March 2019

White Paper: COVE (“COVE”)

A Globally Compliant Digital Reserve Currency

https://covesecurity.io

CYBER OPEN VIEW ENCRYPTION

CONTACT: info@vivecamedia.com

The COVE Tokens White Paper is not an offer or solicitation to sell securities. The COVE Tokens White Paper is intended solely to describe the COVE Tokens token (“COVE”) and matters related to its development and introduction into commerce. The statements contained in this White Paper are exclusively opinions and forward-looking statements, are made only as of the date written above and are not intended to be relied on by any person in connection with their determination to purchase or sell COVE Tokens. All offers to purchase COVE Tokens will be made solely to persons legally permitted to purchase COVE Tokens and will be pursuant to definitive documents and agreements clearly labeled as such and subject to all terms, conditions, disclosures, qualifications and risk factors contained therein.

INTRODUCTION

COVE is:

- Secure Zero Knowledge Encryption device
- Stay Safe on Public Wi-Fi Networks

Access all the blocked and geo-specific content easily, but also encrypt your data and hide your IP. Cove can be used on up to 10 devices simultaneously, it is compatible with any Wi-Fi products, smartphone, tablet, PC, TV box, Ai speaker, Kindle, Xbox, PlayStation, etc. No need to download APP, it’s an ideal solution for sharing and for multiple devices, use in home or office.

Nowadays, the main method of accessing various local and network resources is a password, that has proven itself as a way of identifying and securing users and resources. However, it has one serious drawback: in case of stealing a password, an attacker gets access to all the data of the user who owned this password. In addition, users usually have the same password for multiple services, the situation gets even worse because these passwords can be weak or even be a subject for vocabulary attack. Password databases from a variety of resources periodically fall into open access. In general, even if the resource provides the ability to change the password, this method is somewhat vulnerable, since the user's mailboxes are usually protected by a password, often the same as that used on other resources. Thus, the password can not serve as a sufficient instrument for protecting user data and guarantee the security of the user session.
An approach to this problem is password managers. This software, which provides a secure storage for passwords, and, in the case of integration as a browser extension, is able to withstand numerous ways of stealing passwords. Also, password managers are often able to generate secure passwords that are unique to each resource, which takes security to a new level. The obvious drawback of such protection is that the storage is protected with a master password (Lastpass, 1Password), and in case of theft or brute force the master password, it all boils down to the previous thesis.
Two-factor authentication provides a partial solution of password problems. For two-factor authentication, in addition to the password, it is required to provide the resource with some more data that should be available only to a particular user.

Examples of the second factor:

1. One-time passwords that are generated every n seconds are the most common option. Usually implemented with TOTP protocol.

2. One-time passwords sent in the message. Usually, SMS or instant messengers is used.

3. Hardware tokens.

Another way of authorizing a user into the system is SSL/TLS certificates, which are widely adopted in enterprise solutions, such as banking, tax services, etc.
A system of Public Key Infrastructure supports the creation, distribution and identification of public encryption keys, enabling users and systems to both securely exchange data over untrusted environment such as the Internet as well as verify the identity of the other party of conversation. PKI provides possibilities for digital signature (confirmation of authentication, non-repudiation and message integrity), data encryption (confidentiality during data storing, transfer and processing) and authorization in one complex system. The core of PKI - the public key encryption systems (a private key for encryption, a public key for decryption) based on strong mathematical approaches. But simple presence of public/private key is not enough for trust. There should be a complex and comprehensive system with all functions listed above.
Typically PKI consists of a lot of controls beginning from policies and standards through administration and management to software and hardware. PKI can be realized in different architectures: simple, network, hierarchy etc. But we should understand that the heart of PKI is digital certificates. A digital certificate is a document designed to affirm the identity (user, system etc.) of the certificate subject and bind that identity to the public key contained in the certificate.

The typical scheme of PKI includes next elements:

- Certification Authority (CA) - a trusted party provides services for issue digital certificates.

- Registration Authority (RA) - a trusted party responsible for accepting requests for digital certificates and authenticating the entity making the request. Sometimes RA also called subordinate CA.

- Validation Authority (VA) - a trusted party provides a service used to verify the validity of a digital certificate. It’s clear that different VA should has database of valid certificates, revoked certificates and communication with different CA.

As we can see, functioning of PKI based on trusted authorities with different functions. From our point of view we should focus on several core issues. First of all, PKI now is government regulated or business driven ecosystem depends on a sector of application.

