TIMO PROTOCOLS

White Paper
Version V1.0

Being committed to building super anonymous protocol supporting inter-blockchain

Directory

1. Preface

1.1 Overview

According to the project report "Anonymity and Privacy in Electronic Service (APES)" of a Belgian research institution, at present, anonymity is still in a stage of application analysis, and anonymous application is divided into anonymous communication, anonymous publication, anonymous browsing, anonymous payment, anonymous voting, anonymous auctioning and law, etc.

Currently, systems including Monero, Zcash, Dash and PIVX are the typical application of anonymous payment. In order to solve defects of privacy protection of Bitcoin, for them, various solutions of privacy protection are put forward under scenario of consumption and payment by using enciphering algorithms of ring signature, Darksend algorithm, zkSNARK protocol and Zerocoin protocol, etc. and their combination.

The research shows that the anonymous systems of Monero, Zcash, Dash and PIVX, etc. has bigger limitations in privacy protection because they cannot solve anonymous problem completely from the perspective of cyber space and digital space. Therefore, a brand-new technological path is raised in Timo Protocol.

Timo is a kind of end-to-end high-anonymity basic protocol that is based on network layer and application layer, supports Shuttle inter-blockchain protocol and is managed by privacy domain. Also, as an anonymous privacy protocol supporting inter-blockchain and facing application service, it focuses on providing top-secret support for release of anonymous assets, privacy transmission and interoperation. Relying on Timo Protocol, we can establish military-level privacy network facing Domain, provide measurable anonymous privacy services such as browsing, payment, voting, publication, auction and law, etc. The privacy network called Domain, composed of privacy hardware router and soft node, jointly forms a pluggable concealed pipe so as to provide real privacy protection for cyber space and digital space.

Based on Timo Protocol, we aim to establish numerous privacy networks (Domain) where the customizable anonymous assets can be issued, point-to-point anonymous communication can be realized, and various safe privacy applications can be used. In future three years, Timo Protocol will spare no effort to build Super Privacy Domain aiming at Dark Web and further forge the world's largest full-anonymity network. Then everyone can create their private Domain circle through Timo Protocol, such as Cypherpunk Circle, Marihuana Fan Circle, etc. Finally, all domains are woven into privacy internet through Shuttle Protocol.

Timo is also a hero role of the game "League of Legends". With a good and brave character, it has no fear of difficulties, obstacles and frustrations, and does the best to explore the whole world with matchless passion and cheerful spirit. In the process of innovating old defects by blockchain technology, we hope that Timo Protocol can create a brand-new anonymous privacy world for us and make us shuttle in internet world lightheartedly.

1.2 Important note

At present, the algorithms used for Timo Protocol such as zero-knowledge authentication, ring signature and coin-shuffle technology as well as asymmetric algorithm, symmetric algorithm and hash, etc. are safe. However, from the perspective of cryptography, any algorithm is probably cracked. Currently blockchain technology, however, is still in a process of rapid iteration and development. Accordingly, there also exist certain new technological risks and landing risks. In view of this, we specially warn that this white paper is only used for technological research. Please don't deem it as the investment project for reference. See 10. Risk warning.

1.3 Acknowledgements

If there aren't previous works of Monero, Zcash, Dash, PIVX and

other teams, Timo Protocol will not be realized. Timo team and community thank the cryptograph pioneer and open-source code contributor for their selfless contribution and for their paving the way for our road of innovation.

2. Privacy and anonymity

2.1 Privacy requirements

For human digitalization process, privacy and anonymity are an topic that cannot be evaded forever. From "The right to privacy" written by American lawyers, Louis D. Brandeis and Samuel Warren, to American "Computer Privacy Protection Act" and to the strictest GDPR privacy regulations of EU in history officially implemented last year, with the evolutionary development of human society, especially wide application of computer big-data and internet, people's understanding on the right to privacy is broadened step by step.

The public has a strong appeal for privacy protection, which forces the government to have to take it seriously. In America, the right to privacy has become a controversial hot problem for many years. For privacy in America, there is no constitutional guarantee, but a large number of American federal laws are used to protect the privacy problem. "*Electronic Communications Privacy Act (1986)*" makes invasion of personal

electronic privacy a criminal act in order to prevent abuse of monitoring on e-mail and verbal communication.

However, the laws and regulations for privacy protection cannot effectively prevent data abuse. On the contrary, we are facing a worse situation. For example, data of 50000000 users of Facebook were leaked, or information of about 0.1 billion users on Quora, a famous American online Q&A website were stolen. All these events impossible to defend effectively show that, with further development of big data and mobile internet, privacy and anonymity problem cannot be completely eradicated purely by legal space.

From the view of motive and protective range, evidently, the privacy protection mechanism driven by the public and responded by American government sector is not optimal. It is only a privacy mechanism established under the framework of government sector but cannot solve majorities of people's demands on privacy because people naturally have free and anonymous intercourse and unfettered dream of freedom. Accordingly, the world's largest hidden web TOR, as well as various privacy-currency projects including Monero, Zcash, Dash and PIVX, and various private networks is born.

2.2 Summary of privacy technology

From the point of application scenario, almost all applied ecology have anonymous demands, such as anonymous payment, privacy protection of medical record, secret ballot, anonymous speech, and privacy circle. From the view of technological realization, current anonymous protection is mainly realized through cryptographic technique. For the cryptographic technique based on cryptography, the anonymous models specific to payment, contents, communication, package obfuscation, etc. are put forward. The following is our several typical anonymous projects.

Anonymous-currency technology

In transaction of Bitcoin system, the user can take public-key hash value as the transaction identification without the need to use real name. Public-key hash value can directly represent identity of user, unrelated to real name. Therefore, Bitcoin has its characteristics of pseudonymity. The user's repeatedly using public-key hash value as transaction identification makes it obviously possible to establish connections between transactions. Therefore, Bitcoin isn't really anonymous.

