# BLUE Protocol White Paper

April 12, 2018

# Abstract

Blue is offering a family of developer tools, consumer software, and guidelines for the development of digital assets tools on the Ethereum network. The existing infrastructure relies heavily on the storage of private keys and passwords to authenticate the transfer of funds. These are easily phished, lost, or stolen, and have led to the loss of a massive amount of funds since the inception of the Ethereum network. We use the following major components to protect user funds, improve user experience, secure the safety of digital assets, and help Ethereum and cryptocurrency at large thrive.

## BLUE Protocol

A series of smart contracts and backend systems that allow all the network to function securely and conveniently. The Blue Protocol allows for 2-factor authentication without a central party. Funds are held in smart contracts for users, who maintain complete control over these meta-wallets. This is secured by the blockchain identification system, secure asset storage, smart contract analysis, blockchain analysis, address blacklisting and whitelisting, and anti-phishing capabilities.

## BLUE SDK

We offer wallet developers, exchanges, and e-commerce sites the option of integrating the Blue Protocol in to their own systems with the same automatic verification of digital assets and transactions as the BLUE Wallet offers. By integrating our easy to use SDK, with only a few lines of code our partners are able to demonstrate their commitment to security and protection of user’s digital assets.

## BLUE Wallet

The BLUE Wallet is a multi-platform application that allows for sending, receiving, and storing of ethereum based assets such as ERC20 tokens and beyond. By building our own wallet we are able to integrate our security protocol, including decentralized 2FA, deep integration with dApps, and a user friendly user experience using an internet-wide identification system secured by the blockchain.

## BLUE Standard

We have created an open source set of guidelines that should be followed by token developers, ICOs, and other digital asset creators and fund custodians. By following these guidelines and adhering to the Blue Protocol, our wallet and SDK can automatically validate and verify the safety of crypto assets.

## Table of Contents

# About Blue

## Underlying Beliefs

We believe that decentralization strengthens the individual’s right to privacy and control of their data. This is a benefit to the entire world and all of humanity. As internet technology has grown, so has government and corporate surveillance. The current state of the market means organizations receive rewards for surveillance and trading of the private data of internet users, and decentralized assets are the first realistic solution to this problem.

We believe that the  biggest problem we face today that holds back mainstream adoption of cryptocurrency and digital assets is the combination of poor security and complex user experience. We believe it is critical to relieve both simultaneously before the mainstream audience will be willing and able to adopt cryptocurrencies.

We believe that today there is great complexity in understanding and using decentralized software for the average person. The mainstream audience does not understand decentralization, or how it impacts their security.

## Our Mission

To make crypto safer, easier to use and understand, and easier to develop for.

## Our Vision

By making crypto easier and safer to work with, we aim to bring cryptocurrency and blockchain technology to the mainstream audience, enabling every person in the world to participate in the decentralized revolution.

