

# PEER MOUNTAIN

---

## WHITE PAPER

21/12/2017

## DISCLAIMER

This White Paper is for information purposes only. Peer Mountain does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights. Peer Mountain and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. Peer Mountain does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided "as is". In no event will Peer Mountain or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference

to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.

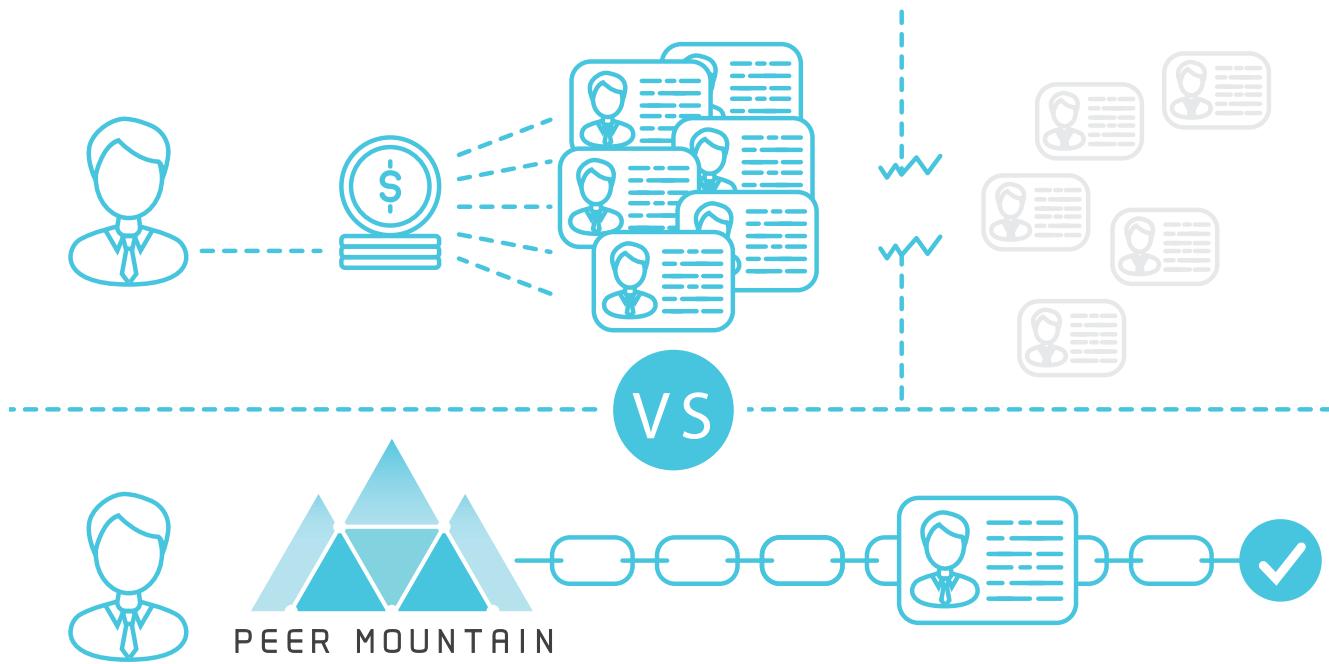
This paper is a description of the current and planned Peer Mountain ecosystem, the actors building it and the project that is working on it. It is neither a solicitation nor a prospectus. This paper may include predictions, estimates or other information that might be considered forward-looking. While these forward-looking statements represent Peer Mountain's current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forward-looking statements, which reflect the opinions of Peer Mountain only as of the date of this publication. Please keep in mind that Peer Mountain is not obligating itself to revise or publicly release the results of any revision to these forward-looking statements in light of new information or future events.

## ABSTRACT

The recent string of high-profile data breaches highlights the dire shortcomings of current data protection and storage methods. In summer 2017, cybercriminals breached Equifax's secure servers and stole the sensitive personal information of 146 million Americans<sup>1</sup>. That information - Social Security Numbers, credit card details, dates of birth - could potentially be sold the dark web, putting the identities and financial security of millions of hard-working people at risk. In response to this crisis, governments and regulators are passing legislation that requires businesses to

collect and store sensitive data more securely and to test existing methods of storage and manipulation of data and documentation - see, for example, the EU's General Data Protection Regulation.

Events like these demand that we make radical and fundamental changes to how we store and guard our identities. The problem is not only that data storage and protection procedures of enterprises like Equifax aren't broad or rigorous enough. The issue lies in the overall method in which these companies store, guard, and transmit data.



Every time a person transacts with a bank, credit agency, government, or online retailer, that organization generates and stores a copy of that person's information following a number of rules and regulations according to the specifics of the interaction. The result is a world of enormous digital fortresses, each holding a duplicate of the identity of anyone who has ever been a customer. These fortresses - the centralized servers that hold all our information - are rich, obvious targets for cybercriminals. No matter how many digital moats, archers, and catapults the defenders build and deploy, the attackers will keep coming. And a single breach of any one of these

fortresses can result in the loss of millions of identities.

Developers can harness blockchain technology to give individuals further ownership of their personal information, and enable them to store that information in a distributed ledger, thus helping effectively mitigate the risk of identity theft. To achieve this goal, many organizations have launched blockchain-based platforms over the past year; several of them have also had successful coin offerings. Peer Mountain goes beyond providing users with further ownership and control over their cryptographically secure identities, offering an end-to-end application ecosystem designed

to facilitate the commerce and exchange of digital and physical services. It facilitates trust and the secure sharing of information with multiple independent parties across broad networks while preserving traceability and compliance at every end of the transference of data.

Peer Mountain is the first decentralized peer-to-peer trust marketplace that connects self-sovereign identity owners with regulatory-compliant service providers, and opens a new paradigm for how and where individuals and organizations conduct business.

1 <http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html>

# THIS IS PEER MOUNTAIN

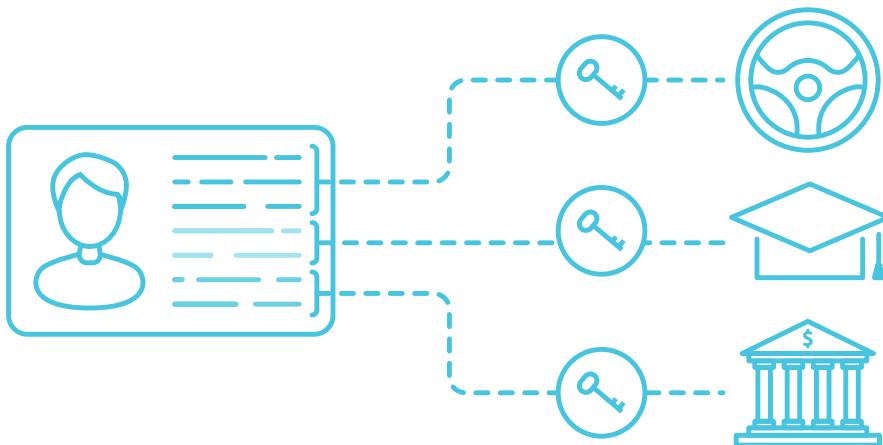
Peer Mountain is a mobile-first distributed system of trust. It uses cryptographic protocols to allow people and institutions to create and own a trusted record that encompasses digital identity, trust relationships, and proof of activities.

System members own and control their data; they decide who can access it, as their information remains inaccessible and unexposed to third parties at all times. Peer Mountain uses such powerful cryptographic protection that data stays guarded from all other entities - **even the platform itself**.

At a more abstract level, the ecosystem allows individuals and companies to assert facts about themselves and other parties, and to attest (i.e. verify) those assertions. This is especially valuable for financial institutions as it can significantly lower the cost of Know Your Customer (KYC)-compliant client onboarding. This paper explores this further in the section [Peer Mountain KYC & Compliance](#).

To organizations in sectors other than financial services and markets, Peer Mountain can also provide considerable value as a distributed platform of trusted facts (e.g. employees could assert that they are sick and HR could attest to this after verifying a doctor's certificate).

Ecosystem participants are only identified by their public keys (analogous to how Cryptocurrencies work) and can assume multiple personas, which are basically public keys derived off their root key. Personas are useful for interacting with multiple external parties and to comply with different set of obligations and requirements. For example, a person may be a university student and the client of a bank. Generally speaking, the university requires an information subset that differs from the subset the bank requires. However, while applying for a loan or grant, a university student may not want the university to know they are a client of a specific bank. By using different personas (i.e. a role), the student controls their privacy.



## EXECUTIVE SUMMARY

### MARKET OPPORTUNITY

The world is evolving toward a new standard in which individuals further control the access to the data and documents which constitute their identities through distributed ledger technology. The past year has seen a number of successful offerings from teams developing platforms for self-sovereign identity, the most visible of which is [Civic<sup>2</sup>](#). There are also many new and established offerings in the

Know Your Customer (KYC), identity verification, and trust provisioning spaces, including [Mitek<sup>3</sup>](#), [Jumio<sup>4</sup>](#), [AriadNext<sup>5</sup>](#), [WorldCheck<sup>6</sup>](#), [KYC3<sup>7</sup>](#), and [LexisNexis<sup>8</sup>](#).

Now is the right time for an ecosystem that realizes the vision of self-sovereign identity across multiple platforms and entities while satisfying compliance and commerce requirements. Peer Mountain delivers the full potential of this emerging paradigm.

2 <https://www.civic.com/>

3 <https://www.miteksystems.com/mobile-verify>

4 <https://www.jumio.com/trusted-identity/netverify/>

5 <https://www.riadnext.com/products/idcheck-io/>

6 <https://risk.thomsonreuters.com/en/products/world-check-k-now-your-customer.html>

7 <https://kyc3.com/>

8 <https://www.lexisnexis.com/en-us/products/lexis-diligence.page>

## SOLUTION: A MARKETPLACE BUILT AROUND SELF-SOVEREIGN IDENTITY

Peer Mountain uses blockchain technology to give individuals and organizations full, secure ownership of their identities, and, for the first time, enable people to safely share their self-sovereign information with organizations and each other. Peer Mountain facilitates the rapid delivery of services through its blockchain framework. Identity is a core component of Peer Mountain, but this is not an identity platform. Peer Mountain is an application ecosystem designed to facilitate the commerce and exchange of digital and physical services.

Later versions of the Peer Mountain architecture will also support organizations, enabling them to model their structure through persona delegation and attach corporate identity documents to the main corporate persona. Organizations using Peer Mountain can use delegation to demonstrate ownership and control. Peer Mountain can then provide a verifiable record of these facts that can be shared with any organization or individual with a need to know. Specific bodies, such as a commercial registry or a trade authorizing body, can implement attestation engines to validate these facts.

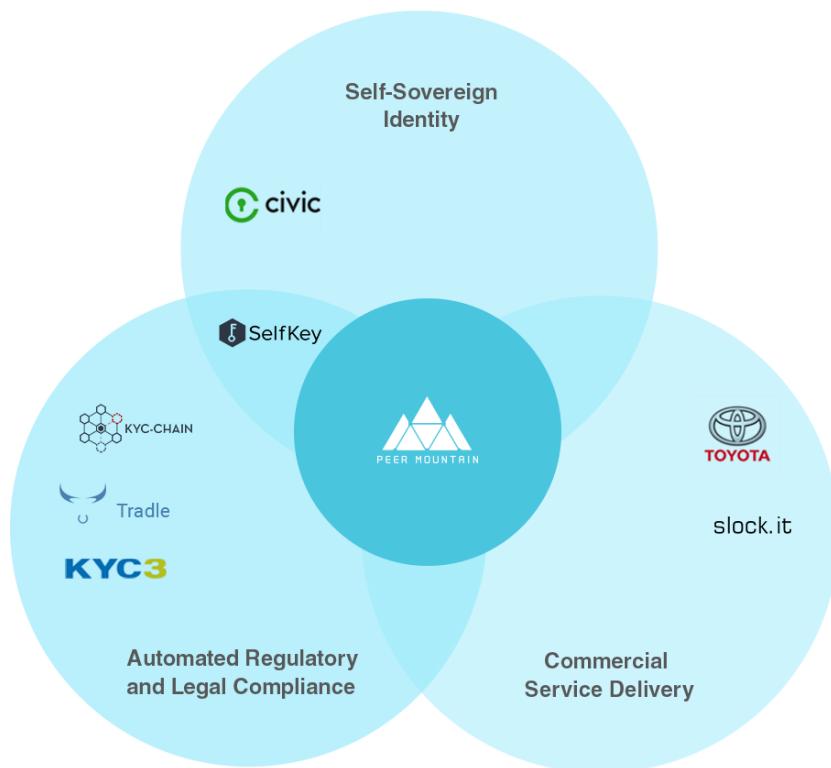


Figure 1: The Peer Mountain Trust Ecosystem

Peer Mountain is at the intersection of consumers who want **Self-Sovereign Identity** and service providers who need **Continuous and Reliable Compliance and Efficient Commercial Service Delivery**. Trust providers offering validation services to third parties further support the ecosystem, which reinforces itself with network effects through **Trust Interoperability and Portability**. Peer Mountain is the facilitating technology for the Trust Ecosystem and sits right in the middle - without requiring that any of the three interests (consumers, service providers and trust providers) make a compromise of using someone else's platform or solution. It's truly peer-to-peer.

Peer Mountain is a secure ecosystem, allowing users of various applications, including those presented in Figure 1 above, to share their information with one another. By building a world of sovereign identities and linking them together securely, Peer Mountain is creating a marketplace of trust across disparate entities operating in the global economy.

Peer Mountain's vision is to enable each of us, whether individual or organization, to manage our real-world trust online - to choose who we trust and

how we trust based on our own assessments, values, and conclusions about the world.

A major technical objective is to enable rapid consumption of services that are complex, difficult to deliver, and subject to regulatory requirements. With Peer Mountain, a user can complete a typical service dossier, such as a credit card application, in under 10 minutes. A person can find a service they want, share required information, and have trusted third parties attest to that information. Then the service provider can simply provide the service, completing the exchange seamlessly.

Each Peer Mountain user maintains control of their data. They never have to leave their personal information with businesses that require identification for any longer than is required by the regulations governing the service. This means that they may no longer need to provide hotels with copies of their passports, or give rental car companies copies of their drivers' licences and credit cards. Peer Mountain provides the platform that facilitates secure sharing and recordkeeping for all of these scenarios, effectively reducing the risk of stolen or exposed customer data.