Currently, there have been a large number of encryption techniques such as Mixers, Ring Signature, Zero knowledge proofs and Channels, etc. In some homomorphic encryption or other trusted execution environments, it has been proven that these encryption techniques can realize privacy and secrecy of payment data.

For Dash, a type of privacy-protection strategy is realized on the basis of Coin Join, specifically, mixing the transaction between itself and unrelated people in capital pool so as to obfuscate input and output of transaction. In this way, other people will not really know the correct corresponding sequence of input and output for the transaction record on blockchain.

For Monero, a scheme of ring signature is introduced on the basis of coin shuffle, that is, mixing the public key of signer and the other public-key set and then signing the information. For the signing verifier, it is impossible to distinguish which public key corresponds to the real signer in the set after mixing, and further it is difficult to verify which one is the sender from the acceptor. Finally, untraceability is realized.

Currently, many similar anonymous-currency concept projects have emerged. On the whole, they are improved on the basis of some encryption techniques. Anonymous currency is not interconnected each other but has an ecological-competition relationship.

TEE

TEE is a trusted execution environment that is based on security extension of CPU hardware and is completely separated from outside. The product based on TEE optimization is called safe house, with its biggest

feature of "separation of data ownership and the right to use data". TBC, a data-circulation platform based on trusted blockchain, can be established through TEE, safe house and blockchain, which is actually a type of distributed and trusted data-operation platform. Based on TBC, the private smart contracts on public-blockchain platform can be operated through TEE so as to realize contract code and data based on hardware protection.

SGX of Intel and other TEE techniques, for instance, isolate code execution, remote attestation, security configuration, secure storage of data, and the trusted path used for code execution. The application program running in TEE is safely protected, so it is scarcely possible to be accessed by the third party.

Tor network

Tor (The Onion Router 1), realized from the second-generation onion routing, can help the user to realize anonymous commination on the internet through Tor. First the project was sponsored by US Naval Research Laboratory. In the later period of 2004, Tor became a project of Electronic Frontier Foundation (EFF). In the later period of 2005, EFF stopped sponsoring Tor project but continued to maintain the official website of Tor.

Tor focuses on defending against traffic filtering, sniffing and analysis so as to protect the user from network harms. For Tor,

anonymous outgoing connection and anonymous concealing can be realized by carrying out communication on overlay network formed by onion routers.

In addition, there are also a large number of privacy projects such as decentralized VPN, network based on mobile internet, and private network, etc.

3. Existing pain points in anonymous technology

3.1 Incomplete anonymous chain

We can see that current anonymous system mostly focuses on bringing forward a anonymous scheme to solve a certain application problem, that is, a certain application scenario. For example, the popular anonymous currency including Monero and Dash focuses on solving defects of pseudonymous mechanism of Bitcoin, while Tor deep web focuses on providing a network hidden in internet. Taking Monero as an example, we open a paying APP supporting Monero to start a new transaction through Iphone. The transaction is anonymous, but all our using behaviors in the process of opening operating system of mobile phone and invoking paying APP are actually visible.

3.2 Solidification of core cryptograph

Anonymous protection is mainly realized through cryptograph technologies including asymmetric encryption, hash algorithm and zero knowledge, etc. The security of anonymous-protection system and the security of cryptographic algorithm is closely bound up It is well known that any a cryptographic algorithm cannot be ensured absolutely safe. According to the difficulty to be deciphered, different cryptographic algorithms have different security levels.

For example, under global deduction of deciphering method, the cryptograph analyzer finds a replacement algorithm A, that is, Dk(C)=P under the circumstance that cryptograph isn't known.

If the cost of deciphering algorithm is greater than the value of encrypting data, it is generally accepted that this algorithm is safe. From the view of cryptography, as the arithmetic capability of computer increases exponentially, it cannot be ensured that all cryptographic algorithms are unbreakable. However, for current anonymous system, after the solidified cryptographic algorithm is adopted, once its core algorithm is cracked, at worst, catastrophic damage will be brought into the whole anonymous system, and, at best, system fork will be caused and community consensus is divided.

3.3 Homogenization, lack of interoperability

Many anonymous systems have very serious homogenization, especially for the anonymous currency based on blockchain. Owing to open-source feature of blockchain project, many emerging anonymous systems directly and simply modify function name of source code of current famous project and conduct certain so-called optimizing process to finally create new anonymous projects. Normally the system after being optimized can operate, the problem is lack of innovation, serious homogenization, and repeated construction. Also, interoperability isn't taken into account for current anonymous system, and the circumstance that various heterogeneous architectures coexist exists, causing failure of cross-system connection and lack of extensibility.

4. Timo positioning

Timo is an anonymous basic protocol focusing on realizing "end to end" from network layer to application layer by blockchain technique, specifically, forming a configurable privacy space through privacy domain by techniques of zero knowledge proof, coin shuffle and mixed network, DOS resistance, decentralized consensus and smart contracts, etc. Its main cores:

- The privacy space to be built by Timo is composed of a number of

privacy domains. **Privacy domain is a relatively independent privacy space carrying a series of anonymous applications designed for application demands.** The first privacy domain built is Original Anonymous Space that includes three basic functions of anonymous payment, anonymous browsing and anonymous voting. In future three years, we will also concentrate on building the largest Super Domain into the Dark Web Platform in blockchain world.

● All the privacy domains form into a privacy internet space under inter-blockchain connection of Shuttle protocol. We hope that the privacy internet space built by Timo will contribute to human's realizing free digitized life space.

