CELARE

CELARE

Cross-chain and anonymous solutions for all assets
Breaking the barrier of cross-chain assets
Protecting user privacy

白皮书Version 1.0

CONTENTS

4.TECHNICAL SPECIFICATION

5.ECOLOGY

1.PREFACE

2019 is the 500th anniversary of the death of Leonardo da Vinci who is the representative of the Renaissance and the 10th anniversary of the birth of Bitcoin.

The root of nearly 300 years' majestic Renaissance is the revival of the humanistic. Its significance is to respect of the value of human beings, to release people's freedom, to liberate people's thinking and energy, and to inspire people's infinite creativity.

It was because of the Renaissance that there were three industrial revolutions behind. As a result, the human society, the economy, and even the ideology and culture have undergone huge changes.

The Celare Co-Founders' Committee believes that human kind is at a turning poin which is the opening of the fourth industrial revolution where Blockchain technology will definitely dominate this trend.

With the continuous upgrading of "Internet +" and the continuous demand of improvement of the quality life, the centralized and large-scale corporate and manufacture are declining. The era of multidimensional competition with perfectionism and ecologicalization is coming with dividing demand and splitting business is getting deeper and deeper, and the organizational model is bound to move from a single vertical control type to a meshed and platformized one, and individuals will get more empowerment.

Therefore, the new industrial revolution must have an ideological revolution that matches with it. This is the idea of Blockchain.

The new era calls for new infrastructure and logical design to bring together new public consensus.We believe that Blockchain innovation can solve the biggest challenges that we face, lead humanity to a new era, and further advance human civilization to an unprecedented height.

Just as Leonardo da Vinci to Renaissance, the creator of Bitcoin, Naka moto Satoshi, has a far-reaching impact on the decentralized distribut ed thinking. Before Nakamoto, although the drawbacks of centralizatio n are obvious to all, no one can really abandon the decaying centralize d system. To a certain extent, Nakamoto is the first person in human hi story to use algorithms and machines to implement decentralized syst ems.

The Renaissance symbolizes that religious theocracy and feudal monarchy gradually withdraw from the center in different political regions with different degrees and different modes, which is followed by the rise of capital power and the formation of political, economic and cultural order in the three industrial revolutions. It is also the current social form.

The emergence of the Blockchain will open the fourth industrial revolution, because it has finally condensed the spirit of "science, democracy, and freedom" that the humanity has been striving for since the Renaissance.

At the same time, we also noticed that the update speed of the Blockchain era far exceeds our imagination.

The Blockchain 1.0 era is a cryptocurrency represented by bitcoin, with monetary functions such as payment and circulation. The most important thing is to establish a set of cryptographic books, providing a set of distributed, non-tamperable, unforgeable, traceable accounting methods.

The Blockchain 2.0 era is based on the Blockchain 1.0 which join the smart contract to support the upper DAPP application development. Represented by Ethereum, a large number of underlying public chains emerged, allowing participants to write arbitrarily complex and intelligent contracts that are transmitted by blocks, with a distributed autonomous organization philosophy.

The Blockchain 3.0 era has enabled Blockchain technology to expand from the economic to more fields. It can be used to realize the increa-

singly automated distribution of physical resources and human assets on a global scale, and promote large-scale collaboration in science, he alth, education and other fields. From the financial sector to the field of social governance, including identity certification, auditing, notariz ation, transportation, logistics, medical, sports and other fields.

The Blockchain will become a base-level protocol that connects all wal ks of life, providing people with more convenient services.

More importantly in the Blockchain 3.0 era, communities are moving to ward rejuvenation, governments and markets become part of society, a nd society is united by highly mature communities across all dimensio ns and tangible and intangible edges.

Everyone in the community enjoys a high degree of freedom，full value realization and happiness.

In the future, the government's borders will be rationalized, the marke t will only retain some of its functional status, individual power will be released to the maximum extent, and individual privacy rights will be p rotected to the maximum extent.

This is the goal that the Celare Co-Founders' Committee will fight for.

The Celare Co-Founders' Committee is committed to defending individ ual privacy and securing individual assets. Core developments have be en completed, including privacy-related protocols and homomorphic e ncryption algorithms. This whitepaper focuses on Celare's work. For ill ustrative purposes, it contains some basic information about the proje ct and will discloses future plans.

Celare Co-Founders’ Committee
August 2019

2.BACKGROUND

2.1 Zero Protection of Citizen Privacy in the Internet World

The right to privacy refers to the personal right to enjoy the privacy of life and the secrets of information, and to be illegally invaded, informed, collected, utilized and disclosed by others.

However, users' information are always on the verge of being collected, utilized and exposed, without any protection.

According to Snowden, a former CTED employee, the British "Guardian" and the US "Washington Post" reported on June 6, 2013, that the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) had launched a secret surveillance project code-named "PRISM" since 2007. This project directly entered the US Internet's central server to mine data and collect information. These server included Microsoft, Yahoo, Google, Apple,Facebook, PalTalk, YouTube, Skype and AOL.

Nowadays, if you find a black market and gray industry chain server, you can buy anyone’ s record for only 100 USD, including 11 records such as hotel checking, flights and bank information. Almost all personal information can be easily found. Moreover, the service provider claims to provide 7×24 hours of uninterrupted service on a global scale.

In addition, Internet giants such as Facebook and WeChat sell mass of personal data, which is called accurate crowd advertising. These personal data include identity information such as age, gender, transaction history, consumption habits, positioning and so on.

Therefore, a single lady is usually harassed by advertisements on the dating website. A young man with a fat body is likely to receive tips for diet pills.

As you can see, the Internet has brought many privacy leaks, and most of the privacy leaks in the Internet application scenario are often caused by the lack of sufficient data security protection mechanisms for the centralized platform, and even more, individual Internet companies born to master the user data to achieved the purpose of selling of them.

Perhaps users whose personal privacy has been compromised are only harassed by telephones and advertisements. However, privacy breaches related to financial transactions are related to the identity and security of assets.

- Personal asset information (including but not limited to bank balances, under-name assets, under-name companies, etc.);
- Personal consumption records (clothing, food, housing, travel);
- Personal investment information (buy and sell records and holding information);
- Consultant service information (new product promotion planning consultants and
other sensitive information) purchased by the business owner;
- The upstream and downstream supply chain records of a company (account exchanges and sensitive information transmission);

- Major news such as mergers and reorganizations of enterprises (including lawyers, accounting and consulting agencies);
- Financial derivatives positions and trading information of investment banks and hedge funds;

The above-mentioned private information directly related to finance is related to the security of individuals' assets, while it may relate to a company's competitiveness in the industry and even relate to the survival of financial institutions.

However, in the traditional centralized Internet system, the above information, if centralized data collectors do evil, can be used or even profitable.

Although the privacy issue has attracted the attention of many governments, such as the European Union's first to promulgate the General Data Protection Regulations (GDPR), which is designed to urge companies to effectively protect the privacy of users, but the restrictions of these laws are minimal. Because the human’s desire cannot be restricted.

Ultimately, a centralized platform or system is controlled by human, and the ultimate use is determined by the controller.

2.2 Traceable Cryptocurrency Transactions

Bitcoin was once considered as a secure cryptocurrency. However, including bitcoin, the mainstream cryptocurrencies on the market always has the risk of privacy leakage. That is to say, bitcoin is not private.

One is its own mechanism;
Second, some centralized exchanges require KYC;

First of all, from the structural design of the mainstream cryptocurrencies trading system represented by Bitcoin:

-Each main chain has a corresponding Blockchain browser, and every transaction can be found, and all transactions can be traced back to the source.

-We all know that the way to package new blocks is that each newly generated block will package all the transaction data and balance of the previous block, and all the transaction data is stored in the public ledger, anyone can get the complete global ledger. The main accusation of miners is accounting, which means that all transaction information does not use encryption to protect data.

Many people think that although anyone can get the so-called global ledger, using a cryptocurrencies network or having a cryptocurrencies wallet address does not require a real name, or we can say it is anonymous, and does not correlate with the actual identity in real life, which means The global ledger obtained is completely anonymous and has no directivity.

But there is no directivity does not mean that the relationship cannot be calculated. After research and deduction, we found that potential attackers can infer the trading rules of cryptocurrencies addresses by analyzing the transaction records in the global ledger, such as the transaction frequency of related addresses, transaction characteristics, and the relationship between addresses.

Based on these laws, it is possible for an attacker to associate a cryptocurrencies address with a particular user's identity in the real world.

One of the methods mainly obtains the regular characteristics of the transaction of the address by analyzing the transaction record related to the address, and estimates the identity information of the corresponding user accordingly. Since there will be its unique transaction characteristics in a particular type of Blockchain transaction, the attacker can restore the real scene of the transaction according to the transaction characteristics of the address, thereby making the user's true identity speculation.

Some people have designed a simulation experiment that matches the Blockchain address and the identity of the housewife. The housewife use ETH as the payment means for daily transactions. The analysts can use the behavior-based clustering technique to match the housewife identity and the Blockchain address successfully at 39% accuracy.

The research continues. If the trading behavior of a certain cryptocurrency is quantified, the user's trading rules are analyzed based on 12 dimensions such as trading time interval and transaction flow. The large amount of data obtained after 6 months of experiments indicates that the analytical model successfully identifies the user's true identity with an accuracy of up to 62% and an error rate of less than 10.1%.

Another way is to use some of the potential knowledge in the Blockchain transaction design to achieve clustering of different addresses and get multiple addresses of the same user. At present, it is possible to calculate different types of addresses, such as the address of the exchange, the mining pool organizer, and the project organizer, because the transaction records of these addresses have a special input and change method, and are easily recognized.

The second reason that makes bitcoin and other mainstream cryptocurrencies easy to trace is that centralized exchanges require KYC, which need to match real-name to an account.

KYC process will require users to upload identity information to the exchange. Currently known mainstream centralized exchanges have launched KYC, which is to obey to regulatory requirements.

However, due to KYC user privacy is collected centrally on the exchange, whether it is a currency transaction or a legal currency OTC, which is related to the information of the real society. So, to a certain extent, these mainstream cryptocurrencies are basically have no privacy.

In addition, in any case, we are unable to avoid all the motives and possibilities of centralizing exchanges do evil, and in this context, the user's privacy rights are subject to unknown risks.

2.3 Inextensible Zcash Dash XMR

Due to emphasis on privacy protection many teams and volunteers are also beginning to study completely anonymous Blockchain networks such as Zcash, Dash and XMR.

Let's take a look at how these three cryptocurrencies works.

2.3.1Zcash

Zcash is the first Blockchain system that uses a zero-knowledge proof mechanism that provides complete payment confidentiality while still maintaining a decentralized network by using a public Blockchain. The Zcash transaction automatically hides the sender, recipient, and amount of all transactions on the Blockchain.

Only those who have a private checking key can see the content of the transaction. Users have full control of the key and they have the option to provide private checking keys to others.

Despite of this, Zcash uses the same underlying framework as the Bitcoin network, so it can only support simple transactions even though it can hide the sender, receiver and transaction amount.

You can understand that this is a bitcoin network with a privacy protection mechanism. In addition, the entire process of using zero-knowledge to prove the process of encrypting transactions is inefficient, and its application scenarios are further limited.

2.3.2.Dash

Dash was founded in 2013 by Evan Duffield and was originally called Darkcoin. It was renamed Dash after March 2015. It is an online instant cryptocurrencies transactions tool with the purpose of protecting users' privacy.
Dash confuses transactions through the original decentralized web server "master node", which can also be called a CoinJoin to achieve anonymity.

The essence of its use of the CoinJoin is to simply transfer a fund multiple times in multiple addresses, which is simple and easy to operate. The CoinJoin has high applicability in various digital currency systems, but the existing scheme requires users involved in the CoinJoin process online.

If the parties cannot agree on the amount of the CoinJoin, it must be postponed. In order to make the CoinJoin fully processed, the transaction is generally delayed, and the CoinJoin is centrally deployed actually(although it is claimed to be decentralized). The node can get all the information of the transaction and can steal money.

Most of the improvement of the CoinJoin scheme are to prevent theft and information leakage by increasing the cost of third-party violations, and it is not possible to fundamentally eliminate violations. However, if a cryptographic technique such as blind signature is used, the cost of the calculation will increase the calculation cost, and the third party execution of the CoinJoin process will inevitably bring additional service overhead.

Unfortunately, Dash does not support smart contracts, and third-party’ s CoinJoin providers rely on its credibility and this will lead to unpredictable risks.

In recent years, based on its good liquidity in the early stage, Dash focused on the development of ecological applications, and strengthened the cooperation with enterprises, trying to make Dash coins a payment tool with strong circulation value, instead of Re-emphasize the advantages of privacy protection.

2.3.3.XMR

Monero (XMR) was launched on April 18, 2014 and focuses on privacy, decentralization and extensibility. Based on the CryptoNote protocol, Monero has significant algorithmic differences in Blockchain fuzzification and is a model in privacy cryptocurrency.

The privacy of Monroe is gradually strengthened. On January 10, 2017, the trading privacy of Monero was further enhanced from the Block#1220516 by using the Ring Confidential Transactions algorithm.

The Ring Confidential Transactions algorithm does not indicate the amount involved in the transaction to those who are not directly involved in the transaction, thereby increasing the confidentiality of Monero.
Monroe also uses a CoinJoin scheme to further enhance its privacy. Monero’ s CoinJoin users do not need to communicate with other nodes, and can participate in the CoinJoin process by themselves, providing effective protection measures for the common denial of service attacks in the decentralized CoinJoin mechanism and the disclosure of information by the users.
If you don't consider that Monroe does not support smart contracts, it is indeed a good choice for anonymous coins.

2.3.4.Overview

So far, we have compared the three major anonymous coins that focus on privacy of identity and transaction. They all have their own advantages. However, what they have in common is that they do not support smart contracts, and their extensibility is too low, which makes their application scenarios very limited. This is why most anonymous coins are only repeated in the field of payment, but they are not widely used.
If you need a Blockchain system with privacy protection mechanism and smart contracts at the same time, the traditional Blockchain solution is to make major changes to the underlying protocol, which inevitably consumes more computing resources, thus affecting the efficiency of the chain. In the following pages, we will explain how Celare solves this pain point.