Peer Mountain therefore creates a trust model that makes business interactions much smoother and efficient. It significantly reduce lengthy certification and identity verification processes, reduces liability, and allows businesses to focus on delivering services to their customers. All data resides in a distributed ledger and is securely transmitted across the

Peer Mountain ecosystem, relieving institutions of the burden of storing each customer's sensitive information in cases when their governing laws allow such relieve. Peer Mountain gives businesses all the information they need in order to transact quickly, at a low cost and with little risk, while simultaneously giving ownership of identity back to the people.

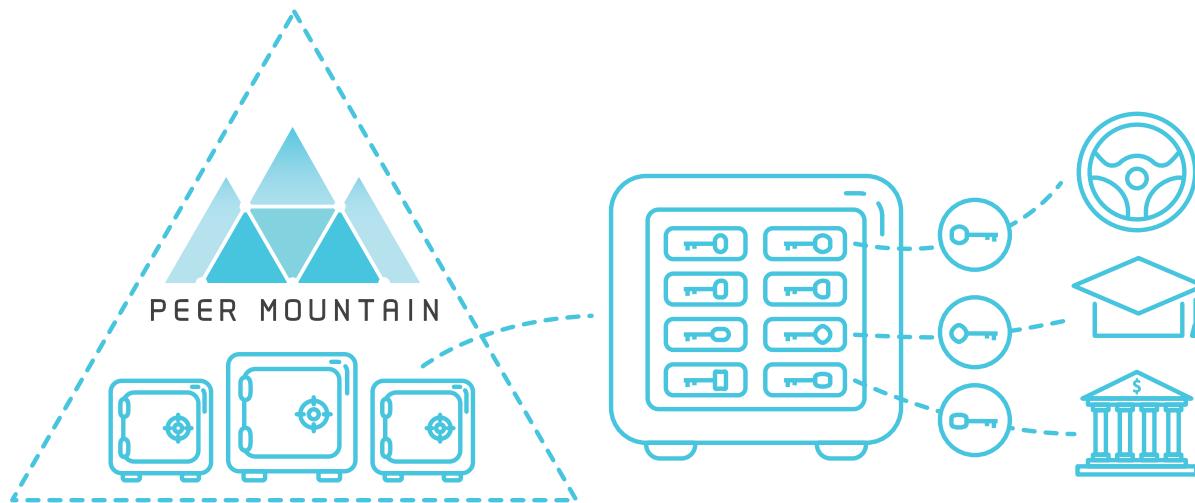
## THE MOST SECURE IDENTITY SOLUTION ON THE MARKET

---

Think of Peer Mountain as a real mountain range with vigilant border guards all around it. Each Peer Mountain user has their own secure "bank vault" full of safety deposit boxes hidden inside these mountains. They can put copies of their documents into different boxes with special keys. Each key is unique and users can share them separately with entities they trust. Using this special key, these entities can access the user's vault and **acquire the information that has been shared with them, and nothing else**. If the user decides to revoke access, the documents vanish from

the drawer and the lock on the drawer is changed as far as this is possible according to governing laws of the business relationship. Furthermore **access to Peer Mountain is by invitation only**.

Activity is pseudo-anonymous and private. With Peer Mountain, you use different personas to interact with different entities, so your activity with one entity remains totally separated from interactions with others. Not only is the data private, interactions are private as well. Of course, you can choose to share this later, but the choice always remains yours.



Peer Mountain is a peer-to-peer solution that gives you control, privately and securely. You can use your persona to conduct business and sign legally-binding, ZertES<sup>9</sup>-compliant documents.

Peer Mountain is open to any service provider. You can access services directly from the source in total security, and review all the services you consume easily - anytime, anywhere.

Your master key is a 4096-bit RSA key. **The time required to crack this key would exceed the lifetime of the Milky Way galaxy**, even with all of the computers available on Earth today. Peer Mountain uses the most secure encryption and authentication algorithms<sup>10</sup> from certified operating system libraries which are thoroughly tested and well-maintained. Information is only decrypted at your device after authentication; nothing is visible anywhere else. Even if you lose your device, **nobody can exploit your keys**, as they are protected by your authentication

PIN and fingerprint. Your keys are stored in your smart device's hardware-backed storage, making them unavailable for extraction. Once keys are in a hardware-backed key store<sup>10</sup>, they can be used but cannot be exported. Other applications can't see or access your keys - not even the OS kernel. Only you have access. If you lose your mobile device, you can safely recover your key using an offline secret that only you keep. You can also create a quorum of friends that can recover your key only if a number of them all agree. And you can still require a secret so that they can't do this without your agreement.

Peer Mountain provides the best protection from identity theft and fraud on the market. Nobody can impersonate you, because they don't have your keys. Stealing identities means stealing the private keys from each person's device, one device at a time, which is an unfeasible amount of work to steal just one identity.

<sup>9</sup> ZertES is a Swiss Federal law that regulates electronic signatures.

<sup>10</sup> RSA-PKI, AES-256, HMAC-SHA256

<sup>11</sup> Secure Element, TPM, or TrustZone

## TOKEN ECOSYSTEM

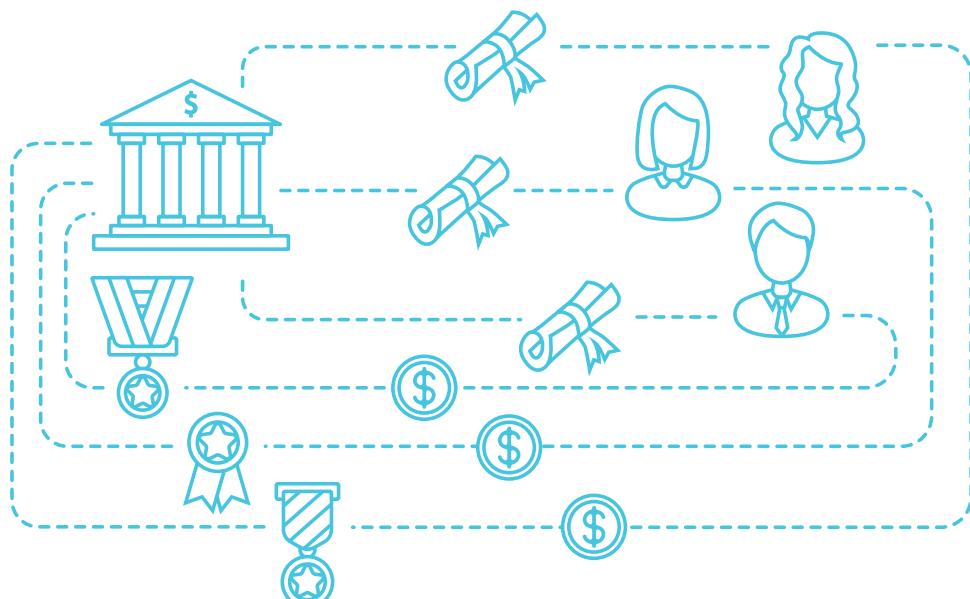
The Peer Mountain Token (PMT) is a utility token used to measure the value of trustworthiness within the Peer Mountain ecosystem. Consumers of trust transfer PMT to the entities they trust the most. The only way to earn PMTs is to be trustworthy. Individuals and enterprises use PMTs to consume attestations and generate invitations. Because Peer Mountain technology is cross-chain capable, entities can use PMTs to move information from one chain application to another, e.g. from Ethereum to Stellar-based Peer Mountain instances.



Figure 2: The Peer Mountain Circular Ecosystem of Trust

There are three components that make up the Peer Mountain ecosystem: the mobile end-user (the consumer); the enterprise back end (the service provider); and the attestation engines (the certificate provider), which are very powerful. Every peer on the system is an attestation provider. Organizations of all sizes can run specialized and sophisticated attestation engines. For instance, a financial institution may want to run its own attestation engine to check clients against a user blacklist and calculate credit scores. The institution can then affirm whitelisted clients based on assertions and other attestations in the system.

The token model for Peer Mountain establishes and sustains an ecosystem for attestation providers, invitations, and service offerings. Every time a prospect consumes an invitation or service offering, the service provider pays a small fee in tokens. This includes the issuance of attestations, which is a service offering; this also prevents "attestation spamming", which would be when a peer produces superfluous attestations with the hopes that they may be used in order to gain PMT. On the other side, each time an entity uses an attestation to establish trust in a relationship as part of a dossier, the provider of that attestation



receives a micro-payment in PMT. This means that the most trustworthy attestations generate the highest income for their issuers. An attestation's trustworthiness accrues naturally based on the decisions of the clients that choose to rely on it. This also means that clients who want to earn a living as attestation providers must maintain the highest standards of integrity in order to maintain their attestations' value.

As the system is peer-to-peer, any client can play any or all of the three roles. Service providers can provide attestations to open up new revenue streams. For example, utility company bills are used to prove residency. With Peer Mountain a utility provider can implement an attestation engine that verifies

service delivery to a person's address, thus proving an individual's connection to a physical address, rather than letting others rely on an easily forged utility bill. The company then receives micropayments for each such attestation. This creates a circular economy in which net service providers need to acquire tokens to fuel their offerings and net attestation providers have surplus tokens to liquidate. In order to facilitate this, the Peer Mountain token will be traded through *regulated* blockchain token trading companies. It is also important to note that peers in a pure consumer role needn't concern themselves with tokens, which is important for the general consumer population's adoption of Peer Mountain. However, as it is peer-to-peer, anyone with

the inclination, technical skill, and value to add can become a service provider or attestation provider. The number of tokens is fixed and transaction costs are variable, decreasing as the velocity of tokens increases. As the number of transactions increases, the economy's velocity will accelerate. This may create a deflationary effect on the PMT. The tokens, being fungible, will naturally need to be divided as product costs will remain fixed in fiat terms but will decrease in token terms. The number of users will drive the number of transactions, which, in turn, will drive the velocity of the token. With our first-rollout community of an estimated 12 million users, we expect sufficient transaction volume to generate significant revenue streams within the economy.

## ESTIMATED MARKET SIZE

---

The market for data security is immense and growing rapidly. According to a 2017 report, the "global cyber security market was valued at USD 105.45 billion in 2015, is expected to reach USD 181.77 billion in 2021, and is anticipated to grow at a CAGR of 9.5% between 2016 and 2021."<sup>12</sup> The development of distributed-ledger-based solutions is helping drive this growth. More and more consumers and businesses are choosing these solutions as they become aware of the risks inherent to legacy information storage systems. Increasing incidences of identity theft are making the cyber security risks of centralized data storage and

transmission painfully clear: a recent Javelin Strategy & Research study estimates that in 2016 consumers lost over USD 16 billion to identity theft.<sup>13</sup> Further fueling this shift to a blockchain model is the market's growing familiarity and comfort with distributed ledger technology. As people come to realize the benefits of a distributed ledger, they will adopt secure systems like Peer Mountain, the first marketplace of its kind based on self-sovereign identity. We expect the highest levels of adoption to come from North America and Europe in the near to medium term.

## CROWDSALE

---

Peer Mountain will be the first offering of "ICO 2.0." We believe in maximum transparency and full regulatory compliance. The Peer Mountain offering debuts and advances a number of important innovations: we are debuting our Smartcap™ algorithm to optimize the ICO and match tokens sold with demonstrated demand, and we have committed to the ICO Charter standardising E.U. token offerings. Peer Mountain will run a transparent and fair token sale.

The PMT sale will take place in early 2018 - the exact date will be announced on the [www.peermountain.com](http://www.peermountain.com). There will be a pre-order phase for whitelisted participants to place pre-orders for the sale, followed by an open token sale. We intend to follow best practices for the most compliant and well-run ICO and token sales to date, with maximum transparency. The token sale will accept Ether, and it will be an ERC-20-compatible token<sup>14</sup> (so within the standard) on the Ethereum network.

## TOKEN SALE

Peer Mountain intends to raise a minimum of 39,488 ETH to build and deploy Peer Mountain into the world's blockchain application standard for trustworthy commerce in nearly any legally regulated environment. PMT shall be issued and sold by Peer Mountain DCB Limited, a special purpose financial company registered in the British Virgin Islands. The Peer Mountain founders are the current beneficial owners of the structure and the governance of the assets in the structure will follow a two signature requirement for access to funds that will be implemented with a series of multi-signature enabled hardware wallets, some of which shall be kept in traditional safe deposit boxes.

12 Source: Zion Market Research. [Cyber Security Market Share & Trends, 2015- 2021: Global Industry to Reach \\$181.77 Bn by 2021](https://www.zionmarketresearch.com/reports/cyber-security-market-share-trends-2015-2021-global-industry-reach-181-77-bn-by-2021), 23 June 2017.

13 Source: Javelin Strategy and Research. [Identity theft, fraud cost consumers more than \\$16 billion](https://www.javelinsolutions.com/research/identity-theft-fraud-cost-consumers-more-than-16-billion), 1 February, 2017.

14 [https://theethereum.wiki/w/index.php/ERC20\\_Token\\_Standard](https://theethereum.wiki/w/index.php/ERC20_Token_Standard)

## SMARTCAP™ TOKEN SALE

The PMT token economy and the PMT token sale have both been carefully designed by Jed Grant and validated by Prof. Jos Van Bommel, an expert in IPO securities, liquidity and valuation. In this regard, we propose a new method of token sale that is embodied in our token sale's smart contract; we call it the Smartcap™ algorithm. Smartcap™ facilitates price discovery within the token sale in a way that is satisfactory to all buyers and enables the sale to be capped at a market-determined amount.

As libertarian capitalists, we believe in individual freedom, fairness, transparency, and great customer service. We conclude that current token sale methods have several deficiencies:

- The traditional pre-sale is opaque, secretive, and lends itself to front-running and insider dealing.

- The open cap creates a greed effect that leads to irresponsible allocation of capital.

- The fixed cap creates a paradox whereby the sale organizers must guess the exact market demand prior to launching the sale; if they guess wrong, they either leave the market unsatisfied or have an "unsuccessful" token sale or ICO - even if they raise substantial amounts of capital.

