

# Etherprise Whitepaper

Ethereum for Enterprise

The Ethereum based blockchain built for privacy, security and performance.

Version 1.5

July 2018



## Disclaimer

Nothing herein constitutes an offer to sell, or the solicitation of an offer to buy, any tokens, nor shall there be any offer, solicitation, or sale of Etherprise Tokens. Acquiring, holding and/or using Etherprise Tokens does not constitute an ownership interest in the company, nor should any Etherprise Token acquirer or holder expect to profit from holding and/or purchasing and selling Etherprise Tokens and/or receive a dividend or similar return from the company's operations. Etherprise Tokens should not be construed as a derivative of any kind. By contributing to our token sale, you expressly agree and acknowledge that you are not located in a jurisdiction where digital currencies ("cryptocurrencies") are partially or completely restricted. The company does not take responsibility for any Etherprise Tokens sold by third parties or through third-party intermediaries. You should carefully read and fully consider the information contained herein this white paper and any subsequent updates. Every potential token contributor will be required to undergo an onboarding registration process. This includes a Know Your Customer (KYC) identity verification and proof of address documentation. Please make sure to consult with your appropriate legal and investment advisors before contributing to our token sale. This whitepaper describes our current vision for the Etherprise platform. While we intend to attempt to realize this vision, please recognize that it is dependent on quite a number of factors and subject to quite a number of risks. It is entirely possible that the Etherprise platform will never be widely implemented or adopted, or that only a portion of our vision will be realized. We do not guarantee, represent, or warrant any of the statements in this white paper, because they are based on our current beliefs, expectations, and assumptions about which there can be no assurance due to various anticipated and/or unanticipated events that may or may not occur. Please know that we plan to work hard in seeking to achieve our vision but that you cannot rely on any of it coming true. Blockchain, cryptocurrencies, and other aspects of our technology and markets are in their infancy and will be subject to many challenges, competition, and a rapidly changing environment. We will try to update our community as we grow and evolve but undertake no obligation to do so.

## Executive Summary - TL;DR

Enterprise companies want to use blockchain technology, in particular Ethereum for its smart contract abilities. Many companies are taking Ethereum off the shelf and trying to use it, but it's missing critical features that enterprises need. The interest is there, just take a look at the hundreds of members of the [Enterprise Ethereum Alliance](#), which includes companies like Microsoft, Accenture, major banks and many other fortune 1000 companies, but there's no good solution.

Enterprises require security, privacy, and control in every piece of software they use, but there isn't a good Ethereum-compatible blockchain solution that meets these requirements. For instance, all data in Ethereum is public and all smart contracts can be accessed by anyone. Etherprise starts on the opposite end of the spectrum making all data private and contracts only accessible to those who have been given explicit access. For enterprises to truly adopt blockchain beyond just experimentation, these features must be native to any solution, uncomplicated to deploy, and straightforward to manage.

Etherprise is building an enterprise-grade, Ethereum-based blockchain that delivers the privacy, security, control and performance that every enterprise requires. Etherprise has key management (KMS), access controls (RBAC) to define who can access what, and encrypted smart contract data in transit and at rest. It will also provide administrative tools to allow companies to easily manage their Etherprise implementations. Lastly, it will be one of the best performing blockchains available today providing greater than 1000 transactions per second.

The Etherprise team consists of successful, silicon valley entrepreneurs that have built highly scalable cloud infrastructure services, have had successful, well funded startups, with several exits under their belts.

## The Problems with Existing Blockchains for Enterprise Use

There are many problems with blockchains today that make it incompatible for use in an enterprise company. This section will go over all of the main problems that exist today, with a focus on Ethereum, as that is what Etherprise is solving for.

### Privacy

Focusing on Ethereum smart contracts, there is basically no privacy at all. Smart contract state (the data stored for a particular contract) is public to all and easily accessible. This is great for a lot of things, in particular public asset ownership such as digital game assets (CryptoKitties), company ownership, real estate ownership and the most popular example: ERC-20 token contracts. But it's completely unusable for a business that needs to keep their data private.

Imagine a company wanting to use Ethereum for payroll processing, affiliate marketing payments or sales commissions. If the company used Ethereum as is, the entire world would know how much they are paying their employees. If they used it for sales commission processing, again, everyone would know how much commissions their sales people are getting, including their own employees knowing how much their co-workers are getting.

The privacy problem is probably the biggest problem affecting enterprise adoption of public blockchains.