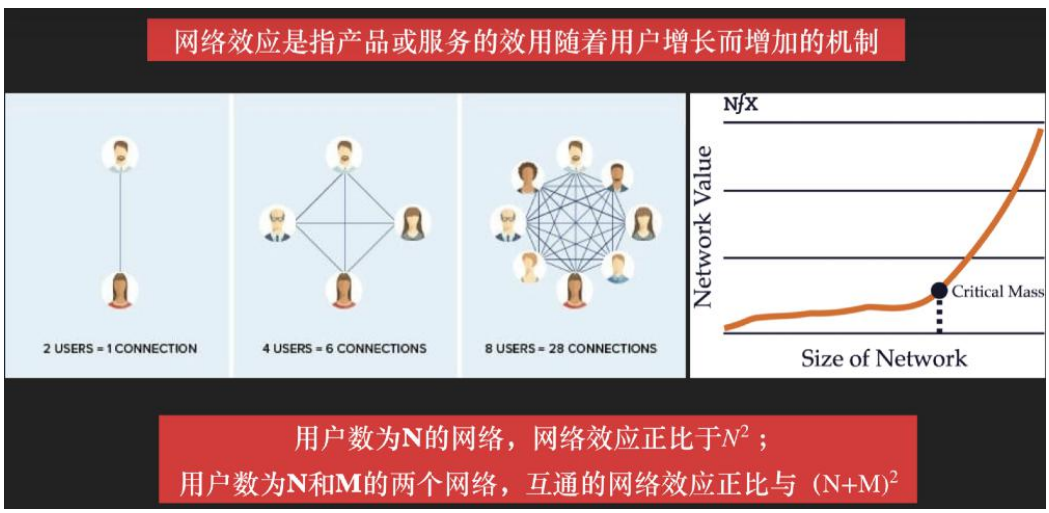
2.4 The split Blockchain world

The current Blockchain underlying technology platform is flourishing. However, there is a lack of a unified interconnection mechanism between different Blockchains, which greatly limits the development of Blockchain technology and application ecology. In particular, the assets of each Blockchain system are trapped within their own systems, resulting in no division of labor, collaboration and exchange.

In the early stage of Blockchain development, perhaps this problem will not affect a single chain, but when more and more independent public chains developed, the growth of community member base cannot keep up with the speed of public chain development, we find that independent chains need to be linked to share the benefits of network effects.

Network Effect refers to the mechanism by which the utility of a product or service increases as the user grows.

According to Metcalfe's law, the network value is proportional to the square of the number of users. As shown in the figure above, the more users there are, the more possible connections between users, and the greater the value of the network to users. For example, there is only one connection between two users, but six possible connections in six users, Even 28 possible connections in eight users.



Use n for the number of users, the communication network value is proportional to n*(n-1), and when n is large enough, n*(n-1) is approximately equal to the square of n.

Network Effect growth is slow in early stage, but begins to accelerate when it reaches a certain size.

According to Metcalfe's law, we can get the inference about network merging: two networks, the number of users are N and M, respectively, and the value of the larger network formed by their combination (or full interoperability) is proportional to the square of (N +M).

It can be seen that the development of Blockchain should not only solve the problem of high TPS. How to make links and exchanges between independent Blockchain networks, and achieve user network effects, which will make the development of Blockchain more flourish.

To achieve the connectivity and communication between Blockchain networks, cross- chain technology is a good and necessary solution.

2.5 Polkadot's Cross-chain Technology Solution

The so-called "cross-chain" means that the information and assets originally stored in a specific Blockchain can be converted into information and assets on another chain through technical means, thereby realizing the exchange of value.

2.5.1.History of Cross-chain Development

2009-2012 Single-chain development stage
This period is the budding stage of Blockchain technology. It is inspired by Bitcoin. It is widely believed that the performance optimization and technology upgrade of Blockchain can be completed in a single chain. Once the members of the chain cannot agree on the project development, only Can be solved by permanent divergence, which also lead to permanent divergence of bitcoin and other chains.

2012-2014 Side chain proposal

The development of Bitcoin is severely constrained by the limitations of Bitcoin in terms of block time, block size and smart contracts. With the emergence of Litecoin, BitShares and Ethereum, the Bitcoin core development team felt the crisis. In 2012, Ripple Labs proposed the Inter ledger protocol to connect different accounts and achieve synergy between them.

2014 Cross-chain proposal

The earliest proposal of cross-chain technology can be traced back to the BlockStream team's research on Bitcoin side chain technology in 2014. Subsequently, there are lightning network， Raiden Network application of hash time lock HTLC technology, Ripple to notary public mechanism and HTLC. The comprehensive practice of the agreement, and now Wanchain, Cosmos, Polkadot and other projects on the cross-chain platform's unremitting pursuit and practice, of which, Polkadot's solution has obvious advantages in technology, pattern and community.

2.5.2 What is Polkadot?

Polkadot is an exploration of cross-chain technology presented by co-founder of Ethereum and funder of Parity Technologies, Gavin Wood on November 14, 2016.

Polkadot is a decentralized and scalable heterogeneous multi-chain framework that supports cross-chain communication between different chains, not only for asset exchange and transfer, but also for data cross-chain communication.

Polkadot is similar to vodafone, an infrastructure service provider that provides communication bandwidth services between networks. Developers can develop applications based on this infrastructure.

Polkadot itself does not develop chains and applications. It provides cross-chain hub services. From the perspective of value transmission, cross-chain technology can bridge the gap between different projects, create an ecological consensus, expand the influence of the project, and increase the value of exchange.

2.5.3.Polkadot's Solution

The Polkadot network has three major functions that address inter-operability, scalability, and shared security issues in the Blockchain.

Interoperability

Polkadot designed Relays to connect different parachains. Data and information on each parachain are passed through the Relays and inter-chain communication is achieved using the Mekle Tree's queuing mechanism. At the same time, there are also bridges between the Relays and Ethereum and Bitcoin for value interoperability. Using multiple interconnected chains will also help spread the transaction load across more nodes, which will reduce the cost of performing functional contracts while increasing scalability and dispersion.

Scalability

Scalability is a key barrier to the use and development of DAPP on Blockchains. In the Polkadot network, a Relay connects multiple parachains, and a secondary Relay can be built on the first Relay. The secondary Relay continues to connect multiple parachains, thus achieving a parachain can be connected to hundreds of parachains. These parachains can process transactions at the same time, which greatly increase the speed and efficiency of the transaction, and enabling the Blockchain network to achieve unlimited extensibility.

Shared Security

Naturally, different Blockchains will compete for security resources. In general, when miners or verifiers migrate to a new Blockchain, the security of other chains will decrease. However, the parachains in the Polkadot network shares the same consensus with the Relays. The parachains will agree to a certain degree of “transfer” to the Relay, thus obtaining the accumulation of security of the whole network, that is, the “safe pool”. Then, these parachains do not need to build an expensive POW mining system or establish a POS mechanism in token economy. This not only reduces resource waste, but also improves transaction efficiency between chains.

3.INTRODUCTION

3.1 Introduction to Celare

Celare — a cross-chain and anonymous solution for all assets

In view of the fact that most anonymous coins are private but not widely applicable and cannot be cross-chain exchanged, the Celare Co-Founders' Committee has been researching cross-chain technology since 2018 and has finally developed a cross- chain solution to the security and privacy of chain assets - Celare.

Celare achieves zero-knowledge proof by selecting the BLS12-381 curve, and truly implements a Blockchain system with privacy protection for Turing-complete smart contracts. Compared with the existing Blockchain privacy protection technology, Celare not only realizes the privacy protection of account information and transaction, but also realizes the privacy protection of Turing's complete smart contract input and output.

At the same time, in order to break the information isolated islands of Blockchain, Celare based on Substrate and developed to share the security cross-chain operation of Polkadot after its launching, thus achieving full asset anonymity.

Celare

Not only decentralized cross-chain trading

Not only decentralized anonymous identity

Not only realizes sharing of ecological benefits

Not only the tools for global developer launching of Blockchain

Not only decentralized anonymous exchanges

Not only share the security and cross-chain operation of Polkadot

Not only the privacy protection of smart contract input and output

4. TECHNICAL SPECIFICATION

4.1.Design Principle

In principle, Celare is a polkadot parachain and developed on the Substrate. The advantage of the it is that it can share the security and cross-chain operation of Polkadot, and independently develop its own in-chain system. Therefore, Celare's design will be compatible with Polkadot, and it also has its own unique algorithms and functions.

4.1.1 Four Basic Roles

Similar to Polkadot, there are four roles in the upkeep of an Celare network.

- Validator: A validator is the highest charge and helps seal new blocks on the Celare network. The validator’s role is contingent upon a sufficiently high bond being deposited, though we allow other bonded parties to nominate one or more validators to act for them and as such some portion of the validator’s bond may not necessarily be owned by the validator itself but rather by these nominators.

A validator must run a relay-chain client implementation with high availability and bandwidth. At each block the node must be ready to accept the role of ratifying a new block on a nominated parachain. This process involves receiving, validating and republishing candidate blocks. The nomination is deterministic but virtually unpredictable much in advance. Since the validator cannot reasonably be expected to maintain a fully synchronized database of all parachains, it is expected that the validator will nominate the task of devising a suggested new parachain block to a third-party, known as a collator.

Once all new parachain blocks have been properly ratified by their appointed validator subgroups, validators must then ratify the relay-chain block itself. This involves updating the state of the transaction

queues (essentially moving data from a parachain’s output queue to another parachain’s input queue), processing the transactions of the ratified relay-chain transaction set and ratifying the final block, including the final parachain changes.

A validator not fulfilling their duty to find consensus under the rules of our chosen consensus algorithm is punished. For initial, unintentional failures, this is through withholding the validator’s reward. Repeated failures result in the reduction of their security bond (through burning). Provably malicious actions such as double- signing or conspiring to provide an invalid block result in the loss of the entire bond (which is partially burnt but mostly given to the informant and the honest actors).

In some sense, validators are similar to the mining pools of current PoW Blockchains.

Nominator: A nominator is a stake-holding party who contributes to the security bond of a validator. They have no additional role except to place risk capital and as such to signal that they trust a particular validator (or set thereof) to act responsibly in their maintenance of the network. They receive a pro-rata increase or reduction in their deposit according to the bond’s growth to which they contribute.

Collator: Transaction collators (collators for short) are parties who assist validators in producing valid parachain blocks. They maintain a “full-node” for a particular parachain; meaning that they retain all necessary information to be able to author new blocks and execute transactions in much the same way as miners do on cur- rent PoW Blockchains. Under normal circumstances, they will collate and execute transactions to create an unsealed block, and provide it, together with a zero- knowledge proof, to one or more validators presently responsible for proposing a parachain block.

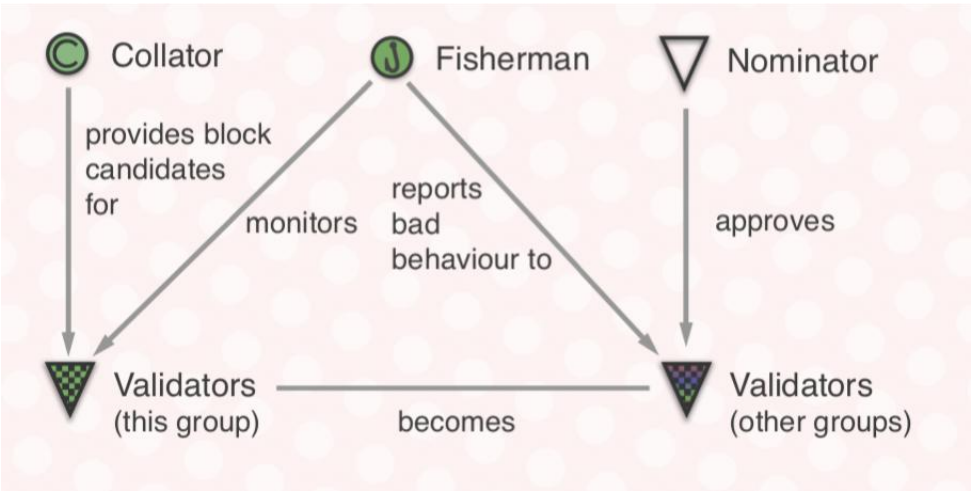
Fisherman: Unlike the other two active parties, fishermen are not directly related to the block-authoring process. Rather they are independent “bounty hunters” motivated by a large one-off reward. Precisely due to the existence of fishermen, we expect events of

misbehaviour to happen seldom, and when they do only due to the bonded party being careless with secret key security, rather than through malicious intent. The name comes from the expected frequency of reward, the minimal requirements to take part and the eventual reward size.

Fishermen get their reward through a timely proof that at least one bonded party acted illegally. Illegal actions include signing two blocks each with the same ratified par- ent or, in the case of parachains, helping ratify an invalid block. To prevent over-rewarding or the compromise and illicit use of a session's secret key, the base reward for providing a single validator's illegally signed message is minimal. This reward increases asymptotically as more corroborating illegal signatures from other validators are provided implying a genuine attack. The asymptote is set at 66% following our base security assertion that at least two-thirds of the validators act benevolently.

Fishermen are somewhat similar to "full nodes" in present-day Blockchain systems that the resources needed are relatively small and the commitment of stable uptime and bandwidth is not necessary. Fishermen differ in so much as they must post a small bond. This bond prevents sybil attacks from wasting validators' time and compute resources. It is immediately withdrawable, probably no more than the equivalent of a few dollars and may lead to reaping a hefty reward from spotting a misbehaving validator.

The interaction between the four roles of Celare:



Celare’s network verification process .

A validator’s main purpose is to testify, as a well-bonded actor, that Celare block is valid, including but not limited to any state transition, any external transactions included, the execution of any waiting posts in the ingress queue and the final state of the egress queue.
The process itself is fairly simple. Once the validator sealed the previous block they are free to begin working to provide a candidate Celare block candidate for the next round of consensus.

Initially, the validator finds a Celare block candidate through a parachain collator (described next) or one of its co-validators. The Celare block candidate data includes the block’s header, the previous block’s header, any external input data included (for Ethereum and Bitcoin, such data would be referred to as transactions, however in principle they may include arbitrary data structures for arbitrary purposes), egress queue data and internal data to prove state-transition validity (for Ethereum this would be the various state/storage trie nodes required to execute each transaction).

Experimental evidence shows this full dataset for a recent Ethereum block to be at the most a few hundred KiB.
Simultaneously, if not yet done, the validator will be attempting to retrieve information pertaining to the previous block’s transition, initially from the previous block’s validators and later from all validators signing for the availability of the data.