The principle of the Smartcap™ is straightforward. The sale proceeds in sequential rounds of fixed amounts of tokens at a fixed price. Orders are accepted for the round. When the order quantity exceeds the number of tokens in the round, the round closes. The closing procedure sorts the orders from largest to smallest and fills them in this order, i.e. larger purchases get priority for the round. Any surplus or partial fills are allocated with priority to the following round. In each round, the quantity of tokens supplied for

the subsequent round increases by an algorithmically determined amount, and the token price also increases by a much smaller algorithmically determined amount. The increase in supply is roughly an order of magnitude greater than the increase in price. The sale closes at the first incomplete round, and all tokens sold in this final round are sold at the price of the prior round. Optionally, a Smartcap™ sale may have a pre-order round where orders of a certain desirable character may be accepted. This character may be order size, the strategic nature of the acquiring partner, or any other criteria that benefits the project. As part of the Smartcap™, these characteristics will be transparent. The Smartcap™ code will be published in the contract. These pre-orders are then guaranteed first-in placement, ordered by the priority level of their character.

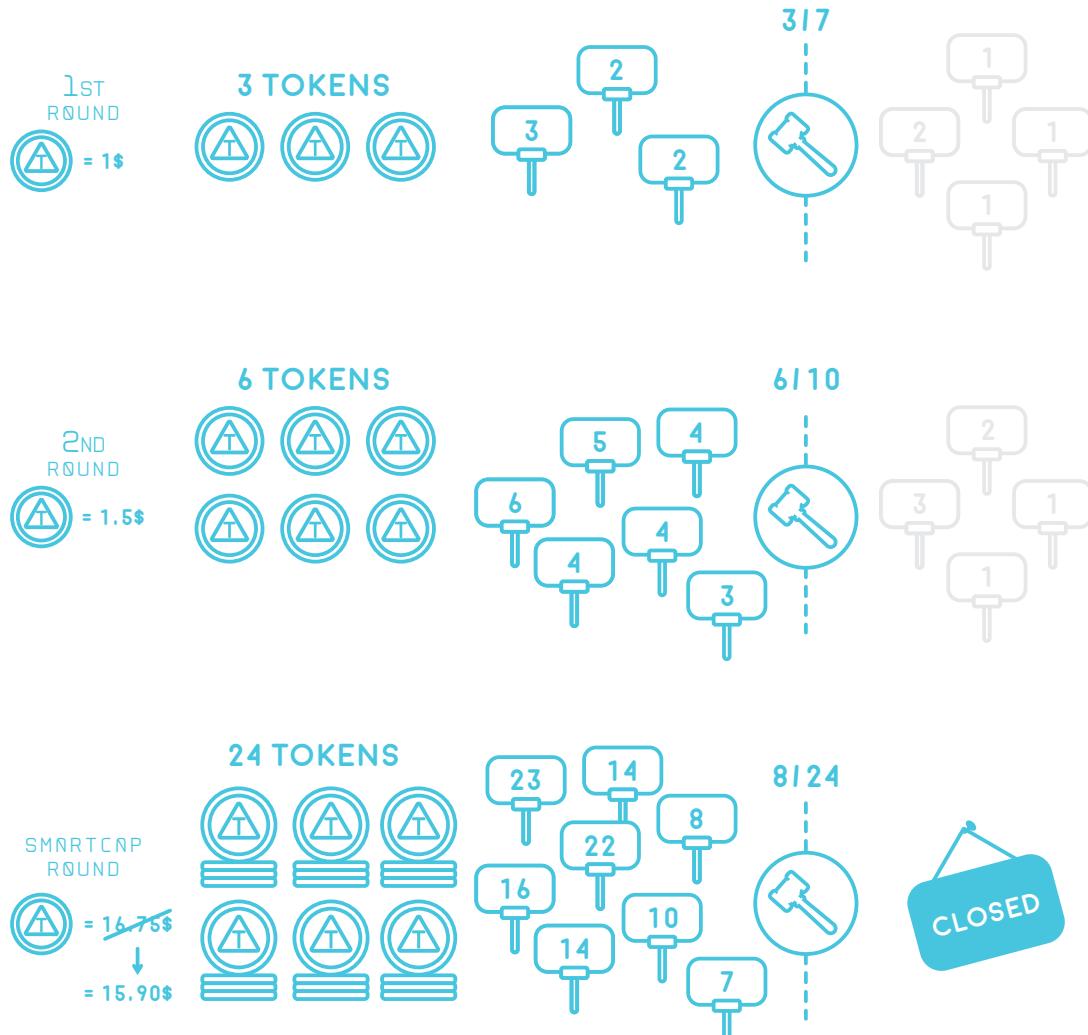


Figure 3: The Peer Mountain Token Sale

The Smartcap™ accomplishes many of our objectives:

- 1 It eliminates the pre-sale and brings transparency to the whole token sale process
- 2 It provides a price discovery mechanism for the sale
- 3 It increases the supply and price of tokens algorithmically until demand / price are satisfied
- 4 It rewards large investors by placing them at the front of the queue in each round

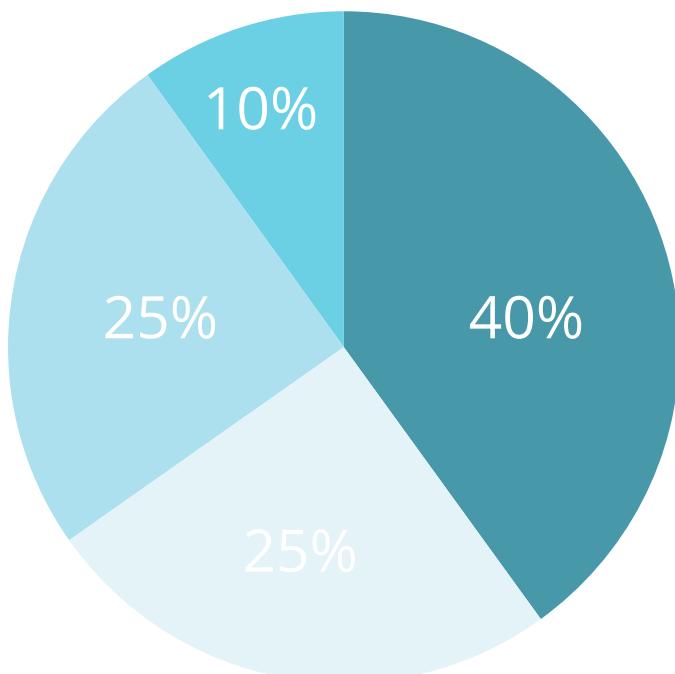
We expect the Peer Mountain Smartcap™ sale to run for four to six rounds, with a pre-order phase of one week that will be open to any buyer that pre-registers. A four-round cap will result in approximately 9,349 ETH being raised. The Smartcap™ details will be visible in the token sale smart contract. The Round 4 close figures presented below illustrate the values

when five rounds would close *to the token* and are for illustrative purposes only. Statistically, it is highly unlikely that these exact figures will be reached as the Smartcap™ will accommodate a partial final round, issuing tokens to buyers that participated in the final round at the price of the last complete round.

#### PEER MOUNTAIN SMARTCAP™ PARAMETERS

NAME	Peer Mountain Token	Sale	40% of PMT issue
TICKER	PMT	Peer Mountain Reserve	40% of PMT issue
Round 1 size	2,000,000 PMT	Team Compensation	10% of PMT issue
Round time limit	30 DAYS	Legal Reserve	8% of PMT issue
<b>Outdated figures. For latest figures see <a href="https://peermountain.com/token-sale/">https://peermountain.com/token-sale/</a></b>			
Price Discovery Factor	5%	Token Type	ERC-20 Standard Tokens
Smartcap™ Round 1 Discount	30%	Accepting	ETH
Token Parity Level	1,500 PMT = 1 ETH	ICO End	At Smartcap™
Round 4 cap cumulative sale	223,437,500 PMT		
Round 4 cumulative ETH	124,181 ETH		
Round 4 price discovery point	1,728 PMT = 1 ETH		

#### ALLOCATION



We will allocate proceeds across four principal areas of interest:

#### 40 %

Technology, which includes the development and audit of Peer Mountain smart contracts, blockchain nodes, application architecture, mobile and enterprise clients, and other milestone objectives

#### 25 %

Corporate development, which includes typical company expenses such as office space and equipment, administrative and managerial salaries, fees, and taxes

#### 25 %

Marketing, which includes PR, marketing, and partnership initiatives

#### 10 %

Regulatory and legal, which includes lobbying and development of regulatory suggestions

We will use the reserve for corporate issuances and to generate income so that the Peer Mountain can continue to develop products and solutions. We will allocate the remainder to other purposes, such as the legal reserves.

We expect the token economy to increase in velocity over time and for token prices for services to have a deflationary effect within the Peer Mountain ecosystem. This may conversely create an appreciation effect of the token vis-a-vis other currencies. We believe that each new attestation provider, end user, and service provider that joins the system will increase the frequency of token exchange. The tokens are fungible; tokens can be subdivided, so prices may decrease in token terms and increase in fiat terms over time.

## USE OF PROCEEDS

The milestones below are our intended goals given the available resources. Our intent is to create a sustainable and long lasting ecosystem that captures the value of trust in business relationships under regulatory constraints. Irrespective of these indicative values given by each milestone, we intend to achieve as many of these objectives as possible irrespective of the amount raised. In this regard, our planning is based on rough amounts which is the only way forward given the volatility of crypto-currencies today. We view the creation of a community driven and sustainable range of Peer Mountain instances across service sectors with as many consumers as possible as the overarching objective of the project.

### MILESTONE 1: 10K ETH

Peer Mountain Development - Financial Services: We are building the Peer Mountain ecosystem with our cobuild partners to deliver service within the confines of the regulatory complexity of the financial services markets EU and Swiss jurisdictions, which will be subsequently expanded to North American and Asian jurisdictions as well. This is our baseline development.

### MILESTONE 2: 20K ETH

Attestation provider partner program - We are working to build a vibrant community of traditional (such as Jumio, Mitek, AriadNext, GBG, LexisNexis, Thomson, etc) and innovative (such as Civic, KYC3, etc) attestation providers, and will establish a program to engage, educate and assist the development of useful attestation engines for the Peer Mountain ecosystem.

### MILESTONE 3: 30K ETH

Service provider partner program - We are working with financial services providers to ensure the widest possible deployment of Peer Mountain instances. We will establish a "train the trainer" program in which we will work with the innovation and business development departments of financial institutions to ensure they apply Peer Mountain to their business models in the most effective way, and to educate and inspire the internal teams that will become the evangelists of Peer Mountain within their respective organizations.

PM Trust-Con - we're planning to hold the first Peer Mountain Trust Convention in late Spring 2018. Open to all our community members. The Peer Mountain team and gathered experts will meet to exchange ideas, techniques, and plans over a two-day period in Europe.

### MILESTONE 4: 50K ETH

Peer Mountain Cryptocurrency Advocacy Group - Non-Profit Industry Advocate - We will develop a non-profit effort designed to advocate for sensible legislation regarding cryptocurrencies and tokens. The purpose of this association will be to engage in the legislative process and ensure that the interests of crypto communities are put front and center in any legislation, and to fight against efforts by special interest groups that seek to prevent innovation and decentralization due to vested interests in "the way it is now".

PM Trust-Con Asia - we're planning to hold the first Peer Mountain Trust Convention Asia in Fall 2018. Open to all our community members. The Peer Mountain team and gathered experts will meet to exchange ideas, techniques, and plans over a two-day period in Asia.

### MILESTONE 5: 75K ETH

Peer Mountain Development - Travel and General Services - We will work with airlines, rental car agencies, hotels, taxi companies, and other businesses in the travel and transport industries to define and implement Peer Mountain extensions into their operations. We consider AirBnB and Uber to be traditional industries at this point and are certain that they will benefit from Peer Mountain, or be disrupted by us.

### MILESTONE 6: 100K ETH

Open-Source Peer Mountain Foundation - Mobile & Attestation Engine SDKs - We will open-source the Mobile SDKs (Android & iOS) and the Attestation Engine SDKs so that the community of Peer Mountain clients and attestation providers can be develop solutions for use cases that we haven't even imagined.

PM Trust-Con Americas - we're planning to hold the first Peer Mountain Trust Convention Americas in Summer 2018. Open to all of our community members. The Peer Mountain team and gathered experts will meet to exchange ideas, techniques and plans over a two-day period in North America.

### MILESTONE 7: 125k ETH

Peer Mountain Standards Group - We will create a group to shepherd the [Peerchain™](#) protocol towards RFC so that the protocol can be implemented consistently and widely, and to ensure that the evolution of the protocol happens in a controlled and well-governed manner.

### MILESTONE 8: 150k ETH

Peer Mountain Development - Healthcare Services - We see the potential in Peer Mountain to provide the foundation for truly portable, patient-owned medical records. We will establish a dedicated team that specializes in this field.

### MILESTONE 9: 175k ETH

Tokenomics research institute in partnership with a recognized university - Through a research grant, we will establish a five-year research program in partnership with a recognized university and/or public research organization. The program will focus on Tokenomics with the objective of understanding and producing token economy models that generate the highest value for all stakeholders. We will involve Peer Mountain and recruit other token ecosystems to participate in the provision of research data to the effort.

### MILESTONE 10: 200k ETH

Governance of decentralized organizations and cryptocurrency regulation research institute in partnership with a recognized university and/or public research organization - Through a research grant, we will establish a five-year research program in partnership with a recognized university and/or public research organization that will focus on the governance of decentralized organizations and cryptocurrency regulations, as well as crypto regtech. We will involve Peer Mountain and recruit other token ecosystems to participate in the provision of research data to the effort.

### MOONSHOT: >200k ETH

The Peer Mountain Institute for Study of the Cryptoarts - In partnership with a university or a public research institute, Peer Mountain will establish an educational center of excellence for the study of all aspects of crypto-trust: technology, currency, and humanity. The Institute will be open to participants in other crypto-driven projects; we are inviting them to contribute to our mutual success by providing support and data to the center for study. This center will develop and disseminate knowledge of how humanity can establish globally decentralized communities in which interests are aligned so that the wellbeing of the community becomes each member's own self-interest. The institute will gather leading minds from all countries and advance the science and art of decentralization for the benefit of the entire Peer Mountain community.



A note on large raises. We believe that efforts that raise ridiculous amounts of funding by placing slick marketing over inexperienced teams without a clear plan, and launching uncapped ICOs, do not serve a purpose. Furthermore, we find the general climate of greed and fast money that pervades many ICOs to be counterproductive for our industry in the long run. Our intent is to raise significant funding to enable the ecosystem to accomplish its goals in a timely manner.

We believe that in the trinity of fast, good, and cheap you can only be two of the three. We are fast and good. We could potentially exceed our ambition in the raise; this does not worry us. We are a very experienced team, with decades of investment, innovation, and entrepreneurship experience backed with a strong track record of impeccable integrity. When we examine the alternative allocators of capital, we rarely find teams that we consider to be equal to ours, and for this reason we are confident that we can actively turn all of the capital raised into value for the Peer Mountain community. If we find we are unable to do that, we may conduct a token buyback.