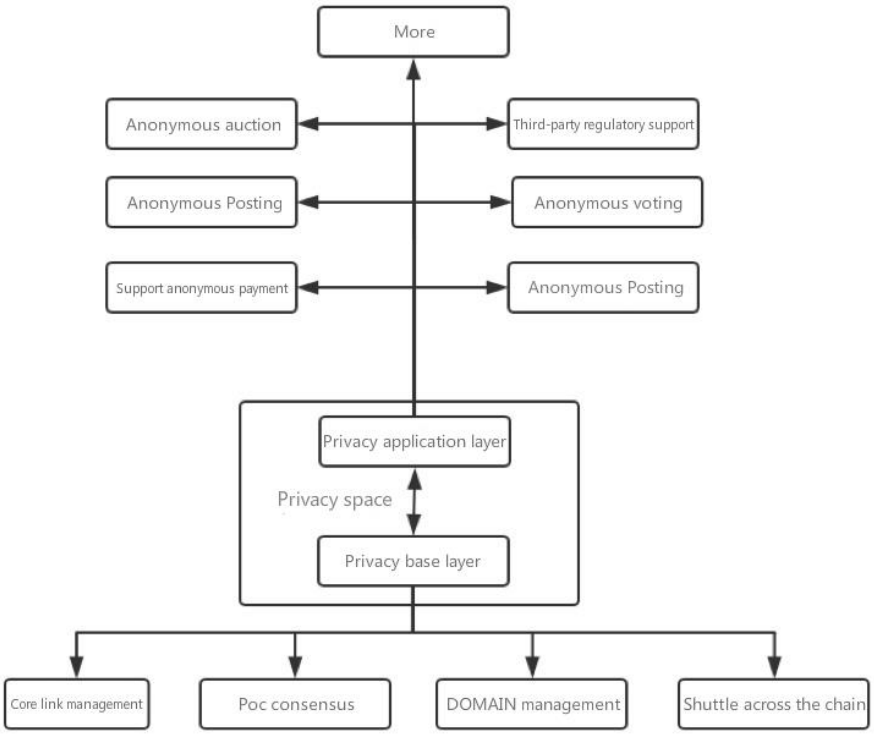
● Our positioning focuses on establishing an anonymous framework, anonymous protocol and anonymous platform but not improving current anonymous currency and anonymous projects. We don't want to compete with current anonymous projects. Our protocol will flexibly support current anonymous project, and promote anonymous application to develop vigorously by means of token motivation through decentralized anonymous development platform.

● Timo conducts hierarchical design of architecture according to the experience of the team in construction of large project. The whole privacy space will be made up of privacy base layer and privacy application layer.

Therein, the privacy base layer is responsible for infrastructure support of core-chain management, consensus mechanism, privacy-domain management, and Shuttle inter-blockchain, etc. while the privacy application layer supports anonymous payment, anonymous publishing, anonymous browsing, anonymous voting, anonymous auctioning and law as well as the third-party supervision, etc.

5. Timo protocol infrastructure

We will forge a anonymous space formed by privacy domain through Timo. The architecture of the whole anonymous space is as follows:



›

Privacy domain

Privacy domain is a privacy LAN facing application scenario and built through blockchain technique and cryptography technique. Each privacy domain will provide the configuration of privacy components named, including anonymous payment, anonymous browser, anonymous mall, and anonymous e-mail, etc. Essentially, privacy domain is a decentralized and distributed network that is made up of hardware node and normal node. Therein, the hardware node is the specialized hardware of built-in Timo that supports IOT firmware, can be integrated on smart device, and can also support 5G module in future; the normal node is the soft node installed with Timo Protocol.

Parent blockchain of Timo provides registration module. The name is registered on registration module of parent blockchain, and after Rule-Audit, can be officially added into Timo to be legal privacy domain and share shuttle service of Timo.

Each privacy domain is corresponding to one 128-bit address space. In order to avoid recognizing difficultly-remembered complex address for the developer and user, privacy domain provides Anony Chain Name Serives (ACNS). ACNS's job is to conduct bidiretional mapping on address space and project name. For example, the name of privacy domain A in Timo network is Timo_A. If the user doesn’t want to expose chain-name

service, he can choose to directly use 128-bit address space but not use ACNS.

During creating privacy domain, domains of four environments will be created at the same time:

- Development privacy domain, named: Name_Domain_Dev
- Test privacy domain, named: Name_Domain_Test
- Quasi-production privacy domain, named: Name_Domain_Pre
- Production privacy domain, named: Name_Domain_Pro

Setting four same-name domains aims to cater to the need of project management. Development privacy domain is used for daily development. The functional module developed is tested in test privacy domain. After passing test, it can be delivered to quasi-production privacy domain for integration and acceptance testing. At last, after being ensured conforming, it can be submitted to final production privacy domain for operation. Here, the environment of quasi-production privacy domain is completely consistent with it of production privacy domain, mainly aiming at ensuring maximum safety of system during go-live.

Timo node

The whole Timo node is composed of Timo infrastructure layer and

privacy application layer. Therein, the privacy base layer is responsible for infrastructure support of core-chain management, consensus mechanism, privacy-domain management, and Shuttle inter-blockchain, etc. while the privacy application layer supports anonymous payment, anonymous publishing, anonymous browsing, anonymous voting, anonymous auctioning and law as well as the third-party supervision, etc.

From the view of data-packet unpacking, one data packet is delivered to Timo infrastructure layer, and then Timo infrastructure layer will add information including public blockchain, route, multi-tier signature, Domain Name, and Shuttle Protocol, etc. After public-key hash, it will be delivered to the privacy application layer.

The privacy application layer is composed of various anonymous applications. Anonymous-currency payment, etc. are just realized in this layer. With good extensibility, Timo can support not only Timo anonymous currency but also Monero, zec and other privacy currency.

Under a point-to-point decentralized and distributed environment, two privacy control shall be considered for each node. Firstly it is Admission detect. Owing to the decentralized and dynamic feature of blockchain node, the system shall detect whether the nodes added are valid or not, malicious or not, attacked or not. Secondly, because the blockchain node is dynamic, many nodes may be frequently rebooted in the network.