# Evaluation of the current market

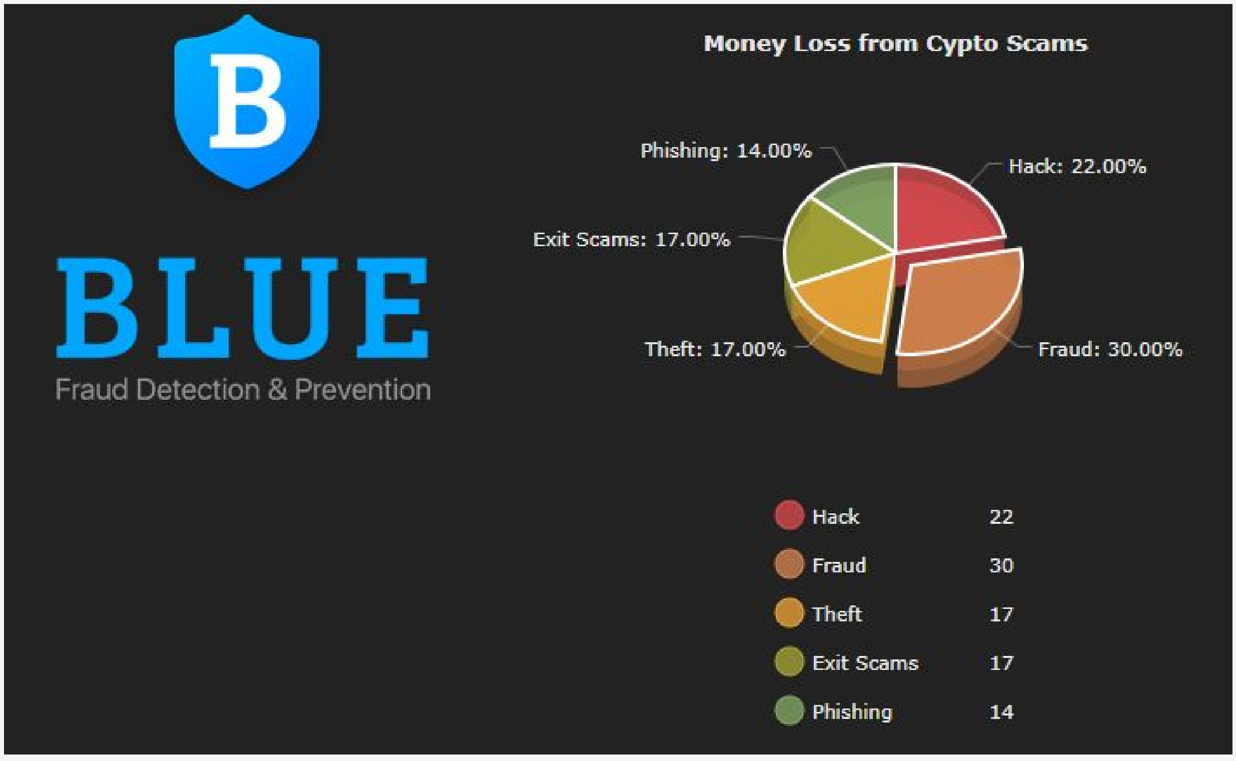
## Proliferation of Fraud

In an analysis of one million smart contracts, a new analysis tool called MAIAN found that 34,200 had security vulnerabilities.[1] Before we transition to a blockchain-based digital economy, we need to address the flaws in this system. MAIAN flagged 34,200 contracts, including a flaw in the Parity blockchain app that rendered $169 million worth of Ether inaccessible to owners back in July 2017. The team then manually analyzed 3,759 contracts and found exploitable vulnerabilities in 3,686 of them. This application was using extremely rudimentary tools for only superficial static analysis of the smart contract code. As a result we believe the 34,200 contracts are just the tip of the iceberg. In our early testing of the Blue Standard on the Ethereum chain, we can determine that the truth is that nearly all smart contracts have at least one vulnerability. Based on our analysis, nearly half of all smart contracts have **critical** flaws.

Within the first 2 months of 2018, over $1.36 billion worth of crypto has been lost due to scams.[2] In the time it takes you to read this sentence, $850 will have been lost. There were over 22 separate cases involving money losses of $400,000 or more in just the first 3 months of 2018. Summing these losses equates to over $14 million a day (Kharpal).

[1] https://arxiv.org/pdf/1802.06038.pdf

[2] https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/



## The ICO Problem

In a recent article published by Sherwin Dowlat & Michael Hodapp of Satis Group, On the basis of the above classification, we found that approximately 81% of ICO's were Scams, ~6% Failed, ~5% had Gone Dead, and ~8% went on to trade on an exchange (Dowlat).[3]

The ICOs were broken down into groups, with the following definitions:

1. Scam (pre-trading): Any project that expressed availability of ICO investment (through a website publishing, ANN thread, or social media posting with a contribution address), did not have/had no intention of fulfilling project development duties with the funds, and/or was deemed by the community (message boards, website or other online information) to be a scam.
2. Failed (pre-trading): Succeeded to raise funding but did not complete the entire process and was abandoned, and/or refunded investors as a result of insufficient funding (missed soft cap).

[3] https://medium.com/satis-group/ico-quality-development-trading-e4fef28df04f

3. Gone Dead (pre-trading): Succeeded to raise funding and completed the process, however was not listed on exchanges for trading and has not had a code contribution in Github on a rolling three-month basis from that point in time.
4. Dwindling (trading): Succeeded to raise funding and completed the process, and was listed on an exchange, however had one or less of the following success criteria: deployment (in test/beta, at minimum) of a chain/distributed ledger (in the case of a base-layer protocol) or product/platform (in the case of an app/utility token), had a transparent project roadmap posted on their website, and had Github code contribution activity in a surrounding three-month period ("Success Criteria").
5. Promising (trading): Two of the above Success Criteria.
6. Successful (trading): All of the above Success Criteria.

## Token Economics as a Distraction

Because so many ICOs are created strictly to raise funds, often the actual need for blockchain technology is not present. This however, does not stop ICOs with no actual use-case from raising millions of dollars from contributors who do not care or know how to evaluate the technical details. This inevitably leads to the team having a focus on token price, exchanges, and other aspects of managing a token-focused project. This detracts from the development process and is an overall net negative for the forward development of blockchain technology overall. Instead of producing results, ICO teams often produce only hype. This may come in the form of partnership announcements where there is no business need, additional exchange listings that are not needed for the project's development, or simply marketing events that focus only on intentionally manipulating price action.

