eidoo

Technology White Paper

v.0.2 – Draft – 2017.09.21

Table of Content

Project Objectives

During the past months and years, the excitement towards cryptocurrencies and so-called "blockchain technologies" (from the "block chain" data structure introduced in Bitcoin as the first successful attempt to solve the double-spending problem in an open, decentralized network) has grown and has reached new heights. New business models and applications are being continuously proposed by both startups, consortia and enterprises. Many of the suggested use-cases for this set of technologies, beyond the simple and obvious applications of permissionless payments and store of value, are showing severe limitations, major drawbacks, naive expectations, unclear goals. One particular class of applications, though, is clearly establishing itself as a clear market trend: the use of blockchain technologies for the purpose of issuing, transmitting, storing and exchanging custom digital assets, or "tokens". The general case for digital assets is quite obvious, while the specific benefits of blockchain technologies for their management is a complex topic, involving deep and not trivial trade-off analysis about features like security, easiness of use, censorship resistance, efficiency, privacy, auditability, permissionless innovation and emergent standardization. The optimization of these trade-offs is an ambitious and difficult problem, involving disciplines as applied cryptography, game theory, distributed system engineering, open source development, user experience analysis, security-oriented electronics and more. So far, efforts to bring to the mainstream user products that could be used in a way that balances all the choices and maximizes the advantages and

minimizes the pains have been few, incomplete, underfinanced and unsatisfying.

The Eidoo Project is the first open, inclusive, global effort dedicated to the creation of an effective "blockchain-to-human interface", simplifying the interaction between users and blockchain-based assets, without sacrificing the main advantages that this technology can bring. Its output will be a set of products and services providing a new intuitive, easy, consistent and safe user experience, focused around a simple and secure way to store, buy, sell, transfer, and exchange blockchain-based digital assets, including all the major "cryptocurrencies" and "tokens", as well as buy or sell any goods paying in cryptocurrencies but without relying on any central authority.

The Eidoo Wallet will be the heart of the entire project. It will be natively multi-asset and designed for the mobile world: a single integrated environment that will be used to manage all tokens intuitively, without the need for complex configurations, but still leveraging the best security standards and best practices. Innovative services to exchange cryptocurrencies and tokens will be directly embedded in the platform. This integrated exchange system will never require the transfer of the assets to any centralized custodian third party that could cause financial losses due to bugs, hacks or exit scams: the user will always be in full control of his funds. In the long run, the Eidoo roadmap also includes a fully decentralized blockchain-based marketplace. Around these decentralized tools, additional services will be created in order to facilitate the use of cryptocurrencies, such as the ability to recharge a debit card directly from the Eidoo app without leaving the application.

For those who need it, Eidoo will also offer Digital Identity solutions, using designs such as the Web of Trust for pseudonymous sovereign identities as well as integrating digital identity cards.

Eidoo will be a value-added integrator that brings together proven technologies and established services that already exist, along with others that at this moment can only be imagined. The purpose of Eidoo is not just to do things that others do not, but to re-think things already accomplished through safer and simpler methods, keeping the focus on the user's experience and offering him the freedom to choose, while rendering the complexity of the “crypto world” easier to manage. We want to build a bridge towards worlds that at today are still far apart. Our attention is focused on offering to users a complete product, allowing them to manage complexity intuitively and safely.

The ambitious challenge of this project is also to give a common home and common goals to tech communities defending very different visions, leading to a healthy competition of approaches, methodologies, design philosophies. Trade-offs in blockchains space are difficult and complex: a simple “compromise” is often just a way to get the worst of the two worlds, while the best choice is sometimes to diversify the paths, to get to the same final objectives, under the same global user experience. This is also a risk management strategy: investing in a project that is not relying on a single paradigm, allows us to mitigate the exposure to technological risks, very high in an innovative industry full of financial and security implications. In a dynamic world, no good solutions stay that way if it doesn’t evolve: as a methodological approach, Eidoo will continue to improve technological efficiency, security and user experience.

User Experience

Our mission is to create a single interface to safely interact with different technology stacks and different design philosophies, always providing a unique, consistent and simple user experience. Eidoo's team include vertical experts in this field, working in conjunction with the technology designers to accomplish this mission.

