ETHERPARTY

# USER-FRIENDLY SMART CONTRACT COMPILER

**KEVIN HOBBS** k@etherparty.io
**LISA CHENG** l@etherparty.io
**JEFFERY WALSH** jeffery@etherparty.io
**BRIAN ONN** brian@etherparty.io

**Abstract:** A user-friendly system for the creation, use, and management of smart contracts may dramatically expand the rate of commercial and consumer adoption of blockchain technology. While blockchain (or distributed ledger technology) has the potential to recast the foundations of electronic commerce and data storage, the technology's use by non-computer professionals has been limited by a lack of user-friendly applications. Etherparty unleashes the speed, cost-reduction and security benefits of smart contracts for individuals and businesses. It represents the next generation of software as a service. Etherparty promises to do for smart contracts what content management systems, like Wordpress and Wix, did for web development. Moreover, much like Legalzoom and Docusign before it, Etherparty goes further to make otherwise complicated contractual agreements and processes simple and accessible, while enabling infrastructure for authentication and automation.

This document contains proprietary information. Written consent is required for distribution or duplication of any portion contained therein.

## THIS IS NOT A PROSPECTUS OF ANY SORT

**This document does not constitute nor implies a prospectus of any sort. No wording contained herein should be construed as a solicitation for investment and this whitepaper does not pertain in any way to an offering of securities in any jurisdiction worldwide whatsoever. This whitepaper constitutes a technical description of the functionality of the Etherparty smart contract and the creation and issuance of FUEL tokens by Etherparty.**

# CONTENTS


04 Introduction

05 Our Approach

08 Next Evolution Is Adoption

10 Security

14 Arbitration

16 Use Cases

18 The FUEL Token

19 The ICO

21 RoadMap


> *We believe the demand for smart contracts will continue to grow as applications that automate peer interactions or facilitate coordinated group actions become more prevalent in everyday society. To meet this demand, Etherparty intends to create a platform and value-add services that allow any user to access smart contract and blockchain technology, without requiring specific technical knowledge of either."*
>
> **ETHERPARTY FOUNDERS**

# INTRODUCTION

What are smart contracts? Although becoming more commonly known, the idea of a smart contract is still relatively unknown by the general public. This concept was originally coined by computer scientist Nick Szabo sometime in the mid-1990s. He used this term to illustrate the potential for corralling highly evolved aspects of contract law and related business applications to the design of electronic commerce transactions between strangers on the internet.

Szabo wrote: *A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs1."*

In 2014, Vitalik Buterin introduced an iteration of this concept with the Ethereum whitepaper, which was later implemented by Gavin Wood in the Ethereum Yellow Paper. In it, Ethereum smart contracts would be executed through the Ethereum Virtual Machine (EVM), an environment designed to calculate arbitrary algorithmic complex instructions. These instructions take the form of function calls or messages, which allow contracts to interact with each other on the network. There are currently over 160 basic function calls that currently exist[2] and they will continue to expand as the Ethereum network switches to proof of stake[3].

We believe the demand for smart contracts will continue to grow as applications that automate peer interactions or facilitate coordinated group actions[4] become more prevalent in everyday society. To meet this demand, Etherparty intends to create a platform and value-add services that allow any user to access smart contract and blockchain technology, without requiring specific technical knowledge of either.

**KEVIN HOBBS**
CEO & Co-Founder
k@etherparty.io

**LISA CHENG**
Founder
l@etherparty.io

**JEFFERY WALSH**
Solidity & Full Stack Developer
jeffery@etherparty.io

**BRIAN ONN**
Chief Architect
brian@etherparty.io

1 Tapscott, Don; Tapscott, Alex (May 2016). The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. pp. 72, 83, 101, 127. ISBN 978-0670069972.
2 Go Ethereum Core Types: https://godoc.org/github.com/ethereum/go-ethereum/core/types
3 'globalRandao' and 'dunkle' are new terms outlined in Vitalik's Mauve paper: https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf
4 What is Ethereum: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

# OUR APPROACH

The mainstream use of smart contracts will require inventing new architectural solutions that combine blockchain with more traditional technologies (web applications, public APIs, and so on). One example of this will be a web application through which the user will sign up through our server and create smart contracts that will be testable and deployable on the blockchain. Our current implementation of this product allows for the creation and crowdfund of ERC20 or ERC223 compliant tokens[5], as well as sports bets of professional baseball to be placed between two users.