Government CA and PKI at all usually are not acceptable for wide public or SMB use according to different limitations and application lockin. For example, specific CA works with specific tax reporting software. Services of business CA very often expensive and there is a collusion between software vendors and CA for including specific CA into a list of trusted for this software. For example, web browsers don't accept all certificates issued by different CA. Sometime ago it was a brilliant vision named "web of trust" where most of noted problems could be resolved with teamwork of count of CA/VA/RA. Unfortunately, it left just as vision according to the disagreement s CA to work in a single network of trust.

Emerald Blockchain works on solving those problems by implementing decentralized public key infrastructure based on blockchain technology. The chosen approach will give our end customers the way of managing their PKI with a high level of security and all advantages of decentralized and distributed system, including fault tolerance.

ADVANTAGES OF COVE:

1. There is no centralized database of certificates and keys that could be compromised.

2. There are no technology lockin and API limitations. Easy integration with existing systems.

3. There are no additional fees for different certificates/credentials in different CA.

4. There are no possibilities for collusion between software/hardware vendors and limited count of CAs.

5. Fast and protected public key distribution process.

6. Fast and protected certificate revocation process.

7. Single point of trust for different systems: easy single-sign-on implementation, decentralized worldwide available authorization.

8. There are no legal limitations and government cooperation issues.

ADDITIONAL ADVANTAGES:

1. Acceptable for different types multi-factor authentication.

2. Full anonymity.

3. It allows to track all issued certificates, provides complete and transparent control.

COVE is bringing blockchain to PKI infrastructure providing immutability of data stored there. For simple user it could look complicated, but all is simple: you don’t need to remember count of login and passwords, you don’t need to pay five or ten authorities for certificates used in tax, legal, bank, technical or other types of software, you don’t need to control the live time of each password/certificate/key.

COVE PRODUCT EVOLUTION

We implemented the current test system based on a custom blockchain on Hyperledger Sawtooth and a custom consensus algorithm heavily inspired by Ethereum Clique and Dash masternodes network.
Sawtooth is a framework for custom blockchains designed to be modular: every part of the framework including the consensus algorithm can be replaced with custom code. Consensus algorithm in a nutshell is Clique – simple PoA protocol which runs on top of the pre-defined list of nodes – with an addendum which makes it somewhat similar to Dash masternodes network: every user can enter the list of signing nodes by locking a certain amount of tokens and will be excluded from the list if their node works against the network rules and does not hold uptime.

CERTIFICATES SUPPORT

As in the first version of the system X.509 certificates are used. The following use cases are supported:

1. Self-signed certificates. In this case certificate data, such as public key, signature, expiration date and revocation status are stored on the blockchain.

2. Certificated signed by an organization. In this case an organization (which is our client) may use its own certificate to sign and manage certificates of its clients and employees.

To support COVE-based certificates it is planned to integrate a server-side software which will continuously check for the status of the certificate on blockchain. There can be different ways, such as implementing plugins for content management systems or incorporating self-signed certificates into the system trusted certificates list. In the framework of this system the following fields of a certificate will be exploited:

UID	The address of a user on COVE blockchain

2FA

The choice of technology for the second factor depends on the characteristics of the system, which is protected by COVE technology.

For example, if a system requires a physical presence of an authorized person, then the best option for the second factor would be to use biometric data, such as a fingerprint scan or an eye retina scan.

If the system uses some local sensor, then the second factor would be the physical connection to the local network check. If the system is remote, it is optimal to use a secondary device (a phone or another PC). The probability of simultaneous malware infection of two devices is lower than of one. It would also help to protect the account with a compromised certificate.

Additionally, an instant messenger can be installed on the second device to receive secret keys via messages from a protected system. In this case, the reliability of the second factor will be equal to the reliability of the messenger account. For example, it is possible to use Telegram (or other messengers), email, or email + PGP key.
Special consideration should be given to the standard TOTP (time-based one-time password) method, which generates one-time codes within certain time intervals (e.g., every thirty seconds). Such a scheme is implemented, for example, in the Google Authenticator application. You can also use an entirely-hardware solution for generating access tokens, for instance with the help of YubiKey, Yubico or Trezor.

TOKEN ECONOMY AND PRICING MODEL

As one of the requirements is to stick prices to a fiat currency, the platform needs some way to update the prices for its services with respect to the exchange rate of the token.

To address this requirement COVE will maintain a server which will periodically (10 minutes) update prices and will be available for masternodes. Every masternode can query this server to get the price of a token for a moment of time.

The token is needed for all internal operations inside of ecosystem and includes:

1. Initialization of a certificate creation process (an amount of tokens gets blocked for revocation transactions) ($1);
2. Establishing a node (will be available after Q2, 2019)
3. Fee for transferring COVE tokens between users on COVE blockchain (0.1%);

FEES DISTRIBUTION

Depending on the number of tokens collected during the token sale COVE will hold a portion of transaction fees to finance the project development:

1. Under 5m collected during the public token sale: 70% of those fees are stored on the account of a master node which created the current block, 30% are transferred directly to COVE and is used to maintain services such as Bitcoin anchoring, cross-blockchain transfers, etc.