Today's solutions are often divided between two opposite extremes: on one hand, solid and secure tools that are conceived and designed "for geeks only", without much effort to provide any easiness of use; on the other hand, simple, "shiny" and good-looking products that can mislead the user, encourage or even force unsafe practices and put his financial asset at risk. It's quite common for blockchain-related project to make use of terms and concepts without worrying about their full understanding. While some of the trade-offs are inherently impossible to escape, we believe that technological state-of-the-art and security best practices should benefit all the users, not only "experts", because the often-irresponsible uses of the technology could negatively affect everybody else, and user's awareness is needed to create a trusted relationship with the tools he deals with. We believe that it's sometime necessary to *accept* the intrinsic complexity of designing the tools of the future: simplifying that which is complex is often merely an illusion. We strive for our work to help mainstream adoption of these technologies,

still promoting a responsible, sustainable and careful use of them. Managing the security of digital assets in the context of decentralized systems has different implications in respect to the traditional world of finance: it requires more attention, practice, and awareness from users. The power to "be our own bank" comes with great responsibilities. Security, transparency, and comprehensibility are the starting points for which we want to design our user-centric solutions.

A single security passphrase, independent from the specific type of blockchain platforms, standards and technological stacks used under the hood, is important to make security practice easy to follow and maintain, even for not strictly technical users. This is the core of the security model of blockchain technologies. At the same time, the existent of a unique, easy to protect access point to the platform shouldn't degrade security features as modular privacy features, good entropy creation, easy portability, safe backup routines, etc. That is why we decided to use the "Hierarchical Deterministic Wallet" approach to make our application safe, allowing users to have much more control over their assets as well as easy processes to adopt. With it, users can secure all their multi-asset accounts and addresses, as well as their signing keys, with a single secret phrase, conveniently encoded in twelve common words. Recognizing and respecting private property of people also means, according to us, to empower them with the ability to organize it in the way they believe is best. That's why we provide a special tool that, without the need for central servers, allows our users to retrieve and recovery digital assets wherever necessary. The Eidoo Recovery Tool is designed to provide users with full availability of their tokens in a simple way, if needed in emergency scenarios as well.

People tend to evaluate the quality of a service based on their past experience, and this also applies to the exchange of digital assets. The transaction history of a Wallet for digital assets should be always easy to read and navigate, consistent, detailed, intuitively organized. We designed a solution that optionally allows to outsource from the local app to the servers much of the complexity needed to process and organize the information stored on blockchain systems, without sacrificing privacy and security. New kind of custom tokens will be automatically detected by the wallet and made available for use, with a simple and secure Naming System, design to avoid phishing attempts and frauds. Optimal management of identities, reputation and addresses is another crucial part of a well-designed user experience: the Eidoo wallet will focus on this, conjugating security best practices with easiness of use.

"Smart" Assets

The Eidoo Wallet, and all products and services orbiting around it, will have as central focus the safe and easy management of digital, blockchain-based "Smart" Assets.

There is a continuous and growing interest for digital assets somehow representing a proxy for shares, bonds, IOUs, rights, etc. Traditional ways to issue and transfer assets are still slow, expensive, inefficient and present a lot of friction, both from a technological and a regulatory point of view. In recent years, some efforts have been done in order to try to leverage blockchain technologies to improve the situation. While sometimes the actual reason for this could be probably linked to marketing (due to the "blockchain" and "cryptocurrency" hype), we think

there are compelling reasons to use blockchain technologies, in conjunction with or instead of centralized fiduciary systems, for digital assets issuing, storing and transferring. The Eidoo Wallet will be developed maintaining the focus on this reason, maximizing the benefits of the new blockchain-related tools and practices, while minimizing pain points, redundancies, useless over-engineering and technological dead ends.

One of these reasons is sometimes called the "social scalability" of an open digital asset protocol: while a centralized and proprietary solution would be difficult to push, open source de-facto standards can be leveraged to lower friction to adoption and boost interoperability. When blockchain technologies reach a critical mass of adoption, in some market niche, for their inner value proposition, then also digital assets could be issued on the same platform leveraging existing strengths: wallets, marketplaces, exchanges, liquidity providers, libraries, block explorers, APIs, regulatory frameworks, secure hardware, user habits, etc. The fewer the customizations necessary, the more frictionless the process.

Another compelling reason is "modular confidentiality": while a centralized and trust-based solution would expose the users to privacy concerns, and the issuer to extreme regulatory burden (KYC, AML, privacy laws, asset-specific regulations and authorizations, etc.), some of these pains could be facilitated in the framework of a technical impossibility.

Any hybrid exchange solution, within which a part of the data is maintained inside the Eidoo cloud, will therefore be subject to the usual

KYC-AML practices while a decentralized solution will maintain this data, when existing, only on the device of the user.