The application uses two hosted Ethereum nodes, one for the actual main Ethereum network, and the other for the testnet. This will allow the contracts to be fully tested by the users before deploying them. In our production environment, we will deploy with multiple, load-balanced Ethereum nodes to handle the expected network traffic, as well as to provide high availability for Etherparty users.

Future development of this web application will include an ever increasing library of smart contracts for the user to choose from, and a marketplace for user-created contract templates. This would enable non-technical users to create blockchain transactions in the form of smart contracts that can reflect any type of agreement in legal and business contexts. Traditional technologies will continue to provide the means to track versions of smart contracts, usernames on the platform, and corresponding email addresses for the purpose of logging in. The EVM will be used to process the escrow and instructions of the smart contracts itself.

5 Brief explanation of what ERC20 tokens are -- https://www.coindesk.com/ethereums-erc-20-tokens-rage-anyway/

# PLATFORM OVERVIEW

Etherparty is a platform that removes the complexities and management of creating and executing smart contracts. What sets Etherparty apart from the other code-based solution includes:

**01 NO OTHER TOOLS REQUIRED**

Using Etherparty means you won't need to install anything else like Geth, Meteor, or Mist to run Smart Contracts.

**02 SMART CONTRACT TEMPLATES**

Your contract drafts are always available and ready to execute. Log in from anywhere and deploy.

**03 NO SYNC REQUIRED**

Etherparty works directly with the Ethereum network so there's no delay for software to sync to quickly execute a contract.

**04 USER-CREATED CONTRACTS**

Users can create custom contracts to suit their needs.

**05 LEGALLY BINDING CONTRACTS**

Users can access simple legal agreements, add conditionality and deploy and the contract will be legally binding under the law placed in the contract.

**06 ENTERPRISE SOLUTION**

Etherparty's enterprise solution allows companies to integrate and upload their own documents and turn them into a smart contract. No need to change their current infrastructure.

**07 FLEXIBILITY**

Parties to the contract can create access for a third-party mediator or arbitrator for contract disputes when necessary.

## SUBSCRIPTION MODEL

The application is structured as a tiered subscription service that starts off with limited access to the platform features and ability to execute one-to-two contracts per month. The second tier will be set with a higher contract limit, while the third tier will increase upon the previous tier, with even higher limits, functions, processes, and integrations. Contracts will require FUEL, the platform's native validation token. Because the price of FUEL may fluctuate, we will peg contracts to a fixed amount of USD, and adjust the amount of FUEL required to execute the smart contract based on this fixed price. Although the current application works through filling out web forms, we have plans to implement an API, a drag and drop interface for users, as well as creation of smart contracts through natural language processing.

The public API will initially be aimed at enterprise customers. The API will allow businesses to keep their existing contracts and processes in place but transform them into smart contracts, enabling these processes to be backed by blockchain technology.

Our long term goal is to be blockchain agnostic. Although Ethereum has the most developed ecosystem with smart contract technology, we will be working with Rootstock[6] to enable smart contract creation with Bitcoin. In the future, we will look at integrating other blockchains into the Etherparty ecosystem.

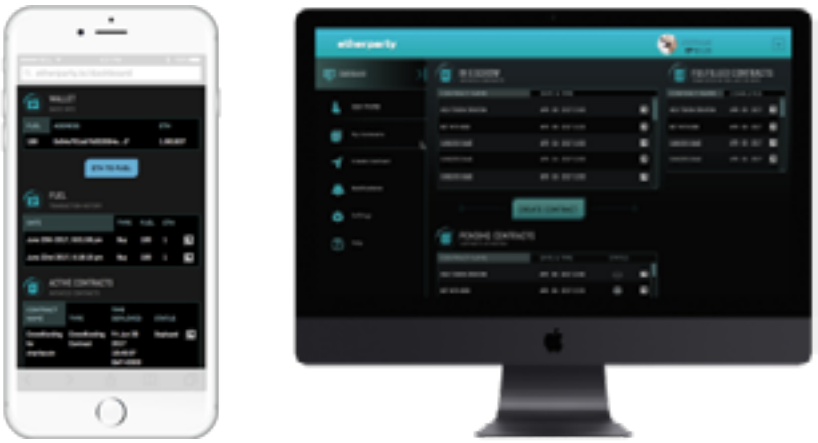
What these services offer is a way of saving our users a lot of time and money. Using Solidity, the programming language that these smart contracts are built upon, development is time consuming and costly. Finding good Solidity developers is difficult. Building the infrastructure to test your code for bugs is expensive. We allow you to outsource this. We give users the ability to test their contracts in a test environment and provide quick updates or redeployment for any buggy contracts, without requiring additional development resources. Smart contract creation will be as easy as filling out a form.