### Security

Similar to privacy, there are no built-in security mechanisms in Ethereum. Smart contracts are accessible to everybody in the world. This means that the writer of a smart contract is responsible for adding security to every contract they write, which may sound simple but leaving this up to the developer is extremely problematic. This problem has become very clear in ICO/token sale contracts, as we've seen 100's of millions of dollars stolen due to people finding security bugs and exploiting them. Almost every month, you hear of another hack on an ERC-20 contract where the hackers are able to steal tokens and sell them for millions of dollars.

The security issue is compounded by the fact that you can't upgrade smart contracts if there is a security bug. Even if you knew there was a bug, there would be nothing you could do to fix it or



prevent the hackers from exploiting your contract. Imagine you saw that someone was hacking your contract, but you could do absolutely nothing about it. The hackers could take their time draining all your funds and there is nothing you could do about it.

## Performance

Public, decentralized cryptocurrencies suffer from slow transactions and low transaction volume. Bitcoin can only process transactions at 7 tps<sup>1</sup> while Ethereum can only process at 13 tps<sup>2</sup>. Additionally, the time to verify transactions can range from several minutes to several hours depending on current volume<sup>3</sup>. Recently, there is almost always a delay of minutes as the networks simply unable to handle the load as more and more people start using the networks. This problem will only get worse as more people start using it and more DApps come online. Keep in mind that these rates are shared amongst all users and DApps on the network. You can read more about this problem [here](#).

In contrast, Visa, Inc. averages 150 million transactions every day and is capable of handling more than 56,000 tps<sup>4</sup>. Public cryptocurrencies are too slow for real world processing by 4 orders of magnitude.

## Centralization

Decentralization is a core tenant of cryptocurrencies. It ensures no one company or government can control it. However, in practice most mining happens in China where electricity is cheapest<sup>5</sup>, <sup>6</sup>. 70-80% of all blocks are mined by large Chinese mining companies. This is true of Bitcoin, Bitcoin Cash, Ethereum and other top cryptocurrencies<sup>7</sup>. In the event of company collusion or government privatization, 51% attacks<sup>8</sup> would be possible.

## Energy Consumption

The process of mining blocks uses an enormous amount of energy because of the PoW consensus algorithm<sup>9</sup>. PoW requires non-trivial computational work by mining nodes which, in turn, makes it cost prohibitive for a bad actor to perform malicious acts. While this has worked

---

<sup>1</sup> [https://en.wikipedia.org/wiki/Bitcoin\\_scalability\\_problem](https://en.wikipedia.org/wiki/Bitcoin_scalability_problem)

<sup>2</sup> <https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a>

<sup>3</sup> <https://www.blockchain.com/charts/median-confirmation-time>

<sup>4</sup> <https://mybroadband.co.za/news/security/190348.html>

<sup>5</sup> [https://en.wikipedia.org/wiki/Electricity\\_sector\\_in\\_China](https://en.wikipedia.org/wiki/Electricity_sector_in_China)

<sup>6</sup> <http://www.businessinsider.com/why-china-mines-more-bitcoin-than-any-other-country-2017-12>

<sup>7</sup> <https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27>

<sup>8</sup> <https://www.investopedia.com/terms/1/51-attack.asp>

<sup>9</sup> [https://en.wikipedia.org/wiki/Proof-of-work\\_system](https://en.wikipedia.org/wiki/Proof-of-work_system)

## 6

exceptionally wall to secure an untrusted network, this computational workload requires enormous amounts of energy.

As of today, 6.5 million US households could be powered with the energy used to run the Bitcoin network<sup>10</sup>, while Ethereum uses power equivalent to running 1.8 million households<sup>11</sup>. All of this energy to process around 10 transactions per second. On a per transaction basis for Bitcoin, the energy used is ~1000 kWh and at an average price of \$0.12 per kWh in the USA<sup>12,13</sup>, a single transaction costs about \$120 USD.

This is unacceptable, unsustainable and unnecessary.

---

<sup>10</sup> <https://digiconomist.net/bitcoin-energy-consumption>

<sup>11</sup> <https://digiconomist.net/ethereum-energy-consumption>

<sup>12</sup> <https://www.npr.org/sections/money/2011/10/27/141766341/the-price-of-electricity-in-your-state>

<sup>13</sup> [https://www.eia.gov/electricity/monthly/epm\\_table\\_grapher.php?t=epmt\\_5\\_6\\_a](https://www.eia.gov/electricity/monthly/epm_table_grapher.php?t=epmt_5_6_a)

## The Solution - Etherprise

Etherprise brings the best of existing public blockchains to the enterprise enabling companies to use an enterprise-ready public blockchain or run a private Ethereum compatible blockchain with the features your company needs. Etherprise gives enterprises the **privacy, security and performance** they need.