This feature would not just be an advantage for users in terms of privacy, an important and growing concern for digital platforms, but also a responsibility relief for the issuer itself, from a regulatory point of view.

A third reason to use blockchain-based "Smart" Assets is "modular auditability": while a centralized and trust-based solution would allow the issuer to modify the ledger in every possible way, for example inflating the supply, changing the distribution, blacklisting amounts and users, changing the transaction history, blockchain technology could be used (given certain condition) to provide solid proofs of correct behavior. The amount of issued assets, the reserve, the immutability of the history of the ledger, could be proved cryptographically and independently audited leveraging blockchain technologies in a correct way.

The last relevant reason is the possibility for "strong automatization": trust-less or trust-minimizing, automatic and unstoppable contracts, with low or zero counterparty risk, are a potential natural extension to blockchain-based asset. Automatic, all-digital proxies of widespread financial instruments and tools like "dividends", "royalties", voting rights, are interesting already for current centralized and hybrid use cases, but could be paramount for more advanced scenarios: oracle-based "smart-contracts", "smart-property", "DAOs", etc. The absence of counterparty risk would be useful for social scalability of many financial, commercial and logistical use cases.

Exchange

The advent of cryptocurrencies has seen a great push towards the decentralization of services, allowing for greater transparency and security towards the user-base, as it avoids a single point of failure and everyone can have a full accounting log of what is happening. Centralized, trust-based exchanges are easy to use and offer advanced trading functionalities, but they represent a security and censorship risk. While some exchanges are better guarded than others, hacks are not an uncommon event in the cryptocurrency scene. Major failures (from MtGox to the more recent hacks) showed the extreme fragility of this particular point of the ecosystem, otherwise extremely robust or even anti-fragile.

A possible solution could be a decentralized, trustless exchange, that does not rely on a central, trusted third party to hold the customer's funds. In this scenario, trades occur directly between users through automated processes. Some benefit of a decentralized exchange over a centralized would be: "trustlessness" (no requirement to trust the security or honesty of the exchange), public auditability, uptime guarantees, privacy.

There are, anyway, serious downsides to this idea. In present experiments, users are sometimes requested to be constantly online or to perform complex actions, trades are extremely slow and expensive, liquidity is very low, advanced features are missing. Even though this is a great benefit, purely decentralized environments for now have been marred by the fact that they cannot perform at the levels of efficiency

that their centralized counterparts can. For a service such as an exchange, speed is paramount, hence why top traders compete for the shortest fiber-to-exchanges lines.

Identity

There are a series of uses for which it is necessary to associate addresses to precise digital identities, such as:

- Addresses associated to identities recognized by the government, for example to pay taxes or receive tokens with specific uses within public administration, or for uses that require KYC-AML like non-decentralized Cryptocurrencies Exchange.
- Addresses that might need to have a certain level of certified reputation, for example such as those of a shop, identity that can be guaranteed through a mechanism of web of trust.

Eidoo will maintain the associated addresses clearly visible to digital identities and therefore to a somewhat reduced privacy level. The user will always remain in charge on whether to use reduced privacy addresses.

One Goal, Two Teams

Eidoo is an ambitious project that will cover two different approaches and implementations. The same vision of an easy, secure wallet for blockchain-based smart assets, will be embodied:

- in a fast, easy to use, disruptive, flexible, feature rich, turn-key Ethereum implementation, based on ERC20 standard and EVM contracts, with an embedded token system to fund the development
- in a secure, scalable, long-term oriented, privacy-compliant Bitcoin implementation, based on the new asset protocol RGB and off-chain trusted computing, with a traditional non-profit open source funding approach

Ethereum Team

Ethereum: Approach and Methodology

The Ethereum blockchain has attracted much attention to itself in the last year and many companies have decided to utilize it for their projects, exploiting the extreme flexibility offered by the "smart contract" of Ethereum.

This has caused a proliferation of Ethereum tokens but, at the same time and in respect to promises, the user applications have not been in step in terms of usability and security level.

The reason for this is that Ethereum is a highly experimental technology still incomplete and in rapid evolution. Furthermore, the "account based"

approach, enabled for the type of smart contract offered by Ethereum, is very weak under other aspects, firstly and especially in regards to privacy.

The objective of Eidoo is that of offering the best possible user experience with currently implemented technologies, striving to fill the major technical gaps, while following and adapting to the platform's evolution.

Ethereum: Wallet Architecture

Light client

In Ethereum, the term “Light Client” means a technology that is the SPV correspondent of the Bitcoin environment.