## BUSINESS PLAN AND REVENUE MODEL

---

Peer Mountain will be free for individuals. The mobile front end is an SDK and a reference user interface. Anybody who downloads it and has an invitation can use it. Invitations will come in the form of QR codes or links that open a Peer Mountain platform for users, allowing them to create their first persona on a Peer Mountain platform. Anyone can get these invitation codes easily.

There will be a marketplace of attestation engines for trusted third parties who validate certain facts. These can range from the simplest timestamping services to more complicated attestation engines, which may do things like check that a passport is real, verify the information it contains, and compare the photo in the passport with another photo of the user. In the latter case, an attestation system consisting of several engines working in concert can generate an intricate and reliable set of verifiable attestations.

One of our first efforts will be to develop this marketplace of attestation providers so that service providers have a wide variety of attestations from trusted and known sources to choose from. In this respect, Peer Mountain is in the process of developing an Attestation Engine SDK that it will deliver to attestation providers so they can rapidly deploy their solutions.

Peer Mountain is also approaching a number of attestation providers, such as AriadNext, Jumio, Mitek, and GBG/IDscan,<sup>15</sup> who have all expressed solid interest in joining Peer Mountain. Our objective is to sign letters of intent with these partners as soon as possible, and to give them an accelerated and assisted Attestation Engine development process in the first half of 2018. KYC3, as a supporter of Peer Mountain, is committed to providing attestation engines and is already developing the code for these.

## KEY TARGET AUDIENCES

---

We expect much initial demand to come from the following sectors:



BANKS



LAWYERS



ACCOUNTANTS



TRAVEL SERVICES



MOBILE PROVIDERS



HR DEPARTMENTS

15 <https://www.gbgplc.com/products/idscan/>

16 One has signed a Letter of Intent and the other has contracted early delivery of Attestation Engine technology with a view to eventual Peer Mountain adoption.

Peer Mountain has a broad potential audience among both individuals and organizations. In particular, we expect the ecosystem will draw in banks, lawyers, accountants, and corporations involved in daily regulated transactions. We also expect that e-commerce players and other businesses likely to be affected by the coming implementation of the EU's General Data Protection Regulation ([GDPR](#)) will be early adopters as this is a regulation that will cause them to seek cost avoidance in Peer Mountain. Mobile providers, who have been slowly moving into the financial services sector, may constitute a major audience as well.

There are also many industries that have been trying to monetize value that they carry and we believe that these will generate a very interesting and innovative marketplace of Peer Mountain Attestation Engines (PM AEs). For example, telecoms providers are getting into the KYC business by providing information on clients and this would naturally be automated with a PM AE. Similarly, official translation services are often required when businesses work across borders; a federation of PM AE-based translation services could provide *legally signed and recognized* translations to and from almost any language, allowing legally recognized translation experts to get revenue every time their translation is used to establish trust.

## POTENTIAL CHALLENGES

---

### GOVERNMENT OVER REGULATION OF TOKEN SALES AND ECOSYSTEMS:

Several jurisdictions, including China, have banned token issuances, while other governments have issued vague or skeptical rulings. In the United States, the US Securities and Exchange Commission (SEC) has issued an ambiguous bulletin indicating that it will evaluate each offering on a case-by-case basis. There is a risk that additional jurisdictions will tighten regulations or outlaw token offerings entirely.

**Mitigant:** While some governments have been less than enthusiastic about token offerings, others have made clear moves in support of them. Multiple EU jurisdictions, and the EU as a whole, have issued guidelines for token offerings, which should be viewed as an endorsement of the likelihood that they will continue to be a part of the financial universe for the foreseeable future. The SEC bulletin, while vague, should be viewed in the same light. While there will certainly be headwinds in certain places, the future of token ecosystems in general looks bright.

### REGULATORY REGIMES SLOW TO ADAPT TO PARADIGM SHIFT:

Many regulators require businesses to maintain data trails and hard copies of personal information they collect in order to prove their compliance with existing laws. The general slowness of regulations to catch up to new technologies may mean businesses are forced to maintain paper records despite the existence of Peer Mountain.

**Mitigant:** Peer Mountain provide the option of creating different personas in order to facilitate the transmission of data when applicable and of documents when required. This ensures that every interaction will be in compliance with the specifics of the applicable regulation.

### SLOW CONSUMER ADOPTION:

While the technology behind Peer Mountain categorically offers the highest degree of security and sovereignty over identity, the possibility exists that broad consumer populations will be slow to adopt it. This raises the risk of Peer Mountain being "ahead of the curve."

**Mitigant:** Peer Mountain has already established partnerships with major European financial institutions; one is a co-build partner and the other is piloting an early version Peer Mountain technology. We expect these partnerships to bring over 20% of the sovereign identity market in Switzerland and Germany into the Peer Mountain ecosystem in the first year, cementing its position as the clear market leader in those countries. Once established in such a way, Peer Mountain will assuredly maintain its market leadership.

### INTERNATIONAL SUPPORT FOR BLOCKCHAIN AND IDENTITIES:

Government regulation on issuance and ownership of identity varies widely today, with multiple agencies responsible for issuing identity information in each country. To ensure complete global adoption of self-sovereign platforms, government entities will need to collaborate and agree on how to issue and hold universally accepted identities. Most importantly, such systems will require additional governance from respected third parties to establish a system of checks and balances that does not favor one government or technology over another.

**Mitigant:** While it is unlikely that governments would accept a technology or approach with third-party vested interests, a neutral party, such as a consortium, could succeed in providing the necessary additional governance. We believe this is the most likely structure for transnational regulation of identity. In this regard, and because you own your data in our ecosystem, Peer Mountain becomes an "identity aggregator". An entity can attach credentials from existing national and private digital identity schemes to a Peer Mountain [persona](#). So, if a service provider would like to accept Estonian eIDs and [Civic](#) Identities as part of their service dossier, the provider can link these to each consumer's Peer Mountain [persona](#), making them identity attestations.

## PROVENANCE / INITIAL ONBOARDING:

Governments are likely to want the capability of exerting some sort of supervision over what onboarding documentation and personal data is required to prove a person's identity. Once these criteria are established, the market will need third-party technology, such as identity verification, to ensure the onboarding process is valid from the outset in the eyes of the government or regulator.

It must be noted that government IDs aren't used globally. An estimated 1.1 billion people worldwide (Africa, Asia, etc.) cannot officially prove their identity, according to the [2017 update](#) of the World Bank's Identification for Development (ID4D) Global Dataset. In order for the ledger to be universal, there would need to be a way to validate those people without traditional identity documentation. Disagreements within and among governments, as well as who has the authority to oversee the onboarding of new identities, could present a significant challenge.

**Mitigant:** While governments tend to move slowly when adopting rules to reflect new technological realities, Peer Mountain is confident in the current regulatory environment in Switzerland and the Eurozone. The stability that exists in this area should allow Peer Mountain to establish itself as the market leader in interoperable self-sovereign identity, positioning it to take full advantage as additional jurisdictions bring their regulations up to date.

## OUR TEAM



JED GRANT | MBA, CEO, Lead Architect [in](#)

Innovator, inventor, technologist, and security professional. At each step of his career, Jed has designed, developed, implemented, and improved technology and processes

that are still in use today. For the last decade, he has focused on practical technology-driven KYC, anti-money laundering (AML), and enhanced due diligence (EDD). In

everything he does, Jed is committed to turning bold ideas into benefit-rich solutions - this commitment and his professional experience inspired him to establish Peer Mountain.



DR. MARKUS FORSTER | Data Scientist [in](#)

An expert in big data evaluation, Markus delivers data mining and analysis solutions for risk management. As an accomplished professional computer scientist, he has a deep understanding of complex data systems and algorithms. Markus leads the data science side of Peer Mountain implementation.



FEDERICO CARDOSO | Blockchain Architect [in](#)

Federico develops innovative blockchain technology solutions that deliver real results. At Peer Mountain, he directs the company's enterprise back-end development team. He's also the co-founder and CTO of Maecenas, the first marketplace for fine art investment, and DXMarkets, which integrates blockchain technology into enterprise-based financial processes.



IGNACIO ALTHABE | Blockchain Developer [in](#)

Ignacio is a talented Full Stack developer and blockchain evangelist who builds complex enterprise-grade systems. He has produced a diverse range of solutions, including a voting and commenting platform for TV shows and user interfaces for public-access government portal. A self-professed fanatic of diagrams, agile methodologies, and continuous integration, Ignacio is presently handling back end development for Peer Mountain.



FLORIAN LAGOUCHE | Blockchain DevOps Engineer [in](#)

Florian is a blockchain devops expert with experience in Ethereum gained at KYC3 and Scorechain. His enthusiasm for blockchain technology, and the way it is completely redefining the way we structure and share data, inspires him to improve agile relationships between development and IT operations teams. He manages Peer Mountain's development cluster, as well as the KYC3 production clusters.



## MARK ROGERS | Mobile Lead [in](#)

Mark is an experienced tech entrepreneur and start-up advisor from Silicon Valley, devoted to ensuring projects achieve their full potential. As the founder and CEO of Futurist Labs, a boutique mobile app provider, he has built a highly skilled and eager mobile development team. Mark is currently overseeing this team at Peer Mountain.



## STEFAN VARTOLOMEEV | Mobile Architect [in](#)

Stefan has a passion for system architecture and data modeling, and helps startups scale from zero to MVP and beyond. He specializes in mobile technologies on both the front end and the back end. On top of leading the development of the mobile Peer Mountain client, Stefan is also the CTO at Futurist Labs and Chief Software Architect and Co-Founder of getti.



## GABRIEL PINEDA [in](#)

Backend developer

Senior software engineer and architect for backend systems who loves working with fellow blockchain tech enthusiasts.



## LUIS GIUNTA [in](#)

Software Engineer

Senior software engineer and frontend developer dedicated to building great user experiences with blockchain technology.



## PAVEL PAVLOV [in](#)

Mobile Developer

17 years of dedication to quality architectures and code. Multinational team scrum master.



## ANTONIA CHERKACHIEVA [in](#)

Mobile Developer

Detail focused mobile developer. Expert in testing and QA.



## JAIME PRIETO [in](#)

Compliance Officer

Lawyer specialising in financial crime, AML, anti-corruption and counter-terrorism financing.



## PATRICK SEGUIN [in](#)

Content Manager

Writer specializing in content production and management for global tech companies.



## MARC GARRIGA [in](#)

Digital Marketing

Blockchain enthusiast and former Fortune 500 business manager.



## DOMINIQUE RADEMACHER [in](#)

Web Developer

Developer and designer specializing in user experience, clean code and lean design.



## ANNA KROL [in](#)

Community Manager

Experienced in building and retaining strong active online communities through social media channels.



## EKATERINA SEMESHINA [in](#)

UI/UX Design

Creating usable and delightful web and mobile experiences.

# TEAM AND ADVISOR COMPENSATION POLICY

At Peer Mountain a reserve of PMT has been set aside to remunerate the team and the advisors. Advisors shall be paid an equal amount each. Advisors are expected to:

- PROVIDE TIMELY FEEDBACK ON MATTERS PERTAINING TO THEIR AREA OF EXPERTISE
- PROMOTE PEER MOUNTAIN IN THEIR PEER GROUPS
- LEND THEIR NAMES AND IMAGES TO THE PROJECT
- FUNCTION IN THIS CAPACITY UNTIL AT LEAST NOVEMBER 2018

Team members shall be paid in variable amounts depending on their contribution to the success of Peer Mountain, meaning its token sale, technical development and commercial development. Team members are expected to:

- LEARN ABOUT PEER MOUNTAIN AND PROVIDE EXPERTISE EQUITABLY AND EFFICIENTLY TO THE PROJECT
- COLLABORATE WITH AN "I WIN WHEN EVERYBODY WINS" ATTITUDE
- OPENLY SHARE INFORMATION AND PROACTIVELY SEEK TO RESOLVE ISSUES
- DYNAMICALLY ACCEPT AND AGREE ON THE MOST QUALIFIED PERSON TO CARRY RESPONSIBILITY FOR ANY COMMON TASKS
- LEAD AND FOLLOW-UP ON ALL ISSUES IN WHICH THEY ARE THE LEADER
- PROVIDE PROACTIVE SUPPORT AND CONSTRUCTIVE ADVICE ON ISSUES WHERE ROLE IS AS A SUPPORTER OR WHERE THERE IS VALUABLE INPUT TO GIVE

Some members are paid in fiat or crypto prior to token sale completion. In these cases, the amounts pre-paid will be deducted from the final allotments for those team members. The amount deducted from the total will be a multiple (e.g. at least 4x) of the value of the amount paid pre-ICO. This is to motivate the team to stand to gain a lot more in PMT when the token sale is done than would be the case today in any other currency.

In the interest of transparency: Peer Mountain is funded by the founders; any payments in EUR, ETH, BTC, GBP, or USD are made by them. They are confident in the future of PMT and the project. They encourage all team members to favor PMT and are offering the highest rewards to the "all-in" team members.

## SMART LOCKUP

As part of the Smartcap™, the PMT paid to team and advisors shall be subject to a Smart Lockup that will govern their sale of PMT over the first 180 days of exchange trading. This will regulate any team sale of PMT during the lockup period, which will be permitted to the normal level of monthly compensation for the team member. During the Smart Lockup period all sales or purchases of PMT by any team member or advisor shall be nominally disclosed on the Peer Mountain website.

# COMPETITION

## CURRENT LANDSCAPE

Incumbent identity systems are demonstrably insufficient; in the wake of Equifax and other high-profile breaches, they are likely to face significant disruption in the near future. While inertia will probably keep legacy systems operational in the short to medium term, we are confident there will be enough consumer defection to guarantee strong growth following the initial PMT offering.

## CURRENT SOLUTION SPACE

A number of sovereign identity platforms have been launched in the past year. We do not view these as competitors but as potential participants in Peer Mountain's marketplace of trust. Users of these platforms, which often go no farther than the level of personal identification, can interact with and validate one another, and transact with businesses, using Peer Mountain's infrastructure.

In the same way, Peer Mountain co-opts traditional enterprises such as certification authorities (CA) that provide digital identity solutions; these CAs can offer their services to Peer Mountain clients. If an individual has a digital ID from a CA, they can simply add that ID to their Peer Mountain persona and co-opt the trust that this ID provides. In this way it is possible to link these directly to Peer Mountain, by digital signatures, and create an even stronger web of trust.