### Privacy and Encryption

In Ethereum and most other blockchains, data is publicly accessible. Etherprise makes all data private by default and is encrypted in transit and at rest. Data in transit means data this is being transmitted across a network (ie: the Internet). Data at rest means inactive data that is stored physically in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

#### Encrypted In Transit

For data in transit, Etherprise enforces Transport Layer Security (TLS) for both system to system communications and user communications. TLS is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deployed security protocol used today, and is used for web browsers and other applications that require data to be securely exchanged over a network.

#### Encrypted at Rest

For data at rest, Etherprise uses Transparent Data Encryption (TDE) which offers encryption at the file level. TDE solves the problem of protecting data at rest, encrypting databases both on the hard drive and consequently on backup media. Enterprises typically employ TDE to solve compliance issues such as PCI DSS which require the protection of data at rest. TDE technology is employed by Microsoft, IBM and Oracle to encrypt database files.

The public network is secure since it's encrypted at rest and during transit. Even though people could potentially get access to the bits stored in the blockchain, they will not be able to access the data without the correct key for the smart contract.

#### Hybrid Cryptosystem



Etherprise uses a [hybrid cryptosystem](#) for encrypting data which combines asymmetric cryptography and symmetric cryptography. This means we get the benefits of asymmetric cryptography (public key cryptography) as well as the efficiency of symmetric cryptography.

### How Hybrid Cryptography Works

To encrypt a message addressed to Alice in a hybrid cryptosystem, Bob does the following:

- Obtains Alice's public key.
- Generates a fresh symmetric key for the data encapsulation scheme.
- Encrypts the message under the data encapsulation scheme, using the symmetric key just generated.
- Encrypt the symmetric key under the key encapsulation scheme, using Alice's public key.
- Send both of these encryptions to Alice.

To decrypt this hybrid ciphertext, Alice does the following:

- Uses her private key to decrypt the symmetric key contained in the key encapsulation segment.
- Uses this symmetric key to decrypt the message contained in the data encapsulation segment.

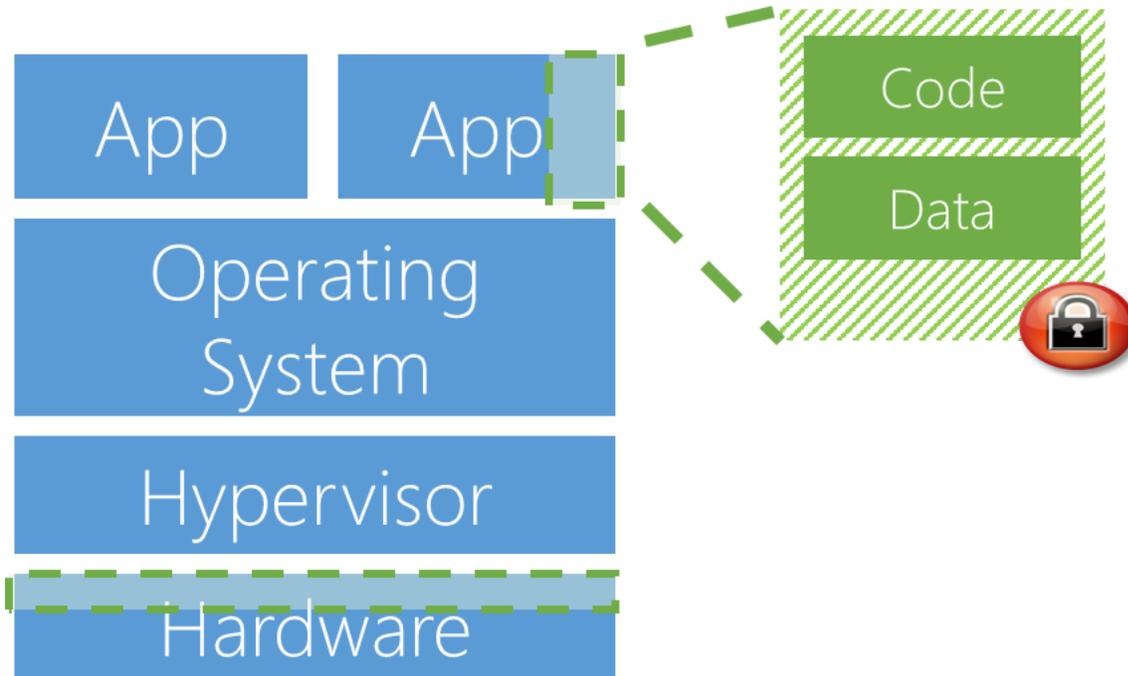
### Trusted Execution Environment

The final step to ensure privacy are executing smart contracts in a trusted execution environment (TEE). TEEs guarantee code and data loaded inside the environment is protected from prying eyes, including the host system it's running on. TEEs make use of new technology such as [Intel SGX](#) and Virtualization Based Security (VBS) to protect data that is actively being processed from anything outside the TEE. Data must be in the clear for processing, ie: decrypted, and TEE's ensure that data is never exposed.