Briefly summarized, it consists in the ability of the "client" to verify all the hash chains necessary to validate the information received by other nodes and concerning only its own Ethereum address, without the need to download and validate the entire blockchain.

Unfortunately, solid implementations of Light Client Ethereum do not exist, they are all experimental, and still too heavy to function on a mobile device.

The goal of Eidoo is in having an Ethereum light client on mobile device but in the meantime, it will utilize a compromise built as follows:

- Servers that index the data of the blockchain
- The client on the user device obtains the information concerning it from the indexing servers
- Optionally, an Ethereum full node of trust of the user, to which it's client will turn to check the data received from the indexing servers

The full node alone is not sufficient since, through this, only the address balances could be known. An Ethereum full node doesn't have the need to index all the transactions that concern an address (or even to know its balance); it does not index the data of the token, which from his perspective are simple codes to execute (smart contract) that modify a group of generic data constituting the memorized state in the blockchain.

The indexing servers have the task to accomplish a high-level analysis of all the transactions of the blockchain, to index the movements by address, to find which represent movements of token and also to index the movements of token.

This is an activity which is too heavy to be done directly on mobile devices.

Mnemonic seed

Ethereum uses the same digital signature algorithm used by Bitcoin and many other blockchains. Bitcoin has long defined standards for key generation and storage: BIP32 andBIP39.
These standards define how to derive many keys from a single seed,

according to a hierarchy, and how to generate and use a mnemonic word phrase to get seed for key generations.
Eidoo will use the same mnemonic phrase to generate keys for all the managed wallets. Whether they are Ethereum, Bitcoin or other Blockchains, the difference will only be in the derivation path. This means that the user will have to worry about saving only a mnemonic phrase.

Multiwallet

Ethereum is an "account-based" blockchain, which means that an Ethereum account has a constant address and all the associated assets (eth, token, but also all the smart contracts with which it interacts) are publicly correlated to that one address, and there is total lack of privacy. Unfortunately, at the present state of affairs, the only way the user can try to achieve a minimum level of privacy is to manually divide the assets on multiple wallets while being careful not to mix them up.
That is why it is crucial for the user that Eidoo enables him with the ability to manage multiple separate wallets, and this is done by generating the appropriate keys from the same seed, keeping only one mnemonic phrase for all wallets, while using different BIP32 derivation paths.

Transactions history

The Ethereum blockchain stores the status of each account directly. Hence, to know the balance of a certain address it is not necessary to know which transactions it concerns. For this reason, most of the wallet clients in circulation do not provide information on the history of transactions (especially for ETH receivables from other accounts).

From a user perspective, the chronology of Ethereum or token transfers is fundamental information nearly as much as the balance.

To complicate things, the fact that when we are in the middle of Smart Ethereum contracts (and all the tokens are smart contracts), there is no longer a one-to-one correspondence between the concept of moving an asset and an Ethereum transaction on the blockchain.

The Eidoo client uses the "index" servers primarily to identify transactions involving their address, all transaction data analysis logic (for example, discovering token shifts) is also replicated on the client so that it can eventually validate the information using a full trusted Ethereum node.

Ethereum: “Smart” Assets

The Ethereum protocol introduced in the blockchain world the ability to write and then globally verify the states of a general-purpose virtual machine residing on each single node of the network. This design allows for generality and flexibility in blockchain uses that go far beyond the simple transfer of value. In addition to the ability to execute and certify the status of smart contracts, Ethereum blockchains can be used natively to create and manage custom assets. These assets are actually smart contracts that are in line with a well-known standard known as ERC-20.

Eidoo Ethereum Wallet fully supports ERC-20 token technology.

At present, it is not possible to enforce unique names and symbols for ERC-20 tokens: users can then create new tokens that have the same name or symbol as other pre-existing ones. This fact is a problem for a simple and secure use of the wallet: each token has a different Ethereum address but, being it a complex alphanumeric code, difficult for human to read, write, memorize and compare, each token is usually recognized with a Name, an abbreviation, and an icon symbol. Eidoo Ethereum Wallet implements a special index that will group tokens issued by companies with legal and/or informal personalities, or legitimate tokens. Tokens having same names/abbreviations/symbols as those in this special index are labeled by Eidoo as untrusted, in order to avoid scams, phishing attempts and/or misunderstandings.

Tokens auto discovery

In the status of an account stored on the Ethereum blockchain, you can only find the Ethereum balance but not the token one. In fact, the tokens - from Ethereum's point of view - are smart contracts like every other one, and their balance remain within the state of the token smart contract. Hence it is necessary for the user to know the balance for a specific token directly querying the smart contract since there is no way to know in advance which tokens are owned by a certain account.