## Lack of Utility

Because so many ICOs are so focused only on using tokens to raise funds, these developers often build a token that does nothing at all. This is bad for everyone because if there is no utility, over time the token is simply sold off by the initial contributors. This in turn causes a loss of excitement over time, and often an abandonment of the project.

## Deliberate Fraud

While the problems we listed above may be present in deliberately fraudulent token sales, they may also be present in well-meaning development team where a lack of knowledge or skill led to an eventual exit. On the other hand, as shown above 81% of all ICOs are outright deliberate scams. These projects are relatively transparent to those with a programming background, as the technical details are often plagiarised, or unusable and obviously not created by a competent development team. However, the average consumer who is interested in contributing to ICOs are easily fooled. This is a huge problem for the crypto space at large, and is the number one threat to cryptocurrency. Not only does the proliferation of fraudulent ICOs create fear and drive away contributors, but it also invites governmental regulations to step in and take drastic regulatory action.

# Self Regulation

Self regulation is the act of putting restrictions and requirements on the activity of an industry, by the industry player's own volition. This is necessary in the cryptocurrency space as the massive number of scams and hacks have proliferated over the years. If we as an industry can't act to present our own regulatory guidelines, world governments will be forced to step in and present potentially harsh regulations that may weigh down innovation and development of the industry. Self-regulation is much preferred, and the time to act is now. This is why we have introduced the Blue Standard, an open source repository of guidelines that anyone can contribute to. (The Blue Standard https://github.com/BlueCrypto/BLUEStandard)

## Intimate Knowledge of the Space

A key benefit to providing self-regulation as opposed to government regulation is that the industry players are best suited to provide these guidelines and standards due to their knowledge of the space. Being close to the business at hand allows for expert strategic decisions that will have the most positive impact to be selected. If left to government regulators, we may find cryptocurrency regulated out of existence due to a lack of understanding and appreciation for the massive benefits this technology can provide.

## A Faster Path to Commercial Applications

With self-regulation, we're able to speak more confidently of our own products, and give peace of mind to the mainstream population. This means more users and improved growth over time. By accelerating adoption we also accelerate development. As it becomes more clear and easier to interpret, these regulations can simply be adopted by developers, allowing for a proliferation of new and innovative technologies with meaningful commercial applications.

## Improved Investor Confidence

Knowing that basic safeguards are in place to police the cryptocurrency industry would allow new or curious investors to join the space with a greater confidence. Calculating risk is a critical aspect of investments, and there are many moving pieces to consider. Even with mature regulations this is a difficult task for investors. This is why it's important to remove the concern, and give investors peace of mind, allowing the space to grow.

## Government Support

Governments around the world have called out for self-regulation in the cryptocurrency industry. According to Forbes, "A top commissioner with the U.S. Commodity Futures Trading Commission (CFTC), Brian Quintenz, a Republican, has said operators in the cryptocurrency space could do well to consider adopting self-regulatory standards and "industry-wide" best practices to policing the new technology-driven space amid the authorities and government mulling further possible regulatory action."[4] This sentiment has been echoed by countless others and represents a positive outlook on self-regulation.

# Solutions

## The Blue Protocol

We invented and pioneered a modular smart contract system. Users assign metadata to a smart contract they control, allowing for proxy controls, identification, 2FA, and more. By just pointing these compatible contracts to another smart contract or series of smart contracts, developers are able to do amazing things. Our platform will be made open to developers through our framework and guides. This opens up an unparalleled way to look at money, wallets, and utility of money, and it's all decentralized. By utilizing this protocol along with the Blue Standard, it becomes easy to enforce self-regulatory actions by scanning tokens, evaluating fraudulent parties, and enforcing guidelines on the standards by which we come to agree upon as an industry.

[4] https://www.forbes.com/sites/rogeraitken/2018/02/15/u-s-cftc-commissioner-says-cryptocurrency-exchanges-adopting-self-regulation-could-spur-standards/

## Improved Security

Through our protocol, we enable the creation of secure ethereum wallets for on-chain transactions. In addition, by following the industry standard security requirements from the traditional financial industry, we pioneer the safest and most secure applications of the protocol.

## Improved User Experience

### Email-based cryptocurrency

Users can send crypto to others knowing only their email. The recipient will get an automated message, that allows them to claim X amount of crypto worth X amount by just downloading an easy to use wallet. This is a similar system that Paypal used to grow and gives us a similar opportunity to grow and market through our users.

### Smart Contract Based Wallets

A Smart contract is a programmable piece of code living on the blockchain, it has an address just like a standard Ethereum wallet. At BLUE we think this presents an untapped opportunity to make amazing things. We have invented a way for everyone to create a smart contract based wallet easily, for any user, and then proceed to use it like a normal wallet. We avoid overcomplicating things, with the additional steps needed for security opaquely happening behind the curtains. This enables boundless additional possibilities and functionality. Here we discuss some examples of the functionality that BLUE SDK will have in this system.