Using these technologies, users of Etherprise can sleep at night knowing that their data is safe not only at rest, but also from common threats:

- Malicious insiders with administrative privilege or direct access to hardware on which it is being processed

- Hackers and malware that exploit bugs in the operating system, application, or hypervisor
- Third parties accessing it without their consent



src: [Microsoft](#)

Etherprise will have two options for node operators, one will be to setup and use Intel SGX manually, the other will be to use cloud provided Trusted Execution Environments, such as [Microsoft Azure Confidential Computing](#). Either will provide the same guarantees.

## Security and Access Controls

A core part of any enterprise software system is security and access controls. Without this, an enterprise would not be able to use it. Etherprise provides everything an enterprise needs to make full use of the blockchain.

In Ethereum and most other blockchains, all contracts are publicly accessible and anyone can access a smart contract and attempt to interact with it. Etherprise sits on the opposite end of the spectrum where nobody can access a smart contract until given explicit access. This is a

core feature of the Etherprise blockchain, not something the developer of the smart contract has to handle.

### **Key Management System (KMS)**

Key management refers to the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. Key management concerns keys at the user level, either between users or systems. Successful key management is critical to the security of a cryptosystem. It is the more challenging side of cryptography in a sense that it involves aspects of social engineering such as system policy, user training, organizational and departmental interactions, and coordination between all of these elements, in contrast to pure mathematical practices that can be automated.

A key management system (KMS), also known as a cryptographic key management system (CKMS), is an integrated approach for generating, distributing and managing cryptographic keys for devices and applications.

For blockchain, without a key management system you have to hand out the core blockchain private keys to your employees in order for them to access and interact with the blockchain and smart contracts. Once you've given an employee one of the core private keys, there is no way to take it back. Even if that person leaves the company, they may still have a copy of that key and can therefore access the same things they could access before they left. If a private key were compromised or an employee shared it with someone else, the key could be in the hands of any number of people and you would never have a way to revoke it or stop an anonymous person from tampering with your smart contracts. This is obviously a huge security risk. There is also no way to know who actually used the key.

The Etherprise Key Manager (EKM) manages and secures your companies private keys to ensure this doesn't happen. An employee can be issued new private keys that map to the core private keys. Use of these keys will be logged so you know who and when anybody accessed a smart contract. User keys can be created and revoked on demand. You can also generate time based (temporary) keys for automatic revocation.

### **Role Based Access Controls (RBAC)**

In computer systems security, role-based access control (RBAC) is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500

employees<sup>14</sup>. RBAC is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. A study by NIST has demonstrated that RBAC addresses many needs of commercial and government organizations. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions. Its popularity is evident from the fact that many products and businesses are using it directly or indirectly.

Etherprise enables RBAC for smart contracts to make it easy for companies to manage access rights to their smart contracts running on the blockchain. This means that you can restrict access at the core blockchain level rather than depending on the smart contract developers to write security into every single contract. This will provide a much higher level of security than exists today.

### **Single Sign-on (SSO) Integration**

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session. On the back end, SSO is helpful for logging user activities as well as monitoring user accounts.

Etherprise will provide single sign-on support for popular SSO services such as Google, Auth0 and Okta, as well as provide the capability for large corporations with their own SSO solution to integrate. This means your employees will be able to sign in using the same username and password they already use to access your companies systems, and from there be given access to their Etherprise keys.

### **Audit Log**

An audit log is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. Audit logs typically result from activities such as financial transactions, scientific research and health care data transactions, or communications by individual people, systems, accounts, or other entities.

---

<sup>14</sup> [http://csrc.nist.gov/groups/SNS/rbac/documents/20101219\\_RBAC2\\_Final\\_Report.pdf](http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf)

Etherprise logs every interaction with the blockchain so you can know when an activity happened, what exactly happened and who did it. This includes read-only events that don't change data that typically would not be written to the blockchain itself.