# NEXT EVOLUTION IS ADOPTION

In order to have mass adoption on a global scale, products and applications must be accessible to non-technical and non-industry users. Etherparty plans to be the trailblazer when it comes to providing such tools so that the next wave of users can take advantage of blockchain and smart-contract technology.

Just about everyone knows how to use email, for example, but the vast majority became acquainted with the technology through service providers—Gmail, Hotmail, Yahoo, and so on. Though possible to do so, only a fraction of users access email technology at the developer level. There's countless other examples across the industry from website development to document signing. So a similar case should be made for smartphone and smart contract technology.

Etherparty is well positioned to take blockchain and smart-contract technology to the next level.



> *Just about everyone knows how to use email, for example, but the vast majority became acquainted with the technology through service providers—Gmail, Hotmail, Yahoo, and so on. Though possible to do so, only a fraction of users access email technology at the developer level. There's countless other examples across the industry from website development to document signing. So a similar case should be made for smartphone and smart contract technology."*

# SECURITY

The main concern in the smart contract ecosystem is security. In the wake of many high-profile programming errors that lead to malicious theft of funds, concern about security is pushed to the forefront every day.

Etherparty stays abreast of these issues and creates templates that mitigate the possibility of these problems. Common issues that have led to loss of funds, like the short address attack[7] that plagues most standard ERC20 tokens, are delegated from being your concern to ours.

Etherparty defines a modular architecture with separated storage contracts that allow the functionality of your deployed contracts to be upgraded as the smart contracts evolve, keeping your data preserved. All contracts start with our base, secure templates.

Private keys for your Ethereum addresses on the Etherparty platform are stored in a locked vault that only you have access to. State management follows modern best practice hashing standards. The same standards for smart contract security are applied to the platform itself, which is continually monitored.