2. From 5m to 10m collected during the public token sale: 80% of those fees are stored on the account of a master node which created the current block, 20% are transferred directly to COVE and is used to maintain services such as Bitcoin anchoring, cross-blockchain transfers, etc.

3. Above 10m collected during the public token sale: 90% of those fees are stored on the account of a master node which created the current block,

10% are transferred directly to COVE and is used to maintain services such as Bitcoin anchoring, cross-blockchain transfers, etc.

ALGORITHM

The solution for this task is the algorithm called “proof-of-service”, which was firstly introduced in Dash masternodes network. It:

1. Do not depend on the hardware capabilities;

2. Can incentivize users to stay online by ranking by their uptime;

3. Suitable for public networks.

This algorithm can be also described as a form of proof-of-stake algorithm with the additional factor of uptime. The core of this algorithm is the network of masternodes. Our concept will be slightly different from one introduced in Dash, masternodes (validators) are responsible for producing new blocks and validating transactions.

The main entity in this algorithm is the global list: it contains the full list of nodes which are eligible to sign new blocks. When a new node is introduced into this list it is placed into the end of the list.
Nodes are selected from the list stored in the blockchain in the order they are introduced to the list.

The algorithm specifies the desired and the maximum time in which blocks should be produced. In the other case, the node is moved out of the global list and have to enter this list again. Blocks produced faster than in the desired time should be rejected. Producing a block is rewarded by fees from transactions included to the block (see Pricing policy for the details). Note, that the system can produce empty blocks, which will not be rewarded as there are no fees. This is required by the consensus algorithm, as it is using timings between blocks to check if nodes are operating correctly.

Each certificate stores a digital signature of a string (signed by the certificate holder, the string itself will be referred as “canary string”) defined by COVE standard and the Bitcoin address of the certificate holder. Having that, the data of the certificate can be used to form the string mentioned above and check the validity of the signature using the given Bitcoin address.

In the framework of the system following fields of certificates are used:

UID	Bitcoin address of the certificate holder.
L	Digital signature of the canary string signed with Bitcoin sign message.
OU	The identifier of a transaction used for certificate revocation management.
ST	The number of an output of the transaction mentioned above.

Canary string is formed from the following pattern:
https://COVE.io/certificate/$CERT_SN/$PUBKEY_HASH/$CERT_OU/$CERT_ST

where:
$CERT_SN – "certificate serial number;
$PUBKEY_HASH – SHA256 hash of the certificate public key;
$CERT_OU – the identifier of the used transaction;
$CERT_ST – the number of the used transaction output.

This string is signed with signmessage function of the standard Bitcoin implementation (Bitcoin Core) and included in the corresponding field of the certificate.

So the full process of creation of the COVE compatible certificate looks as follows:

1. Generate a key pair.
2. Create a Bitcoin transaction to be used for revocation management.
3. Create a certificate and fill its subject fields in according to COVE specification.
4. Create a canary string.
5. Sign the canary string with the signmessage function.
6. Include the canary string to the corresponding certificate field.
7. Sign the certificate.

To check the certificate:

1. Fetch the certificate.
2. Ensure that the associated transaction output is unspent (i.e. the certificate is valid).
3. Form the canary string from the certificate data.
4. Check the signature of the canary string included to the certificate using Bitcoin verify message function.

The proposed systems enable its users with the certificates management system based on the Bitcoin distributed storage. It is worth noting, that this system is highly portable because it is based on terms, which are essentially the same for most of existing blockchains.

ARCHITECTURE

Based on the system requirements, the following list of system components is formed:

1. COVE Core. The main task of this component is to safely and reliably store self-signed certificates and their revocation status. When used in the public service, it is also responsible for payment processing.

    a. In the framework of COVE blockchain there is a separate type of nodes, called master nodes, which are responsible for handling new blocks production. In private network the list of master nodes is maintained by system administrators. In a public service it is maintained automatically as described in “Consensus algorithm” section.

    b. Anyone can run a node which stores the whole blockchain for verification purposes.

    c. Most of the clients are supposed to work in light node mode. In this case user is not required to store the whole blockchain, just some chunks of data needed to verify user’s operations.

2. Client software (server-side integration) needed to verify provided COVE certificates.

3. Bitcoin anchoring system for improved auditability.

4. The system for token cross-blockchain migration.

ROADMAP

Q1 2019
COVE Core MVP V 0.2 - CRL infrastructure on Bitcoin blockchain, certificate generation in a browser.