## Performance

An enterprise blockchain needs to be able to keep up with enterprise workloads and the existing blockchains, to put it simply, just can't do it. At around 10 transactions per second for the most popular blockchains, the performance is orders of magnitude off from where they need to be.

Etherprise provides a highly optimized, enterprise ready, Ethereum compatible blockchain. Etherprise uses [GoChain](#) code as a base because it is the fastest and most reliable Ethereum blockchain right now. GoChain can handle 1300 transactions per second in a public blockchain, whereas Ethereum itself can only do ~13 transactions per second, a > 100x increase in performance.

Etherprise will have similar performance characteristics as GoChain on the public network with a slight decrease due to the overhead incurred for the added privacy and security features. Etherprise will target 1000 tx/sec.

## Compliance

Etherprise will work towards compliance in several key areas that can improve enterprise adoption. While it may not be in compliance from day one, Etherprise will be working towards the following compliance goals.

### HIPAA Compliance

Health Insurance Portability and Accountability Act (HIPAA) compliance covers many things to protect consumers health data. At a high level, there are 4 rules:

1. HIPAA Privacy Rule
2. HIPAA Security Rule
3. HIPAA Enforcement Rule
4. HIPAA Breach Notification Rule

Etherprise will be working towards covering all of the aspects of HIPAA compliance from a software/technical perspective as well as having all the nodes in the network be HIPAA compliant from a physical perspective. This would mean every company running a node and every node in the network would have to follow stringent guidelines. It would also make Etherprise the first public blockchain that healthcare companies could actually use.

## GDPR Compliance

The General Data Protection Regulation (GDPR) is an extensive new law regulating the collection and use of personal data of individuals in the European Union. GDPR came into effect in May 2018. GDPR covers all kinds of personal data, which is any information relating to an identifiable individual. Since blockchains store data, some of which is personal, they are affected by this law.

Some aspects of GDPR are hard to comply with due to the nature of blockchains being immutable databases. If someone wants to delete their data completely, it's typically not possible. Due to the privacy aspects of Etherprise, we may be able to still comply by destroying the encryption keys for a users data.

Etherprise will do everything possible to comply with the GDPR laws to enable enterprise companies in the EU region to use it.

## Interoperability

While existing public blockchains are great for public use cases like asset ownership and Etherprise will be great for private use cases such as internal business operations, there are use cases where you might need both. One example is using a private contract on Etherprise to handle a complex sales transaction, but the asset you are selling lives on a public blockchain. Take a real estate transaction for example, the asset ownership is public on Ethereum or GoChain while the parts of the sale leading up to the transfer of the real estate asset need to be private. Things like escrow, down payment, mortgage contract and commissions to the brokers and/or real estate agents.

Etherprise will support these types of cross-chain transactions to enable use cases that aren't possible right now. Initially, Etherprise will be partnering with GoChain to work on an



interoperability layer. After that, we will attempt to work with other chains to support similar functionality.

## Enterprise Ethereum Alliance

The [Enterprise Ethereum Alliance](#) (EEA) connects Fortune 500 enterprises, startups, academics, and technology vendors on a mission to bring Ethereum to the enterprise. The EEA will define enterprise-grade software capable of handling the most complex, highly demanding applications at the speed of business. The EEA states “Privacy and Performance improvements will be mandatory to achieve enterprise-ready status and will be the focus of Enterprise Ethereum’s roadmap.”