Once the validator has received such a candidate block, they then validate it locally. The validation process is contained within the parachain class’s validator module, a consensus-sensitive software module that must be written for any implementation of Polkadot (though in principle a library with a CABI could enable a single library to be shared between implementations with the appropriate reduction in safety coming from having only a single “reference” implementation).

The process takes the previous block’s header and verifies its identity through the recently agreed relay-chain block in which its hash should be recorded. Once the parent header’s validity is ascertained, the specific parachain class’s validation function may be called. This is a single function accepting a number of data fields (roughly those given previously) and returning a simple Boolean proclaiming the validity of the block.

Most such validation functions will first check the header-fields which are able to be derived directly from the parent block (e.g. parent hash, number). Following this, they will populate any internal data structures as necessary in order to process transactions and/or posts. For an Ethereum-like chain this amounts to populating a trie database with the nodes that will be needed for the full execution of transactions. Other chain types may have other preparatory mechanisms.

Once done, the ingress posts and external transactions (or whatever the external data represents) will be enacted, balanced according to chain’s specification. (A sensible default might be to require all ingress posts be processed before external transactions be serviced, how- ever this should be for the parachain’s logic to decide.) Through this enactment, a series of egress posts will be created and it will be verified that these do indeed match the collator’s candidate. Finally, the properly populated header will be checked against the candidate’s header.

With a fully validated candidate block, the validator can then vote for the hash of its header and send all requisite validation information to the co-validators in its sub- group.

Celare network collection process

Celare collators are un-bonded operators who fulfill much of the task of miners on the present-day Blockchain networks. They are specific to a particular parachain. In order to operate they must maintain both the relay-chain and the fully synchronized parachain.

The precise meaning of “fully synchronized” will depend on the class of parachain, though will always include the present state of the parachain’s ingress queue. In Ethereum’s case it also involves at least maintaining a Merkletree database of the last few blocks, but might also include various other data structures including Bloom filters for account existence, familial information, logging outputs and reverse lookup tables for block number.

In addition to keeping the two chains synchronized, it must also “fish” for transactions by maintaining a transaction queue and accepting properly validated transactions from the public network. With the queue and chain, it is able to create new candidate blocks for the validators chosen at each block (whose identity is known since the relay- chain is synchronized) and submit them, together with the various ancillary information such as proof-of-validity, via the peer network.

For its trouble, it collects all fees relating to the transactions it includes. Various economics float around this arrangement. In a heavily competitive market where there is a surplus of collators, it is possible that the transaction fees be shared with the Celare validators to incentivize the inclusion of a particular collator’s block. Similarly, some collators may even raise the required fees that need to be paid in order to make the block more attractive to validators. In this case, a natural market should form with transactions paying higher fees skipping the queue and having faster inclusion in the chain.

Cross-chain transfer basic logic

According to Polkadot's design, the asset exchange process between Celare and other parachains can refer to the cross-chain exchange between two parachains.

If chain A needs to send an amount to chain B, the process is as follows:

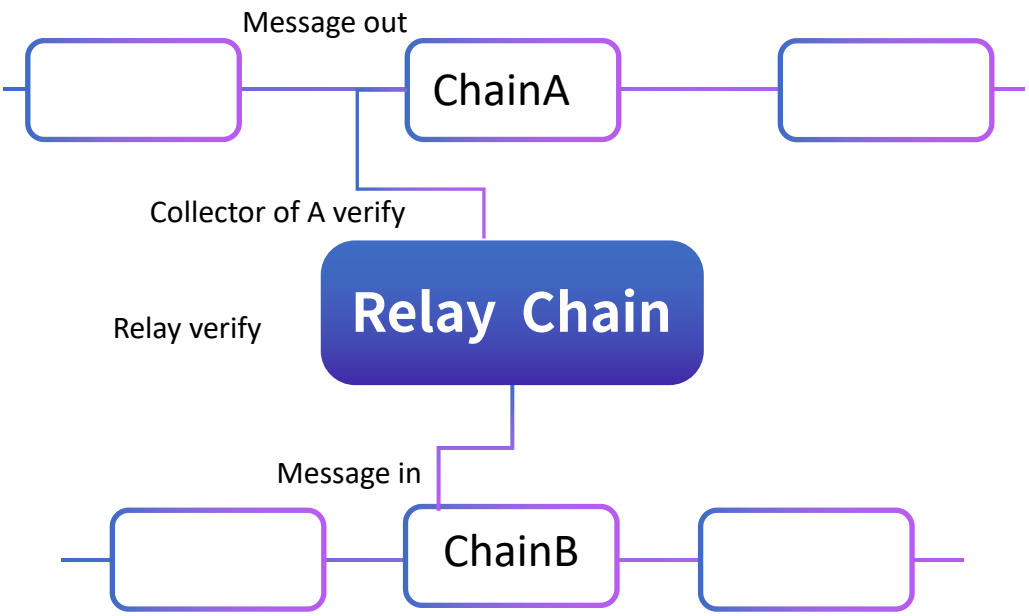
1 The A chain puts transaction information on its own egress (each parachain has a message output queue egress and a message input queue ingress);

2 Chain A Collator collects both of normal transactions and cross-chain transactions and submits to chain A’ s set of validators;

3 If the validators of the chain A successfully verified, and the block header information of the chain A and the information of the egress of the chain A are submitted to the Relay chain;

4 The relay chain runs consensus algorithm performing block acknowledgment and cross-chain transaction routing. The validateor on the relay chain moves the corresponding transaction of the chain A from the egress queue of A to the ingress queue of B;

5 The chain B executes the block and executes the corresponding transaction in the ingress queue and modifies its own ledger.
The above process can be simplified as follows:



4.1.2.Technical Framework

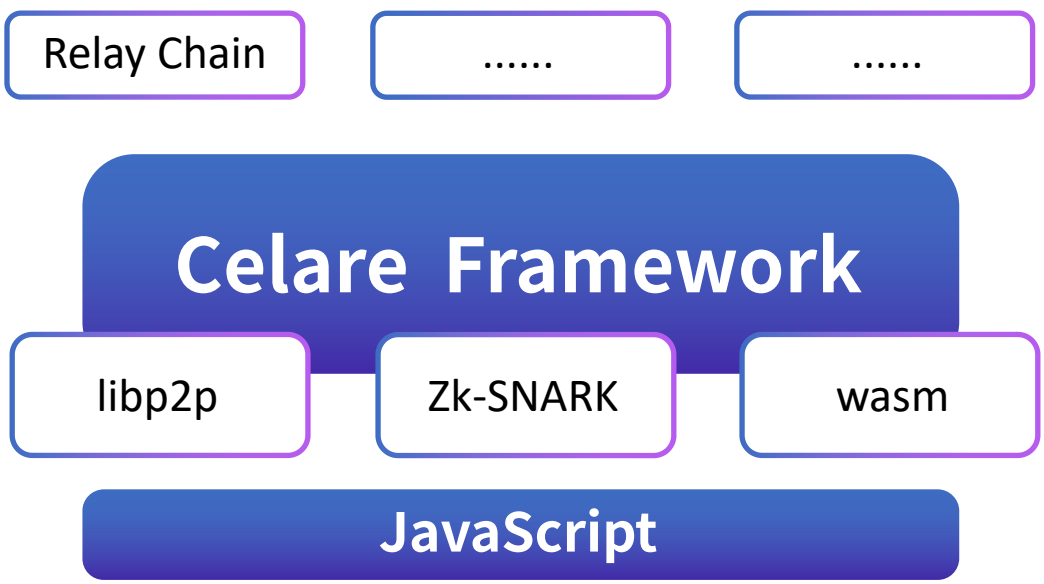
When cross-chain technology becomes possible, the Blockchain will usher in a major turning point in the history.

One of the excellent cross-chain solutions, the Polkadot, uses the Relay chain solution. The initial Polkadot of the Relay Chain consists of a relay chain and several parachains.

Parachains can be developed using different types of Blockchain underlying technologies. The Relay chain is responsible for the shared security consensus across the network and the cross-chain transaction forwarding of parachains. The Relay chain itself does not contain any applications which are deployed on parachains. Polkadot has pushed the development level of the entire Blockchain to a dimension, accelerating the leap of the Blockchain to the 3.0 era.

Celare is a parachain developed on Substrate. By reserving of bridge to Relay chain, it can easily access the Polkadot relay chain and maintain efficient communication with other parachains under the polkadot ecology after launching of Polkadot.

The technical Framework of Celare is as follows:



In Celare’s framework, the data and consensus layers are basically shared with Polkadot.

At the network level, the underlying protocol of Celare is libp2p. Libp2p is a peer-to- peer protocol for discovering nodes, connecting them, discovering content, and transferring them. 。

In terms of the verification mechanism, the non-interactive zk-SNARK zero- knowledge proof is used to completely solve the privacy and anonymity problems.

In particular, Wasm is widely used in Celare's smart contract development.

Wasm's advantages are obvious. It allows users to write in their preferred language (currently supporting C,C++ and Rust) and then run on the browser in the virtual machine engine. It also supports sandbox mode, which is to write the wasm module in a high-level language and then load it as a library function in JavaScript. Wasm can achieve untrusted programming without increasing cost. Accurate calculations can be performed by stack analysis and metrology on Wasm.

It is mainly used for:
1 WebDAPPdevelopment
2 EVM

4.1.3Cryptographic Algorithm

The cryptographic algorithm used by Celare is the discrete logarithmic encryption and elliptic curve encryption which are commonly used in modern public key crypto systems.

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E, consider the primitive P and another element T. Then the DL problem is to find the integer d ($1 \leqslant d \leqslant \#dE$), which satisfies:

$$\underbrace{P+P+\cdots+P}_{d次}=dP=T. \qquad (9.2)$$

In the crypto system, d is usually an integer and is also a private key, and the public key T is a point on the curve with coordinates =(xT,yT). The two keys in the DL problem in Zp are integers. The operation in equation (9.2) is also called point multiplication because the result can be written as T = dP. However, this term is somewhat misleading because the integer d cannot be directly multiplied by a point P on the curve. So dP is only a simple representation of the group operation of the group operation repeated in equation (9.2).

Let's look at an example of an ECDLP.
We perform a dot multiplication on the curve y2=x3+2x+2mod17. Assume that you want to calculate

$$13P=P+P+P...+P$$

Where P = (5, 1). In this case, you can directly use the pre-compiled table and get the result:

$$13P=(16,4)$$

Point multiplication is similar to an exponential operation on a multiplicative group. In order to efficiently calculate the point multiplication, we can directly use the square-multiplication algorithm; the only difference is that the square becomes doubling and the multiplication becomes the addition of P. The algorithm process is as follows:

Double-and-Add algorithm in point multiplication Input: elliptic curve E and point P on the elliptic curve Scalar

$$d=\sum_{i=0}^{t} d_i 2^i \ , \ \text{且} \ d_i \in 0,1 \ , \ d_t=1$$

Output: T = dP
initialization:
T= P
algorithm:
1 FOR i=t- 1 DOWNTO 0
1.1 T=T + T mod n IF di=1
1.2 T= T + P mod n
2 RETURN (T)

For a random scalar of length t + 1 bits, this algorithm requires an average of 1.5t point doubling and point addition. Briefly, the algorithm scans the bit representation of the scalar d from left to right and performs a double doubling in each iteration; it only performs a P addition if the current bit has a value of 1. Let's look at an example.

For scalar multiplication 26P, its corresponding binary representation is:
This algorithm scans each scalar bit in turn from the leftmost d4 until the rightmost d0 bit.

#0	$P=1_2P$	初始化设置，被处理的位为：$d_4=1$
#1a	$P+P=2P=10_2P$	DOUBLE, 被处理的位为：d_3
#1b	$2P+P=3P=10_2P+1_2P=11_2P$	ADD,因为$d_3=1$
#2a	$3P+3P=6P=2(11_2P) =110_2P$	DOUBLE, 被处理的位为：d_2
#2b		没有ADD,因为$d_2=0$
#3a	$6P+6P=12P=2(110_2P) =1100_2P$	DOUBLE, 被处理的位为：d_1
#3b	$12P+P=13P=1100_2P+1_2P=1101_2P$	ADD,因为$d_1=1$

#4a $13P+13P=26P=2(1101_2P) =11010_2P$ DOUBLE, 被处理的位为：d_0

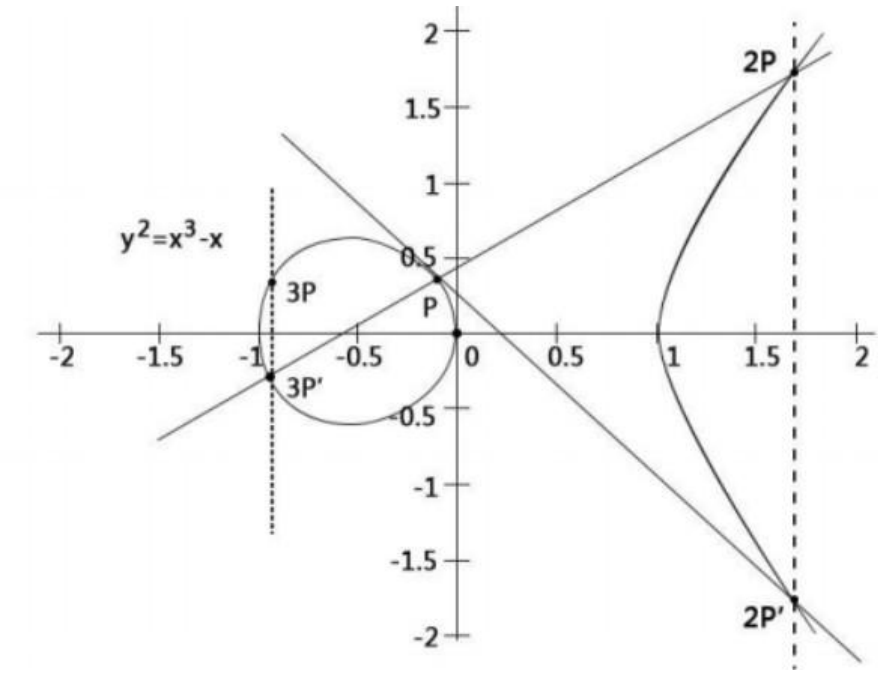
#4b 没有ADD,因为$d_0=0$

This process is a very intuitive reflection of the binary representation of the exponential transformation process. It can be seen that doubling the point will move the scalar one bit to the left and 0 to the rightmost position. Performing an addition of P inserts a 1 at the rightmost position of the scalar. Compare the way the highlighted index is transformed in each iteration.