When one node leaves, the log sheet of access path of route of node shall change dynamically so that the latest state can be recorded. Thirdly, Timo has both hardware node and software node. Each node has different processing performance. There is much difference in processing performance between the same hardware node or the same software node. For example, a node with poor performance may affect the whole route path.

All of the above need to be taken into account for node design of Timo. In general, in order to adapt to the environment of mobile communication, Timo adopts Rerouting (redirection route) and distributed agent technology to realize anonymous communication.

According to the node route, if information needs to be sent, the source node Node broadcasts DREQ message in domain: <DREQ, Timonum,tr(B),Droute >. Therein, Timonum is the global unique serial number; tr(Node B) = E(IDB, NA,k(SD)), k(SD') is the working key exchanged through public key in adavance; Droute is the route message encrypted. It is signed and encrypted in the process of forwarding via intermediate node. The generating process of Droute is as follows: Each node generates its own Droute through random number during forwarding. Droute generated from Node A is E (N(A), A, K(A)). The node will try opening covert channel when receiving the request message for the first

time. For Node B, there is a private key. Thus only Node B can be successfully opened. Node B packages data packet with transmit-channel route or representative and fragments for handy multicasting broadcasting. The neighbor node checks whether there are records or not. If any, above working mechanism and forwarding shall be continued, otherwise it shall be discarded.

The following is topological environment axiom and timing axiom. A 4 refers to the case that, if one end of single hop has sent a message, the message occurs on this hop.

Timing axiom

Name	Axiom
A 1	*A E{X,~XY)*
A2	*j o i n{XY.YZ)*
A3	*XY = YX*
A 4 4	*Se{X,t)A E{X,XY)* ZD *A c c (t^XY)*
T1	0(^ A Z) (O ^A O y /)
T2	*0(^(G ^ A Oy/)*
T3	O—i^ —>*o<f>*

Timo hardware node

To sum up, hardware node and software node execute the same function. Comparatively speaking, hardware node is integrated on system, so its treatment efficiency is higher. Moreover, Timo hardware node also

supports generation of true random number. Our hardware node will support three categories as follows:

√ Small-type and standalone family node, including router

√ IOT devices, such as intelligent air conditioning, refrigerator

◎ 5G module (direction, to be verified)

The user can connect hardware device to home network to become a member of big Timo family, and use Web UI to configure, join it with a certain identity of Timo Domain so as to make contributions to Timo ecology, while Timo will also provide token reward to motivate more users to buy hardware node.

Synchronously, 5G module is under study. We hope that those Timo ecological smart devices with a function of edge computing can provide the privacy computing resource that is faster realized and is more easily extended with the help of the cross-platform and low power-consumption techniques of Timo as well as the intelligent scheduling technique of handy point-to-point access of node. Aided by Token Motivation System of Timo, the smart device will be motivated to actively contribute the idle hashing power and storage so as to activate the global tera-scalesmart device to join and finally provide huge hashing-power pool and storage pool for various application scenarios of Timo Domain.

(Please see the following section for details about anonymous protection of IOT)

POC consensus mechanism

Consensus and smart contracts are the core of majorities of anonymous applications. In the point-to-point distributed and decentralized architecture, more nodes means higher security of anonymity. Therefore, we are committed to motivating more users to join Timo node through motivation system.

In terms of the anonymous project, the function of consensus mechanism shall focus on promoting healthy development of the whole token economy model, preventing "mining overlord" from threatening the whole economic system, and also attracting more users to join. Only in this way can the anonymous system is ensured absolutely safe.

After 3-month consideration, the team finally selects POC mining. POW focuses on guessing the correct hash value through ceaselessly changing a certain digit of block headers, while POC focuses on utilizing plotting workload in hard-disk space. Each block in POC will be bound with an exclusive "puzzle". Before mining, the network will store the solutions to the puzzle in hard-disk space of user. If there happens to be a solution in user's hard disk, and the solution is the "fastest solution" that

the puzzle in the block generated recently at present corresponds, the user will win the accounting right of block.

The real mining algorithm behind POC is very complex, and also the time of generation of a block is too short (a new block is generated averagely every four minutes). Therefore, such a mining solution shall be stored in space of hard-disk drive in advance. At last, more solutions (also known as plots) stored in hard-disk space will make higher probability to solve the puzzle in this block with the fastest speed.

Practice shows that POC can effectively prevent the problem of monopoly, hashing-power centralization and energy consumption, and can motivate more users to join, thus it is the optimal consensus algorithm of Timo. Of course, in consideration of rapid evolution of blockchain technique, Timo reserves the interface for changing consensus algorithm in order to support POS consensus algorithm in future.

Shuttle protocol

Shuttle protocol, as the operation protocol between domains, is mainly used in privacy interoperability between domains as well as the secrecy interface with external network (optional). It is composed of two protocols of Inter-Domain Communication (IDC) and Out-Domain Communication (ODC). Therein, IDC is mainly used in inter-blockchain

between DomainIBC, and Cosmos developing framework is adopted; while for ODC, in view of the circumstance that introducing external connection may cause a risk of privacy exposure to the whole domain, it is necessary to be developed prudently in the later period and is opened through community poll.

It is worth noting that only the domain issuing token can use Shuttle protocol. As for the following circumstances, Shuttle protocol need not be used:

- Domain ecology token. TIMO issues anonymous assets
- Domain doesn't issue anonymous assets

Shuttle protocol defines a group of semanteme to be used for passing the verified strict-ordering message between two blockchains with independent-conformity algorithm.

We take two privacy domains of Domain T1 and Domain T 2 as an example. Shuttle protocol focuses on verifying whether the data packet T1 received on Domain T2 can generate correct Domain T1 on the chain. Here, a inter-blockchain linear guarantee is established: after the data packet is verified on the chain, we know that the data packet Domain T2 has be executed on the chain, and the data packet T1 and any relevant logic are parsed (for example, asset trusteeship). Then we can safely execute application program logic Domain T2 on the chain.