A person can put all the digital identities they've received from multiple jurisdictions into their secure Peer Mountain profile and create a cross-jurisdictional web of trust. At present, nationally accredited CAs are unable to agree on and establish an international digital ID standard. To solve this problem, Peer Mountain provides the unique opportunity to tie digital IDs together in each user's self-sovereign identity, which it can then share through its Peerchain™ Protocol.

Peer Mountain is a circular economy of trust. This innovative concept is unique to Peer Mountain, keeping incentives for all peers fully aligned. Unlike other initiatives to develop blockchain-based identity and service provisioning solutions, Peer Mountain is offering economic incentives that will ensure that all participants consistently create value. The system only rewards document-certifying peers when their attestations are used, thereby encouraging them to be accurate and faithful. As a spam prevention mechanism, peers must pay a fee in PMT to submit certifications.

Along the same lines, service providers pay a fee when they post service offerings and process service applications.

We're certain that because they use a centralised approach, other existing and upcoming digital identity solutions won't gain the traction they require to gain mass adoption, and therefore will only offer incremental improvements rather than a paradigm shift.

## FIRST MOVER ADVANTAGE

Peer Mountain is the first marketplace that connects self-sovereign identity owners with service providers. As a facilitator of commerce between numerous platforms, it is poised to cement itself as industry leader.

# USER JOURNEYS

While Peer Mountain user journeys present a vast array of possibilities in several industries, it will initially be deployed in the financial services sector, where there is a massive need for more efficient dossier management, compliance, and client onboarding. Peer Mountain delivers on all three of these points.

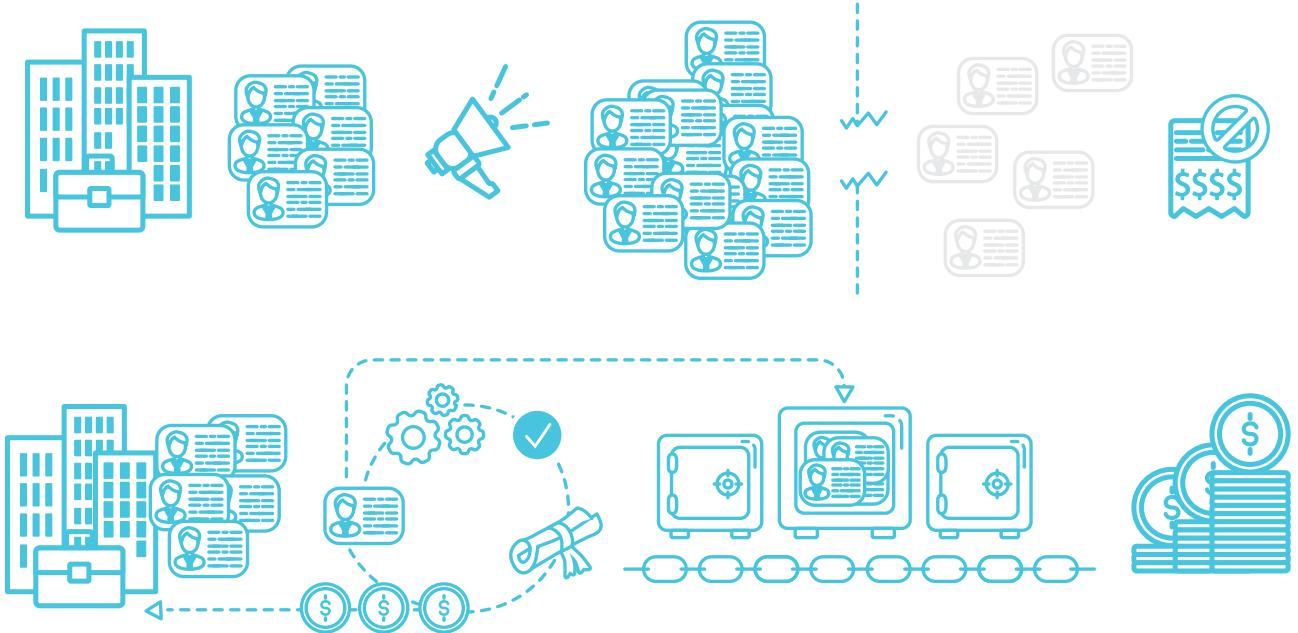
To launch service requests, Peer Mountain uses QR codes and other simple access points. For example, you see an ad for a new credit card and decide you want one. Using Peer Mountain, you scan the QR code and swipe your documents into the card application file, and within minutes you have your new digital card on your phone, ready for contactless payment. The total transaction time is under five minutes. Peer Mountain speeds up trust so that you can get things done, now.

## USER JOURNEY 1: BUSINESS PERSPECTIVE

ABC Gifts Plc. is a major London-based online retailer that has customers from all over the world. Founded during the first dot-com boom, it has grown to become a household name, with billions of pounds in annual revenues. Its powerful CEO is widely known as a market leader in innovation, and speaks at many global events.

The CEO is convinced of the power of online retail and believes it will continue to represent an ever-growing share of global consumption. New technologies, including drones and driverless trucks, offer seemingly unlimited possibilities for reshaping the consumer landscape. ABC has invested deeply in projects aimed at establishing a leadership position in the adoption of these capabilities.

But ever-improving technology also has a dark side that the CEO knows all too well. Companies like ABC transact with millions of individual consumers around the world each day. As a result, the company stores the personal details - names, addresses, birth dates, credit card details - of hundreds of millions of people. To protect this data, ABC has significant security measures in place: firewalls, strong password requirements, automatic log-out after a period of inactivity. Yet the CEO worries that this is not enough. In recent years, he has watched as several large, respected companies fell victim to major hacks, putting the identities of hundreds of millions of people at risk. Target, Yahoo!, Equifax, ... the list goes on.



Adding to the urgency of the situation, the EU's General Data Protection Regulation ([GDPR](#)) is set to take effect in May of next year. This law states that any business that stores the personal information of individuals is liable to be fined up to 4% of its annual revenues if that information is compromised. This could put billions of pounds at risk for ABC. And while the company generates significant revenue from selling personal information to advertisers, the CEO believes that the potential risks are beginning to outweigh the benefits.

Fortunately, there is a solution. The CEO hears about Peer Mountain, and makes the decision to join its circular economy of trust. By doing so,

he relieves his business of the risk - which [GDPR](#) now starkly defines in material terms - of storing customer data, especially on such a massive scale. His business can continue to grow its core segments and develop exciting new technology that will make online retail even more convenient and accessible without the fear that a single breach could bring the whole house crashing down. As time goes on, he finds that customer volumes are increasing, since more people feel comfortable shopping and paying online now that their identities are secure in Peer Mountain's blockchain ecosystem.

The only resistance the CEO encounters in his push to join the marketplace of

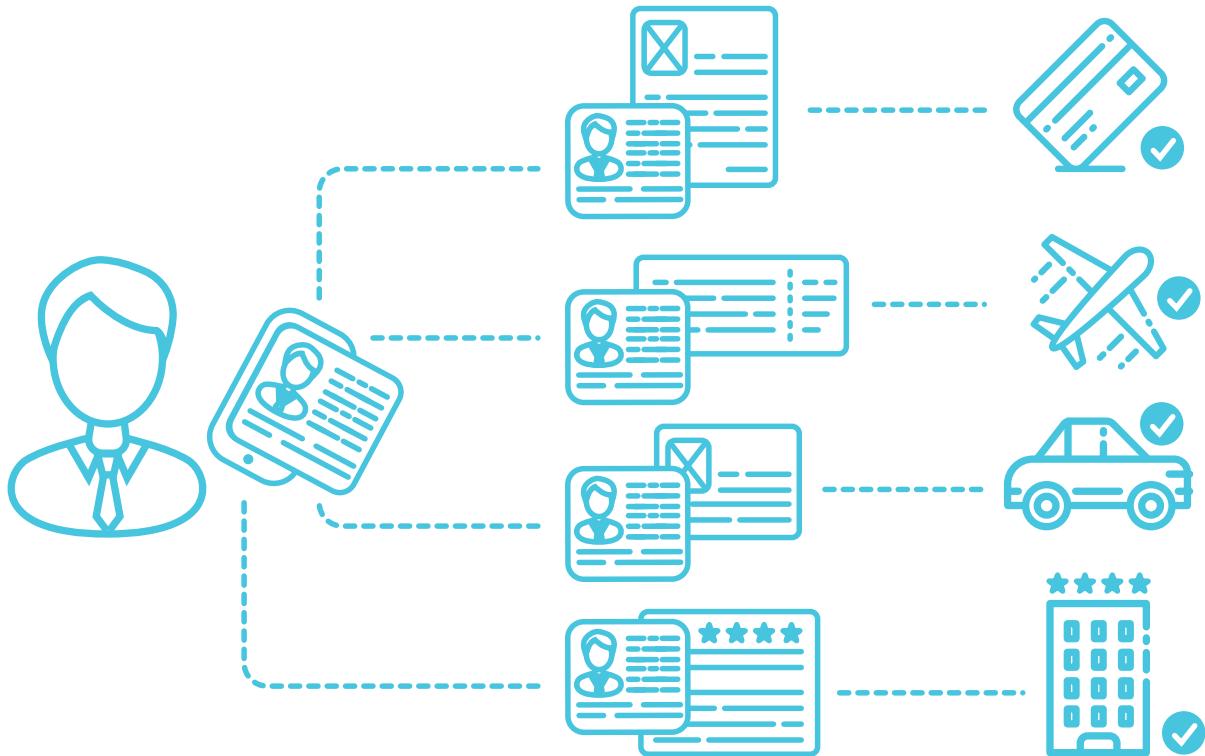
self-sovereign identities comes from board members who fear the loss of revenue from selling information to advertisers. Peer Mountain offers a solution that addresses this concern. Because it does business with millions of people every day, ABC can act as an attestation provider on a massive scale and receive millions of micropayments daily. This can replace the lost revenue stream, while simultaneously bolstering ABC's reputation as a company that cares about its customers, and positioning it as a responsible custodian of information. The board is satisfied. Peer Mountain brings the company into guaranteed full compliance with [GDPR](#), cements the CEO's reputation as a leader in innovation, and helps ABC continue to grow.

## USER JOURNEY 2: CONSUMER PERSPECTIVE

Bob is looking for a new credit card. He's leafing through a magazine and finds an ad for a Miles and More card that will give him double miles for every purchase. Bob says, "This is cool. I need this card!" He uses his smartphone to scan the QR code in the ad, triggering Peer Mountain to present Bob with a service dossier that shows him everything he needs to provide in order to receive the card. Bob swipes his passport (already validated and stored in his profile) and his contact information (which is essentially in an ID card format, with his name, address, telephone number, and email address) into the dossier. He completes a couple of simple forms to certify that he's a resident of the country

where this credit card is being offered, and he's good to go. About three minutes later, Bob receives a notification via his Peer Mountain-enabled app that he's got his new dematerialized credit card and can begin using it immediately.

Now that he has more credit, Bob decides he wants to take a trip. He goes online, finds an airline offering great deals on flights to Italy, and starts the process of buying his plane ticket. To provide his details, Bob simply swipes his information into the airline's service dossier. Peer Mountain's interoperable ecosystem allows his personal information, provably verified by his home country's government, to be securely and granularly shared with Italian customs



and border control. He swipes in his passport and traveler profile, enters a few flight preferences (e.g. seat and type of meal), and gets his ticket. He's cleared and ready to travel.

Once Bob arrives in Italy, he goes to a rental car lot, which, with Peer Mountain, doesn't need to have an attendant onsite. He scans a code printed on the car's passenger door. Scanning this code activates the company's Peer Mountain-powered app, which asks him for relevant information: driver's license, credit card, etc. Bob swipes to verify his identity and pay the car rental company, which sees that his information has been validated and he is a trusted user. They even upload the car key onto his phone, which he can use to unlock and start the car through NFC technology.

In this scenario, Peer Mountain establishes the rental contract. Bob provides the required information and the rental car company confirms that it can fulfill his request. In the process, Peer Mountain creates a new dossier.

Bob drives his rental car into town and finds a nice

hotel. Instead of the standard check-in procedure, he uses Peer Mountain again. At reception, he sees QR codes defining the hotel's service offerings. Bob makes his selection and swipes in his identity using Peer Mountain. He doesn't need to give the hotel a copy of his passport; he can check in using a validated, digitally signed document. With Peer Mountain, Bob only gives the hotel the information it needs. The data is cryptographically secure, and the hotel can validate it using cryptographic protocols on the Peer Mountain system to make sure that a trusted third party has attested to Bob's trustworthiness. The day Bob checks out, his information disappears from the hotel's systems (after the legal retention period). Using Peer Mountain, he has kept his personal information safe, while enjoying a smooth, hassle-free trip.

Peer Mountain works with XADES-T XML digital signature standards, which are time-stamped securely and legally accepted under Swiss, EU, US, and many other countries' regulations. This keeps Bob's Peer Mountain usage seamless as he travels.

## PLATFORM AND TECHNOLOGY

### PATENT-PENDING TECHNOLOGY

Peer Mountain has been in development for several years. In fact, founder Jed Grant has been working on the solution for over a decade; he filed the first technical specification with the Benelux Office of Intellectual Property as i-Depot number 68499 dated 12 November 2015. This filing was for

"The Trust Project", "a technical architecture and concept project plan for an infrastructure of trust. The premise is a totally decentralized peer-to-peer secure trust management system that facilitates the transfer of any type of digital object or stream".

## i-DEPOT 68499

Reference	The Trust Project	
Title	Trust infrastructure for global use	
Status	Secret	
i-DEPOT details	Your details	History
Description	This is a technical architecture and concept project plan for an infrastructure of trust. The premise is a totally decentralized peer-to-peer secure trust management system that facilitates the transfer of any type of digital object or stream between parties who choose to trust each other.	
Language i-DEPOT certificate		
Date of filing	12-11-2015	
Date end of storage period	12-11-2020	
Type of file ▲	Title	
i-DEPOT certificate	Trust infrastructure for global use	<a href="#"></a>

Figure 6: The First Technical Specification for Peer Mountain (The Trust Project)

The Peerchain™ protocol, architecture, and system design are protected by the 9 October 2017 European Patent filing 17195509.9 - "Method and system for decentralized messaging and data access". We have also filed trademarks for the Peer Mountain and Peerchain™ brands with EUIPO trade mark numbers 017282931 and 017350182, respectively. We take intellectual property seriously and have

taken steps to protect it. We also believe in a free and open economy. It is our intent to release the Peer Mountain client SDK for Android and iOS as open source, and to open-source the Peer Mountain Attestation Engine SDK. It is also our intent to submit the Peerchain™ Protocol for RFC in order to develop an open standard that can be used as widely as possible in any economic context.