Fortunately, Ethereum transactions that move Ethereum tokens are recognizable by a data structure stored in blockchains, called transaction receipts.

Indexing servers catalog all transactions related to a specific address, including token shifts. The Eidoo client from this list of transactions also deducts what the token is, querying their smart contracts to know the balance.

Token sale engine

The mechanism of participation in all the Ethereum Token Sale's is based on the publication on a website of the subscription data (essentially, the address where you can send the ETH to). Unfortunately, a website is not the right tool for publishing such critical data as it does not incorporate any mechanism for validating published data.

The result is that the Token Sale's subscription data publishing system is the first point of attack, and has been exploited on several recent occasions.

Digital signature tools such as PGP could be used, but these are less familiar tools for users who would end up ignoring them.

Eidoo will provide Token Sale's organizers with a secure distribution service, using digital signatures, for subscription data. Integrating this service into the wallet will allow signatures to be fully transparent to the user and subscription through a simplified user interface, as all parameters can be automated.

Ethereum: Exchange

The Eidoo Ethereum Wallet aims to integrate a secure, transparent and partially decentralized asset exchange built via Ethereum smart contracts, which settle and finalize trades. Security will be provided by the fact that each user will have the funds they are trading with within their own smart contract wallet. The traditional sluggishness and costliness of a decentralized exchange will be counteracted via an off-chain order book and server. This will provide the end-user with a familiar experience of a traditional exchange, where they are able to create as many orders as their trading balance allows for, and they are not charged anything until the order is matched and executed on Ethereum. The architecture is not limited to just providing the ability for off-chain order creation, but it also clears orders on behalf of users, and directly broadcasts them to Ethereum to be settled. This provides multiple layers of security, as all the different parts such as the front-end and order-book server are doing accounting checks on whether orders are valid and can be executed, and if those checks pass, they are pushed to the Ethereum network, to be settled, whereby a final set of immutable checks occur, and if they pass, the trades are settled. This hybrid system provides much faster speeds than even other decentralized exchanges that have a central order book, but require users to clear the trades themselves, creating additional issues where multiple users may even vie for the same order, and will have to wait for a miner to decide which takes precedence. A system of smart contracts running on Ethereum can be designed to use the key pair residing on the chip as the ownership key for a cryptocurrency balance (both tokens and Ether). The ownership

key is then tied to the digital identity, which it is certified by the government. This would enable some interesting optional features, such as recovery from key loss (smart card loss or theft), or more secure validation of transactions receiving address (e.g. sending tokens or Ether directly to an identity validated by the government).

This is solved by the Eidoo central order-book server, as it automatically clears and delists any orders that are pending to be settled on-chain, and will appear to the end-user to be much quicker, expecting to work near the efficiency of centralized exchanges.

Thanks to a cryptographic authenticity proof of the process being executed on the centralized code, Eidoo will provide strong guarantees around the correct execution of such code: no malicious alteration of the expected order matching algorithm will be possible.

Additionally, this architecture provides at least three layers of accountancy and security, while leaving the final and most critical layer up to an immutable smart contract.

Ethereum: Identity

In high-income countries in the last decade, governments have trialled and deployed public key infrastructures (PKI) to provide digital identity to citizens and enable easier, more efficient access to governmental services. These PKIs usually work by providing each citizen with a personal smart card with a chip. The chip contains a key pair: the private part of the key pair can be used to digitally sign documents or to authenticate to different governmental services. Governments retains

the public parts of the key pair, and they organize and administrate the certificate authority of the PKI. These smart cards retain the same security guarantees that hardware wallets provide: namely, that the private part of the key pair cannot be easily extracted from the chip.

Ethereum: Market

Cryptocurrencies have the ability to also eliminate intermediaries in the commerce of goods, allowing users and merchants to save on transactions fees. In order to boost this commerce, we are also going to develop a Decentralized Market.

Here users will be able to freely open their store and sell the result of their work. The content of their store will be hosted by their own server but with the support of the IPFS protocol. (https://ipfs.io/)

At the beginning, as it is for the exchange service, the search feature on the stores will be furnished by a centralized service from Eidoo.

As soon we will be sure of its solidity, we will add a more decentralized way to perform a search. A Kademlia-network is probably the way that we will use to achieve this.

All the keys to move the tokens will still be in full control of the users. Trades will be done by using both smart-contract or human escrows, every time chosen in agreement by both the buyer and the seller.