The geometric interpretation of ECDLP is also very simple:
Given a starting point P (public parameter), you can effectively calculate 2 P, 3 P ,...,dP = T (public key) by jumping back and forth on the elliptic curve;

Then publish the starting point P and the ending point T. In order to decipher the cryptosystem, the attacker must figure out the frequency of "jumping" on the elliptic curve;

The number of times this jump is the password d, the private key.



Hash function algorithm

The hash function algorithm is widely used in the chain of Celare. The hash function is also called a hash function, a message digest function, and the like. Its purpose is to compress a message m of any length into data of a specified length H(m). H(m) is also known as the fingerprint of m.

More hash function algorithms are used. For example: message authentication, pseudo-random functions, and so on.

The hash function has the following characteristics:

I. Anti-first originality The hash function has unidirectionality, and H(m) is known. It is impossible to calculate the m value by H(m).

2、 Violence Crack For the n-bit hash value, the exhaustive scale is 2 to the nth power.
3、Collision Resistance The possible values for each element in the hash function are n 2 , where n is the output width of H(). The number of hash operations t needed to find a conflict is expressed as a function of the hash output length n and the collision probability λ.

$$t \approx 2^{(n+1)/2} \sqrt{\ln(\frac{1}{1-\lambda})}$$

For a hash function with an output length of 256 bits, to find a collision pair with a probability of success of 50%, 2129 hash calculations are required. Assuming that the computer can perform 10,000 hash calculations per second, it will take 1027 years to complete these hash calculations.

4.1.4.Non-interactive Zero Knowledge Proof

Zero-knowledge proof of non-interactive zk-SNARKs
Celare uses a non-interactive zk-SNARKs zero-knowledge proof system to completely address the issue of transactions being traced to expose user privacy.

zk-SNARKs is an encryption method based on purely mathematical theory. It is the same as the nature of Blockchain. The advantage of this method is that it does not need to rely on the external operating environment to be self-contained, so it has a wide range of application scenarios.

Its basic meaning is "zero knowledge Succinct Non-interactive Argument of Knowledge", to see what they mean:

- zero knowledge:Zero knowledge, that is, does not reveal any insider in the process of proof;

•succinct:Concise, mainly means that the verification process does not involve a large amount of data transmission and the verification algorithm is simple;

•non-interactive:No interaction, technique attempts to completely avoid interactions.

In a nutshell, zk-SNARK is a kind of technology that proves that I know the inside story. It is simple and easy to operate. The most important thing is that you can get the conclusion that it is correct, and you don’t know anything about the content of the message or transaction, so this process can achieve privacy and anonymous.

It is worth noting that Celare chose a BLS12-381 curve with a higher safety level when specifically selecting the zk-SNARK zero-knowledge proof curve.

BN128曲线（Barreto-Naehrig curves）vs BLS 12-381曲线（Barreto-Lynn-Scott curves ）

The same pairing-friendly elliptic curve, BN128 and BLS 12-381 are still different.

According to the corresponding parameters in the paper "Implementing Pairings at the 192-bit Security Level" are as follows:

KSS curves: $k = 18,\ \rho \approx 4/3$ $p(z) = (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 + 1763z + 2401)/21$ $r(z) = (z^6 + 37z^3 + 343)/343,\ \ t(z) = (z^4 + 16z + 7)/7$
BN curves: $k = 12,\ \rho \approx 1$ $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ $r(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1,\quad t(z) = 6z^2 + 1$
BLS12 curves: $k = 12,\ \rho \approx 1.5$ $p(z) = (z-1)^2(z^4 - z^2 + 1)/3 + z,\quad r(z) = z^4 - z^2 + 1,\quad t(z) = z + 1$
BLS24 curves: $k = 24,\ \rho \approx 1.25$ $p(z) = (z-1)^2(z^8 - z^4 + 1)/3 + z,\quad r(z) = z^8 - z^4 + 1,\quad t(z) = z + 1$

According to the description in https://electriccoin.co/blog/new-snark-curve/, the BN128 curve is conservatively estimated, and the safety factor that can be achieved is only 110-bit, which is not the 128-bit security previously mentioned. To achieve 128- bit security, $q \approx 2384$ is required, and the order r value of the corresponding BN curve will be increased to 2384. The increase of r value will affect the performance of multi-exponentiation, FFT, etc., thus affecting the execution efficiency of zk- SNARKs and secure multiparty computing also affects the unnecessary increase of key files.

The BLS12-381 curve is a more cost effective solution.

According to the report of the Zcash protocol:

5.4.8.2 BLS12-381

The *represented pairing* BLS12-381 is defined in this section. Parameters are taken from [Bowe2017].

Let $q_{\mathbb{S}} := 40024095552216673934177898257359041565568828199390078853320581361240316504908378644426876291290156640378942725597 87.$

Let $r_{\mathbb{S}} := 52435875175126190479447740508185965837690552500527637822603658699938581184513.$

Let $u_{\mathbb{S}} := -15132376222941642752.$

Let $b_{\mathbb{S}} := 4.$

($q_{\mathbb{S}}$ and $r_{\mathbb{S}}$ are prime.)

Let $\mathbb{S}_1^{(r)}$ be the subgroup of order $r_{\mathbb{S}}$ of the group of rational points on a Barreto–Lynn–Scott ([BLS2002]) curve $E_{\mathbb{S}_1}$ over $\mathbb{F}_{q_{\mathbb{S}}}$ with equation $y^2 = x^3 + b_{\mathbb{S}}$. This curve has embedding degree 12 with respect to $r_{\mathbb{S}}$.

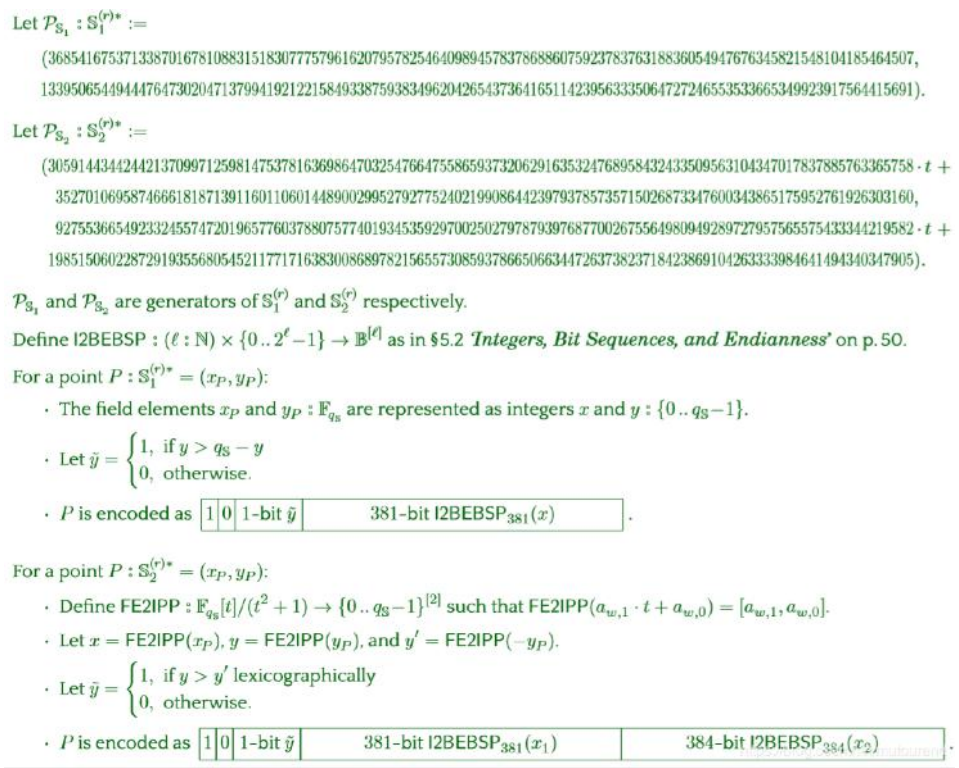
Let $\mathbb{S}_2^{(r)}$ be the subgroup of order $r_{\mathbb{S}}$ in the sextic twist $E_{\mathbb{S}_2}$ of $E_{\mathbb{S}_1}$ over $\mathbb{F}_{q_{\mathbb{S}}{}^2}$ with equation $y^2 = x^3 + 4(i+1)$, where $i : \mathbb{F}_{q_{\mathbb{S}}{}^2}$.

We represent elements of $\mathbb{F}_{q_{\mathbb{S}}{}^2}$ as polynomials $a_1 \cdot t + a_0 : \mathbb{F}_{q_{\mathbb{S}}}[t]$, modulo the irreducible polynomial $t^2 + 1$; in this representation, i is given by t.

Let $\mathbb{S}_T^{(r)}$ be the subgroup of $r_{\mathbb{S}}{}^{\text{th}}$ roots of unity in $\mathbb{F}^*_{q_{\mathbb{S}}{}^{12}}$, with multiplicative identity $\mathbf{1}_{\mathbb{S}}$.

Let $\hat{e}_{\mathbb{S}}$ be the optimal ate pairing of type $\mathbb{S}_1^{(r)} \times \mathbb{S}_2^{(r)} \to \mathbb{S}_T^{(r)}$.

For $i : \{1 .. 2\}$, let $\mathcal{O}_{\mathbb{S}_i}$ be the point at infinity in $\mathbb{S}_i^{(r)}$, and let $\mathbb{S}_i^{(r)*} := \mathbb{S}_i^{(r)} \setminus \{\mathcal{O}_{\mathbb{S}_i}\}$.



Let $\mathcal{P}_{\mathbb{S}_1} : \mathbb{S}_1^{(r)*} :=$

(3685416753713387016781088315183077757961620795782546409894578378688607592378376318836054947676345821548104185464507,
1339506544944476473020471379941921221584933875938349620426543736416511423956333506472724655353366534992391756441569 1).

Let $\mathcal{P}_{\mathbb{S}_2} : \mathbb{S}_2^{(r)*} :=$

(3059144344244213709971259814753781636986470325476647558659373206291635324768958432433509563104347017837885763365758 · t +
3527010695874666181871391160110601448900299527927752402199086442397937857357150268733476003438651759527619263031 60,
9275536654923324557472019657760378807577401934535929700250279787939768770026755649809492897279575655754333442195 82 · t +
1985150602287291935568054521177171638300868978215655730859378665066344726373823718423869104263333984641494340347905).

$\mathcal{P}_{\mathbb{S}_1}$ and $\mathcal{P}_{\mathbb{S}_2}$ are generators of $\mathbb{S}_1^{(r)}$ and $\mathbb{S}_2^{(r)}$ respectively.

Define I2BEBSP : $(\ell : \mathbb{N}) \times \{0 .. 2^\ell - 1\} \to \mathbb{B}^{[\ell]}$ as in §5.2 *'Integers, Bit Sequences, and Endianness'* on p. 50.

For a point $P : \mathbb{S}_1^{(r)*} = (x_P, y_P)$:

- The field elements x_P and $y_P : \mathbb{F}_{q_S}$ are represented as integers x and $y : \{0 .. q_S - 1\}$.
- Let $\tilde{y} = \begin{cases} 1, & \text{if } y > q_S - y \\ 0, & \text{otherwise.} \end{cases}$
- P is encoded as | 1 | 0 | 1-bit $\tilde{y}$ | 381-bit I2BEBSP$_{381}(x)$ |.

For a point $P : \mathbb{S}_2^{(r)*} = (x_P, y_P)$:

- Define FE2IPP : $\mathbb{F}_{q_S}[t]/(t^2+1) \to \{0 .. q_S - 1\}^{[2]}$ such that FE2IPP$(a_{w,1} \cdot t + a_{w,0}) = [a_{w,1}, a_{w,0}]$.
- Let $x =$ FE2IPP(x_P), $y =$ FE2IPP(y_P), and $y' =$ FE2IPP$(-y_P)$.
- Let $\tilde{y} = \begin{cases} 1, & \text{if } y > y' \text{ lexicographically} \\ 0, & \text{otherwise.} \end{cases}$
- P is encoded as | 1 | 0 | 1-bit $\tilde{y}$ | 381-bit I2BEBSP$_{381}(x_1)$ | 384-bit I2BEBSP$_{384}(x_2)$ |.

After comprehensively balancing security and performance, we found that the BLS12-381 curve is q≈2384, so Celare chose the BLS12-381 curve to achieve zero- knowledge proof to ensure true 128-bit security.

By using the non-interactive zk-SNARKs zero-knowledge proof algorithm of BLS12-381, the trading process taking place in Celare is as follows:

Transactions are divided into two categories: transparent addresses and hidden addresses. The input and output of transparent address transactions are directly visible transaction information, which is similar to the current centralized currency trading mechanism.

For hidden address transactions, the address and amount of input and / or output are hidden. The input and output fields are empty and the address is unknown (there are actually inputs and outputs, not none, just not shown).

In addition, the total amount of the transaction only knows "⩾ a certain value", and the specific amount is unknown.

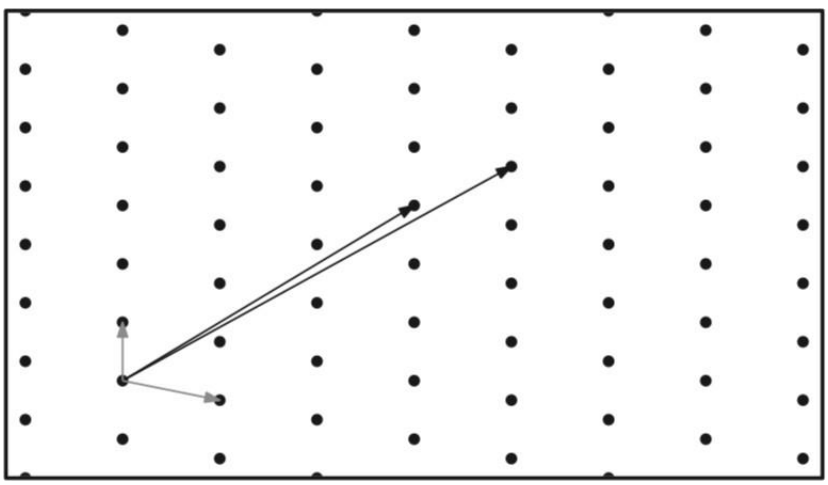
The transparent address and the hidden address can also be mixed. In the transaction of the hidden address, the input and output are no longer clear transaction information, but are the abolition notice and the issuance notification of the transaction information.
This greatly protects Celare's privacy and anonymity.