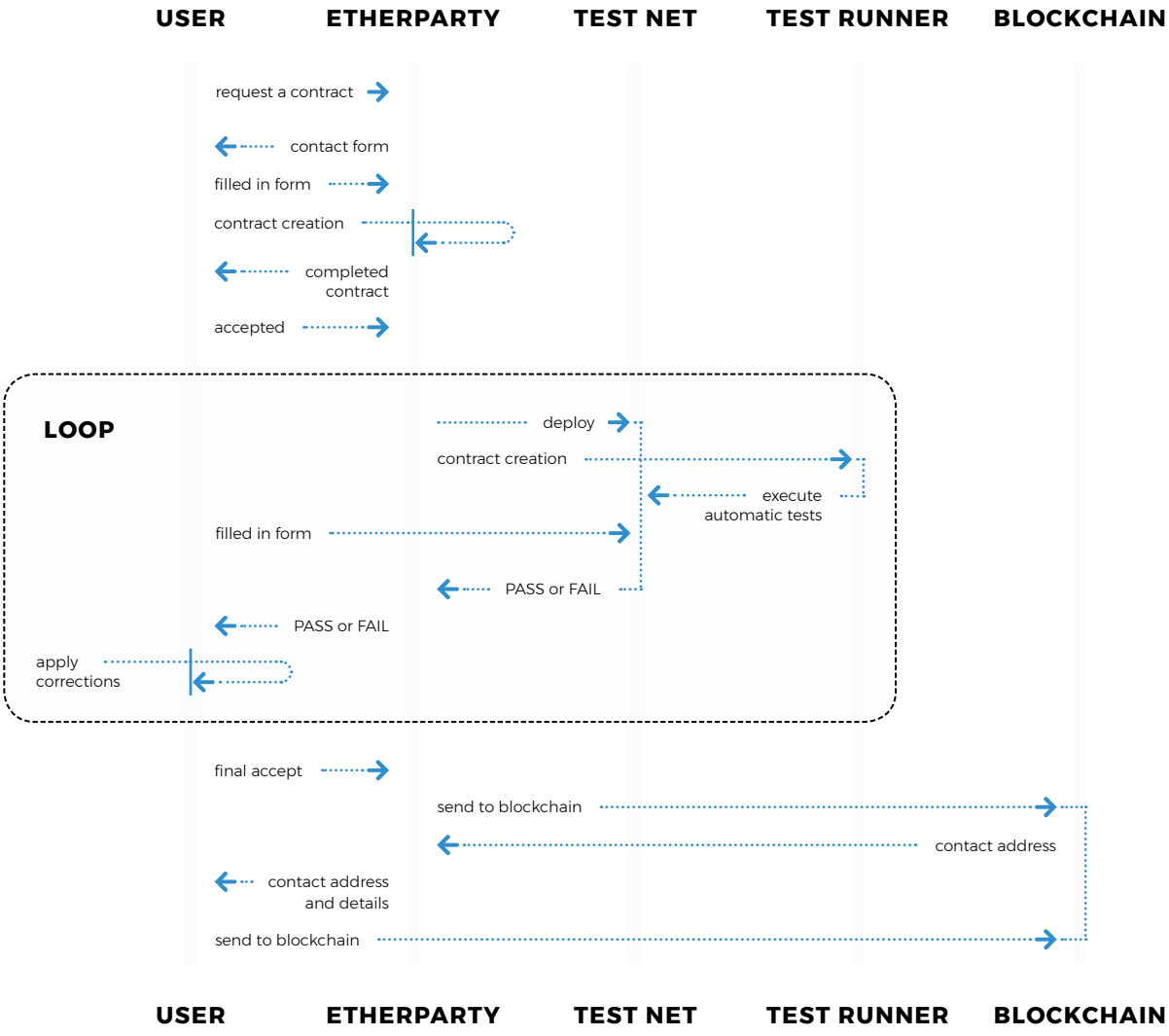
In the current implementation, our Ethereum smart contracts are built in Solidity using the most recent version of the compiler available. Solidity provides the most secure and robust interface for programming on the Ethereum network, as opposed to Serpent[8].

In the next iteration, we plan to deploy monitoring tools to detect contracts that need to be patched, and begin an automation process for streamlining updates. This will be accompanied by an automated testing service that will continually stress test the contracts before deployment.

7 http://vessenes.com/the-erc20-short-address-attack-explained/
8 https://blog.zeppelin.solutions/augur-rep-token-critical-vulnerability-disclosure-3d8bdffd79d2

Before users can deploy our smart contracts, they have to go through a diligence process on Etherparty itself. This will prevent the misuse of our platform. We are particularly concerned about users launching crowdfunding contracts, and will take extra steps to ensure crowdfunding contracts on Etherparty follow acceptable standards.

## CONTRACT DEPLOYMENT SEQUENCE

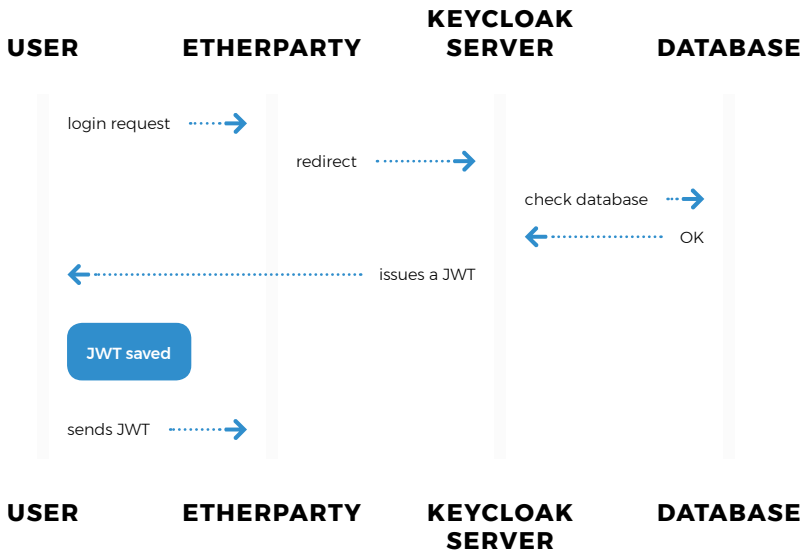


## PLATFORM SECURITY

Etherparty will launch with user authentication provided entirely by a Keycloak server. This is an open source and well known identity and access management (IAM) platform. Keycloak provides our Etherparty users with the safety and security of knowing that their personal data is protected by current and up-to-date security protocols. Keycloak is peer-reviewed and uses the established best practices in user identity and access control and is constantly being upgraded by the open-source community to stay on top of any known security issues.