Every trade will produce a feedback signed by both the user and the store. All feedbacks will be saved both locally and online again with the help of the IPFS protocol.

The proposals to have identities on Eidoo will have a very important role on this part of the project, and they will be studied to find the better suited for this use case. Currently there are also many teams that are working to develop the Lightning Network technology on both Ethereum (Raiden Network and Plasma) and Bitcoin.

We are closely following their development, to be ready to integrate them as soon as they are stable for the use of the common users.

Bitcoin Team

Bitcoin: Approach and Methodology

The Eidoo Bitcoin wallet will maximize the key aspects that we think benefit the most from blockchain-based solutions for digital assets: social scalability, auditability, automatization and, in particular, confidentiality. All of this with a conservative and security-oriented approach based upon adversarial thinking, and with a particular focus on off-chain technical scalability, as typical of the Bitcoin philosophy.

We believe that pushing a new solution specifically for a particular use case, such as generic asset distribution, is very difficult. Instead, we believe in leveraging an already widespread and well adopted solution exploiting not only the infrastructure itself, but also its ecosystem,

reducing the customizations needed, minimizing the risks to break backward compatibility, and increasing the adoption rate. This will make the project less reluctant to be adopted and easier to picked up.

Moreover, leveraging an already existing ecosystem which has been proven to be immutable, censorship resistant and secure, gives to the issuer a solid, fair and provable environment. Due to the provably honest and deterministic nature of this environment, an issuer has the possibility to cryptographically prove the fairness of any transaction without a centralized and trust-based party.

We also take strongly into consideration counterparty risks because even if trust-less, unstoppable and full automatic contracts are getting developed, they are still far from actual commercial use. Solutions as automatic atomic swaps and proxies to “dividends” or “buybacks” are already used for some centralized use cases and could be the building blocks of futures scenarios as decentralized exchanges, oracle-based smart contracts, smart property, etc. Of course, these scenarios assume the direct use of independent blockchain assets as collateral.

Also, it is of primary importance the scalability concept, which has played a key role during the last month. Being able to handle a large amount of transactions is one of the fundamental requirements of the project since this limitation could restrain the opportunity of the project.

Lighting Network offers a top-quality solution not only to overcome this problem but also to improve other already discussed primary aspects of the project such as confidentiality.

But the most important aspect of all of the project has been the confidentiality and privacy of the users. Trust-based solutions and Ethereum ERC20 offer several drawbacks for the issuer which could have some technical impossibilities in keeping track, managing or regulating transactions. For sure this would be of particular interest to informal issuers and, could be, for regulated legal entities for whom it could be riskier in terms of regulations and reputation.

Bitcoin: Wallet Architecture

The Eidoo Bitcoin Wallet will be able to manage generic assets on Bitcoin's blockchain, in a secure and user-friendly way. We have chosen to build the wallet according to the best practices currently available in Bitcoin's ecosystem in order to exploit not only a higher level of security, but also a greater level of interoperability and compatibility with the existing solutions and services.

A key feature of the wallet is the generation of deterministic key pairs from 12/24 words, called *seed* as per BIP39 standard. This design choice is made for security purposes. Other alternatives such as generating the wallet using a passphrase (brainwallet) are not taken into consideration due to their low level of entropy, which makes them an easier target to fund theft. On top of that, in order to improve security, during the creation of the wallet the user can introduce a passphrase which will be used to encrypt the private key generated by the above process, as described in BIP38.

Another main feature of the wallet is the generation of private keys and addresses according to BIP32, thus exploiting a hierarchical deterministic tree. This allows to do without a pool of key pairs, which is inconvenient, prone to errors, and possibly faulty. This process is also improved by two augmentations described in BIP43 and BIP44 aimed at standardizing the creation of the tree. This component is fundamental to ensure the compatibility with the finest wallets in the Bitcoin ecosystem.

Best practices are used by default. In fact, since confidentiality is of primary concern, every time a new address is needed, for example in case of change, the wallet will generate, with respect to BIP32, BIP43 and BIP44 as discussed above, a new address avoiding the reuse of an old one.

Of main concern, in addition to confidentiality, is also the ability to be able to leverage as much as possible on Bitcoin infrastructure and its ecosystem. For this reason, the wallet will be realized taking advantage of LibWally, a cross-platform and cross-language library containing a collection of well tested primitive functions focused for the development of a wallet. This will increase the robustness, security and speed development of the project.