4.1.5 Full Homomorphic Encryption

Unlike additive homomorphic encryption in most technical solutions, Celare applies a fully homomorphic encryption scheme.

Fully homomorphic encryption supports arbitrary calculation of cipher text without decryption, so it can solve data privacy security problems immediately and has great application requirements. Fully homomorphic encryption not only protects data by encryption, it also does not lose computational power.

In 2009, Gentry proposed a fully homomorphic encryption scheme based on ideal Lattice.The so-called Lattice is the point formed by the linear combination of the whole coefficient base. In layman's terms, it is some discrete and regular points in a space. Since it is a discrete point, there must be a distance between the points, and the distance produces beauty, which leads to some difficult problems, such as the shortest vector problem (SVP).



图：lattice based cryptography

If it is a two-dimensional plane, it is simple to find the shortest vector problem on the lattice. However, when the dimension becomes larger, for example, 200 multidimensional, it is extremely difficult to find the shortest vector problem on the lattice. The problem of standard difficulty is an exponential difficulty. You can imagine that when you are in a maze (the real world is 3D), it is not difficult to find an exit, but when in a 200-dimensional maze, the difficulty level rises exponentially.

There is no quantum algorithm to solve or incite it. Therefore, the standard difficulty problem is considered to be anti-quantum.

The biggest feature of the encryption scheme on the grid: it is a scheme containing noise. Add noise to the encryption when it is encrypted, mainly to further improve security. However, this is exactly the noise, which makes the form of encryption and the form of decryption relatively simple.

The key to Celare's fully homomorphic encryption is the control of noise so that it can decrypt any cipher text. In fully homomorphic encryption, we usually measure the number of calculations by the number of multiplications, because the noise of multiplication is much faster than the addition noise.

4.1.6 Smart Contract

In most of the current decentralized privacy protection Blockchain systems (such as Zcah, Dash, and XMR), there are few matching smart contract systems and less privacy protection for smart contract execution.

Based on Substrate, Celare has a natural bias in supporting smart contracts. The following is an introduction to Celare's smart contract related mechanisms.

About consensus algorithm

Like other parachains, Celare follows Boca's PoS consensus algorithm and contract technology. As a strong cross-chain and high-confidence Celare, in order to maintain data transmission speed and efficiency on the chain, a large-scale PoS node network will be established, which can support nearly a thousand consensus nodes, thereby reducing the outbound time and finalizing the line delay indefinitely. time.

The number of Celare consensus nodes will gradually increase from dozens to nearly a thousand. The consensus node needs to maintain a good network operating environment and computing power to maintain the transmission and stability of Celare network data. It is worth noting that if the block node is delayed due to poor operating environment of the consensus node network, the consensus node will be punished, and the penalty funds will be transferred to the self-government fund. The usage of the fund will be decided by autonomous community through voting.

Celare will follow the DAO autonomy principle to govern the community, adopt a one-vote one-shot model, fully self-governing, and voting users must hold a certain amount of Celare tokens in order to obtain voting rights.

About cross-chain smart contracts

Celare's asset cross-chain logic is that the user locks the asset in the original chain and then issues the mapped asset on the target chain. At the same time, the user can apply for cash withdrawal in the target chain and finally unlock the original chain.

You can understand that assets do not disappear in the original chain, but instead are kept by decentralized node protocols, or managed by a single individual or multi- person. The asset cross-chain mapping here uses the node relay mode. The node relay mode is a truly practical and secure decentralized cross-chain mapping solution. The security of the cross-chain mapping is guaranteed by the original chain consensus algorithm and is the highest level of security. If the original chain cannot integrate the nodes of the target chain, then the original chain assets can only be managed by individual or multiple signed address.

If so, the target chain is hosted by the node protocol on the original chain.

Celare supports high-level languages based on Web Assembly (WASM) compatibility, from C, C++ to Rust, which further enhances system performance, while EVM compatibility is provided in Celare systems (described in subsequent stacks)), then all cross-chain assets also have EVM contract functionality. This has greatly increased the scalability and expressiveness of Celare.

Anyone holding Celare can develop smart contracts on Celare, and contracts can also call other contracts. Of course, it will consume the gas of the Celare system.

4.2The Advantages of Celare

4.2.1.The design of Parachain slot

As a parachain of privacy smart contracts under the Polkadot ecosystem, Celare is able to seamlessly access to other parallel chains under the Polkadot ecosystem. At the same time, Celare is developing BTC, ETH and other cross-chain bridges under the non-Polkadot ecosystem.

Parachain slot

At present, Polkadot is nearly to lauch， and the development of parachains is hot in develpers. Thanks to Celare's parachain slot and cross-chain transaction routing design, Celare can fully access to the Polkadot ecosystem and share the prosperity with other parachains in Polkadot ecosystem.

① Universal chain , Wasm smart contracts (eg Edgeware, Charred Cherry testnet, Shasper on Substrate)
② Transaction chain for fast payment(Blink Network)
③ Predictive chain that provides out-of-chain data for all contracts on the Polkadot network (ChainLink)

④ An identity chain that connects accounts to persistent identities and accesses other parallel chains with fewer accounts(Speckle OS)
⑤ File storage chain, stimulating storage of data on the chain
⑥ Data management network that connects all file storage chains to the planning data set (Ocean Protocol)
⑦ IoT chain, setting the IoT standard for machine-to-machine communication(MXC Protocol)
⑧ The financial chain allows you to hold all your assets in one portfolio, including by bridging Bitcoin, Ethereum, Bitcoin Cash, Litecoin and Zcash (chain of all PoW Consensus and UTXO Transaction Formats) (ChainX，Katallassos)
⑨ A zero-knowledge privacy chain or bridge to the existing ZK-snarks chain (Zcash will be a potential chain built using Polkadot, but it seems to have not yet worked on it)

Interchain transaction routing

Interchain transaction routing is one of the essential maintenance tasks of the relay- chain and its validators. This is the logic which governs how a posted transaction (often shortened to simply “post”) gets from being a desired output from one source parachain to being a non-negotiable in- put of another destination parachain without any trust requirements.

We choose the wording above carefully; notably we don’t require there to have been a transaction in the source parachain to have explicitly sanctioned this post. The only constraints we place upon our model is that parachains must provide, packaged as a part of their overall block processing output, the posts which are the result of the block’s execution.

These posts are structured as several FIFO queues; the number of lists is known as the routing base and may be around 16. Notably, this number represents the quantity of parachains we can support without having to resort to multi-phase routing. Initially, Polkadot will support this kind of direct routing, however we will outline one possible multi-phase routing process (“hyper-routing”) as a means of scaling out well past the initial set of parachains.

We assume that all participants know the sub- groupings for next two blocks n, n + 1. In summary, the routing system follows these stages:

• CollatorS : Contact members of Validators[n][S]
• CollatorS: FOR EACH subgroup s: ensure at
least 1 member of Validators[n][s] in contact
• CollatorS : FOR EACH subgroup s: assume egress[n — 1][s][S] is available (all incoming post data to ‘S ‘ from last block)
• CollatorS: Compose block candidate b for S:
(b.header, b.ext, b.proof, b.receipt, b.egress)
• CollatorS : Send proof information proof[S] = (b.header, b.ext, b.proof, b.receipt) to Validators[n][S]
• CollatorS : Ensure external transaction data b.ext
is made available to other collators and validators
• CollatorS : FOR EACH subgroup s: Send egress information egress[n][S][s] = (b.header, b.receipt, b.egress[s]) to the receiving sub-group’ s members of next block Validators[n + 1][s]
• ValidatorV : Pre-connect all same-set members
for next block: let N = Chain[n + 1][V]; connect
all validators v such that Chain[n + 1][v] = N
• ValidatorV : Collate all data ingress for this block: FOR EACH subgroup s: Retrieve egress[n — 1][s][Chain[n][V]], get from other validators v such that Chain[n][v] = Chain[n][V].Possibly going via randomly selected other validators for proof of attempt.
• ValidatorV : Accept candidate proofs for this
block proof[Chain[n][V]]. Vote block validity
• ValidatorV : Accept candidate egress data for next block: FOR EACH subgroup s, accept egress[n][s][N]. Vote block egress availability; re-publish among interested validators v such that
Chain[n + 1][v] = Chain[n + 1][V].
• ValidatorV : UNTIL CONSENSUS

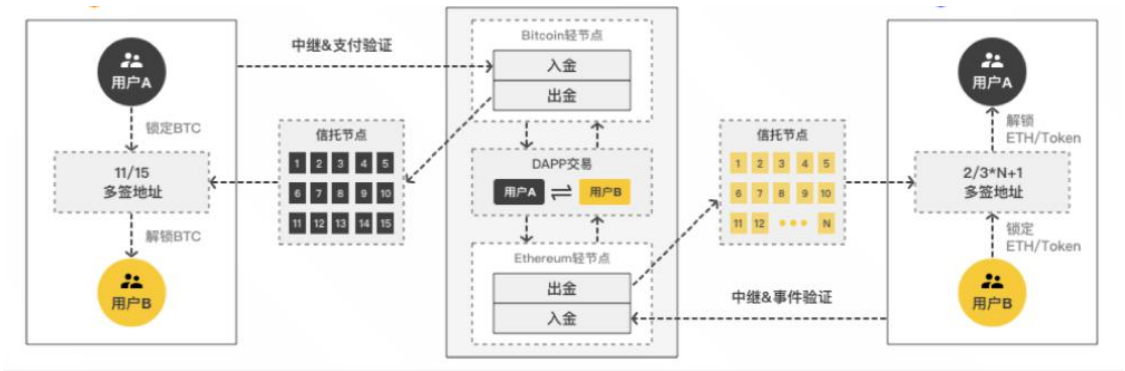
Where: egress[n][from][to] is the current egress queue information for posts going from parachain ‘from ‘, to parachain ‘to ‘ in block number ‘n ‘. CollatorS is a collator for parachain S. Validators[n][s] is the set of validators for parachain s at block number n. Conversely, Chain[n][v] is the parachain to which validator v is as- signed on block number n. block.egress[to] is the egress queue of posts from some parachain block block whose destination parachain is to.

Since collators collect (transaction) fees based upon their blocks becoming canonical they are incentivized to ensure that for each next-block destination, the subgroup’s members are informed of the egress queue from the present block. Validators are incentivized only to form a consensus on a (parachain) block, as such they care little about which collator’s block ultimately becomes canonical. In principle, a validator could form an allegiance with a collator and conspire to reduce the chances of other collators’ blocks becoming canonical, however this is both difficult to arrange due to the random selection of validators for parachains and could be defended against with a reduction in fees payable for parachain blocks which hold up the consensus process.

The above is Celare's principle of cross-chain operation, and for other public chains other than the Polkadot ecosystem, Celare is developing a cross-chain bridge. At present, Celare uses the node bridge method to access other public chains.

Cross-chain mapping

The basic logic is: BTC-Map-P-BTC-Value Anchor-P-ETH-Redemption-ETH.



4.2.2.High Security

Celare's security is guaranteed in two ways: the benefits of Polkadot's security sharing and its own encryption algorithms.

Security sharing with Polkadot

Polkadot itself is not an application, but a commitment to form a secure cross-chain connection to different chains while maintaining security. All parachains based on the Polkadot Ecology are like a highway, Polkadot provides a connection hub for these roads (similar to overpasses, conversion stations), while other public chains, such as BTC, ETH, EOS, etc., are like high-speed railway or It is an airplane, how to connect these vehicles, so that users with different needs globally can communicate freely across the chain, which is what Polkadot has to do.

The premise of implementing cross-chain technology is to ensure security. Therefore, Polkadot has always attached great importance to the security of transit. How does Polkadot provide security to parachains?

The first is that the consensus algorithm is a PoS variant with Byzantine fault tolerance. Simply speaking, because in the current consensus algorithm, PoS with Byzantine fault tolerance is a very advanced consensus algorithm, which has more advantages than POW and POS.

Second, in Polkadot’s verification mechanism, we mentioned that Polkadot has four roles: validator, nominator, collector, and fisherman. It is based on the decision of the fisherman to dig and point out those invalid blocks to ensure the security of Polkadot's network.

Polkadot can provide:
5-7 validator signatures
The fisherman went to find the invalid block If the block proves to be invalid, the validator will be revoked, otherwise, the fisherman will be revoked.
When the fisherman find that a certain block is invalid, they need to pledge some Celare tokens and propose that the block is invalid. Therefore, this block will need to be verified

and reviewed again. If this block is confirmed to be invalid. Then, the DOT tokens will be confiscated, so that the fisherman will be rewarded. Otherwise, the DOT tokens pledged by the fishermen will be confiscated.

Therefore, the security sharing of Polkadot is an advantage for Celare. In addition, Celare itself has the four roles in the system, which has been described in detail in the previous section and will not be described here.

Double verification and phishing enforcement make Celare a very high security.

4.2.3.Privacy

Celare's main concern is privacy. Privacy is the first priority when we do any further developing of smart contract.

In the previous encryption algorithm, we introduced the five major encryption methods of Celare, namely:

① Discrete logarithmic encryption and elliptic curve encryption
② Hash function algorithm
③ Zero-knowledge proof of non-interactive zk-SNARKs
④ BLS 12-381curve
⑤ Fully homomorphic encryption

In addition, the distributed node transmission method also makes the Celare network more flexible, which is the most powerful guarantee for decentralization.

4.2.4.Support smart contracts

Developed on Substrate, Celare wants to build a fair-distributed, POS-based WebAssembly smart contract platform.

Developed on Substrate, Celare wants to build a fair-distributed, POS-based WebAssembly smart contract platform.

Smart contracts are one of the important technical foundations of value Internet networks, but the current frustrating situation is that the Blockchain systems currently running around the world do not support encryption protection for smart contracts, and the existing privacy protection mechanisms are used is greatly reduced by the influence of this technical limitation.

However, the emergence of Celare has broken this restriction, not only with privacy and cross-chain capabilities, but also supports smart contract development on the chain.