### Two Factor Authentication

Every website and bank has caught up on this. We need more security because the end user often does not have adequate security. We have created a two-factor-authentication system living on the blockchain.
Here is how it works :

- User makes a smart contract wallet (1)
- User opts in for two-factor-authentication, which creates another smart contract
- Your smart contract (1) points to two-factor-authentication smart contract, requiring it to sign off on the transaction. For it to proceed. This can be triggered by a specific sum, or at all times, this too is specified by the user.
- User downloads a app providing him with two factor codes or user gets two factor codes from a trusted party via a message on request.

- Smart Contract (1) looks up if smart contract 2 agrees and transaction goes through

## Spending Limits

Spending limits are a floating point calculation on every transfer the user makes. He sets his limits of transfers or amount of transfers per unit of time (for example max of 5ETH per day). The smart contract tracks the transactions, and triggers whatever the user wants, similar to a throw operation. This can also be presented as a security escalation to request for two factor authentication before proceeding.

## Identity and Collectibles Management

Our groundbreaking modular wallet system allows anyone to prove their identity to whoever they want, with whichever portion of the identity they want.
How this works :

- User types his secret message, his secret message is hashed and put on the blockchain
- A trusted party signs of on this message, saying it's truthful
- This data now lives in an anonymised form on the blockchain validated by a trusted party
- User wants to sign in somewhere proving their identity
- User submits the parts of the identity they want
- The person receiving this message hashes it through the same hash that user has in their smart contract
- The person looks up who said this data was truthful (eg. a government)
- We can now trust the data and the identity of the user

## Inheritance

Our modular smart contract system will allow users to add trusted parties in their contract. This effectively allows users to select various wallet addresses, which can spend all funds in the wallet. We can also indicate a criteria where this is only true after a certain amount of inactivity, or a set time frame.

## Recovery

BLUE will offer a recovery of your tokens and ETH in the same way inheritance works. Users set an amount of time of inactivity and register an email or their preferred method to be contacted. If this time passes users can trigger a recovery request by sending a request to the BLUE company, or any other provider that adopts the same system using our open standard. BLUE will charge a small, fixed percentage of the funds for recovery. In the event of 2 years of inactivity, the user will be prompted via email. If there's no activity or response, BLUE will empty the wallet, and proceed according to current laws for forfeiture.

### Automated Clearing House

The automated clearing house allows for merchants or other providers to elect to enable spending limits, refund opportunities, and to integrate between multiple types of digital assets in a seamless way.

# Blue SDK Definition

With the Blue SDK, we are offering an SDK that allows third parties to easily utilize our systems and standards without building every aspect from scratch. This means wallets, exchanges, and others building on the Ethereum network can greatly improve their security, while also saving development time.

Developer’s innovating with Ethereum can spend their time best working on their product and trying new things. Today they are currently forced to instead focus on building out complex security solutions as no standard for security exists. Our SDK allows these developers to integrate with the Blue Protocol, saving them much-needed time and energy, allowing them to focus on innovation, all while keeping customer funds safe.

Because the Blue SDK is built using industry standard npm packaging, it is easy to use across multiple platforms. Developers are free to choose which aspects they need, and which aspects they don’t, allowing for a high level of customization and modularity.

The Blue SDK offers support for two-factor authentication, fraud prevention, secure asset storage, smart contract analysis, blockchain analysis, address blacklisting, address whitelisting, and anti-phishing capabilities.

## Off-Chain Smart Contract Scanning

Additionally our SDK provides the ability for a consumer to request a scan of a smart contract or wallet address. The scan is requested by using one of our client libraries to call a smart contract that queues the scan job to be picked up by one of our many scan workers. These scan workers can be horizontally scaled to meet the demands of clients. Once a scan worker picks up a job they will run a number of tests against the smart contract. Examples of these tests include the below.

### Integration Testing

A copy of the contract in question is deployed to a local blockchain.  Compatible tests are selected from our database of test cases using the contracts ABI, and run against the smart contract.

### Static Analysis

The contract opcodes are scanned for patterns that indicate vulnerabilities using a number of different algorithms.

### Blacklisting and Whitelisting

Addresses are checked against a number of community and Blue-maintained black and whitelists which identify known attackers, and verified recipients of funds. Once the scan worker has completed the testing the results are compiled and hosted on our blue servers. Users can view their results and get friendly descriptions of each vulnerability found.

### Single Sign-On for Login

SSO Would allow for users to use a single identity for dApps, websites, services. The identify platform includes detailed permissions. So users can share only what they want to share. Government agencies, companies, and others will be able to build upon our platform to provide identity support for Ethereum wallets. This is decentralized using smart contracts, allowing any group to offer identity access to Ethereum consumers. For example a government agency performing KYC may include support for the following fields:

1. Public address
2. Username
3. Real name
4. Email
5. Government ID Hash

These identities are verifiable with issuing agency, for KYC or other key factors currently missing from the Ethereum ecosystem. These can not be reversed to discover ID without issuing agencies private keys.