## REAL SERVICE SUPPORT

Peer Mountain supports the delivery of real services, such as credit, loans, transactions, settlement, insurance or any other service, in any fiat or crypto currency. We've developed Peer Mountain to allow individuals not only to own their content and intellectual property, but also to monetize it through services. Peer Mountain makes it easy for entities to define and offer a limitless range of services through its ecosystem. Anyone can use it to provide, for instance, fortune-telling, white paper-writing, an escrow service, or a credit card – they can offer all of these, and much more, easily and in compliance with their respective regulatory requirements on Peer Mountain.

## SIMPLICITY IN THE USER EXPERIENCE

Peer Mountain and the reference client implementations are intuitive and easy to use. There is no need for an end user to understand anything about blockchain, peer-to-peer protocols, or cryptography, and no need to set up a secure local wallet. The Peer Mountain clients and protocols handle all of this invisibly.

## REAL WORLD TRUST AND DELEGATION MODEL

Peer Mountain is built around a real-world trust model. Each actor chooses which entities to trust and how much to trust them, and what to share. Trust can also be transitive. For example, having a high-level of trust in a friend may also mean that the friend's friends are trusted at a lower level by default. As always, this is under the control of the user.

The Peerchain™ Protocol includes delegation of authority that can be used to model complex real-world situations, such as the governance structure of a company, and works with legal digital signatures, making it possible to use Peer Mountain in the most complex of corporate and legal environments. Revocation of delegated authority is also possible, including revocation of one's own persona in the event that a keypair is stolen.

## DIRECT TRANSACTIONS

---

Peer Mountain is designed to facilitate peer-to-peer transactions, whether entirely digital or with real-world goods. The ecosystem supports direct transactions using the Peer Mountain mobile client, so payments can be made face-to-face, over the phone, or over the Internet - however parties are comfortable with each other.

## LEGALLY BINDING SIGNATURES

---

Peer Mountain leverages XAdES-T digital signatures that meet the eIDAS, ZertES and DSS legislative requirements for legally binding digital signatures. This means that business concluded on Peer Mountain is legally binding and can be arbitrated in the courts of any country with appropriate digital signature legislation, such as the United States, all EU member states, Singapore, and many more.

## MULTIPLE SIGNATURES

---

Entities can also use the delegation model in Peer Mountain to create legally binding commitments that require multiple signatures.

## HIGHLY SECURE

---

The encryption scheme in Peer Mountain is built with 4096bit RSA keys at its foundation. The time required to crack 4096-bit key encryption would exceed the lifetime of the Milky Way Galaxy<sup>17</sup>. All information is securely encrypted both in motion and at rest. Data is not exposed unless the owner of the content decides to share it.

## AUDITABLE AND ACCOUNTABLE

---

Peer Mountain enables the independent audit and verification of claims reliably and securely, making fraud and identity theft much more difficult for criminals. In fact, the distributed nature of Peer Mountain means that identity thefts would have to be performed one at a time and require compromising each individual end client's protected device (secure wallet).

## RECOVERABLE

---

Peer Mountain provides a highly secure personal key recovery mechanism so that an individual can recover their keys if they lose or change their device. Similarly, we have a secure quorum-based recovery complement based on Shamir's secret-sharing scheme that individuals can use to further safeguard their keys. By choosing trusted counterparties, a Peer Mountain user is ensuring that a quorum of such counterparties can recover their keys, even after their death.

Using a  $(k, n)$  threshold scheme, we divide an individual's keys  $S$  into  $n$  pieces of data  $S_1, \dots, S_n$  in such a way that:

- Knowledge of any  $k$  or more  $S_i$  pieces makes  $S$  easily computable.
- Knowledge of any  $k - 1$  or fewer  $S_i$  pieces leaves  $S$  completely undetermined

Using this method, we can securely share  $S_1, \dots, S_n$  with trusted quorum members  $Q_1, \dots, Q_n$ , who can then recover the key with a quorum of  $k$ .

## DATA PROTECTION-READY

---

Peer Mountain solves compliance problems. We've designed the Peerchain™ Protocol (PMP) with international data protection standards in mind. This means that PMP is GDPR compliant.

## AML / KYC COMPLIANT

---

By its design, PMP facilitates AML and KYC requirements among transacting parties in a secure and granular fashion. Nothing but the information required to meet regulatory compliance is shared. And the manner in which authority and identity is structured in Peer Mountain means that PMP clients meet BSA/AML and the EU 4th Anti-Money Laundering Directive requirements.

<sup>17</sup> <https://crypto.stackexchange.com/questions/3043/how-much-computing-resource-is-required-to-brute-force-rsa>

## FLEXIBLE AND EASY TO DEPLOY

Peer Mountain is built as a federated set of microservices that interact using the Peer Mountain Service Protocol. This makes Peer Mountain easy to deploy in a multitude of configurations, from full-service deployment at a financial exchange to a ledger-only node at a regulator. It also simplifies the abstraction from the blockchain and storage implementations – making it as easy as adapting a simple microservice and re-deploying the module to enable new blockchain or storage technologies under Peer Mountain.

## BLOCKCHAIN-AGNOSTIC

PMP is blockchain-agnostic. This means that Peer Mountain can be deployed on any blockchain implementation and can provide continuous services as blockchain technology matures and evolves. Peer Mountain can run on Bitcoin variants, Ethereum, Hyperledger, Stellar, Eos, or whatever the next great distributed ledger technology may be – and it can run on all of these at once and reliably manage transactions across these deployments.

## UNIFIED LEDGER AND OBJECT STORAGE

Peer Mountain unifies the ledger and object storage, both of which are abstracted. Just as any blockchain can be used under Peer Mountain, object containers (encrypted objects) can be stored in IPFS, HBase, HDFS, Tahoe, MongoDB or any other storage medium with the appropriate capacity.

## SCALABLE BEYOND TODAY'S BLOCKCHAIN CAPACITY

Peer Mountain solves the problem of blockchain scalability. Using PMP, services can be segmented across blockchain deployments transparently and securely. In practical terms, this means that services with modest transaction requirements can be deployed on a common Peer Mountain instance while a service that needs high volume transaction capabilities can be deployed on a dedicated Peer Mountain instance.

## CROSS BLOCKCHAIN TRUST

"COMPONENTS OF ENTERPRISE DEPLOYMENT      NODES REPLICATED AS REQUIRED"

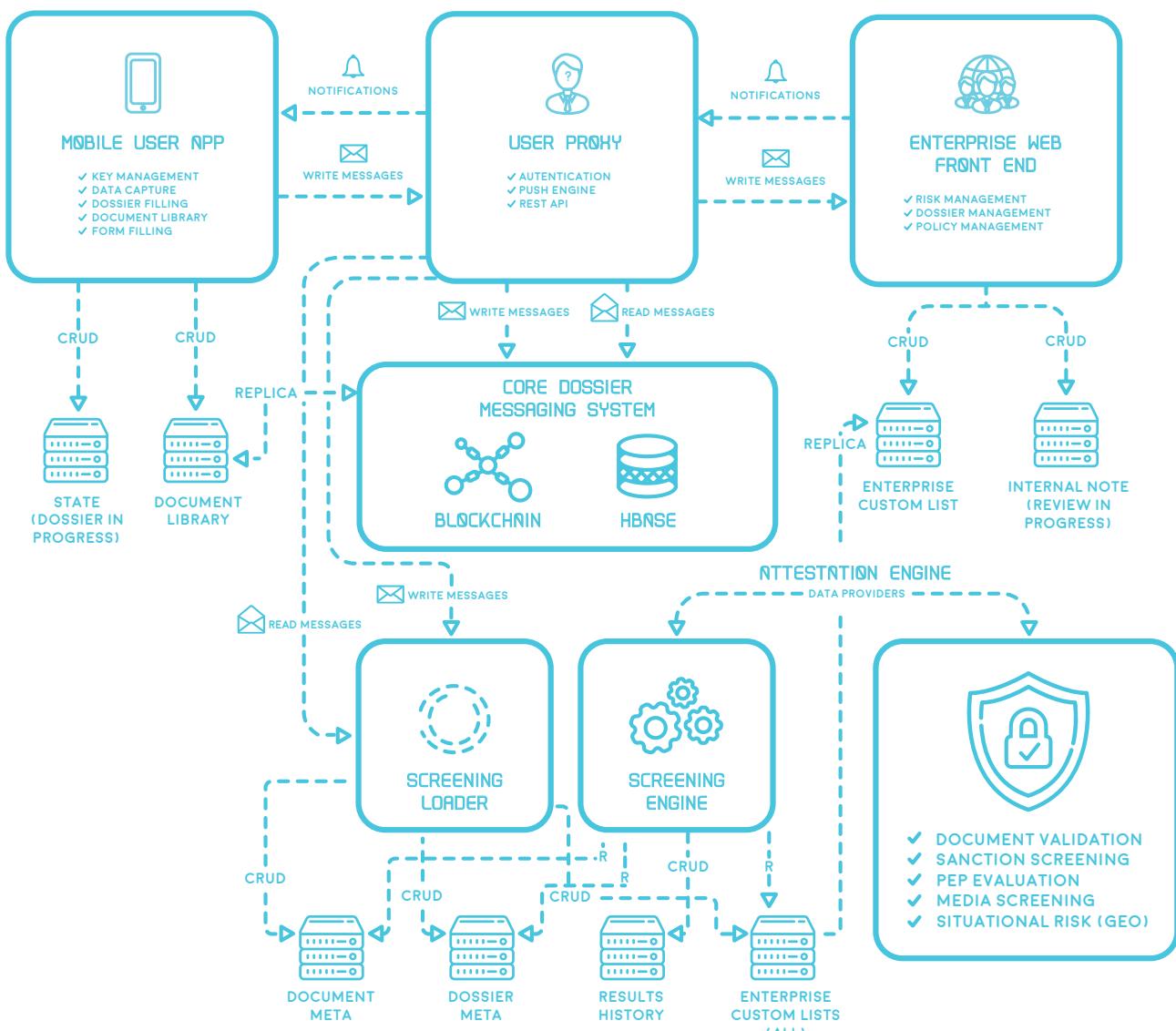


Figure 7: Peer Mountain Enterprise Deployment Diagram

Peer Mountain solves the problem of cross-blockchain trust. As PMP is blockchain-agnostic, it can be deployed across multiple instances on different types of blockchains. The protocol facilitates cross-chain trust and validation. Any Peer Mountain client can easily access any Peer Mountain deployment, provided they have the right invitation and credentials. Although quite different in the details, PMP facilitates an OAuth-style cross chain trust mechanism that allows the delegation and verification of information.

## DECENTRALIZED NAME SPACES

---

Peer Mountain implements a peer-to-peer naming scheme that is totally decentralized, yet can still interoperate with standard DNS clients. The owner manages the namespaces, which are cryptographically protected using digital signatures. As these are dynamic and individually managed namespaces, the use of the chain is not required for the PMNS. Owners declare their names within their own space and these are hashed and shared using a Kademlia-based protocol.

## PSEUDO-ANONYMOUS

---

Peer Mountain is pseudo-anonymous at the public level. That is, no private information is visible, only cryptographic hashes and public keys are required to be shared at the public level.

## STRONG IDENTITY

---

If an individual chooses to share information with another party, the identity of both parties may be shared and confirmed. Peer Mountain implements an open attestation system with several common and unique methods to confirm identities on the platform.

## GRANULAR CONTROL

---

Information is atomized in Peer Mountain, and the system provides granularity so that only the required information for a transaction can be shared and validated. For example, with Peer Mountain it is not necessary to share your complete identity document to prove that you are over 21 years of age. You only need to share the validated birthdate information that enables the third party to confirm age and the level of trust in the birthdate fact as provided. As an example of a potentially popular use of this, Peer Mountain makes it possible to have an alcohol vending machine that accepts cash, e-payment, or cryptocurrency and can verify the purchaser's age without having to know who the purchaser is.

## DATA DECONSTRUCTION (ATOMICITY)

---

Each attestation is digitally signed and given to the owner of the data in atomic form. The hash of an attestation is logged on the ledger and Peer Mountain provides content privately to the owner of the object being attested on. By validating the signature on the object and verifying the hash on the ledger, owners can share attestations, and third parties can confirm attestations.

For example, a passport creates many different attestations:

- Attestation that the image is good copy of a passport
- Attestation that the photo matches another photo
- Attestation of the content of the document Machine Readable Zone (MRZ)
- Attestation of the elements of the passport individually:



PHOTO  
FIRST NAME(S)  
LAST NAME  
DATE OF BIRTH  
PLACE OF BIRTH  
NATIONALITY  
PASSPORT NUMBER  
PASSPORT EXPIRATION DATE  
PASSPORT ISSUING AUTHORITY  
AND SO ON...

By design, each attestation can be used independently and verified by parties who do not need to see the original document or the specific information contained within the document.

## DECENTRALIZED CHAINS

---

Peer Mountain does not require consensus across every Peer Mountain node globally. Rather, it needs a number of nodes across the parties that require trust - this is the Peer Mountain Instance. The blockchain instance provides a cryptographically secure ledger, providing trust among parties that may not necessarily trust each other. So for the right deployment of a blockchain, blockchain nodes must be deployed across different independent entities that are required to establish trust amongst each other, and only to those entities, no more.

## PEERCHAIN™ PROTOCOL

---

Each operation is defined by a message type. Messages are wrapped in an envelope that provides the basic and common information about all operations. These messages contain the specifics about each operation type. Messages that alter the state of the system are hashed and timestamped in an immutable blockchain layer. Service providers or other external entities (e.g. regulators) may run blockchain nodes without necessarily running message/object storage nodes.

Only the message identifier and hashes related to the content of the message are stored on the blockchain layer. All other information is kept in a high-performance distributed database. The current alpha version of Peer Mountain is built on [Ethereum](#) and HBase.