Shuttle protocol is irrelevant to payload. On the Shuttle protocol, the developer can realize semanteme of the specific application program so as to ensure that the user can transfer valuable assets between different blockchains and the contract warranty of relevant assets can be reserved at the same time.

For Shuttle protocol, two blockchains with inexpensive verifiable fast terminality and Merkle tree substate data are required. For this protocol, there is no hypothesis on the confirming time of grouping or the maximum network latency of grouping transmission, and two consensus algorithms maintain completely independent. Each chain's local order is maintained. As for inter-chain message ordering, cross chain shall be ensured linear. Once a trust relationship is registered between two chains, the verifiable encryption grouping can be sent between them.

To be convenient for connection of shuttle protocol, for two blockchains, the following domain authentication shall be provided:

● When trusted T_h and C_h imputable updated message U_h is given, T_h' C_h' == C_h and dt(now, T_h) < P can be proven

● When trusted T_h and C_h imputable updated message X_h is given, _h' C_h' /= C_h and dt(now, T_h) < P can be proven

● In view of reliable T_h and Merkle T_kvh, V_kh can be proven

In terms of authentication, we also put forward cross-domain Shuttle protocol that focuses on meeting distributed-network parallel, high performance and cooperative work of computer by using trusted collection of K_DAA and K_TPM. Shuttle protocol is developed on the basis of Cosmos SDK, thus it is similar to Cosmos SDK in processing mechanism.

6. Extendable anonymous application-layer technology

Above we expound privacy technique architecture of Timo and focus on describing fundamental framework of Timo protocol and the technique feature of privacy network. Here, we focus on introducing application architecture of Timo. Timo integrates various anonymous elements into application architecture in a form of configuration to really realize the anonymous application architecture that the user can control independently. In Timo architecture, we incorporate the mainstream stable open-source technique into application framework. In the first phase, the mainstream anonymous techniques of XMR, Zcash and PART, etc. are incorporated into the self-owned anonymous system of Timo Electronic Auction and Timo Anonymous Currency, etc.

In terms of techcological realization, each anonymous application scenario will be delivered to Timo application protocol for processing in a form of application layer. On Timo privacy application layer, asymmetric key signature is added, and privacy-address processing is conducted. Then it will be delivered to infrastructure layer of Timo layer by layer.

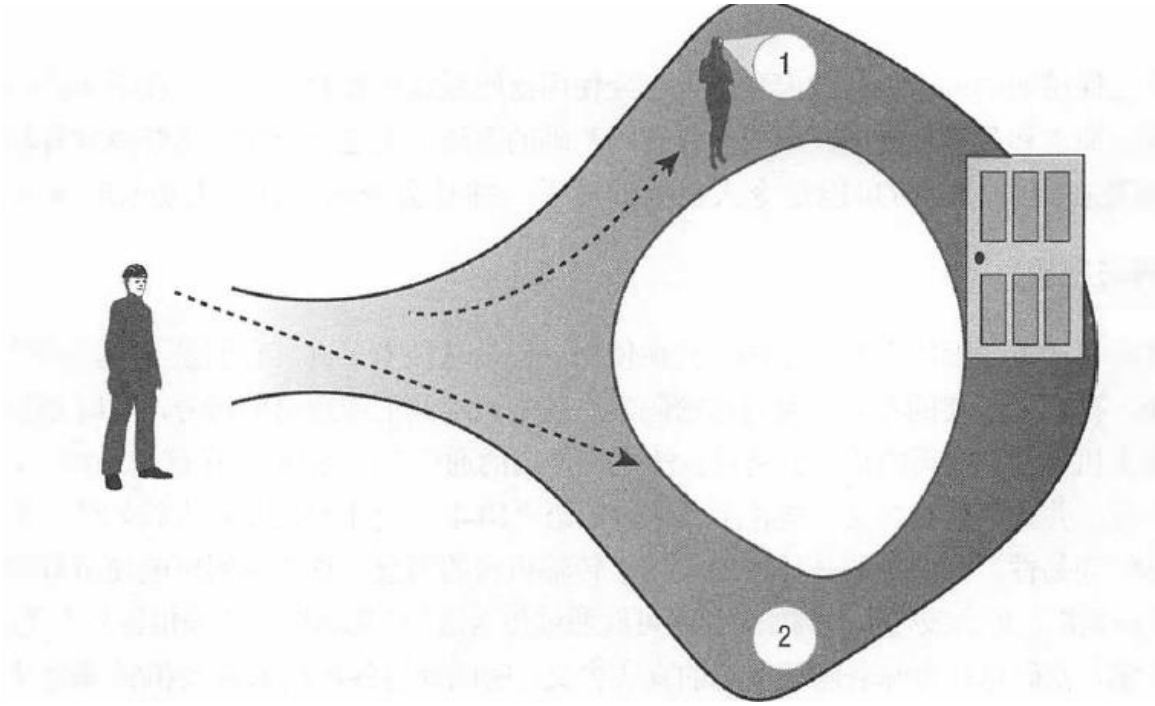
Timo anonymous application platform provides a variety of technical components including blind-signature and fair blind-signature technique, zero-knowledge proof theory, non-repudiation protocol, optimist fair exchange protocols, trusted secret sharing and response protocol, Bit commitment, and support supervision, etc. where the anonymous metrics is optional. Following main technical components are introduced:

Zero-knowledge proof element

Zero-knowledge proof is the standard configuration for anonymous system. Its mechanism focuses on proving the understanding towards the fact to the third party under the circumstance of not revealing the truth to the third party.

The sample is displayed as shown in the following figure. Peggy knows the password of secret door inside circular cave. Victor is willing to buy password from Peggy but hopes Peggy to prove that she really knows

password before payment. However, Peggy is unwilling to tell Victor password in advance because she worries about that Victor will not give the reward. Accordingly, zero-knowledge proof will solve the dilemmatic problem.