Keycloak has built-in support for two-factor authentication (2FA), enabling us to launch with the highest levels of security built into the product (not as an afterthought at some future date). We will also require authentication via Keycloak before or during any transactions on the platform where there is the possibility for value to change hands. This means that users can trust that merely having access to the platform is not enough to transfer value—you must also re-authenticate, thus protecting any value you have stored on the platform.

## AUTHENTICATION SEQUENCE

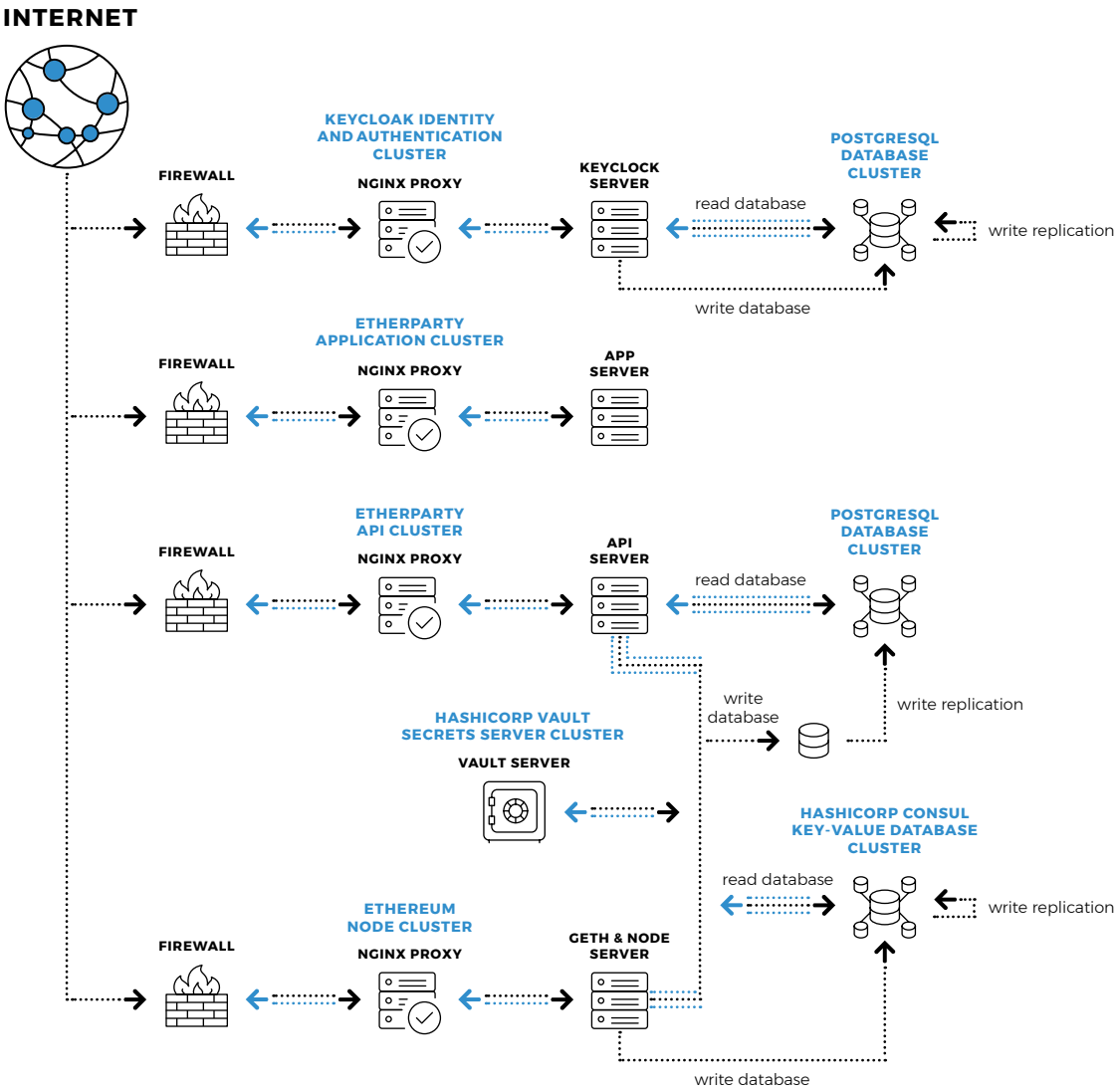



The Etherparty platform will log the last time and place of login, and show this to the user each time. If we detect any unusual activity, such as a new device login, or a new login from another location, we will send an email or SMS notification with an action item to lock down the account if desired. During this critical time, the ability to lock-down the account is provided to the owner of the account, thereby not requiring Etherparty support personnel in the event of an attempted breach.

The Platform will also attempt to automatically lockdown an account with any unusual activity outside of specified parameters, while accommodating legitimate use. We do this by building up a security profile and can then make automatic decisions about when to lockdown an account, for investigation. Etherparty personnel will also be notified of unusual activity such as a login from a suspicious geolocation. We also log all failed login attempts and notify the user via email of the attempt. The user is then well informed and can take appropriate steps to protect their account.

The Etherparty platform will always use the current best practices in identifying attacks and account takeover attempts (ATO) and lockdown the account before it can be taken over.

## ETHERPARTY NETWORK ARCHITECTURE



# ARBITRATION

For settlement of contracts, users may require information from a third party data source. This is currently addressed by a connected arbitrary third party API. As the use of smart contracts extends to the enterprise and everyday use cases, third party data sources will be required for automating contract processes. An on-chain approach that currently exists involves creating a proof system for third party data sources . This approach is valuable when we are working with trusted sources.

Our approach must address the plausible outcome that a trusted source may act malicious at a future point in time. Therefore we will require on-chain verification against data that would be directly injected into the blockchain. This information will need to be mapped to the input functions available in the contract[10] but still does not address whether the information can be trusted. We hope to address this problem with further research.