An additional use-case of this system is for collectible dApps (such as CryptoKitties.) These may offer data on the collectible items in a way that they can be easily read and written by other supporting dApps, truly decentralizing the collectibles model.

# The Case for an SDK

True to our mission, we want to make crypto secure and more user friendly. Choosing the SDK route means current software developers can easily implement this into their code base, improving security of already onboarded clients instantly. This allows for a strengthening of crypto as a whole and speeding up the mainstream adoption.
Our SDK also allows us to shift the current path Ethereum tokens are heading towards, something we call “token madness”. We are heading towards a future where users need 6 different tokens to do one transaction. This is not how Ethereum should work. This multi-token approach will lead to slowdowns of the ETH network, and reduce user friendliness. We are avoiding this by pioneering a new type of token utility through our SDK and developer tools.

# The BLUE Token

The utility of the BLUE token is very simple. By holding a variable amount of BLUE decided by the platform in real-time, any Ethereum wallet is given full free access to the Blue Protocol features. This works for the BLUE wallet, any wallet using the BLUE SDK, exchanges using the BLUE SDK, and any supported dApps. This token can be bought and sold on secondary markets any time, enabling users to use the BLUE services via the token, and effectively return it if it they decide to stop using it, or to easily transfer it to any wallet that they own. The token also features unique replay protection both in terms of spending and in threat analysis. The BLUE token system contains a cryptographic signature that is altered by a nonce, and the associated metadata, so threat definition changes can never be replayed or spammed in order to attack the token's security model.

## BLUE Token Utility

A token for this is needed due to a few reasons. First, it would simply be impossible to provide the BLUE membership services for free if user's only needed to hold ETH. By having the BLUE token be used to stake for decentralized services, we avoid a per-transaction fee structure where ETH would need to be spent upon every transaction, or during any scan of an Ethereum address.

Second, we are able to use the token's smart contract to do tracking and versioning of the blacklist and whitelist using a custom metadata field inside the token's smart contract, along with a nonce. This allows the token to be used to alter the signing of transactions for threat signatures, to avoid false threat signatures from being broadcast to the network.

Third, by only providing services to those who have purchased BLUE tokens, we are able to reasonably assume that botnets, spammers, and other attackers will not be able to successfully spam the protocol with bad transactions in an effort to render them ineffective, or too slow to use. It would simply be too costly for an attacker to purchase enough tokens to perform an effective sybil attack.

## BLUE Membership

We would like to offer institutions such as exchanges an easy way to assign Blue Protocol capabilities to their users. This is needed in certain situations such as when an exchange generates new deposit addresses on the fly, which regularly change. It would be costly in gas to continuously shift tokens around between wallets. Additionally, having a large exchange simply buy millions of BLUE on the open market would have a destabilizing effect on the economics of the token. Particularly concerning is if use is discontinued, the exchange would then need to sell those tokens back to the market. To address this concern, we have created the BLUE Membership. As an alternative for B2B customers who would like to perform mass deployment of the BLUE token, we provide a Smart Contract that can ascribe all the features in the Blue Protocol to a fixed number of Ethereum wallet addresses quickly and easily using a side-chain that is under the company's control. We use the dev team tokens held in escrow to power these features without the exchange needing to go to secondary markets for their tokens.

Users can also directly purchase BLUE Memberships instead of holding BLUE tokens, leveraging the token reserve, however this is a fixed fee that is non-refundable and non-transferable.

The most common approach for individuals will be to utilize BLUE tokens directly. Individuals have significantly better mobility with their memberships, and never need to pay for these services. They will always be provided for free to BLUE token holders.

# The BLUE Wallet

The BLUE Wallet is our best foot forward in the wallet development game, and a showcase for our technology. We anticipate dozens of wallets supporting our SDK, and use our own as a demonstration as to how our technology improves the safety and ease of use of Ethereum based cryptocurrencies today. This wallet we've created as a demo is one of the best experiences available for token usage. We're able to deliver on this streamlined experience because we take security seriously, which enables us to also provide great convenience. In the future, all wallets using our technology will be safer and easier to use.

## Multi-platform Support

Today our demo wallet is available as a Chrome extension, but over the next year we will be shipping updated versions with support for iOS, Android, Windows, Mac OS, and Linux. Each of these wallets will use our SDK to deliver safety and convenience to our users, regardless of where they prefer to transact their business.