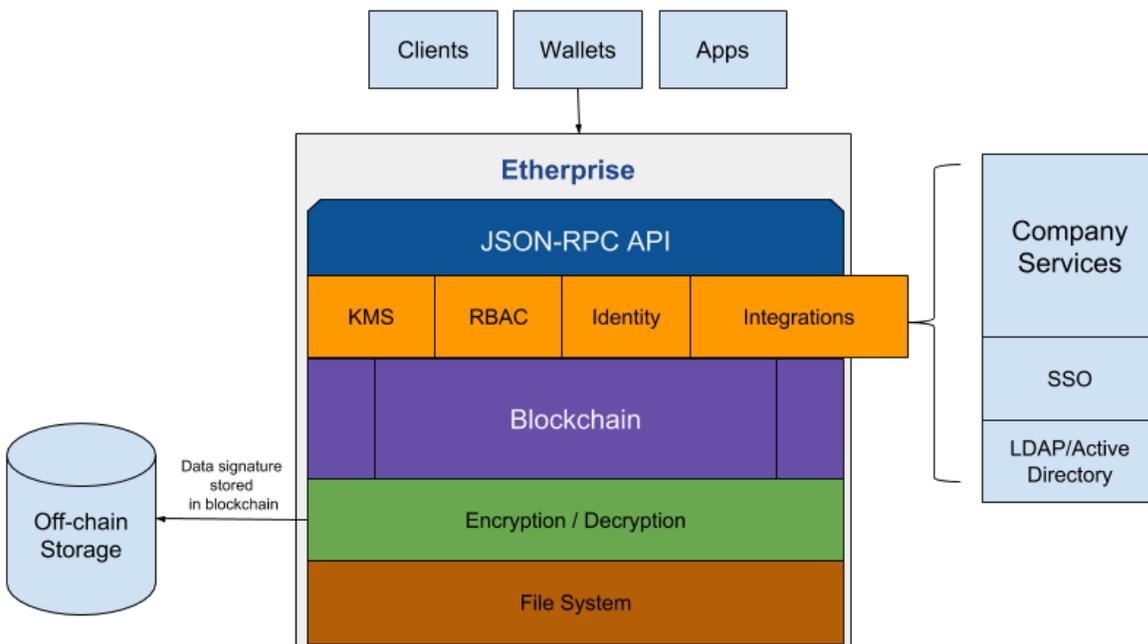
Etherprise solves the core problems the EEA is trying to solve and will be the first enterprise ready, Ethereum based blockchain to come to market. Etherprise will try to adhere to the EEA specs and standards as much as possible. Etherprise will join the EEA and work together with the alliance and its members to bring Ethereum to the enterprise.

The 500+ members of the EEA consist of many fortune 500 companies including Microsoft, BP, Credit Suisse, Intel and many others. All of these companies are looking for an enterprise ready solution for Ethereum.

## Technical Details

This section will cover the technical aspects of the Etherprise blockchain.

### Architecture



### Proof of Reputation

The Etherprise public network will use [Proof of Reputation](#) for its consensus algorithm. We believe Proof of Reputation is the the best way to provide a secure, trusted network in a public, decentralized environment, especially for enterprise workloads. Proof of Work and Proof of Stake consensus use untrusted, anonymous nodes to execute your smart contracts which means you have no control, no privacy and no idea where (what country) or what hardware is running.

Etherprise will have a public list of trusted companies running all the nodes in the network, ensuring we can provide consistent hardware, consistent privacy and known geographic

locations. Etherprise will have very high standards and requirements for the companies running the nodes to ensure maximum privacy and security.

Although it's not a requirement, nodes may be run by the enterprise companies using it.

For further reading on Proof of Reputation, please read [this article](#) that explains how and why it works.

In addition, Etherprise will not allow nodes that are not signers of the network to even run a non signing node. All blocks will be available to the public, but only after data is encrypted and written. A non signing node would not be able to fully process blocks since it won't be able to encrypt and decrypt the data.

## On-chain and Off-Chain storage

In order to meet the demands of enterprise with large data requirements, Etherprise will support both on-chain and off-chain storage. On-chain storage will have a much higher cost compared to off-chain storage and the user can decide which is a better fit.

Off-chain storage allows a company to store any amount of data off-chain, typically in a cloud storage service like Amazon S3. The data is cryptographically signed so that when the data is used, the nodes (or any other system that needs that data) can verify the data is correct and unchanged.

The advantages of on-chain storage:

- Fast access
- Replicated across all nodes in the network, ensures zero data loss
- Data management built in

The disadvantages of on-chain storage:

- Higher costs due to replication on all nodes
- Burden on the core blockchain

The advantages of off-chain storage:

- Unlimited capacity

- More privacy and security

The disadvantages of off-chain storage:

- Slower retrieval
- More complicated setup
- Users must maintain and pay separately for storage
- Potential for loss of data if user doesn't manage it correctly

## Automated Upgrades - CI/CD

Etherprise nodes will be automatically upgraded to the latest versions as they are released, enabling both better security and faster development. Using a continuous integration and continuous deployment strategy, Etherprise nodes will get updates and upgrades, early and often.

One problem with existing blockchains is that all the nodes are owned and operated by a large group of people and/or companies. When a security release comes out, it is up to each and every person/company running each node to upgrade their own server and it can take a long time for every node in the network to get upgraded. First off, each node operator must be notified that there is a release, then they have to take the time to download the release, apply the upgrade, test to make sure it works, etc. This means that a security flaw could be in the wild for long periods of time.