4.3.Celare’s extensible scenarios

Since the development of Blockchain technology, there are many imperfections. However, it can be seen that all individual teams and communities that have faith in the Blockchain are actively promoting the healthy development of Blockchain ecology.

On the one hand, there is a strong demand of cross-chain interaction, on the other hand, the need to protect privacy is increasing, the emergence of Celare will greatly change the status.

4.2.4.Support smart contracts

Developed on Substrate, Celare wants to build a fair-distributed, POS-based WebAssembly smart contract platform.

Privacy protection is a strong demand for individuals and organizations in the real world. Celare supports Turing's comprehensive smart contracts, cross-chain asset transactions and various related privacy protections to support the expansion of different economic ecosystems. Starting with the Celare system, the issuance and control of anonymous assets will no longer be exclusive to a few geeks who have deep knowledge of cryptography. Ordinary

developers can issue their own assets on the Celare chain as long as they have relevant business needs. Anonymous assets, establish their own privacy ecology, which greatly expands the scope of application of Blockchain privacy protection technologies, such as the following scenarios:

AI The convergence of AI and Blockchain is now more at the data level, while AI needs data to train. In the past two years, Blockchain projects have used Token to motivate everyone to contribute data, but AI needs data, especially for special industries. The data is sensitive data, and Celare's protection of private data will have great application value, which is helpful for AI to process data. In addition, the integration of Blockchain and IoT technology is promising. For example, smart terminals in the future will be different. It is not only the action of completing the similar power payment, because the smart device itself generates data, so when others use its data. Need to pay, this cost is not necessarily money, it may be a value measure that the demand side and the supply side agree with each other, but it is certain that this value measure is difficult to reflect through the existing legal currency, and Celare can fills the gap.

Medical healthIn the health care-related industry, data privacy is reflected in all aspects, from individual cases to medical records, for multi-color privacy protection and authorization mechanisms that require flexible and secure privacy protection, involving hospitals, patients, Insurance companies, pharmaceutical companies, etc., data privacy protection and restrictions on the use of authorization is particularly important. The Celare system addresses the privacy issues faced by patients and hospitals, and opens the door for insurance companies and pharmaceutical companies to use security and compliance with patient data.

Supplychain system The Blockchain can solve the problem of upstream and downstream transaction vouchers and traceability of the supply chain system, simplify the management of supply chain center enterprises and provide corresponding solutions for financing of upstream and downstream enterprises. However, sensitive data such as prices and goods are facing the problem of leaking trade secrets when they are on the chain. With the Celare system, the problem of exposure to trade secrets can be completely solved, and at the same time, the participating parties can enjoy the benefits brought by the application Blockchain system.

Online auction In many online auctions that pursue fairness, the privacy of bids is very important, but it is often difficult to do so, and Celare can provide a completely secure, independent and fair bidding system.

Online gaming The development of the online gaming industry has always been constrained by the centralization mechanism. In this huge cash flow industry, there is a great need for a decentralized smart contract system that can provide multi-person bidding, payment, and settlement. Celare The system can fully support this type of business.

Games Large-scale games often require a monetary system that is easy to circulate, trade, and settle, and can be issued and circulated based on smart contracts, while also taking into account the privacy protection of transactions. At present, Celare is the only technical solution that can achieve multi-currency system based on the same smart contract system to issue and distribute, and take into account of transaction privacy.

Of course, there are more industries involved in the digitization of assets and related to the privacy of digital assets, such as insurance industry, metals trading, futures trading, digital asset trading (such as credit reporting and intellectual property), and credit industries and so on.

In these areas, the Celare system is very useful!

4.4.Celare’ s Technical Vision

When you look back at the development of the Blockchain for 10 years, you will find that dreams, especially technical dreams, if realized, will be a good thing for the benefit of human, so there will be so many technical geeks going forward bravely to to liberating all human.

Let's take a look at what the technical vision of the former people in the Blockchain has been:

BTC: Internet payments should be as real as the real world cash, even if there is no bank, everyone in the network can prove that a transfer is true and effective.

ETH: The network is like a super computer. We can not only exchange money, but also handle information, work and life in a peer-to-peer manner.

LTC: Bitcoin is expensive and slow, and we are cheap and fast.

XRP: Banks are not required. Credits between countries can be settled point-to-point. As for the rest, we have the final say.

EOS: The world can't be completely without a center, so the efficiency is too low, free transfer, efficiency is the king, find the balance between decentralization and centralization, we are serious.

The appearance of Polkadot has the spirit of unifying all the chains.

Polkadot: Security and cross-chain are our mission.
And Celare's technical vision is simple: security, privacy and cross-chain.

To realize this technology vision, we need both of the Celare Co-Founders Committee and support from peers.
Celare will bring together all parachain developers and community to witness the first big fusion in the history of Blockchain. The Blockchain is no longer an isolated island, no longer competing for users, and Polkadot will lead the world's developers to witness the arrival of the cross-chain era.

5.ECOLOGY

5.1.All Assets Anonymity

General privacy transaction
In Celare, the data in the ordinary transaction is encrypted, and the non-transaction parties cannot know the details such as source, destination, asset type, and amount. The system does not distinguish between the assets generated by the smart contract and the assets of Celare itself when the transaction is processed.

Online privacy assets
Smart contracts are assets that are issued by calling the online private asset issuance method. The total amount of assets is public and has the same trading attributes as Celare coins, which can be processed through general privacy transactions.

Offline privacy assets
The assets issued by the user by using the offline private asset issuance method, the total number of assets is not shown, and has the same transaction attributes as the Celare currency, which can be processed through the general privacy transaction.

Regardless of the assets, Celare can fully guarantee the privacy and anonymity of assets, and truly realize the anonymity of all assets.

5.2.Anonymous asset exchange

Before the cross-chain technology really came, to achieve the cross-chain assets flow and trading, we cannot leave out the centralized exchanges, but the use of KYC makes these centralized exchanges out of control in privacy and asset anonymity.

Celare is a veritable anonymous asset exchange through Polkadot relay cross-chain technology, which fully protects user privacy and asset anonymity.

5.3.Anonymous chat tool with OTC

The essential problem to be solved by the Blockchain is decentralization, such as centralized trading, centralized storage, and centralized socialization.

Therefore, Celare hopes to bring users an anonymous chat tool that combines OTC functions.

One of the essence of Celare's is anonymous chat, and it is a secure anonymous channel that breaks the Internet blockade and does not require a VPN.

The so-called anonymity is not only the authentication without personal identity information, but also the hidden high-anonymity Celare of the communication channel uses distributed nodes to support the entire network operation. The node itself has a layer of port encryption, so that the primary node IP will not be exposed.

Not only that, in the process of using covert chat, no third party stores the message content, and the chat content will only be stored in the local file. The master node is only responsible for providing network transmission and content delivery.

This is closer to the offline communication between people: the main node is like the air, responsible for spreading the sound, and the other two are left behind, which is safer than storing the chat content on the centralized server.

On the basis of peer-to-peer anonymous chat, Celare users and groups in the community can independently launch OTC (over-the-counter transaction), and the transaction information and chat content are

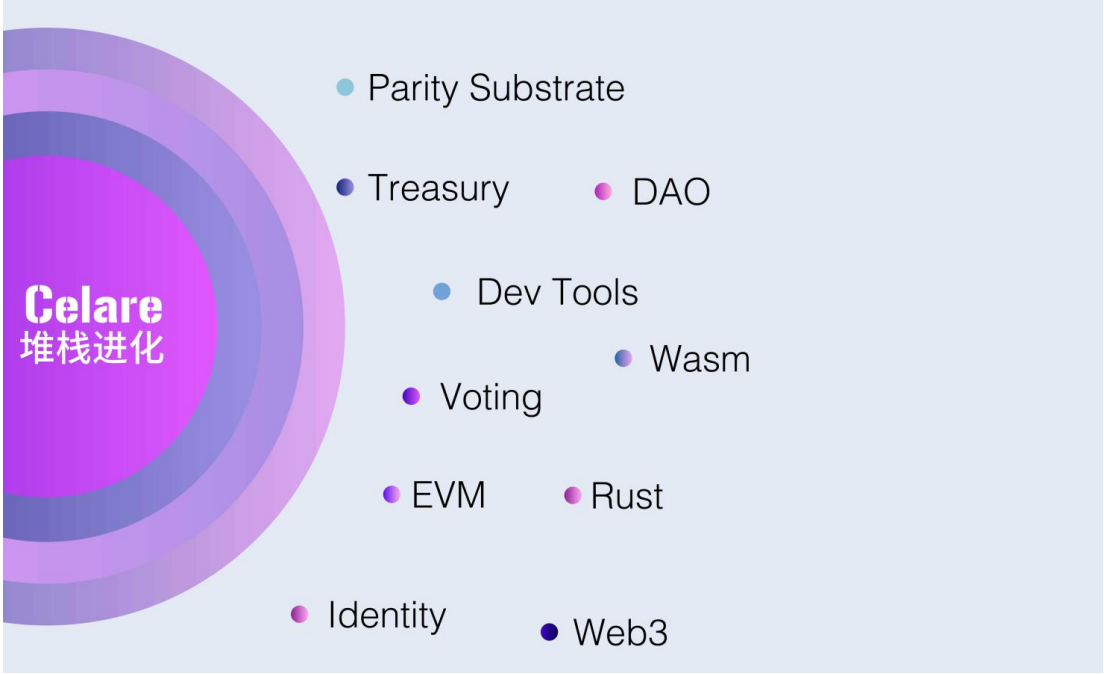
completely secret, without worrying about being supervised or eavesdropped, to protect user privacy and security for entire Celare ecosystem.

5.4.Stack extension

If you look at what is happening now from the perspective of the future, just like the Internet that emerged in the 1990s, it is also a variety of technological update iterations. Every entrepreneur with dreams of improving traditional industries. And they realized it.

Today's technological innovation represented by Blockchain is hot as well. Today, we are changing the Internet technology that we have been proud of. Because the Internet has developed so far, there have been too many restrictions on our freedom and control. There are things that must change.

Here is the stack ecology diagram that has evolved and absorbed in the Celare development process:



Parity Substrate

Parity Substrate is a project independent of Polkadot. Developers can use Substrate to build a new Blockchain without having to wait for Polkadot to complete the development, or even to wait for proof of concept release, to start developing the Blockchain using this framework.

Celare is a parachain of Poikadot developed based on Substrate. It follows the standard Parity Substrate API. Before launching of Polkadot, Celare can run independently. After Polkadot launched, it shares the security and cross-chain functions of Polkadot.

Wasm（webassembly）

WebAssembly or wasm is a new, portable, small, fast-loading, web-compatible format.

Wasm is completely grammatically out of JavaScript and has a sandboxed execution environment. The same mandatory static type for WebAssembly is the compilation target for C/C++/Rust.

Because of its superior performance, WebAssembly is used in large projects such as AutoCAD, GoogleEarth, Unity, Unreal, PSPDKit, and WebPack. Therefore, Celare's smart contract portion will use Wasm.

Based on a new generation of universal WASM smart contract technology, Celare can develop and deploy various Dapps.

Currently, runtime contract development can be supported, and contract development will be supported later. Developers can use any language that can be compiled into WASM for development, but the development support for Rust will be perfect in the early days. The current chain performance can reach hundreds of TPS, and has a full state root verification.

The system-integrated cross-chain asset transaction will adopt the free transfer mode, without any percentage form of matching fee. Celare's

completely decentralized community business model will not have centralized interests and truly become the user's own system.

Various applications developed by community developers can freely design economic models and application scenarios, such as BTC-secured stable currency, privacy payment system by using Celare, and various games or high-end financial derivatives services.

DAO

DAO is a decentralized autonomous organization. The goal is to create code for decentralized management structures by writing code for organizational rules and decision-making bodies, eliminating the need for written documents, and reducing administrators.

The Celare Co-Founders' Committee is only the early initiator of the Celare project, and we firmly believe that the entire Celare's ecological development need support from all ecological participants.

Celare's ecology can complement each other, and with the development of the Celare ecosystem, communities need to coordinate beyond the initial governance structure of the network. Ecological governance will follow the principle of decentralization and adopt a way of community autonomy. This is the spirit of decentralized autonomous organization - DAO. This allows for the exploration of alternative decision structures without changing core governance. For example, DAO can follow the decision- making process, including one person one vote, delegate vote, second vote, and more complex models.

To promote decentralized governance in the community, the Celare Council will be expanded to include a node community that has matured. As the initial development team of Celare and the organizer and implementer of future system upgrades, the Celare Co-Founders' committee will retain one parliamentary seat and add 10 parliamentary seats. The 10 parliamentary seats are held by the honesty nodes who are the top 10 votes and intend to join the

parliament. Any node that has a bribe- rewarding will not be able to participate in the parliamentary elections.

Since the total number of votes of the nodes changes frequently, the parliament needs to maintain a certain fixed group for a certain period of time, so the term of each parliament is one month. After the expiration of each term, the next member of the Parliament will be elected based on the new total number of votes and the integrity of the node. Eleven members of the parliament can collect community feedback and submit any proposals to the parliament. The proposal is voted by the members of the parliament by voting (one person one vote) , and if more than half of the members agree (greater than or equal to 6), the proposal passes the preliminary examination. The referendum will enter the public process, and the referendum needs to be greater than or equal to 2/3 to pass the vote (greater than or equal to 66.67%). After passing, it will be implemented and launched by the Celare Co-founder’ s committee team.

Since bribery and rebates seriously affect the credibility of the total number of votes, and increase the risk of the node's evil behavior in the future, the parliamentary seats obtained through improper means will seriously hinder the overall interests of the community.

Therefore, the parliamentary fund has opened bribery and fishing rewards. The standard of bribery is very clear. There can be no rebates. Any member of the community can anonymously submit screenshots or transfer records of bribery and rebates at a certain node. If more than half of the members think that the evidence is valid (greater than or equal to 6), the election qualification of the next member of the node will be removed, and the report will be rewarded as appropriate from the parliamentary fund. In addition, the parliament will have the right to punish the self- collateral of the bribery node. The nodes claiming not to participate in the parliamentary elections are not in the scope of reporting, but still hope that all nodes maintain fair and open election rules, guiding the community to vote by contribution, rather than vicious competition for short-sighted rebates.

Treasury

Treasury is a community fund on the Celare chain that is an important part of the incentive distribution within the system and is relevant to all participants.

In many Blockchain systems, validators contribute to the system by paying more time and effort, and they are usually the only motivated stakeholders, such as BTC miners.