Bitcoin: “Smart” Assets

The other main product, together with the RGB wallet, is the RGB protocol which aims to develop a different way to exchange generic

assets making confidentiality and compatibility with the existing Bitcoin ecosystem a priority.

In order to archive the confidentiality levels needed we have developed a different way of tagging the colored asset which is unique to any other already existing colored coin protocol, and indistinguishable for any party running forensic analytics on Bitcoin blockchain or on its network.

In fact, our solution focuses on the asset history confidentiality. It differs from existing colored coin protocols in that instead of using order, padding order or any other version based on the index position of the outputs, we exploit merely the presence of an output address to identify a colored transaction and verify its integrity. The key to achieve the desired level of privacy is that the colored transaction can't be decoded by anyone else except by the two parties involved in the transaction.

Confidentiality is not the only benefit we aimed to achieve: both compatibility with SPV nodes, which is something most of the current protocols failed to archive, and fees customizable by different asset – which is achieved with a strong level of privacy until one of the token holders decides to redeem the asset – are important features. Both of them are considered as optional meaning that firstly any changes to the protocol doesn't particularly affect the protocol itself and second they give the issuer full control over the issuing of his own asset.

Scalability is another key factor in the RGB protocol. For this reason, we will look into the implementation of a new concept developed by Peter Todd called Proof Chains. In fact, just looking at the asset history for the issuance transaction is not enough, since there are double spending

related problems. In order to address and solve this issue, actual solution trade their confidentiality and scalability. Using this new concept, we can improve the current situation by exploiting the publisher, which will create, using a single use seal commitment and without the possibility to cheat, the proof that a party with that seal, is not double spending.

The RGB protocol will also have its own scripting language giving the possibility to the asset issuers to create functions to describe the behavior against which the token transfers will have to adhere, but will not be Turing complete, to avoid unpredictability of the smart contracts and undefined code behaviors.

Directly in conjunction with the scripting language, there is also a validation system which checks if the asset history is valid against the rules described in the contract script. Finally, the issuer will attach a human readable contract to each and every RGB colored coin. Such note will make it explicit what the asset bearer will be entitled with when redeeming the asset with its final transaction directed to the issuer. This contract will be digitally signed by the issuer, timestamped and committed to the issuing transaction and it will be passed along by every user to the next and it will be stored – together with the necessary proofs, the digital signature and the timestamp proof – directly on the Eidoo wallet, thus making it even easier for an Eidoo user to claim his/her rights and grant that the issuer will behave in a provably honest way.

The RGB scripting language will be versioned and its primary version will grant the validation rules to pass along the digital assets between the users on the secondary market. The following versions will not only grant

that the digital asset has always been transferred correctly by all users in each and every transaction, but also that the transaction respected a set of more complex conditions granting the ultimate redeemability of the asset. Examples of such rules could be a fee proportional to the amount of asset being transferred, or the block height, to be attached in each transaction and destined to the asset issuer in order for the asset to be finally redeemable. This conservative approach will grant safety and usability of the protocol for transferring the assets from day one, while additional features needing additional testing and validation will be easily introduced without breaking backward compatibility.

Finally, in order to improve the scripting expressivity, the RGB protocol will make use of the Hardware Secure Module. The HSM are hardware tamper-proof trusted computing devices able to run generic scripts such as the ones used to describe the behavior of an asset. The HSM servers will allow to enforce arbitrarily more complex smart contracts directly on Bitcoin blockchain, but also, they will serve as hardware oracles, retrieving the data that triggers a smart contract from off-chain outlets. In fact, natively the RGB protocol – just like any other transfer protocol on a blockchain – can make use of data endogenous to its blockchain, therefore very elementary data such as time, fees or amounts. When an issuer wants to program a digital asset to be transferred only when some event happens in the real world, then an oracle is needed in order to trigger the smart contract. This is exactly what an HSM, a hardware oracle which provide a trusted computing environment, can serve for, thus enabling unimaginable use cases both for issuers and users.

Using such technology, an issuer or the traders exchanging the asset are forced to obey to the contracts terms and the various conditions for the asset transferability, leaving the only option to issuers or to users to partially cheat by breaking the HSM, which will not make them able to steal anything in any case. Eidoo will therefore provide several HSM machines which will be securely stored and will provide smart contract and oracle services to the entire network.

Bitcoin: Exchange

Lightning Network will be heavily exploited for the development of a Decentralized Exchange, which will enable Eidoo users to transfer, in a safer, cheaper and more confidential environment, a generic asset or cryptocurrency.