The [Peerchain™](#) protocol is a reliable asynchronous messaging system on a distributed message and attachment store with a blockchain message record index. The protocol implements a variety of messages needed to establish and manage trust, and to exchange information among trusted parties. Each message is well-structured and defined. All messages are wrapped in a standard envelope format.

HMAC-SHA256 calculations use salt values from the message structure as the secret key for their calculation. Peer Mountain salt values are 40-byte entropy-generated values.

```
{  
  "messageHash": "sha256",  
  "messageType": "typecode",  
  "dossierHash": "hmac-sha256",  
  "bodyHash": "sha256",  
  "messageSig": "RSA signature",  
  "message": "(enc)BLOB",  
  "senderAddr": "PM Address",  
  "ACL": [{  
    "reader": "(enc) key"  
  }],  
  "containerHash": "sha256",  
  "containerSig": "RSA signature",  
  "objectContainer": "(enc) BLOB",  
  "objectHash": "sha256",  
  "Metahashes": ["hmac-sha256"],  
  "replacesMsgHash": "messageHash"  
}
```

# PEERCHAIN™ TECH

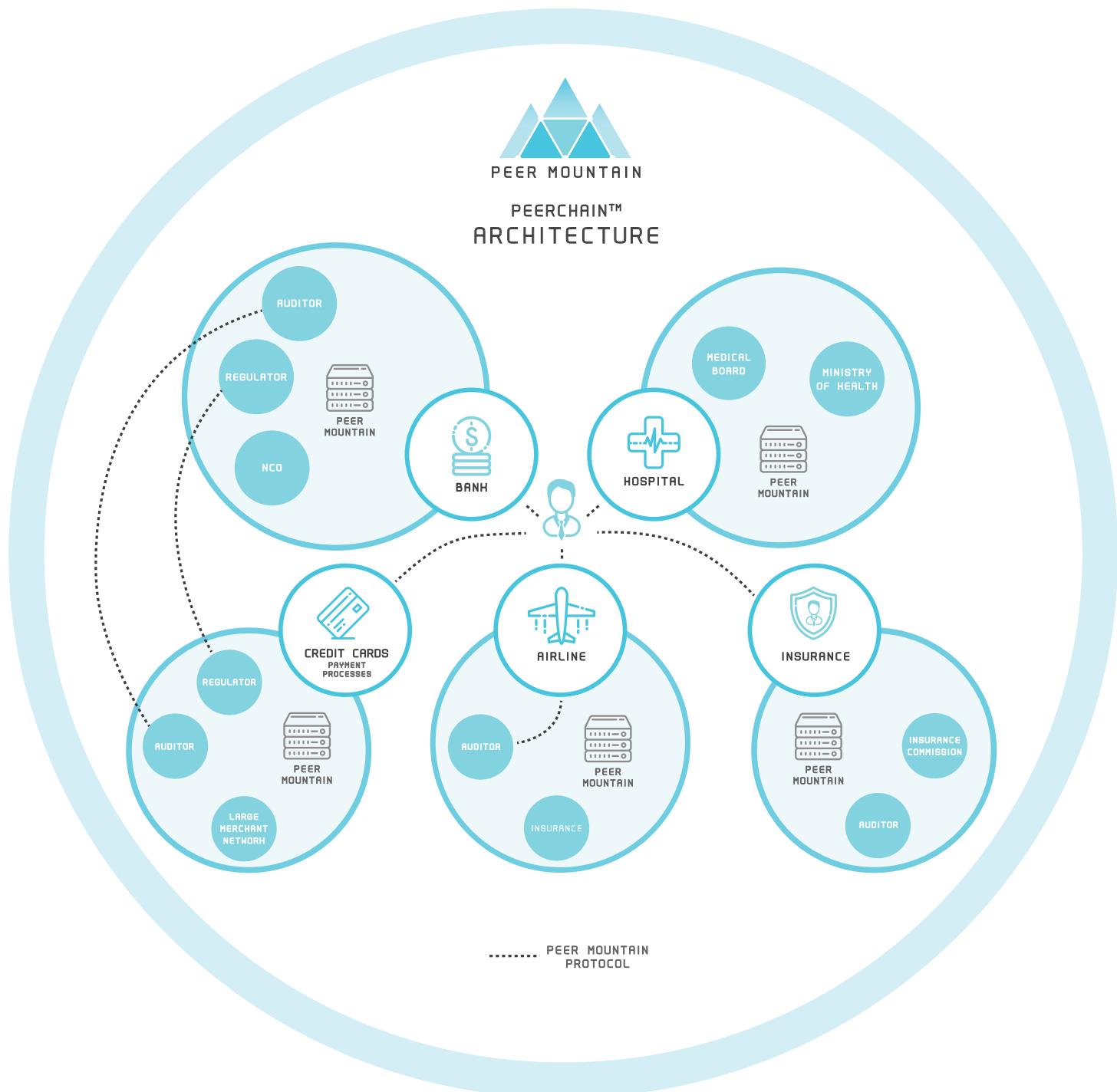


Figure 8: Peerchain™ Technology

CLIENTS SEE  
PEER MOUNTAIN  
INSTANCES  
TRANSPARENTLY

ATTESTATIONS ARE  
PORTABLE ACROSS  
INSTANCES

INSTANCES ARE  
DEPLOYED BY SERVICE  
PROVIDERS OPERATING  
IN REGULATED  
INDUSTRIES

## OPEN

---

Peer Mountain is a flexible and extensible ecosystem, in which it is easy to deploy new services. On the back end, the enterprise sees the above-mentioned messages and checks them against its service requirements. In most cases, when a service dossier is complete and verified, this check can be fully automated. So you just get the service.

## SCALABLE

---

Peer Mountain can run on multiple chain instances. Services can have their own instances, or they can share them. Because of the consensus mechanism in blockchains, there is a need for a higher throughput. Today, blockchains have trouble handling large numbers of transactions. Peer Mountain can solve this problem by allowing an institution to run multiple Peer Mountain instances. For example, a user could run separate Peer Mountain instances for current accounts, a specific type of credit card, and auto loans. The transaction volume gets split across them, and the user achieves a higher transaction throughput across all services while having cross-instance compatibility with the information, so the same dossier used for the credit card service can be used for the car loan and the other accounts. The information can still be shared across these, but you have the capability to have a higher throughput in terms of messages sent.

## FREE

---

Peer Mountain is free. The mobile front end is an SDK and a reference user interface. It is free of charge and can be used by anybody who downloads it and has an invitation, which is simple to get as invitations come in the form of QR codes that open a Peer Mountain platform for users, allowing them to create their first persona on a Peer Mountain platform.

## IDENTITY AND PERSONA IDENTIFICATION

---

Each Identity has at its core an RSA 4096 key pair. The public key is hashed to generate an address. This address is used in messages and solicitations (QR codes, links or other invitation methods) for messages. The hash is calculated much like a Bitcoin address and appears, for all intents and purposes, very similar.

However, the hashing method has been slightly modified so that Peer Mountain addresses will not validate as Bitcoin addresses. The exact procedure is as follows:

- The public key of the pair is hashed SHA-256.
- The resulting hash is further hashed with RIPEMD-160.
- Five bytes are prefixed to the resulting RIPEMD-160 hash. Byte 0 identifies the PM protocol version in use. Bytes 1-4 identify the PM deployment.
- A checksum is calculated by SHA-256 hashing the extended RIPEMD-160 hash, then hashing the resulting hash once more.
- The last 4 bytes of the final hash are added as the trailing 4 bytes of the extended RIPEMD-160 hash. This is the checksum.
- The resulting object is Base58 encoded.

## DIGITAL SIGNATURE MANAGEMENT

---

Application keypairs (as opposed to blockchain system keypairs) are generated on the end device and used from that device only. Each Identity and Persona has a dedicated keypair and address. These are stored securely in the device and decrypted only when the user authenticates with the symmetric key to this storage.

## OBJECT IDENTIFICATION AND MANAGEMENT

---

Objects are identified by three hashes which permit the identification of duplicate or highly similar objects at three levels. These are the Container Hash, the Object Hash, and the Meta Hash.

Container Hash is the hash of the encrypted container object. Obviously, this will be different for each Object-Encryption action; this is used to record the container storage and tie the container to the message that is written on chain.

Object Hash is the hash of the decrypted object. This permits validation of the object with respect to tampering and proof of integrity, and can be compared with the original object registration to ascertain that the document is valid and legitimate.

Meta Hash is the hash of the well-formed non-instance specific meta-data from the object. For example, the Meta Hash of an electronic passport will be the hash of the MRZ content and/or the hash of the RFID content. An object may have multiple Meta Hash results, each identified by the definition of the well-formed meta-data structure without content and the resulting hash of that structure with content. This permits the identification of duplicate logical objects. Using this hash it is possible to detect multiple uses of the same document - for example to avoid multiple uses of the same passport across root identities.

## DELEGATION OF PERSONAS AND MULTIPLE SIGNATORIES ON A PERSONA

Delegation and Multiple Signatories are accomplished through key signing activity. A system of trust rules allows complex trust rules to be defined and included in the delegation, for example: "may sign for value of less than 5,000 Euros singly, or may sign jointly with one of [array of other personas] for any value".

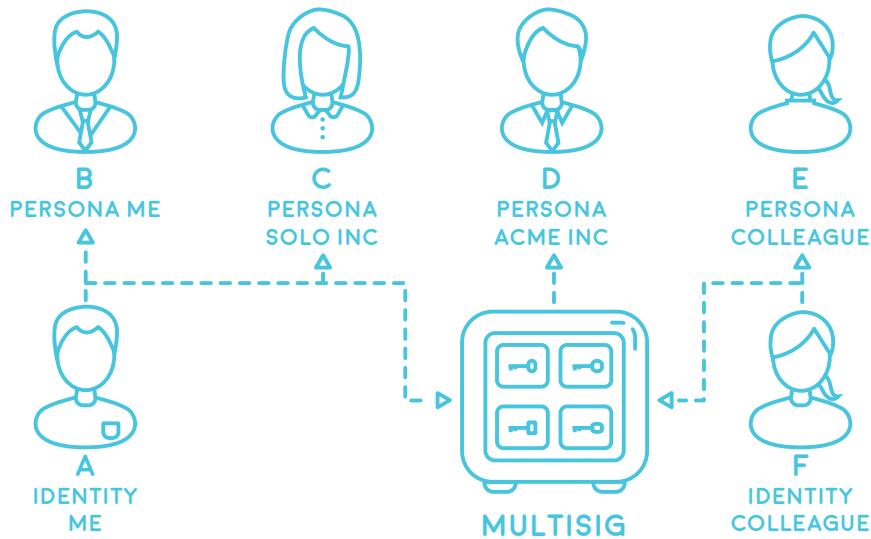


Figure X: Peer Mountain multi-signature and delegation model.

S= Signing function; PK= Pubkey; R= Trust Rule (see doc); all operations XAdES-T signed and on chain.

- A generates keypair B and asserts ownership of B by  $S_B(S_a(PK_B, R))$  // here R is usually "equivalent to signer"
- A does the same for C and D
- F does the same for E
- A via D invites F to partecipate with D.  $S_B(PK_1, (PK_B, R))$  // here R is the proposed TrustRole for F over D
- F generates keypair D<sub>1</sub> and asserts ownership with  $S_B(PK_1, (PK_B, R))$  // here R is usually "equivalent to signer"
- A via D asserts D<sub>1</sub> validity over D with  $S_B(PK_1, (PK_B, R))$ . // here R is the level of delegation A gives to F
- F accepts with  $S_B(PK_1, (PK_B, R))$ . // here R is from the previous operation. This step may be omitted.

Trust Rule changes can be also be used to remove rights to a persona for a specific keypair.

- A resignes D: First, steps 1-7 must be performed such that D<sub>1</sub> (or another key) has full control on D, than A writes  $S_B(PK_1, (PK_B, R))$  with R restricted to "none".
- Assuming F is the other key, F via D<sub>1</sub> accepts with  $S_B(PK_1, (PK_B, R))$ . // here R is from the previous operation. This step may be omitted.

Peer Mountain uses delegation messages to generate a local data store of accepted delegations. A delegation message may be public or permissioned. Permissioned delegations are similar to a traditional proxy. For example, a persona that is used to possess and manage a stock portfolio could be delegated with buy/sell rights (no withdrawal of funds) to a wealth manager. The delegation messages would only be visible to the owner (delegator), the wealth manager (delegee), and the service provider (stock brokerage), although the delegation message could be shared by any of these parties later if needed.

## TRUST RULES AND ACTION MATRICES

Trust rules automate actions that a profile can take. Trust rules are used in two types of matrices: the Information Sharing Matrix and the Commitment Action Matrix.

### INFORMATION SHARING MATRICES (ISM)

Each persona has an associated Information Sharing Matrix, which is a matrix of default actions that correspond with matches between the trust level of the counterparty and the classification level of the information (document). These are byte-to-byte values, making a 255x255 matrix of values possible; however, the default system should use the standard matrix presented below. The labels for trust level and classification level are arbitrary; the user can change them to suit their needs.

<b>Trust Level / Classification</b>	0: Public <b>(Unclassified)</b>	10: Private <b>(Confidential)</b>	20: Secret	30: Top Secret	40: Code Word
<i>0: None</i> <i>10: Acquaintance</i> <i>20: Friend</i> <i>30: Close Friend</i> <i>40: Blind Trust</i>	Share	Ask	Deny	Deny	Deny
	Share	Share	Ask	Authenticate	Deny
	Share	Share	Share	Authenticate	Authenticate
	Share	Share	Share	Ask	Authenticate
	Share	Share	Share	Share	Ask

Figure 10: Information sharing matrix

## COMMITMENT ACTION MATRIX (CAM)

Each persona has an associated Commitment Action Matrix. This is an array of trust levels and permissible commitments for a persona. The master keypair (creation keypair) of a persona has the default maximum CAM of 255, no limit. Each delegated persona is assigned a trust level between 0 and 255 in the delegation, and may further delegate any level up to the same level as their own. This is used to automate specific actions that may be requested from trusted third parties.

## PRODUCTION AND SECURITY OVERVIEW

The first Peer Mountain production servers will be located in the Mount10 data center in a bunker in the Swiss Alps protected by armed guards and managed under certified ISO 27001 standards, and in Luxembourg on a selection of hosts from respected operators who, at present test phase, comprise the founding host providers of the non-profit blockchain infrastructure orchestrator Infrachain: such as the State Data Center (CTIE), University of Luxembourg (SNT), Luxembourg Institute of Science & Technology (LIST), Telindus, Scorechain, and Bitbank<sup>18</sup>.