But Celare is a more inclusive and open system, so we will use block rewards to motivate all stakeholders.

Initially, 50% of community funds came from block rewards. Celare holders can assign incentive votes to:

① Core technology: Perform scalability technology development, such as improvements during operation, fragmentation and chain expansion.
② Governance: Governance systems, including chain identity and organization and coordination of core developer work.
③Developer Testing: Used to develop, debug, and test smart contracts.
④ User testing: Wallets and user experience primitives (for example, JavaScript libraries) make decentralized applications easy to use.
⑤Ecosystem Support: Organize support for live activities by developers, users, and other stakeholders.

Dev Tools

There are many tools available for Blockchain developers, and Parity is one in this. Parity is one of the fastest and safest ways to interact with Blockchains. It was founded by the former CTO of Ethereum, Gavin Wood, and written in the Rust programming language.

Of course, there are many tools, such as Solidity, Remix IDE, Text Editors, SoLC — Solidity Compiler, Solium, Geth, MetaMask, Truffle, DAppBoard, etc., all of which are good Blockchain development tools.

Celare has the ability to develop smart contracts thus so many developers will come together to develop smart contracts and Dapp.

Celare supports a variety of development tools in order to attract many outstanding developers to build the Celare ecosystem.

Voting

Celare will follow the DAO autonomy principle to govern the community, adopt a one person one vote model, fully self-governing, and voting users must hold a certain amount of Celare tokens in order to obtain voting rights.

The voting mechanism is often used in Celare, especially anonymous voting on the chain. The specific voting scenarios and related mechanisms are as follows:

① Anonymous voting: Celare users can vote anonymously, which prevents the brushing behavior and requires encryption primitives to be implemented at the protocol level.
② Node voting: When electing Celare's nodes, node voting is used to determine the candidate and winner of the node.
③ Verifier Vote: After the validator completes the verification of the candidate block, it votes on the block header hash and sends the necessary verification information to the other co-validators in the group.
④ The distribution of community fund awards can be determined by community vote.

Rust

As a system programming language, Rust focuses on security, especially concurrent security, to provide robust maintenance for the entire platform. Smart contracts on Celare can be written in any high-level WASM-compatible language, including C, C, and Rust. At the same time, Celare is compiling a subset of JavaScript into a standalone tool on WASM through the AssemblyScript project. Benefiting from WASM, this means that Celare is friendly to most developers.

Celare's smart contracts will also interact with some of the whitelisted contracts and developers' modules to perform functions like querying accounts in the identity and board modules.

EVM

The Environment Virtual Machine (EVM) is used to compile smart contract code into machine code that can be executed on Ethereum and to provide a smart contract runtime environment. It is a completely isolated sandbox environment that does not have access to networks and files during runtime, even with limited access between different contracts.

The use of high-level programming languages that are constantly being upgraded allows more and more developers to focus on the application itself, making it easier and faster to develop decentralized applications, while greatly reducing the difficulty of development.

Because the EVM compatibility is provided in the Celare system (described in the subsequent stack), all cross-chain assets also have EVM contract functionality. This has greatly increased the extensibility and expressiveness of Celare.

Identity

We know that in the Internet, mail and mobile phone numbers are the de facto standard for common user authentication. Many websites and Apps can identify these authentications, but there is no such extensive identification system in Blockchain.

In Celare, we know that there are at least six identities: validators, collators, nominators, fisherman, consensus nodes, and users. At the same time, in many scenarios, users who need Celare vote according to their own identity.

Therefore, the establishment of identity standards will be related to the rights and obligations of all participants in the celare system.

To this end, Celare has established a set of its own identification system. This identification system is divided into public functions and privacy features.

The privacy function identity is similar to the address and private key of the current Blockchain system. When a transaction occurs, an anonymous vote is required, etc., you can choose to log in to the private identity.

The public function in the identity module allows account registration and verification.

Once the user is registered, the individual can prove by connecting to an external third party. such as:

Github: Identity is Github username. After the username is registered, the registrar should post a Github Gist certificate under the username's account with the Celare registration link.

Ethereum: Identity is Ethereum public key or address. After the username is registered, the user should send 0 ETH to the address of its corresponding Celare account and submit a hash value as a proof. At the time of the inspection, the validator should have sufficient proof that if the owner of the Ethereum account does not have a Celare account, they will not issue such a transaction.

Web 3

The Internet has undergone a major transformation before. These shifts have expanded performance, functionality, and scale, moving from textual Internet to streaming video and Internet, from static web pages to full-featured applications, from list services to global social networks, and driving modern political and cultural development.

As the network matures, we gradually tend to rely on a few companies. Google offers the fastest and most convenient search service, with 74% control over search traffic. Facebook built the largest social network and gained control of the online identity of 2.2 billion people.

Web3 is different from the previous generation of Internet transformation. The core of Web 3 is not speed, performance or convenience. In fact, many Web 3 applications are very slow and inconvenient compared to today's applications.

Web3 is about control. It is about who controls the technology and our everyday applications. It is breaking the momentum that shaped the network for nearly a decade: the balance between convenience and control. We are used to this motivation and think that everything is taken for granted: using the network means being monitored, and using social networks means that we pass personal data to the platform. How can there be other ways?

But Web 3 refused to accept it, and it believes it can benefit from the Internet, but there is no need to hand over control to a few companies. The above motivation is not the law of the universe. It is only the product of science and technology in the circumstances, and it is the choice we made in this process.

Web3 is a movement that aims to build different technologies to make better choices. Web 3 is not trying to replace the network, but to keep the things we like while changing its underlying framework - reform, not revolution.

Web 3 is a set of technologies designed to refactor Internet control. These include financial items (cryptocurrency), basic communication technologies (end-to-end encrypted messaging), mass consumption scenarios (open social networks, p2p markets), and key Internet facilities (decentralized DNS).

Web3 includes not only cryptocurrencies, Blockchains, and other products based on cryptographic economics. It contains any technology that helps change Internet centralization and gives users control over digital life.

The concept of Web3 was proposed by Dr. Gavin Wood, co-founder of Ethereum. Later, he created Parity Substrate and Polkadot, and incorporated the ecology of polkadot and other technologies that are consistent with the Web 3 concept into Web 3.

Celare is an important parachain in the Boca ecosystem and an outstanding contributor to the development of Web 3. It is hoped that in the near future, users will have control over their own privacy and data.

6.TOKEN MECHANISM

6.1.Token Name

CELARE

Celare is the basic unit of circulation within the Celare ecosystem. It also represent of users and participants in the system, and is the only commercial and financial delivery medium within the system.
At the beginning of the release, it is compatible with ERC20, and will be switched after the Celare network launch officially.

6.2.Token Distribution

Total	100%	200 Million	ERC 20 Token, will switch to Celare network after launching officially
Entangled Lockdrop	50%	100 Million	Participants only need to lock USDT for a certain period of time in the smart contract to get the token reward, and redeem the locked 100% USDTafter main network launched. Donating USDT each time can accelerate the unlocking process and the USDTconsumed by donating cannot be redeemed.
POS Staking	40%	80 Million	After Celare launching, it will take a stake. Vote for mining. The specific rules will be announced after launching
Team	5%	10 Million	Public team address and unlocked in 4 years
Commu nity	3%	6 Million	A community-oriented economic model, rewards + discounted prices for community contributors.
Ecology	2%	4 Million	News media, self-media, ecological construction, code auditing, code contribution, community organizer, Meet-up activities.

6.3.Ecological Rewards

Ecological Rewards include news media, self-media, ecological construction, code auditing, code contribution, community organizer, meet-up activities and so on.

Celare Co-founders' committee convinces that any project cannot be separated from ecological contributors. The Celare Foundation will award a total of 5% of the token to reward ecological contributors, including code auditors and contributors, exchange partners, premium Blockchain media, Blockchain KOL and meet-up activities.

The official will update the details of specific rewards.

7. ROADMAP

Celare's development is independent of Polkadot and link to it as well. Polkadot will launch the main network in the second and third quarter of this year, focusing on the communication among new chains in the Polkadot ecosystem. For the existing Blockchains, it will build a Ethereum contract bridge to integrate Ethereum into the Polkadot network and others chains will be handled by the community in terms of integration.

Parachains can be developed using different types of Blockchain underlying technologies. The relay chain is re- sponsible for the shared security consensus across the network and the inter-chain transaction of parachains.

Preparing

- 2019.03

The Celare Co-Founders' Committee was established and conduct project feasibility report on the Polkadot parachain.

- 2019.05

Determine the project framework and carry out the underlying technology research.

- 2019.06

Finish the underlying logical and technical framework designing.

- 2019.08

Confirm the project concepts Whitepaper released

- 2019.Q4

Beta Network in Version 1 release
Celare will recite the global community as a standalone chain

Before **Polkadot Launching**

- 2020.Q1

Start Entangled Lockdrop

After **Polkadot Launching**

- 2020.Q2

Launch the Beta network in Version 1
Build the transfer bridges with the main-stream chains
* Support for general transaction
* Support for smart contract
* Full asset anonymity

- 2020.Q3

Celare will add a new transfer bridge chain as a parallel chain of Polkadot to connect Polkadot assets.

- 2020.Q4

Celare will evolve into a multi-chain architecture and operate as the second-layer relay network of Polkadot.

- 2021.Q1

Celare will continue to support the community in developing various DApps.
* Code open source, support smart contracts to issue anonymous assets
* Publish client wallet
* Multi-party secure computing and privacy protection mechanisms for data under the chain.
*Anonymous Asset Exchange
*Anonymous chat tool with OTC

8. APPENDIX

Disclaimer

PLEASE READ THIS SECTION AND THE FOLLOWING SECTIONS ENTITLED "DISCLAIMER OF LIABILITY", "NO REPRESENTATIONS AND WARRANTIES", "REPRESENTATIONS AND WARRANTIES BY YOU", CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS", "MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS", "NO ADVICE", "NO FURTHER INFORMATION OR UPDATE", "RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION", "NO OFFER OF SECURITIES OR REGISTRATION", "RISKS AND UNCERTAINTIES", "REGULATORY CONCERNS", "MARKET RISK" AND "CELARE TOKEN VALUATION" CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

The Celare tokens are not intended to constitute securities in any jurisdiction. This whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.
This whitepaper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by the distributor and/or issuer of the Celare tokens ("Issuer") to purchase any Celare tokens nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision.
No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of the Celare tokens and no cryptocurrency or other form of payment is to be accepted on the basis of this whitepaper.

Any agreement as between the Issuer and you as an acquirer of the Celare tokens (as referred to in this whitepaper) is to be governed by a separate document setting out the terms and conditions ("T&Cs") of such agreement. In the event of any inconsistencies between the T&Cs and this whitepaper, the T&Cs shall prevail.
You are not eligible, and you are not to acquire any Celare tokens if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America, or a citizen or resident of the People's Republic of China, the Republic of Singapore or the Republic of Korea (South Korea) or any other jurisdiction where you are not legally permitted to acquire any Celare tokens.

No regulatory authority has examined or approved of any of the information set out in this whitepaper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

This whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this whitepaper is prohibited or restricted.

No part of this whitepaper is to be reproduced, distributed or disseminated without including this section and the following sections entitled, "Disclaimer of Liability", "No Representations and Warranties", "Representations and Warranties By You", "Cautionary Note On Forward-Looking Statements", "Market and Industry Information and No Consent of Other Persons", "Terms Used", "No Advice", "No Further Information or Update", "Restrictions On Distribution and Dissemination", "No Offer of Securities Or Registration", "Risks and Uncertainties", "Regulatory Concerns", "Market Risk" and "Celare Token Valuation".

"REGULATORY CONCERNS", "MARKET RISK" AND "Celare TOKEN VALUATION" DISCLAIMER OF LIABILITY

To the maximum extent permitted by the applicable laws, regulations and rules, the Issuer or the associates or affiliates of the Issuer shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this whitepaper or any part thereof by you.

NO REPRESENTATIONS AND WARRANTIES

The Issuer or the associates or affiliates of the Issuer does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this whitepaper.

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this whitepaper or such part thereof (as the case may be), you represent and warrant to the Issuer or the associates or affiliates of the Issuer as follows:

A. you agree and acknowledge that the Celare tokens do not constitute securities in any form in any jurisdiction;
B. you agree and acknowledge that this whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities in any jurisdiction or a solicitation for investment in securities and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this whitepaper;
C. you agree, acknowledge and confirm that no regulatory authority has examined or approved of the information set out in this whitepaper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this whitepaper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;
D. you agree and acknowledge that this whitepaper, the undertaking and/or the completion of the issuance of Celare tokens, or future trading of the Celare tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of the Issuer or the associates or affiliates of the Issuer and/or the Celare tokens; and
E. the distribution or dissemination of this whitepaper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession is applicable, you have observed and complied with all such restrictions at your own expense and without liability to the Issuer or the associates or affiliates of the Issuer;
F. you agree and acknowledge that in the case where you wish to acquire any Celare tokens, the Celare tokens are not to be construed, interpreted, classified or treated as:

•any kind of currency other than cryptocurrency;

•debentures, stocks or shares issued by any person or entity (whether the Issuer or the associates or affiliates of the Issuer);

•rights, options or derivatives in respect of such debentures, stocks or shares;

•rights under a contract for differences or under any other contract for the purpose or pretended purpose of which is to secure a profit or avoid a loss;

•units in a collective investment scheme;

•units in a business trust;

•derivatives of units in a business trust;

•any other security or class of securities; or

•an investment contract.

G. you are fully aware of and understand that you are not eligible to acquire any Celare tokens if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the People's Republic of China, the Republic of Singapore or the Republic of Korea (South Korea);
H. you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, Blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, Blockchain technology and smart contract technology;
I. you are fully aware and understand that in the case where you wish to acquire any Celare tokens, there are risks associated with the Issuer or the associates or affiliates of the Issuer, and their respective business and operations, and the Celare tokens.
J. you agree and acknowledge that neither the Issuer or the associates or affiliates of the Issuer is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this whitepaper or any part thereof by you; and all of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession this whitepaper or such part thereof (as the case may be).

CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

All statements contained in this whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Issuer or the associates or affiliates of the Issuer or their respective directors, executive officers or employees acting on behalf of the Issuer or the associates or affiliates of the Issuer (as the case may be), that are not statements of historical fact, constitute "forward-looking statements". Some of these statements can be identified by forward-looking terms such as "aim", "target", "anticipate", "believe", "could", "estimate", "expect", "if", "intend", "may", "plan", "possible", "probable", "project", "should", "would", "will" or other similar

terms. However, these terms are not the exclusive means of identifying forward- looking statements. All statements regarding Celare token, the Issuer or the associates or affiliates of the Issuer’ s financial position, business strategies, plans and prospects and the future prospects of the industry which the Issuer or the associates or affiliates of the Issuer is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to the Issuer or the associates or affiliates of the Issuer’ s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this whitepaper regarding the Issuer or the associates or affiliates of the Issuer are matters that are not historical facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of the Issuer or the associates or affiliates of the Issuer to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others:

A. changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which the Issuer or the associates or affiliates of the Issuer conducts its respective businesses and operations;
B. the risk that the Issuer or the associates or affiliates of the Issuer may be unable or execute or implement their respective business strategies and future plans;
C. changes in interest rates or exchange rates of fiat currencies and cryptocurrencies;
D. changes in the anticipated growth strategies and expected internal growth of the Issuer or the
associates or affiliates of the Issuer;
E. changes in the availability and fees billable to the associates or affiliates of the Issuer or the associates or affiliates of the Issuer;
F. changes in the availability and salaries of employees who are required by the Issuer or the associates or affiliates of the Issuer to operate their respective businesses and operations;
G. changes in preferences of customers of the Issuer or the associates or affiliates of the Issuer;
H. changes in competitive conditions under which the Issuer or the associates or affiliates of the Issuer operate, and the ability of the athe Issuer or the associates or affiliates of the Issuer to compete under such conditions;

J. war or acts of international or domestic terrorism;

K. occurrences of catastrophic events, natural disasters and acts of God that affect the businesses
and/or operations of the Issuer or the associates or affiliates of the Issuer;
L. other factors beyond the control of the Issuer or the associates or affiliates of the Issuer; and any risk and uncertainties associated with the Issuer or the associates or affiliates of the Issuer and their businesses and operations, or the Celare tokens.
All forward-looking statements made by or attributable to the Issuer or the associates or affiliates of the Issuer, or persons acting on behalf of the Issuer or the associates or affiliates of the Issuer are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or
achievements of the Issuer or the associates or affiliates of the Issuer, to be materially different from that expected, expressed or implied by the forward-looking statements in this whitepaper, undue reliance must not be placed on these statements. These forward- looking statements are applicable only as of the date of this whitepaper.
Neither the Issuer or the associates or affiliates of the Issuer, nor any other person represents, warrants and/or undertakes that the actual future results, performance or achievements of the Issuer or the associates or affiliates of the Issuer, will be as discussed in those forward-looking statements. The actual results, performance or achievements of the Issuer or the associates or affiliates of the Issuer may differ materially from those anticipated in these forward-looking statements. Nothing contained in this whitepaper is or may be relied upon as a promise, representation or undertaking as to the future performance or policies of the Issuer or the associates or affiliates of the Issuer. Further, the Issuer or the associates or affiliates of the Issuer disclaim any responsibility to update any of those forward-looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future .

MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS

This whitepaper includes market and industry information and forecasts that have been obtained from internal surveys, reports and studies, where appropriate, as well as market research, publicly available information and industry publications. Such surveys, reports, studies, market research, publicly available information and publications generally state that the information that they contain has been obtained from sources believed to be reliable, but there can be no assurance as to the accuracy or completeness of such included information.

Save for the Issuer or the associates or affiliates of the Issuer and their respective directors, executive officers and employees, no person has provided his or her consent to the inclusion of his or her name and/or other information attributed or perceived to be attributed to such person in connection therewith in this whitepaper and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information by such person and such persons shall not be obliged to provide any updates on the same.

While the Issuer or the associates or affiliates of the Issuer have taken reasonable actions to ensure that the information is extracted accurately and in its proper context, the Issuer or the associates or affiliates of the Issuer have not conducted any independent review of the information extracted from third party sources, verified the accuracy or completeness of such information or ascertained the underlying economic assumptions relied upon therein.

Consequently, neither the Issuer or the associates or affiliates of the Issuer, nor their respective directors, executive officers and employees acting on their behalf makes any representation or warranty as to the accuracy or completeness of such information and shall not be obliged to provide any updates on the same.

TERMS USED

To facilitate a better understanding of the Celare tokens, and the businesses and operations of the Issuer or the associates or affiliates of the Issuer, certain technical terms and abbreviations, as well as, in certain instances, their descriptions, have been used in this whitepaper. These descriptions and assigned meanings should not be treated as being definitive of their meanings and may not correspond to standard industry meanings or usage.

Words importing the singular shall, where applicable, include the plural and vice versa and words importing the masculine gender shall, where applicable, include the feminine and neuter genders and vice versa. References to persons shall include corporations .

NO ADVICE

No information in this whitepaper should be considered to be business, legal, financial or tax advice regarding the Issuer or the associates or affiliates of the Issuer and/or the Celare tokens. You should consult your own legal, financial, tax or other professional advisor(s) regarding the Issuer or the associates or affiliates of the Issuer and/or the Celare tokens and their respective businesses and operations. You should be aware that you may be required to bear the financial risk of holding Celare tokens for an indefinite period of time.

NO FURTHER INFORMATION OR UPDATE

No person has been or is authorized to give any information or representation not contained in this whitepaper in connection with the Issuer or the associates or affiliates of the Issuer and their respective businesses and operations, the Celare tokens and, if given, such information or representation must not be relied upon as having been authorized by or on behalf of the Issuer or the associates or affiliates of the Issuer. Nothing in this whitepaper shall, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of the Issuer or the associates or affiliates of the Issuer or in any statement of fact or information contained in this whitepaper since the date hereof.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION

The distribution or dissemination of this whitepaper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this whitepaper or such part thereof (as the case may be) at your own expense and without liability to the Issuer or the associates or affiliates of the Issuer. Persons to whom a copy of this whitepaper has been distributed or disseminated, provided access to or who otherwise have the whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

NO OFFER OF SECURITIES OR REGISTRATION

This whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this whitepaper. Any agreement in relation to any acquisition of Celare tokens (as referred to in this whitepaper) is to be governed by only the T&Cs of such agreement and no other document. In the event of any inconsistencies between the T&Cs and this whitepaper, the T&Cs shall prevail. You are not eligible to acquire any Celare tokens if you are a citizen, resident (tax or other-wise) or green

card holder of the United States of America, or a citizen or resident of the People’ s Republic of China or a citizen or resident of, the Republic of Singapore or the Republic of Korea (South Korea). No regulatory authority has examined or approved of any of the information set out in this whitepaper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

RISKS AND UNCERTAINTIES

Prospective acquirers of Celare tokens (as referred to in this whitepaper) should carefully consider and evaluate all risks and uncertainties associated with the Issuer or the associates or affiliates of the Issuer and their respective businesses and operations, the Celare tokens, all information set out in this whitepaper and the T&Cs prior to any acquisition of Celare tokens. If any of such risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of the Issuer or the associates or affiliates of the Issuer could be materially and adversely affected. In such cases, you may lose all or part of the value of the Celare tokens.

REGULATORY CONCERNS

Blockchain technology, including the issue of Blockchain-based tokens, is a whole new concept to certain regulatory jurisdictions. As such, there exist a situation where new regulations or rules may apply to Blockchain application and it is inherently possible that these new regulations may conflict with Celare smart contract script & application. However, it is important to note that it might require an adjustment and it is in no way an indication of the termination or loss of Celare tokens.

Encrypted tokens are being or may be regulated by regulators in different countries and project participants may from time to time receive inquiries, notices, warnings, orders or rulings from one or more regulatory bodies which may even suspend or stop Celare token’ s development or related activity. In different countries, Celare tokens may be defined as virtual goods, digital assets or securities at any time, while in some countries, according to local regulatory requirements, Celare tokens may be prohibited from trading or holding.

Celare and Celare Community Blockchain Incubator places great emphasis on compliance and being regulatory friendly within its legal jurisdictions that it operates in. Celare is supported by a team of legal advisors and lawyers who helps to ensure that each and every project and initiative complies with the relevant laws and regulations and an international audit and accounting firm is appointed to perform all the necessary tax and accounting compliance requirements. Celare is constantly monitoring and assessing potential risk and will take all the necessary action to stay within legal compliance and to avoid any future potential risk.

MARKET RISK

Market risk refers to a slowdown in the entire industry. In the event of a market recession or other such uncontrollable forces, businesses will therefore be similarly affected. Celare expressly states that the intended users shall have a clear understanding of the risk of Celare tokens. By holding Celare tokens, users understand and accept the risk of the project and are willing to bear all the corresponding market risks or consequences thereof on their own.

Celare TOKEN VALUATION

The value of Celare token is subject to market forces based on supply demand and as such, Celare is not able to guarantee any tangible valuation at any given point in time. Celare will not be responsible for any changes in Celare token price and expressly disclaims any direct or indirect loss caused from the acquisition or holding of Celare tokens which includes and not limited to economic loss due to user transactions, errors or inaccurate information to arise from personal misunderstanding and any other losses pertaining through trading.

9.REFERENCE LIST

[1]Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell; Enabling Blockchain Innovations with Pegged Sidechains; 2014.10.22

[2]Vitalik Buterin; Chain Interoperability;14,9,2016

[3]BitCoin Timelock; https://en.bitcoin.it/wiki/ Timelock# Relativelocktime

[4]Hashed-Timelock Agreements (HTLAs); https://interledger.org/rfcs/ 0022-hashed-timelock-agreements/#simple-ayment-channels

[5]MONACO J V. Identifying Bitcoin users by transaction behavior[C]// The SPIE DSS, April 20-25, 2015, Baltimore, USA. Baltimore: SPIE, 2015.

[6]GENNARO R, GENTRY C, PARNO B, et al. Quadratic span programs and succinct NIZKs without PCPs [C]//The 32nd Annual International Conference on the Theory & Applications of Cryptographic Techniques, May 26-30, 2013, Athens, Greece. [S.l.:s.n.], 2013: 626-645.

[7]PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: nearly practical verifiable computation[C]//The 2013 IEEE Symposium on Security & Privacy, May 19-22, 2013, San Francisco, USA. Washington, DC: IEEE Computer Society, 2013: 103-112.

[8]REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[C]//The 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, October 9-11, 2011, Boston, USA. Piscataway: IEEE Press, 2011: 1318-1326.

[9]ANDROULAKI E, KARAME GO, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1-5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 34-51.

[10]CHAUM D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 2003: 211-219.

[11]Johnny Dilley* , Andrew Poelstra* , Jonathan Wilkins* , Marta Piekarska* , Ben Gorlick* , Mark Friedenbach, Strong Federations: An Interoperable Blockchain Solution to CentralizedThird PartyRisks,2017.1.

[12]J. Aspnes, C. Jackson, and A.Krishnamurthy,Exposing computationally-challenged Byzantine impostors, Tech. Report YALEU/DCS/TR-1332, Yale University, 2005, http://www.cs.yale.edu/homes/aspnes/papers/tr1332.pdf.

[13]Merkle tree：https://brilliant.org/wiki/merkle-tree/

[14]Whitepaper of ELA： https://www.elastos.org/wp-content/uploads/2018/White%20Papers/elastos_sidechain_whitepaper_v0.3.0.6_ZH.pdf?_t=1526918341

[15]Whitepaper of Cosmos： https://github.com/cosmos/cosmos

[16]DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]// The 12th Annual International Cryptology Conference on Advances in Cryptology, August 16-20, 1992, Santa Barbara, USA. Piscataway: IEEE Press, 1992: 139-147.

[17]Whitepaper of Bytom：https://bytom.io/wp-content /themes/freddo/book/BytomWhite PaperV1.1.pdf

[18]Joseph Poon, Vitalik Buterin, Plasma: Scalable Autonomous Smart Contracts,2017.8

[19]Anna Osello, Andrea Acquaviva, Daniele Dalmasso, BIM and Interoperability for Cultural Heritage through ICT,2015

[20]Whitepaper of Wanchain https://wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf

[21]SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.

[22]Whitepaper of Polkadot：《POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK DRAFT 1》

[23]Polkadot Github：https://github.com/w3f/Web3-wiki/wiki/Substrate

[24]Polkadot official website：https://polkadot.network/faq

[25]Thibaut Sardan，《Polkadot & the Internet of Blockchains explained in simple words》，Dec 13, 2017.

[26]ARANHA D F, FUENTES-CASTAÑEDA L, KNAPP E, et al. Implementing pairings at the 192-bit security level[C]//The 5th International Conference on Pairing- Based Cryptography, May 16-18, 2012, Cologne, Germany. Heidelberg: Springer- Verlag, 2012: 177-195.

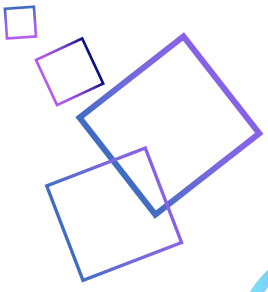
[27]ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: secure multi -party mixing of Bitcoins[C]//The 5th ACM Conference on Data and Application Security and Privacy, March 2-4, 2015.

[28]JENS G. Short pairing-based non-interactive zero-knowledge arguments[C]//The 16th International Conference on the Theory and Application of Cryptology and Information Security, December 5-9, 2010, Singapore. Heidelberg: Springer, 2010: 321-340.

[29]LIPMAA H. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments[C]//The 9th International Conference on Theory of Cryptography, March 18-21, 2012, Sicily, Italy. Heidelberg: Springer-Verlag, 2012: 169-189.

[30]NIR B, ALESSANDRO C, YUVAL I. Succinct non-interactive arguments via linear interactive proofs[C]// The 10th Theory of Cryptography Conference on Theory of
Cryptography, March 3-6, 2013, Tokyo, Japan. Heidelberg: Springer-Verlag, 2013: 315-333.

[31]BEN-SASSON E, CHIESA A, GENKIN D, et al. Verifying program executions succinctly and in zero knowledge[C]// The 33rd International Cryptology Conference(CRYPTO 2013), August 18-22, 2013, Santa Barbara, USA. Heidelberg: Springer-Verlag, 2013: 90-108.



CELARE

Cross-chain and anonymous solutions for all assets
Breaking the barrier of cross-chain assets
Protecting user privacy