Victor can stand at the entrance of cave and watch Peggy enter cave. Then Peggy arrives at secret door and opens it with password. She goes through secret door, and finally returns the entrance of cave through path 2. Victor sees Peggy's entering cave from path 1 and returning through path 2, which proves that she must know the password of secret door.

Timo supports zk-SNARKs, the zero-knowledge proof. Its mechanism focuses on confirming that the function of transaction validity must return the solution to transaction validity according to the rule

consensus of network but not disclosing any information of computing execution. Above is realized through encoding the consensus rule of network inside zk-SNARKs. On a higher level, the operation mode of zk-SNARKs is to first transform the thing that the user wants to prove into an equivalent form, that is, knowing the solution of some algebraic equations.

Computation → Arithmetic Circuit → R1CS → QAP → zk-SNARK

zk-SNARKs is suitable for solving QAP problem (Quadratic Arithmetic Programs). Generally speaking, it is the problem including polynomial. In this process, the main thing is how to transform a common problem into a QAP problem. Please see following polynomial equation, assuming x = 2.

```
1 | x ^ 3 + x ^ 2 + x = 14
```

Firstly we introduce a number of variables and transform above equation into some basic simple equations. All these simple equations are either x = y or x = y (op) z. Wherein, op represents four operational symbols of adding, subtracting, multiplying, dividing (+ , - , * , /). These computations can be completed through digital circuits.

After a series of calculus, we will get such a result. In this way, the problem is transformed into a computational problem, specifically, to get

solution vector s and make the equation s . C(n) - s . A(n) * s . B(n) = 0 established when n=1,2,3,4, equivalent to:

There exists a polynomial H（n）making s . C(n) - s . A(n) * s . B(n) = H(n) * Z(n). Wherein, Z(n) = (n-1)(n-2)(n-3)(n-4).

In the process of verification, degree of these polynomials is very big. The highest degree of some polynomials may reach up to a million. Accordingly, transmitting these polynomials will greatly lower transmission efficiency. The solution is to take a sampling point n = t. In this way, P(t), H(t) is actually two numbers, becoming very concise.

The specific steps are as follows:

Verifier randomly selects a sampling point t to send to Prover.

Prover calculates P(t),H(t). Please pay attention to P(t),H(t) that isn't a polynomial but becomes two numbers.

Prover sends P(t),H(t) to Verifier.

Verifier verifies P(t) ? = H(t) * Z(t)

Above, the core of zk-SNARKs, has become the standard configuration for popular anonymous payment. We can consult relevant papers from the official website. Timo application layer first supports zk-SNARKs and evolving version.

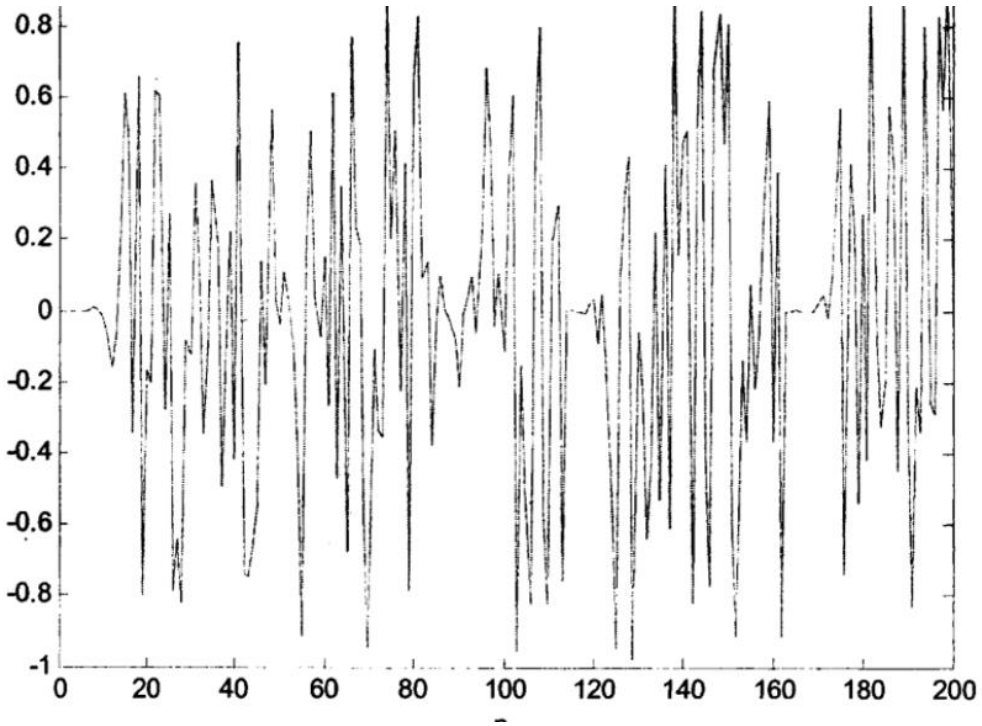
Measurable nonce

Nonce is the most common technical demands for anonymous application, such as voting, winning rate of lottery, seed parameters generated from key, and parameters of work password. However, there is a golden sentence in the computer world, going like "there is no true random in program". The nonce is generated by computer according to a set of fixed algorithm but not the figure randomly generated in the real sense. As long as the random seed is the same, the nonce generated will also be the same. Taking random in numpy of Python as an example, seed parameters can be set so as to make two groups of nonce generated the same.

The true nonce is realized through hardware. Thanks to hardware node, Timo has its conditions for generating nonce. To sum up, it means that a physical method is used to realize nonce generator. Also, it is the indeterminacy reaction of physical phenomenon generated by the random physical process of the natural world. In this respect, it will be completed by hardware node of Timo. Specifically, hardware node will introduce various true random sources such as circuit noise field, heating-power noise field, computer clock, arrival time of IP packet, and transform to generate by using mathematical method.