Notwithstanding the high quality and security of these data centers, Peer Mountain is designed to run on the hostile network known as the open Internet. Even if a thief got into Mount10, there is nothing to see on the Peer Mountain servers except encrypted gibberish.

Your data is protected by design<sup>19</sup>. You control what is private and what can be shared. You can set up Peer Mountain so that it notifies you about requests for your information, and you can decide what action to take. Peer Mountain also enables you to automate safe and efficient information sharing.

Peer Mountain is a true peer-to-peer system, so any

peer can take on any role: consumer, provider, or trustee. This means enterprise clients are also able to reinforce trust, so if one bank (Bank A) gives you an attestation of good credit, you can take this attestation and share it on another bank's (Bank B) Peer Mountain deployment, which is completely separate. Bank B's system can access Bank A's reference to the system, which is all encrypted. In this secure ecosystem, Bank B can access the encrypted references and verify for themselves that the hashes are good, because the record on the blockchain validates that the attestation on that Bank A installation on a different Peer Mountain instance existed at a specific time. After all, a blockchain is nothing but a bunch of hashes that are blocked together with cryptographic security so that each block locks in the previous block.

You will also see the digital signatures in that attestation and you can verify that the signatures are good. Once you've proven that the expected party, or keyset, was used to sign the attestation, and the attestation was indeed produced and recorded on another Peer Mountain installation, Credit Suisse could then know with certainty that they could trust

you, or they can validate and use the level of trust that they have with BoA for you.

Additionally, Peer Mountain is built on a microservice architecture, meaning it's very flexible and agile, and it's blockchain- and storage-agnostic. You can run Peer Mountain on an [Ethereum](#) or [Stellar](#) blockchain, and on Hbase and IBFS. All you need is the microservice

that handles the specific blockchain or data storage and retrieval microservice, then change that one component to get Peer Mountain working on any blockchain and distributed storage solution. This opens up very interesting possibilities: using cross-Peer Mountain instances enables information to cross from blockchain technology to blockchain technology.

## VALIDATION

Peer Mountain is being co-built by [KYC3](#) and its co-build partners: a major Swiss Financial Institution and the payment processing arm of a major German firm. Both have already signed adoption LOIs or delivery contracts for Peer Mountain technology. [KYC3](#) is leading core tech teams in the build effort with support from FuturistLabs. The Zurich-based user experience design studio Fjord has worked with the teams to deliver a first class user experience for both the mobile and enterprise platforms.

Once the first commercial release is completed (2Q18), the Swiss partner intends to deploy Peer Mountain to its clients. The German corporation has expressed intent to use the Peer Mountain SDK in all three of its mobile apps. Across the two, they will

initially deploy to a few hundred thousand end users; with Peer Mountain's projected usage growing to 12 million Swiss and EU residents by end 2019.

Our co-build partners are participating on the business side and we are building a solution that meets their requirements in terms of security, scalability, and functionality. We have vetted Peer Mountain with their Chief Information Security Officers, we will have independent audits of the solution done before deploying it in live production, and we're working with their risk and compliance teams and their product teams so that we can enable the solution to deliver their services. With that in mind, our co-builders have privileged access to Peer Mountain, and plan to deploy the platform for their use in Switzerland in 2018.

## PEER MOUNTAIN KYC & COMPLIANCE

From the service side, we're offering a solution that allows organizations to establish trust with their clients, suppliers, stakeholders, regulators, and auditors, and have a continuous real-time compliance and risk management function at a very small price. In real terms this should translate to between one and three Euros per dossier per month, which is much less than a typical financial institution is spending in KYC per client. For major banks, maintaining KYC on corporate accounts can cost upwards of 5,000 Euros per annum. Peer Mountain eliminates this enormous expense.

Peer Mountain effectively merges customer relationship management (CRM), compliance, and KYC into one platform. Peer Mountain is the ultimate

CRM - your customer manages himself. It's also the ultimate compliance platform because the customer manages himself against the service dossier, and it is very easy to see whether the dossier is compliant.

Peer Mountain can easily handle the full KYC and strong identity reporting to meet the anti-money-laundering and counter-terror-financing requirements of a distributed exchange. Peer Mountain could run on the Bitcoin, [Ethereum](#), or public blockchains, and could handle the exchange of Bitcoin to [Ethereum](#) and vice-versa when there are buyers and sellers. These apps could easily be deployed on Peer Mountain, and they would then be compliant with regulated financial services requirements because Peer Mountain will provide that strong capability to provide identity and record-keeping.

18 The token sale will *not* be conducted on Infrachain. It will be on the public Ethereum network.

19 Peer Mountain is [GDPR](#) compliant for data protection and consent

# ADVISORS



**PROF. JORGE SANZ**

Head of Finance Innovation, LIST

IBM research fellow in banking; head of R&D in Regtech. Committed to projects that grow economies, create jobs, and improve lives.



**PROF. JOS VAN BOMMEL**

Assoc. Prof. of Finance,  
University of Luxembourg

Associate professor of Finance at the University of Luxembourg. His research on IPOs, private equity, and market microstructure has been published in numerous peer-reviewed journals.



**PROF. THOMAS ENGEL**

Head of SECAN-LAB, Uni.lu

Cryptography researcher on ToR and related topics. Member of the European Security Research Advisory Board (ESRAB).



**MARCELO GARCIA CASIL**

CEO, Maecenas.co

Fintech innovation expert. Builder of mission-critical systems for European and Asian investment banks.



**GUILLAUME DUBRAY**

Partner, Polytech Ventures

VC with a strong interest in fintech, blockchain, distributed apps, cyber security, and digital health. Experienced investor in listed and private equities.



**CHRISTOPHE BACH**

Mentor, Fintech Fusion

Expert management of complex banking IT projects. Innovation and business development leader for Swisscom's Digital Banking initiative.



**JEREMY EPSTEIN**

CEO, Never Stop Marketing

As Sprinklr CMO, took company from \$20 mil and 30 people to \$1.8 bil and 1400 people in four years. Founder of CryptoExplorers.



**DR. THOMAS ANKENBRAND**

Lecturer, IFZ, Hochschule Luzern

Experienced CEO and board member of several financial enterprises. Fintech researcher and advocate. Docent at IFZ - Hochschule Luzern.



**JAVIER TAMASHIRO**

APAC FCC CTA, Credit Suisse

KYC/AML Officer at Credit Suisse. Fortune 500 and fintech blockchain advocate. Expert in risk management via tech and data.



**JAN C. REINHART**

CEO, Reinhard Capital

PE/VC investor. Former Swisscom and SAP executive.



**MARCO HOUWEN**

Project Lead, Infrachain.com

"Fintech and Cloud" evangelist. Infrachain project lead and promoter of Luxembourg's online ecosystem.



**BERTRAND MANHE**

COO, GENII Capital

Private equity and M&A expert with IT security skills. F1 team investment manager. Fintech angel investor.



**LAURENT LELOUP**

CEO, Chaineum

Pioneering blockchain entrepreneur and author. Founder of influential blockchain projects, including Blockchain Valley and Voxchain.



**MAX WOLTER**

CEO, Alantor

IT entrepreneur pioneering blockchain technology with Alvalor, a blockchain platform focusing on scalability, and Alantor, an exclusive investment club for blockchain assets.

# SUMMARY MILESTONES & ROADMAP

**2005**

Research on distributed hash tables (Kademlia) with personal realm based security (Kerberos) sparks the idea to design a system of trust management that works for the human scale

**2006**

Discovery of the NSA paper "How to Make a Mint", which was first published in 1996

**2010**

Blockchain technology makes the possibility of a human scale trust system feasible and the year in which Jed's "identity" was stolen for the first time

**2014/06**

Founding of KYC3 begins the journey into compliance and regulatory trust

**2015/05**

Office of Personnel Management informs Jed that his security clearance file has been stolen from their systems

**2015/10**

KYC3 inducted into Fintech Fusion

**2015/11**

First Peer Mountain tech spec filed as iDepot 68499 at the Benelux Office of Intellectual Property

**2016/04**

KYC3 selected for L'Atelier by BNP Paribas

**2016/10**

KYC3 completes Fintech Fusion

**2016/12**

KYC3 secures capital increase for March 2017

**2017/03**

Peer Mountain project is born, KYC3 leads and will be a service provider to the platform

**2017/04**

Major Swiss financial services provider agrees to co-build Peer Mountain for 3 million users and signs Letter of Intent to do so.

**2017/05**

KYC3 achieves 2016 revenue level

**2017/06**

Peer Mountain development begins

**2017/07**

German Corporation expresses intent to deploy Peer Mountain when ready with 9 million users

**2017/08**

Peer Mountain prototyping

**2017/10**

German Corporation contracts Peer Mountain technology for early deployment

**2017/10**

Peer Mountain exits stealth mode

**2017/12**

Peer Mountain v1 deployment

**2018/05**

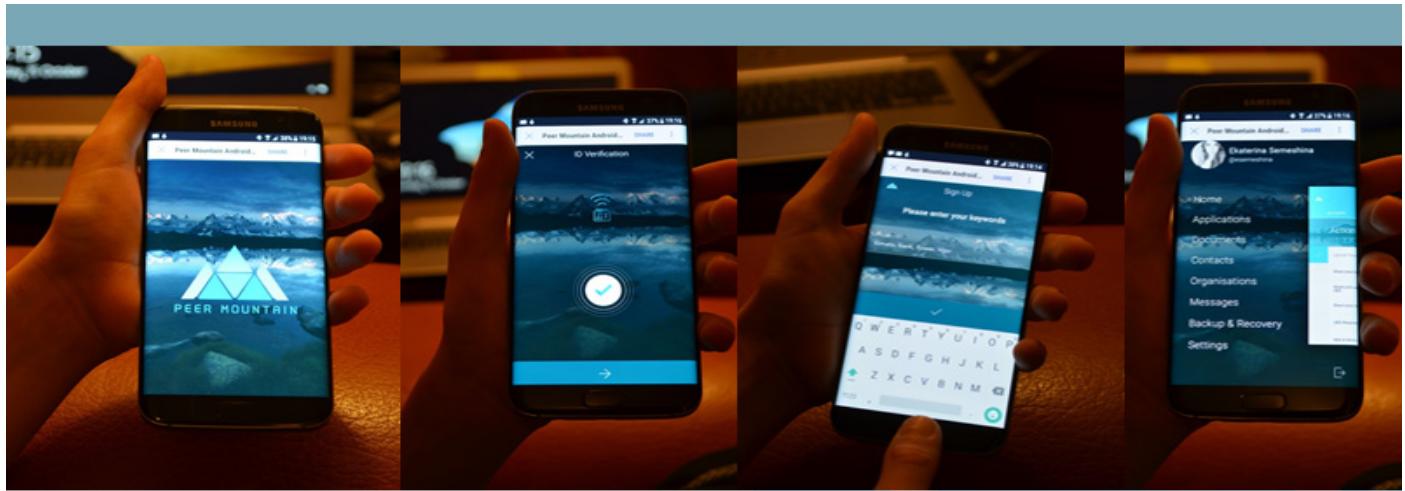
Peer Mountain production deployment by Swiss financial services partner

**2018/09**

Peer Mountain deployment to 3 million end users in Switzerland

**2018/12**

Peer Mountain deployment by German corporation to 9 million end users



## CURRENTLY IN ALPHA

- Rollout planned to start in 2018 with two Enterprise Partners, already onboard
- Intended rollout to 3 million Swiss and 9 million Germans by end 2019

## GLOSSARY OF TERMS

### ARIADNEXT:

Platform providing digital solutions for customer acquisition. <https://www.riadnext.com/>

### CIVIC:

Secure identity platform. <https://www.civic.com>

### GDPR:

The General Data Protection Regulation, a new regulation entering into force across the European Union, including the U.K., in 2018. GDPR requires all businesses that store sensitive personal information to use appropriate security measures. If these measures fail, businesses are subject to a penalty with an upper limit of €20 million or 4% of annual global turnover – whichever is higher. <http://www.eugdpr.org/>

### EOS:

Platform for decentralized applications. <https://eos.io>

### EQUIFAX:

One of the three major credit-reporting agencies in the United States. It was hacked in the summer of 2017, putting at risk the identities of over 140 million people.

### ETHEREUM:

A major public blockchain. <https://www.ethereum.org>

### HYPERLEDGER:

An enterprise-focused blockchain platform. <https://hyperledger.org/>

### ICO 2.0:

The next stage of token offerings. Led by the Peer Mountain ICO, ICO 2.0 offers transparency, full and upfront regulatory compliance, and new innovations such as the Smartcap™ algorithm to optimize the offering. <https://peermountain.com>

### ICO CHARTER:

A groundbreaking charter outlining ICO best practices for the European Union. [http://www.icocharter.eu/](http://www.icocharter.eu)

### INFRACHAIN:

A non-profit organisation created by blockchain organizations and supported by the Luxembourg government. <https://infrachain.com/>

### JUMIO:

Digital ID verification platform <https://www.jumio.com/>

### KYC3:

Co-developer partner of Peer Mountain; founded by Peer Mountain CEO Jed Grant. [https://kyc3.com/](https://kyc3.com)

### LEXISNEXIS:

Provider of legal, government, business and high-tech information sources. <https://www.lexisnexis.com>

### MITEK:

Global Leader in Digital Identity Verification. <https://www.miteksystems.com/>

### PERSONA:

A user's Peer Mountain Persona is the cumulative identity they have and maintain on Peer Mountain, which can be selectively and divisibly shared with other parties in the ecosystem. A persona might consist of a passport, driver's license, proof of residence, and credit card payment history, for example.

### PEERCHAIN™:

Peer Mountain's patented technology allowing sharing of information across multiple blockchains.

**PM AE:**

Peer Mountain Attestation Engine, a system that accepts an input assertion and returns its attestation to the input.

**PMT:**

Peer Mountain Token, the coin at the center of the Peer Mountain ecosystem.

**RSA KEY:**

A public/private key pair used for authentication, encryption and non-repudiation.

**SHAMIR S SECRET-SHARING SCHEME:**

an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. [https://en.wikipedia.org/wiki/Shamir%27s\\_Secret\\_Sharing](https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing)

**STELLAR:**

An open-source platform for distributed payments.

<https://www.stellar.org/>

**WORLDCHECK:**

Risk-intelligence service provided by Thomson-Reuters.

<https://risk.thomsonreuters.com/en/products/world-check-know-your-customer.html>