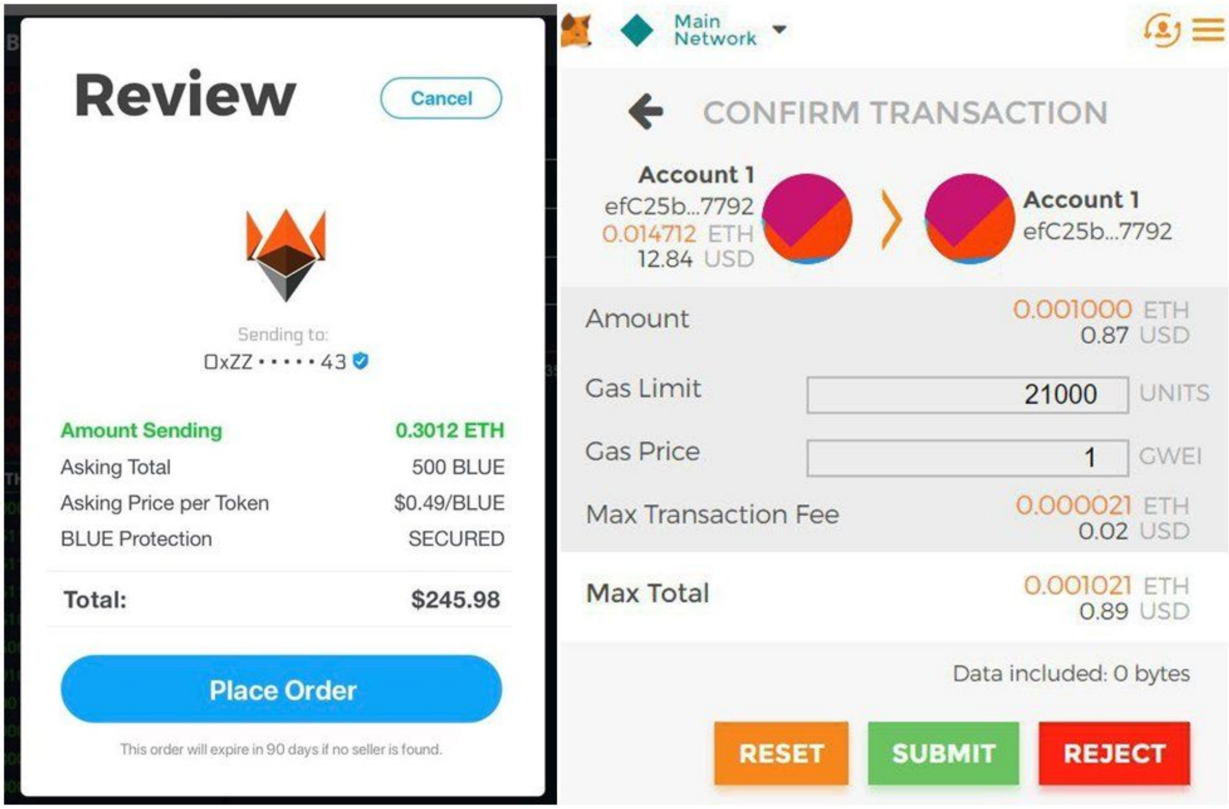
## dApp Support

A common use of the Ethereum network today is to power dApps, decentralized apps. Popular dApps today include EtherDelta, IDEX, and CryptoKitties to name just a few. By injecting a web3 instance in to the user’s browser, we offer an interface to these dApps using your securely stored wallet information. This means you can trade on EtherDelta, or buy and sell your CryptoKitties with just the BLUE wallet in a secured environment.

Because transactions are so easy to perform on your behalf using basic web3 calls, it is a security issue to simply sign in with your private key. MetaMask partially solved this problem by intercepting these calls and providing an authentication prompt before letting them go through. However because of the interface currently provided by MetaMask, phishing is still quite easy. We have solved this problem with a feature called Deep dApp Integration.

### Deep dApp Integration

By integrating with the most popular dApps in the world, we are able to show user friendly dialog prompts when authenticating transactions in dApps. We also uniquely identify the smart contract you are working with using a logo display, and verified checkmark. If using the BLUE wallet, you will never get phished with a fake dApp ever again. If that sounds complex, see the figure below comparing BLUE Deep Integration with ForkDelta, as opposed to how MetaMask renders the same information today.



Sending to:
0xZZ•••••43

| | |
|---|---|
| Amount Sending | 0.3012 ETH |
| Asking Total | 500 BLUE |
| Asking Price per Token | $0.49/BLUE |
| BLUE Protection | SECURED |
| **Total:** | **$245.98** |

This order will expire in 90 days if no seller is found.