9 Oraclize.it
10 https://ethereum.stackexchange.com/questions/11589/how-do-oracle-services-work-under-the-hood

> *Smart contracts offer substantial benefits by automating contractual agreements that reduce transactional friction, cuts costs, while boosting data security."*

# USE CASES

Applications of smart contracts are widespread. The Etherparty platform will create a library of smart contracts aimed at a variety of industries, including banking and finance, trade, healthcare, supply chain management, insurance, foreign exchange trading, real estate, digital identity, and more. Adoption by these industries will happen because smart contracts offer substantial benefits by automating contractual agreements that reduce transactional friction, cuts costs, while boosting data security. Any type of contract can be improved by using smart contract technology.

To outline how Etherparty smart contracts are able to address different real world problems, we have compiled the following industry studies:

## FINANCIAL SERVICES

> Milestone-based payments
> Escrow

**Problem:** Managing a payment process with another party can lead to discrepancies, error, and confusion. Whether a personal agreement or business contract, there is room for mistakes, disagreement, and lost paperwork.

**Solution:** A smart contract binds both parties to steadfast rules that function exactly as written, eliminating the possibility of disagreement. Etherparty handles the security to make sure your contracts aren't vulnerable to tampering, providing a completely trustful payment process.

## MANUFACTURING

> Supply chain management
> Trade finance

**Problem:** Tracking goods and information can be a hassle and a lengthy process given a complex amount of conditions in a value chain and the reliance on paper based systems. This problem becomes worse if tracking needs to be done across international lines.

**Solution:** With Etherparty's enterprise API, integrating any information system into the platform will be simple and streamlined. Writing a smart contract will bring all parties onto a single shared ledger (the blockchain), which is faster, more secure, and more transparent to all parties involved.

## CROSS-INDUSTRY

> Peer-to-peer transactions
> Contractor agreements
> Contracts with executable conditions (e.g. smart probate or smart wills)
> Record keeping

**Problem:** From a simple wager between two private citizens to maintaining a record of data, the internet has turned commercial interactions into a digital arrangement.