Q2 2019
COVE Core public Alpha
Legal structure
Product's security audits and pen-tests
Extending team of software engineers
Public sale phase.

Q3 2019
Blockchain-based certificate data storage.
Integrations with different clients' systems.
Open source integration libraries for websites and web applications
Additional 2FA options, such as Signal, Status, WeChat, Trezor
Algorithm update

CONCLUSION

The goal of the COVE high-end secure system is to help people and organizations like infrastructure companies, IoT, medtech, financial and blockchain companies protect sensitive data. It is a distributed Public Key Infrastructure ("PKI") management technology built on top of the X.509 certificate standard that uses SSL/TLS to protect the entire channel from an attack.
COVE token is needed for all internal operations inside of ecosystem, so it is obviously utility token. COVE will use the blockchain technology as a vehicle of transportation and a source of consensus to offer a solution to this problem: decentralization.

TOKEN SALE

COVE Token (COVE) is designed to perform a function of a pre-order access key that enables access to the software program ones it is developed. COVE Token enables pre-order by functioning as a key enabling access.
COVE Token Utility
COVE uses blockchain technology to create a distributed certificate management system that has no single point of failure. And COVE token is the superpower boosting the whole ecosystem, operating like a license or digital key and granting its holders access to COVE PKI and DApps. Token holders will be able to use the COVE token in a variety of

ways: certificate generation, revocation, node creation, developing DApps, fees covering conversion of fiat payments, etc.

DETAILS OVERVIEW

Total token supply: 1 billion
Hard cap (including pre-sale stage): $20 M
Soft cap: $480,000 (reached during Pre-Sale)
Initial price: 1 COVE = $1
Type: ERC-20
Currencies accepted: ETH, BTC
Pre-sale dates: March 1 - March 31
Public sale start: April 1st, 2019 (20:00, UTC)
Whitelist: yes. Start date TBA
KYC: basic
Country restriction: everyone can participate

USE OF PROCEEDS

Development 35%
Business Development 25%
Operations 20%
Marketing 15%
Legal 5%

WHAT HAPPENS AFTER THE ICO?

The real work for any new cryptocurrency offering, and especially for COVE Tokens, begins after a successful ICO, and happens along many concurrent streams, such as

- Ongoing technology development and R&D, especially in respect to security through aggressive investments in AI and quantum computing / quantum cryptography, and in blockchain technology improvements
- Continual development and roll-out to the market of the product and service suite
- Marketing and Public Relations, and Investor relations
- Build-out and integration of the physical banking organization, including acquisitions of wealth management and corporate advisory firms, development of trade financing services and payments and processing services
- Building out our own cryptocurrency exchange platform
- Building robust treasury management systems
- Ensuring the right corporate and management infrastructures are in place
- Continually developing relationships with merchants and vendors globally
- Developing and maintaining relationships with cryptocurrency exchanges as well as building out our internal exchange platform
- Developing and managing our portfolio of energy assets, and optimizing production, while exploring for new energy reserves in sometimes remote parts of the world, and adding to our portfolio and reserves constantly, through new acquisitions and partnerships

To meet the day to day operational needs and expenses of the above, while we develop new revenue models and streams, requires significant ongoing capital and staffing. The ICO includes a provision for capital reserves to ensure that our developmental, management, marketing and operational needs are covered for at least a 2-year period following the ICO.

Our goal is to, in tandem with other cryptocurrency issuers, reinvent and redefine the global banking, investment banking, and venture capital industries, redefining and overturning the ways in which retail consumers bank and pay for goods and services, and move money around, while at the same time redefining the way private and public businesses, especially technology startups, raise new money in the capital markets. We intend to bring new thinking and radical new funding and monetary concepts to both corporate and sovereign entities, while at the same time allowing millions of “unbanked” people around the world to have access to physical and virtual banking, depository, lending, and payments services on an ultra-secure, tamper-proof platform remote from government meddling and interference.

To be sure, the opportunities wrought by the advent of cryptocurrencies are not merely disruptive to the several-hundred year’s old traditional banking and capital markets worlds and their status quo, they represent a complete revolution. One that is far greater

even than the advent of the computer, and the internet. And one that governments will struggle to control.

ADVISORY AND SUPPORT:

EBC and Emerald Tokens are assembling a world-class team of management, service providers, and advisors across the full spectrum of legal support, compliance, technology development and platforms, product development, audit, exchanges, marketing, and the ICO process, etc.

Legal, USA	Joshua J. Horowitz, Esq. Horowitz Tech Law P.C.
Audit	Deloitte or Ernst & Young (TBD)
Technology	Ethereum blockchain platform Viveca Media R&D
Marketing	Viveca Media
Compliance	Investor accreditation: www.verifyinvestor.com