Account 1
efC25b...7792
0.014712 ETH
12.84 USD

Account 1
efC25b...7792

| | |
|---|---|
| Amount | 0.001000 ETH<br>0.87 USD |
| Gas Limit | 21000 UNITS |
| Gas Price | 1 GWEI |
| Max Transaction Fee | 0.000021 ETH<br>0.02 USD |
| Max Total | 0.001021 ETH<br>0.89 USD |

Data included: 0 bytes

*Deep dApp Integration with ForkDelta*

# Decentralized Two-Factor Authentication

## The need for a decentralized 2FA

Currently the best way to secure an Ethereum wallet is to purchase a hardware wallet. This is because the private key is used on the wallet outside of the computer being used to interact with the blockchain, and the key is never exposed to the computer being used. Without a hardware wallet, the second best option is to use an encrypted signing bridge like the BLUE Wallet. However, when this private key is stored on the user's computer it is far too easy to lose access to it, or have it stolen by phishers, malware, or social engineering. The private key for a hardware wallet can be stolen if the recovery mnemonic is lost. The funds on a hardware wallet are easily stolen by simply restoring to another hardware wallet with the same mnemonic. By providing two-factor authentication, even a lost private key is safe from theft because no thief will have access to the changing second authentication code. This is more secure than a hardware wallet, and is highly needed for crypto to thrive.

## Centralized 2FA

Currently, many exchanges and platforms offer 2FA, but this is done in a centralized way. This is not to be confused with decentralized 2FA. Two factor authentication typically operates by confirming a secret key, that is shared with both the authenticating device (such as a smartphone app) and the centralized authority who validates login. When an exchange is hacked or it's database is otherwise exposed, this secret key can be stolen by attackers, and user's funds can be lost. To add to this concern, exchanges are frequently losing their own funds which back the representative funds in user accounts. When this happens there is often no recourse. These centralized authorities take custody of user funds, and your balance is only truly available because you place trust that they will accurately maintain your correct balances as a form of an IOU. This is not secured by the blockchain properly, and poses a constant threat to the entire crypto industry when these funds are lost. Simply enabling 2FA on a centralized exchange does nothing to protect digital assets, and only serves to protect your account credentials to the exchange.

## Our Solution

The Blue team has designed a modified version of the HOTP algorithm for 2FA support on the Ethereum blockchain. By delegating support for code injection in to the smart contract (the meta-wallet), we allow support for third party providers of 2FA. Providers use the open standard for BLUE HOTP codes. Any developer or team can implement their own version and integrate with their own authentication system. This allows for 2FA that is not dependent on our service. We will however offer our own provider support as a convenience.

Using the 2FA codes should be very familiar to anyone who has used such systems in the past. When sending funds, a user will be prompted to provide a HOTP code to the wallet before funds can be sent. This code can be retrieved from compatible smartphone apps that produce the one time code.

This is enabled by our use of the meta-wallet, a smart contract and proxy for the user that stores funds, not in the user's wallet, but inside the smart contract. The smart contract effectively implements multi-signature requirements where both the private key of the owner, and a second key are required to authenticate and process transactions on the user's behalf. Because the key recovery process changes on each transaction, the same code can not be used for a second follow-up transaction by an attacker.

A native mobile BLUE Auth app will be developed that produces HOTP codes, based on our modified algorithm. This algorithm is open source, meaning any developer can implement a competing app or software using the same scheme. The BLUE Auth app will be offered for convenience, and the added security of BLUE's engineering efforts.

# Blockchain Analysis

BLUE Geth is our modified Ethereum node, written in the Go programming language. The BGETH node is responsible for utilizing a full node's worth of data, and performing blockchain analysis on ERC20, ERC223, and Ethereum transfers, for the purpose of identifying flawed contracts, bad actors, and phishing attempts. By integrating directly we are able to extend the Ethereum RPC API, and add evaluations for tokens, addresses, transfers, and balances. This system simplifies access to the node and performs much faster. Instead of accessing the node via a REST call, we access the data directly, and present the aggregated information in an aggregate REST call. This greatly simplifies the amount of chatter between implementing applications, thereby reducing latency, bandwidth, and round-trip time constraints currently present in the ethereum network.

## Fuzz Testing

The BLUE geth server allows us to do fuzz analysis on smart contracts, so even without manual review we are able to identify problematic contracts. This enables us to detect cases where a token may have support for locking of transfers, freezing assets, transferring funds without the owner's approval, destruction of funds, infinite minting, and much more.

## Market Manipulation Detection

By being fully compatible with the main Ethereum network, we can identify faked volume on major exchanges, calculate true liquidity on any token, detect pump and dump behaviour on exchanges, and warn users of this activity. Using this we can warn users of spiking volume and trading price, and notify them to look for evidence that the change in price legitimate. This works for all ERC20 and ERC223 tokens

## Blockchain analysis for token distribution

When purchasing tokens from an ICO or in secondary markets, it’s important to be able to get a general sense of the fairness of distribution. If a token developer still controls 50% or more of the supply, it is very easy for them to sell massive quantities, putting heavy downward pressure on the price. This is seen too often in this space, and until now the average user has not had the tools necessary to determine this specific risk factor. The Blue Protocol helps make this easy, and the wallet makes it seamless and user friendly.