**Solution:** Smart contracts and blockchain technology can alleviate concern over a breach of contract or the veracity of a digital record. By establishing appropriate terms, Etherparty makes it easy to create a smart contract which will auto-enforce the agreements as outlined by each party. Further, a smart contract can hash a record to the blockchain, which removes any degree of ambiguity over the digital upload.

## LEGAL

> Forming a business
> Corporate filing
> Dividends
> Chain of custody

**Problem:** Lost paperwork, uncertainty over whether something has been filed, missing information over handling of sensitive documents.

**Solution:** Business formation and corporate filings stored in a shared ledger, information is immutable and indisputable, and authorizations and access to documents are recorded.

## ICO CREATION

> Crowdfunding
> Token creation
> Watching the progress

**Problem:** Errors in security tests, deployment requires an ethereum server and familiarity with command line.

**Solution:** Etherparty provides a hosted solution for deploying and a GUI for interacting with the contract. All contracts are security tested and conform to the latest security standards.

# THE FUEL TOKEN

FUEL Tokens are the key to using Etherparty, they manage the contract library, security testing, network fees, monitoring, and management of the entire smart contract process.

FUEL is a transferable ERC-20 compliant digital token deployed on the Ethereum network, and is the in-app currency that powers the Etherparty platform. The FUEL token serves as a method of validating the user's interactions with Etherparty and will allow users to buy, execute, or barter for other smart contracts in the platform. In the future, FUEL will serve as access for smart contracts on multiple blockchains, integrating these disparate blockchains into one unified view within the Etherparty platform.

The total supply will be one billion FUEL tokens and will never be increased beyond this cap. The smallest unit of FUEL is one wei. Tokens that are used on the platform will go back into the platform supply. We will provide a service for users to purchase FUEL from this supply.

> *Fuel is a network currency to create Smart Contracts across multiple industries and platforms."*

 One wei is 10^18

# THE ICO

The ICO will allow us to hire new talent, pay for marketing, as well as for business and product development so that we can be the first to market with a smart contract platform that anyone can use.

## ALLOCATION

Only one billion FUEL tokens will ever be created. The FUEL tokens are intended to be allocated as follows:

- 40% (400,000,000) to be sold by the Company to pre-Crowdsale purchasers pursuant to a SAFT[12] offering or through Company Approved Affiliates. If all pre sale tokens get sold at the highest bonus 35% then there will be a total of 540,000,000 million FUEL tokens sold.
- 40% (400,000,000) to be sold by the Company to Crowdsale purchasers. If the pre sale sells out in full at the highest bonus level 35% there would only be 260,000,000 tokens available in the public sale
- 10% (100,000,000) reserved by the Company to incentivize community, beta testers, and strategic partners.
- 5% (50,000,000) to be sold directly on the platform at a minimum of $1 USD
- Etherparty Platform tokens that are owned by the company will be priced at $1 USD or the highest traded market price.
- 5% (50,000,000) to be distributed by the Company to the Etherparty team.
- Etherparty platform and Company Staff tokens will be locked for 6 months after the end of the crowdsale.
- Any unsold tokens in the pre sale will go into the public sale.
- All unsold tokens from the public sale will stay on the Etherparty platform held by the Company for sale only on the platform at a minimum of $1 USD

12 https://coinlist.co/about/help/saft

# PRE-CROWDSALE

Starting on September 15th, 2017 and ending on October 15th or when sold out whichever comes first (dates are subject to change). The Company is pre-selling Tokens (prior to the Crowdsale) at a discount on a wholesale basis for larger volume purchasers or through authorized Affiliates:

> $50,000 USD + receives a 15% bonus

> $100,000 USD + receives a 35% bonus

For information on the terms of the pre sale please contact k@etherparty.io.

# PUBLIC CROWDSALE

FUEL Tokens are intended to be sold at the following rates:

**Week 1:** 2500 FUEL tokens for 1 ETH

**Week 2:** 2000 FUEL tokens for 1 ETH

**Week 3:** 1500 FUEL tokens for 1 ETH

**Week 4:** 1125 FUEL tokens for 1 ETH

*Note ETH exchange rates are subject to change without notice prior to the start of the public crowdsale. Once the public crowdsale starts the exchange rate will be locked.
**Note The prices for the pre sale are not subject to change and will remain the same and have no effect on the public crowdsale.