One of the biggest and underrated problem of existing exchanges is the fact that users need to trust the counterparty, giving them full control of your own goods. Counterparty risks, even when dealing with generally reliable and trusted ones, have always to be taken in consideration since casualties are always behind the door. Leveraging Lightning Network, we are able to get rid of any counterparty risk, as transactions are happening between users which are not able to cheat in any way.

Another big improvement is the fact that users will enjoy a better privacy due to exploiting off-chain transaction, in a peer-to-peer decentralized environment.

To be absolutely mentioned the fact that Lightning will bring a huge improvement in regards to fee costs and waiting time, two of the biggest

weakness of Bitcoin during 2017, thanks to a technology called off-chain transactions. Taking advantage of the aforementioned mechanism, we are able to create a market almost free of transactions fee with a confirmation time reduced of more than 10 times.

Moreover, Lightning Network indirectly brings others important features, improving both security, and privacy. In fact, Lightning transactions are atomic by default, meaning that either the exchange of funds goes well or you get your money back. There is no way for a counterparty to either steal your money or even block them for an undefined amount of time.

The wallet will take care of opening and managing a lightning channel with a specific asset, giving the user full control over the configuration. At the same time, it will leverage the excellent route-finding algorithm which will be in charge of seeking the best price to exchange the user assets for the wanted one according to time, rate/cost and fee trade-offs.

Bitcoin: Identity

During the last years, a lot of effort has been put towards the topic of Digital Identity, the set of information from which a system is able to describe an external agent.

Currently existing production-ready solutions either:

-include centralized authorities, which have several drawbacks such as single point of failure, censorship prone and privacy deficient or,

-provide user-unfriendly experience – that lead the user in making poor decisions and compromise his security, such as happened in 1991 with PGP, an encryption program that provides cryptographic privacy and authentication for data communication.

For this reason, we will provide a solution based on the awesome work of Christopher Allen, whose researches goes under the name of "Rebooting Web of Trust" and is based on the concept of self-sovereign identity.

Self-sovereign identity is an evolution of the previous solutions, which does not rely on any centralized institutions and it is based on three main concepts: user control, security and portability, also key concepts of the Eidoo project.

The above concept can be further expanded with projects like Smart Signature and Decentralize Public Key Infrastructures. The first is a new system aimed to improve the limited traditional cryptographic signature system with the ability to define and program conditions for verification. Instead, the latter describe an approach to fix several usability and security challenge of the old Public Key Infrastructure, exploiting a decentralized environment.

Eidoo will follow the researches of Rebooting Web of Trust, in order to integrate into the wallet a working solution for the user to create his own, personal Digital Identity.

Bitcoin: Market

Another feature, which can be created by leveraging Lightning Network, is the Decentralized Market, where Eidoo users could, instead of transferring only asset, exchange also generic goods and services in a decentralized and provably honest way using either an HSM or an escrow system.

The wallet will take care of abstracting the raw unfriendly function of Lightning Network, giving to the end user a more pleasant environment to manage their assets.

Most of the rules that applies to the Decentralized Exchange, applies also to the Decentralized Market due to the fact that Lightning Network is the common element shared by both systems: the possibility to avoid any presence of counterparty, which increase the privacy while suppressing a malicious third-party, and take advantage of the latest technologies, such as atomic swap transactions or even cross-chain atomic swap transactions, which will make the market more active and competitive and low fee instant time transaction, which is a huge improvement if we watch at how had Bitcoin behaved, with respect of those two properties, during 2017..

The difference between the Decentralized Market and the Decentralized exchange is the presence of an escrow, whose task is to decide which of the two parties involved in the transaction should receive the money. Escrows, which base their roles on reputation, should have incentives to act as third neutral parties without any possibility to divert funds or act dishonestly towards one of the participants.

Different research has been made, some of them are already in production, for example Bits, other are still a concept, like Discrete Log Contracts; the first has some centralized elements which decides which party is right, while instead the second is a blind trustless type of escrow system whose output can't be influenced. Due to the fact that we are leveraging Lightning Network, the realization of a blind, fully trustless escrow on top of it has not been archived yet.

We will study the argument to understand the different tradeoff between oracles, looking at both production ready example, such as Bisq or OpenBazaar, and best research available in the field at the moment.

DISCLAIMER:

This Eidoo Technical White Paper is for information purposes only. Eidoo Sagl does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided "as is". Eidoo Sagl does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to:

(i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement;

(ii) that the contents of this white paper are free from error; and

(iii) that such contents will not infringe third-party rights.

Eidoo Sagl and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. In no event will Eidoo Sagl or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.