Many tokens developers hold significant portions of their own supply. We are able to detect and notify users of this if the amount is higher than a certain threshold. Using our BGETH system, we can perform these analyses with ease

1. Analyze the top 10 wallets
2. Determine the true circulating supply.
3. Detect trades between the top wallets, which are often a form of wash trades.
4. Detect if developer wallets are frozen.
5. Analyze the top 10 wallets and determine if the token distribution is healthy.

# The BLUE Standard

The standard by which BLUE evaluates all ERC20 tokens for participation in the BLUE Seal of Approval program This format highly inspired by the Ethereum EIP contributor standard.

BLUE Improvement Proposals (BIPs) describe the standards by which we hold tokens, wallets, exchanges, and other blockchain actors to when assigning reputation in the BLUE ecosystem.

Blue standard is a community driven standard that will be applied to every ICO and blockchain focused company/token. To keep bad actors accountable, and give well meaning actors a way to look up what's expected of them. As well as a “to do” list of good practices. As an example, see the infinite minting item in the Blue Standard below.

# Blue Standard: Infinite minting

## Abstract

Token creators can optionally choose to opt-in to giving themselves or others the ability to mint tokens. We believe this should be limited in time, scope, or quantity. Whether intentional or accidental we should introduce a fuzz-testing layer to the EVM that can try random inputs until it is determined that the total supply may be increased or decreased through smart contract interactions.

## Motivation

Currently, there is no clear way for the average investor to know that a token may increase or decrease it's supply. The only way for investors to understand the different is to read and understand the source code of every item they trade. Not only is this time-consuming for the skilled investor, it is impossible for the novice investor. As a result there is a large quantity of blind trading happening, where investors have no idea whether or not their tokens are backed by a constant supply, or a fixed-rate fluctuating supply

## Implementation Details

It is trivial to implement fuzz testing on an ethereum side-chain and simply try random input parameters, and then calculate the total supply to measure whether or not any set of inputs changes the total supply. If it does, as a matter of standard metadata output, we include this as a boolean flag in the `tokenMeta.json` in BLUE Geth.

Other Examples from the Blue Standard include:

1. Token Locking
2. Clear cash flow standard
3. Token locking for founders
4. Clear howey results
5. Clear token economics
6. Separation of concerns with tokens and ico code
7. Code standards - clear descriptions of functions so investors know if they are being deceived easily. No excuses after the fact
8. ICO standards - why does your ICO need to have a token? Why does it need to be on blockchain - an explanation
9. Code standards - gas usage. Useless functions and dependencies
10. dApp Standardisation of naming conventions
11. Acceptable plagiarism definitions (math equations etc)
12. Anti-Kill switch unless conditional multisig

# Integrations of BLUE Protocol

## Integrations for wallet providers

Wallet providers will be able to use our SDK and work with our tools to enable many of our features in partner wallets, such as:

1. 2FA
2. Blacklisting
3. Whitelisting
4. Token analysis

## Integrations for exchanges

Exchanges will be able to use our SDK and work with our tools to enable many of our features in partner exchanges. Common uses may include:

1. 2FA
2. Real volume calculations
3. Pump warnings
4. Token analysis
5. Blacklisting

6. Market cap calculations
7. Dev holdings calculations

### Integrations for block explorers and price charts

Common features used by block explorers may include:

1. Real volume calculations
2. Identifying bad tokens
3. Real liquidity
4. Ratings for tokens

## Spearheading the crypto self governance

Today, Blue is the only organization actively seeking to solve the self governance problem. This is important, and must happen, as we pointed out earlier in this document. Hacks, loss of funds, custodial failures, and other reasons lead to problems every day in the industry. Cryptocurrency is not yet adopted by the mainstream, or even the early adopters. We need standards and compliant partners to step up and join forces in the self-regulatory effort. This is what we need to bring adoption to this new and exciting industry.

## Words to regulators

The crypto world is more knowledgeable of crypto-currency than regulators, and is better suited to self-regulate. Given the complexity of crypto and the unique needs, a self-regulatory effort will help protect crypto investors, without sacrificing the technological leaps made possible by blockchain technology. If the world governments want to continue regulating cryptocurrency, they will be met with more and more resistance with modern tools to obscure crypto trading, and pushback from the community. Cryptography is both ubiquitous and unbreakable. These tools are important for the world, and we must protect the rights of those who choose to work with them. We urge regulators to let this infant crypto community educate, and self-regulate for themselves.