# ROADMAP

**ETHERPARTY FUTURE ENHANCEMENTS AND EXPECTED RELEASE TIMELINE***

## RELEASE 1

**(END OF Q4, 2017)**

### BACKEND SYSTEMS

- Move from Firebase database backend to Postgresql
- Build out a secure representational state transfer (REST) application programming interface (API) to the contract platform to be sold as a platform as a Service (PaaS) for ongoing subscription income
- Additional REST API features will be included to support supply chain management
- Improve ease of deployment and scalability via Docker containers
- Microservice architecture with JSON Web Tokens throughout the application servers
- Inclusion of a web server proxy with server affinity
- Fully managed DAPP model on the blockchain with contract factories for deployment

### FRONTEND SYSTEMS

- Web3 single sign-on (SSO) integration creating a no-click Web3 sign-on to the platform
- Metamask integration
- Two factor authentication (2FA) with a proper identity and access management solution (IAM)
- Last place and time of sign-on
- Require additional security checks when doing anything that transfers value

### AUTHENTICATION AND AUTHORIZATION

- Utilization of an established and publicly vetted open source IAM server like Keycloak, or one of the verified cloud based IAM services like ForgeRock, Stormpath or Okta
- Additional sign-on security with 2FA
- User account takeover (ATO) fraud prevention solutions

### NETWORK ORGANIZATION

- Multi-tiered load balancing and monitoring
- Distributed cache layer between the backend service and the database using either ehcache or memcached products

### CLOUD

- Google Container Engine[13] with Kubernetes[14] or Mist.io[15] for Docker container management, Red Hat Openshift[16], or a similar Kubernetes supporting cloud platform.
- Integration with ElasticSearch, Graphite, or Prometheus for alerting on operational data that is out of specified boundaries
- Integration with Slack, Skype, BigPanda, and/or PagerDuty for notifications

*Note All release dates and enhancement groupings are estimates and subject to change

13 http://vessenes.com/the-erc20-short-address-attack-explained/

14 https://kubernetes.io/

15 https://mist.io/

16 http://openshift.com/

# RELEASE 2

**(END OF Q2, 2018)**

### MOBILE APP

- Push notifications
- Full mobile device support for Android and iOS

### NOTIFICATIONS

- Transaction history logging
- Desktop notifications while on the platform
- Notifications via SMS while off the platform
- Notification integrations with messaging apps

### CONTRACT TEMPLATES AND LIBRARY

Expand library to include:

- Legally binding contracts
- Voting and ballot box contracts
- Notary services
- Multi-person escrow contracts
- Family trusts
- Money manager
- Corporate stock
- A virtual democracy
- Crowdfunding
- Timesharing
- Time-locked vault
- M of N (multisignature) escrow
- M of N (multisignature) vault
- Real estate sales
- Supply chain management needs

ORACLE®

### ORACLE SYSTEM

- Server to integrate third party APIs
- Marketplace of APIs for selection

*Note All release dates and enhancement groupings are estimates and subject to change

# RELEASE 3

**(END OF Q4, 2018)**

### FRONTEND SYSTEMS

- Drag-and-drop contract building capabilities

### MOBILE APP

- Integration with Google Assistant on Android
- Call interactive voice response (IVR)
- Enterprise integration features
- Additional features of REST API for enterprise customers to add users to their team, create contract templates, test contracts on our test networks, submit contracts to the main blockchain, and get results of those contracts

### ENTERPRISE SOLUTION

- Etherparty advanced user interface additional features that are necessary for enterprise customers
- User created templates

### TEAM AND TEAM FEATURES

- Add team members, share and annotate contracts, and collaborate on new contract templates

*Note All release dates and enhancement groupings are estimates and subject to change

ETHERPARTY


**KEVIN HOBBS**
CEO & Co-Founder
k@etherparty.io

**LISA CHENG**
Founder
l@etherparty.io

**JEFFERY WALSH**
Solidity & Full Stack Developer
jeffery@etherparty.io

**BRIAN ONN**
Chief Architect
brian@etherparty.io

**ETHERPARTY**
300-717 W Pender, Vancouver, BC, V6C 2X6


© Copyright 2017 Etherparty | All rights reserved

**www.etherparty.io**