The chaos model is used to analyze sensibility of the initial value. Logistic chaotic mapping is taken as an example. The initial value X_0 is given, iterative sequence is gotten, and two curve graphs of difference

value of iterative sequence are drawn. According to the display, after dozens of times of iteration, the sequence is totally different.



The third-party supervision and support

Focusing on forging configurable anonymous space, Timo needs to meet diversified demands of anonymous and privacy application scenario. Taking the anonymous transaction and anonymous contract monitored by the policy as an example, under such a scenario, the anonymous transaction arising from smart contract needs to be notarized if necessary. In order to support the third-party supervision, Timo will

support multiple supervision mechanisms including CA, domain authentication, and center authentication on the basis of asymmetric cryptograph protection. The supervision organization and enterprise generate their respective public and private key pair. Therein, the private key is kept by themselves, while the public key is released on the official channel. When a transaction is launched, the account-transferring person gets the public key of the organization. After that, the supervision organization may use the private key to track transaction behavior and protect the privacy among users.

If necessary, the supervision organization can view information with the private key. But others cannot view the transaction information as they don't have the private key.

In the framework of the third-party supervision of Timo, we need also to consider the circumstances of cross-domain supervision authentication and CA authentication center, etc., including the trusted third-party certificate authentication center (Arbitration Center of Certificate, CAC) and two trusted domains (DOA, DOB). Therein, each trusted domain includes two entities, that is, TCP and the certification authority DAA. If the trusted computing platform of trusted domain DOA attempts to apply for service, the certificate can be showed. Please see also descriptions for specific realization.

Privacy technology of TA_ONS of IOT

With the commercial progress of 5G, IOT has been increasingly widely used. Timo will introduce IOT privacy technology to meet the new application demands of IOT.

Its mechanism focuses on introducing ONS query mechanism of IOT, adding the anonymous authentication process, and verifying credibility and legality of local identity. Aiming at the existing deficiencies in the process of transmission of item information of traditional IOT, Timo will apply the trusted anonymous information transmission protocol of IOT to use neighbor-node session key to encrypt detailed information of items layer by layer from back to front according to the node order of link response path under a decentralized state.

Before system is established, authentication is required. The trusted authentication protocol is designed on the basis of bilinear pairing and bilinear intractable problem: selecting the parameters meeting requirements bilinear ray including G1, G2, e, q, P. Wherein, G1 and G2 are the group of order prime q, G1 is the cyclic group of addition, G2 is the cyclic group of multiplication, P is the generator of G, and bilinear pairing e is G1 X G2 -> G2; selecting hash H:(0,1)-》G, opening parameter e、q、P> through security approach.

Updatable cryptographic algorithm (Quantum resistance)

In terms of the safety problem of cryptographic algorithm, at worst, we assume that cryptographic algorithm is broken, endangering the whole anonymous system. In response, based on domain, we suggest that the cryptographic algorithm of each privacy domain can be different according to the strategy of input of cryptographic algorithm. When safety problem may happen to a certain algorithm, domain can duplicate the similar domain but, for the latter, new algorithm will be used. Of course, such an updatable cryptographic algorithm is still in a stage of concept validation.

To cope with the imminent quantum of solace, currently we integrate the algorithms as follows:

Lattice-based cryptography

Lattice-based cryptography is a kind of concerned public-key cryptograph system focusing on resisting attack of quantum computing. Lattice-based cryptography involves many research problems of mathematics of cryptography, with distinct characteristics of interdisciplinarity and diversified research methods. The development of lattice-based cryptography is generally divided into two main lines. One is the development from the research on classic lattice-based mathematical problem with a long history to the solution algorithm of high-dimensional

lattice-based problem and the theoretical research on computing complexity over the last 30 years; the other is the development from the analysis on safety of non-lattice public-key cryptograph system with the solution algorithm of lattice-based problem to the design of cryptosystem based on lattice-based problem.

Blockchain post-quantum (PQ) signature

Inspired by the blockchain architecture and current signature scheme based on Merkle tree, the researcher puts forwards BPQS, a kind of digital signature scheme that can expand PQ resistance. It is most suitable for blockchain and distributed ledger technology (DLT). A unique characteristic of this protocol lies in that it can reduce the cost of key generation, signature and verification as well as the size of signature by using special chain or image structure. Compared with other improvement schemes appeared recently, when a key is reused for reasonable amount of signature, BPQS will be superior to the current hash algorithm. If needed, it also supports a kind of roll-back mechanism and allows the signature with an unlimited actual amount.

7. Development plan (two two-year development plans)

- From 2019 to 2020: **the year of fundamental framework**

→ To complete construction of Timo test network and major network

→ To complete design of primitive protocols of mining function, browser, network layer protocol and shuttle protocol, etc. and operate

→ To complete design of application architecture of zero knowledge, ring signature, coin shuffle, invisible address, and the third-party supervision interface, etc.

→ To complete system integration go-live of fundamental framework and build the first prototyped anonymous space Original Domain. Original Domain is the first anonymous space of Timo integrated with three basic major prototype applications of anonymous payment, anonymous voting and anonymous browsing through advanced blockchain technology.

→ To establish decentralized anonymous-space development service, and provide the most popular and advanced encrypted components and anonymous components.

● From 2021 to 2022: **the year of ecology**

→ To complete the plan of Super Dark Web and establish Super Domain, that is, the largest full-anonymous space aiming at dark web. Super Domain will realize full-process, full-chain and comprehensive anonymous space from network layer to application layer and provide the

most comprehensive and the most anonymous applications including anonymous payment, anonymous browsing, anonymous publishing and anonymous voting, etc.

→ To conduct ecological promotion and establish the anonymous space including Cypherpunk Circle domain, Private Circle domain, Marihuana Fan Circle, and the judicial domain that can be notarized in order to meet diversified demands of anonymous and privacy application.

8. Highly-professional and diversified top team

Members of TIMO founding team have a profound background in the industry of encryption informatics, cryptography and internet, etc. Combining with blockchain, they will bring a great revolution of anonymous digital assets:

● Ahmad Kharbat： IT Solutions, Inc.