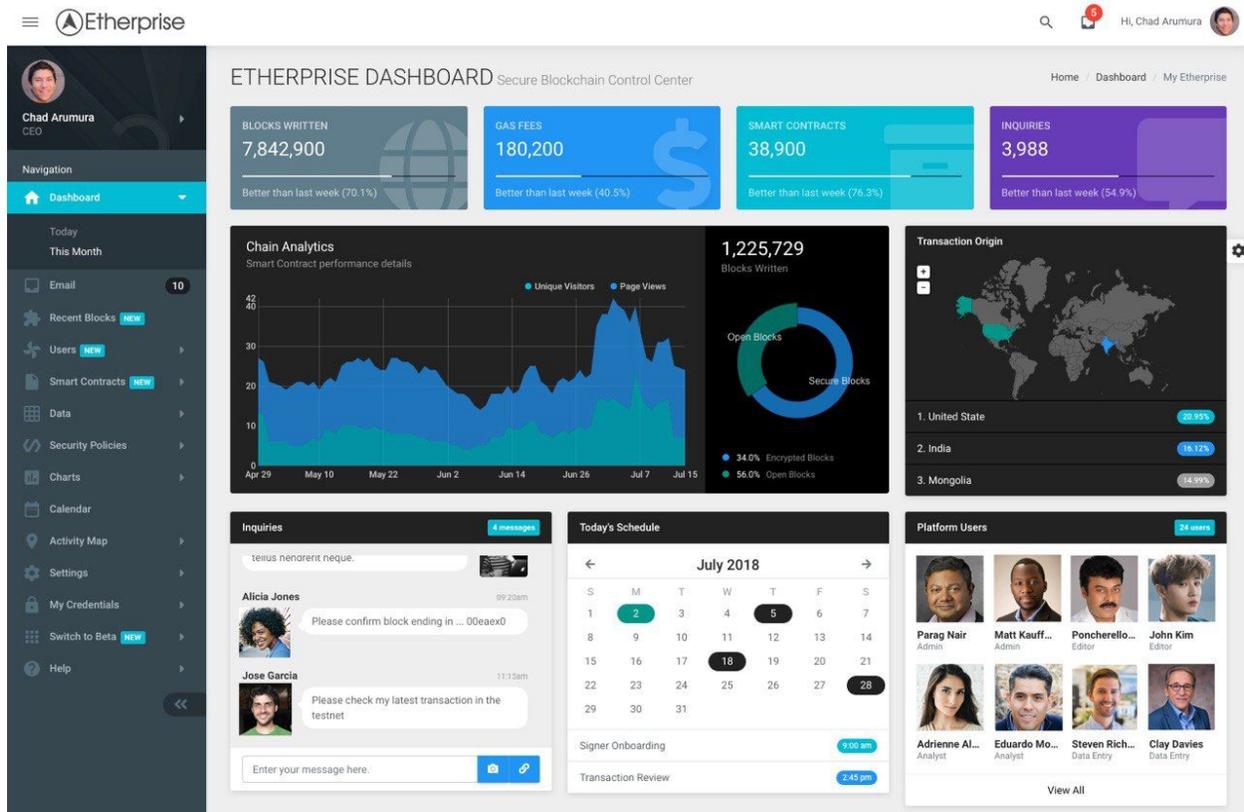
With Etherprise, bugs and security patches can be deployed to the entire network in minutes. Once a release is made public, every node will automatically see the new release, download it and upgrade itself. This ensures the network will be only be exposed to known flaws for the shortest time possible.

In addition to security fixes, this allows Etherprise to develop and release new features and enhancements at a rapid pace. It would be no harder to have a new release every day than it would to have a release every six months.

## Etherprise Management Console



Etherprise will provide an easy to use, easily accessible browser interface to control every aspect of an Etherprise blockchain instance. Administrators can set up role based access to smart contracts, issue and revoke keys, view audit logs and generate reports on usage of the chain. Users can use it to interact with smart contracts and DApps.



## Apache 2.0 License Rewrite

Etherprise will work on rewriting from scratch, any code that is hindered by a restrictive license like GPL/LGPL, which is unfortunately the licenses used by a lot of the existing Ethereum clients and tools. Most enterprise companies will not touch code with those licenses so in order to gain enterprise adoption, a non-restrictive license like Apache 2.0 must be used.

## Utility



The Etherprise network public blockchain enables companies to deploy and run DApps and smart contracts in an ultra secure and private system. The tokens sold during the token sale are intended for use on the Etherprise network to pay fees to the hosting nodes for executing smart contracts (compute) and storing smart contract state (storage).

## Team

The Etherprise team has decades of experience with enterprise software, coming from companies such as Oracle, Microsoft and IBM. The team has deep knowledge and expertise in the enterprise space and know what is required for enterprise software.

