatory compliance career at the Financial Industry Regulatory Authority (FINRA) which is responsible for regulating brokerage firms and exchange markets in the United States. He holds FINRA Series 7, 24, and 66 licenses. Matt graduated Summa Cum Laude from the University of Kansas where he earned his degree in Finance.

Disclaimer

This information (the “Information”) is not intended to be an offer to sell, or a solicitation of any offer to buy, any security or other financial instrument or to invest in ASK and are for informational, illustration and discussion purposes only. This Information may not be complete or final, may be estimated, based on predictions and assumptions, subject to change and does not identify all material risks. The offering of ASK has not been registered or approved under any securities, commodity, futures, financial instruments, capital markets legislation, regulation, or ordinance of any jurisdiction. This Information does not constitute an offer, solicitation, or marketing to the retail public in any jurisdiction where such offering is unlawful. Opinions, assumptions, assessments, statements or the like regarding future events are forward-looking statements. These forward-looking statements are expressed in good faith and based upon a reasonable basis when made, but there can be no assurance that these expectations will be achieved or accomplished. These forward-looking statements are subject to known and unknown risks, uncertainties and assumptions that may affect actual results of the Permission Marketplace such as audience growth, user experience, speed of payments to the viewer of advertisements, or achievements expressed or implied by such forward-looking statements. In some cases you can identify forward-looking statements by terminology such as “may”, “should”, “could”, “would”, “expect”, “plan”, “anticipate”, “believe”, “estimate”. The Permission Marketplace and ASK have inherent risks and uncertainties, both general and specific, many of which cannot be predicted or quantified and are beyond the control of Permission.io. Permission.io does not make any representation or warranty as to the accuracy or completeness of the information contained in this Information. Permission.io has no obligation to update or keep current any material or projections contained in this Information. Permission.io may be subject to complex and evolving laws and regulations, both foreign and domestic; Permision.io may not successfully develop, market and launch the Permission Marketplace and, even if launched the Permission® Marketplace may not be widely adopted and may have limited users and could be subject to significant competition.