IT system engineer and solution architect, senior all-source intelligence analysis specialist of former U.S. Special Forces.

● Joux Antoine: getting lots of achievement in discrete-logarithm problem on extension field and elliptic curve, and making great contributions to the development of ECC.

● PhD Biodun Gennaro：Served as the senior architect of Azure cloud product group of Microsoft, he was responsible for analysis of architecture security and consultation of high-end commercial clients. As the network-safety doctor of University of North Texas, MBA and network-safety master of University of Dallas, he has held the post of the leader of network safety and architecture project in multiple American IT enterprises.

● Goldreich: holding the office of SAAB at present) common fund VP, managing a capital scale of about 2 billion dollars. With an overseas study tour in America and Europe, he owns MFA and SPM authentication as well as a MBA degree. Also, he has an in-depth study on investment of digital currency.

9. Ecological token TIMO

TIMO will serve as the pillar of development for anonymous ecosystem of digital currency and issue a total token amount of 210,000,000.

● Cornerstone price: 0.06usdt, locking position for 1 year, linearly unlocked in batches according to 12 months after one year

● Token distribution: 10% for premining, 80% for miner award under POC consensus mechanism, 10% for team motivation (the community

determines unlocking or not by votes according to the performance of the team)

TIMO utilizes motivation system of blockchain. Tokens of TIMO will play a very important role and embody value of TIMO as follows:

One main line of value of TIMO is the carriers of value. Each anonymous application scenario accesses or directly uses a certain amount of TIMO or define its own token and exchanges with TIMO according to a certain ratio. With the application scenario's being gradually enriched, TIMO consumption becomes more and more, and meanwhile TIMO's value is bigger and bigger.

Another main line of value of TIMO is the transaction attribute. Similar to Ethereum, each transaction of TIMO needs to be paid. Also, its anonymous application and shuttle inter-blockchain transaction also need to be paid by using TIMO. TIMO supports smart contract. TIMO on contract will interact through transaction.

One more important main line of value of TIMO is motivation system. Normally, TIMO is one part of motivation plan focusing on motivating people to help system to verify transaction, create blocks and utilize economic means to generate positive feedback so as to promote continuous

development of system. Token will be the reward that motivates community to continuously make contributes to the system.

After the decentralized anonymous development platform is built, the developer will receive award through sharing software so as to motivate more developers to join ecology.

10. Risk warning and disclaimer

10.1 Risk warning

Policy risk As of the launching day of the white paper, the national governments haven't released a set of complete law system directing at the blockchain project yet. In future, the possibility that various countries prohibit blockchain financing by official order cannot be completely ruled out, which possibly causes a loss to the investor.

Supervision risk As of the launching day of the white paper, there doesn't exist the powerful supervising subject in the field of digital asset transaction. Also, the penalty rule for the behaviors of going against business ethics including fraud, malicious manipulation and spreading of false information, etc. is not found. The investor needs to make a decision making of investment on the basis of knowing that the protective measures

of investor aren't complete at present.

Market risk If the digital-asset market is overvalued, investment risk will be increased. The investor needs to prudently determine investing or not, and avoid setting a too-high expected return. In addition, even if the overall market suffers from downturn, the project may also be smoothly boosted.

Technical risk The smooth growth of underlying basic techniques including blockchain, distributed ledger, decentralization and tamper disagreeing, etc. is the premise of the development of core business of the project. At present, the possibility of cases that above techniques fail to land in the future developing process as it fails to reach the expected target, or fundamental defects are proven existing owing to a hacker attack cannot be completely ruled out.

Competition risk Currently, there are too many projects in the field of blockchain, causing tremendous market competition pressure. The project team will do the best to advance development so as to stand out from many projects as early as possible. But the project may be caused blocked in advancement owing to vicious competition of market.

Security risk Features of electronic token including anonymity and untraceability are easy to become the criminal aim of lawbreaker. At

present, the possibility of the criminal behaviors of suffering a hacker attack or illicit-asset transfer, etc. cannot be completely ruled out. Meanwhile, the development of quantum computer cannot be accurately estimated. In future, the case that, owing to a surge of computer performance, cryptograph cracking increases sharply but token is caused lost may occur.

Coordinating risk In future, the possibility of the case that the developing work of the project is hampered owing to the core member's leaving and internal conflict of the team cannot be ruled out.

Development risk At present, it is impossible to make a promise on whether lots of individual or organization recognition and participation can be gained or not. The interest of general public and the external developers on developing relevant distributed applications will affect development of the platform.

Other risks With the development of blockchain technique and virtual currency industry as well as the promoting of project development, the project possibly face the current unforeseen uncertain risks. The project team will do the best to avoid or cope with the risks but cannot guarantee that these risks will not affect the project.

10.2 Disclaimer

File property The white paper is only used for conveying information. The file contents are only for reference only and will not constitute any investment-business suggestions, invitation or instigation, and any contract or commitment. The team will be not responsible for any investment loss possibly occurred in future.

Token property Token of this project is the tool that the platform exerts performance but not investment goods. The team doesn't make any commitment of appreciation. The investor's owing tokens of the project doesn't mean that he is awarded the ownership, control right or decision-making right of the platform. It has not any form of legal-restraint effect.

Investment premise The default investor of the project meets the age demands, has complete civil capacity of conduct, and has fully known the possible risks of the project and investment environment. The contract is signed on a voluntary basis, and is true and valid. The project is not responsible for the problem caused by investor's violating above items.

Information updating The industry-analysis data involved in the white paper come from internet, for reference only. It cannot be ensured accurate.

Real-time The project contents involved may be irregularly updated with the project forwarding. At the scheduled time, the project

team will announce the updated contents publicly through releasing announcement on the website or launching new-edition white paper, etc. The investor shall bear any consequence potentially caused by failing to get the latest information.