The team has also worked together on successful startups in the past and is taking that knowledge and skill and applying it to Etherprise.

Some highlights:

- Founded Iron.io, a cloud infrastructure provider
  - Raised \$17M from top tier VCs such as Bain Capital Ventures, Baseline Ventures and Sapphire Ventures (SAP's venture arm)
  - [Pioneered serverless cloud computing](#) which is now one of the hottest compute paradigms today
  - Scaled IronMQ to [1 million transactions per second](#), one of the few companies in the world that can claim that
  - Many enterprise customers including CNN, Philips, Turner Broadcasting, Pfizer, GoPro, Farmer's Insurance, Twitter and Google
- Founded [GoChain](#), a next generation, scalable blockchain
  - 100% Ethereum compatible
  - 10x more decentralized
  - 100x faster (1300 tx/sec vs ~10)
  - 1000x greener
  - Next generation smart contracts

## Core Team

### Chad Arimura - CEO

Chad is a 3x entrepreneur, with over 20 years experience leading technical teams and building software, most recently as co-founder and CEO of Iron.io where he led the company to a



multi-million dollar ARR business helping pioneer serverless computing. The company was acquired in 2017 and Chad and team joined Oracle.

He is now Vice President of Serverless at Oracle, currently leading The Fn Project, open source serverless FaaS platform and orchestration.

[LinkedIn](#)

### **Travis Reeder - CTO**

Travis has over 20 years of experience developing high-throughput, high scale applications and cloud services. He founded several successful technology companies including Iron.io and GoChain, and has raised tens of millions in funding from some of the top VC firms in Silicon Valley. Having solved scaling problems and delivering scalable services for his entire career, he is now applying that knowledge and experience to blockchain. Travis holds a Bachelor's degree in Computer Science.

[LinkedIn](#)

### **Jameson Stafford - CMO**

Jameson is a serial entrepreneur and technology executive who's built and sold two large-scale SaaS platform companies, led corporate development for a tier 1 venture-backed AI/automation platform, and played a hands-on role in the marketing of a leading blockchain platform and its successful ICO. He has driven enterprise platform adoption with Fortune and Global 100 Innovation teams, managed entire lifecycle branding and marketing across multiple entities and held numerous public speaking engagements, ranging from the US Bank Speaker Series to South by Southwest to TEDx talks. Jameson graduated summa cum laude from Michigan State University with a BBA in Marketing, studied graduate Film Production at USC, and was certified in multiple MIS programs during his early career at PwC.

[LinkedIn](#)

### **VP Sales - TBA**

We will be bringing on an enterprise VP Sales candidate that has generated \$100's of millions in revenue over his career.

## Advisors

### **Jason Dekker**

Jason is a serial entrepreneur, former hedge fund manager managing in excess of \$250 million, angel investor, board member and advisor with an exit to a public company. He has extensive C-level experience in finance, biotech, tech, and the food & beverage industries. He is currently the CEO and co-founder of GoChain.

[LinkedIn](#)

### **Benn Godenzi**

As an early adopter of Bitcoin in 2010 Benn has always had a very keen interest in blockchain technology and has adopted his marketing skills from to now focus on full time ICO marketing team management, fundraising, networking, private investor relations and project exposure within the cryptocurrency space. Benn is an advisor for WanChain and Aion and is the founder of the Interoperability Alliance.

[LinkedIn](#)

## Timeline

- September 2018
  - TestNet Launch
    - Beta release for early integration testing, outside reviews and security audits.
- November 2018
  - Beta MainNet Launch
    - MainNet live and available for public use.
    - Privacy and encryption features complete.
- January 2019
  - MainNet GA Release
    - Full featured mainnet with security and key management features complete.
    - Ready for production usage.
- February 2019
  - Etherprise Management Console Released
    - The Etherprise Management console available for public use.
- March 2019
  - Interoperability with GoChain
    - Cross-chain smart contract integration for private/public hybrid use cases.

## FAQ

### What are some key differences between Ethereum/GoChain and Etherprise?

	Ethereum / GoChain	Etherprise
<b>Security</b>	Private key access only	Key management (KMS) with revocable keys and role based access control (RBAC)
<b>Privacy</b>	Data is public and readable by anyone	Data is private and encrypted, only accessible to people who have access to the contract
<b>Use Cases</b>	Great for public asset ownership such as tokens, real estate, art and cryptokitties.	Great for business use cases such as payroll, sales comp, payments supply chain and b2b contracts.
<b>Target User</b>	Individuals	Businesses
<b>Management</b>	Wallets	Etherprise management console to manage users, keys and usage