Trinity White Paper

Universal Off-chain Scaling Solution

(Exposure Draft)

Table of Contents

I. Abstract

While the blockchain technology is lauded for its ability to reshape our economy and world, we are also concerned about its slow consensus building process, high transaction cost, and weak anonymity.

Trinity adopts state channel technology as an off-chain scaling solution for Neo. By providing a series of solutions, such as protocol layer, pluggable services, customizable services, free basic services, and incentives for value-added service providers, Trinity offers convenient, fast and safe blockchain services to users.

II. Background

The birth of the blockchain marks the beginning of establishing a truly trustable Internet.

The blockchain technology creates an Internet with value uniqueness and transmission, which in essence, is to realize the trustable flow of asset value.

The blockchain is freeing us from intermediaries in different industries, clearing/settlement agencies and centralized services providers, thus changing the world gradually.

The blockchain technology is not a single innovative technology, but an integrated technology system that gathers research outcomes from different fields, in which consensus mechanism is an indispensable core technology.

Due to limitations such as hardware, bandwidth, node number, node distribution and consensus algorithm, consensus building on the blockchain usually takes tens of seconds or even minutes, which poses a great barrier to the landing of commercial blockchain projects.

Due to the limited data structure of the blocks, spatial resources in the blocks are rare and very expensive. Putting unnecessary instructional operations or non-settlement intermediary data on the blockchain leads to high cost and places a huge burden on synchronizing with the P2P network.

As data on the blockchain is public to all users, storing all data and processes on the blockchain poses a great threat to user privacy.

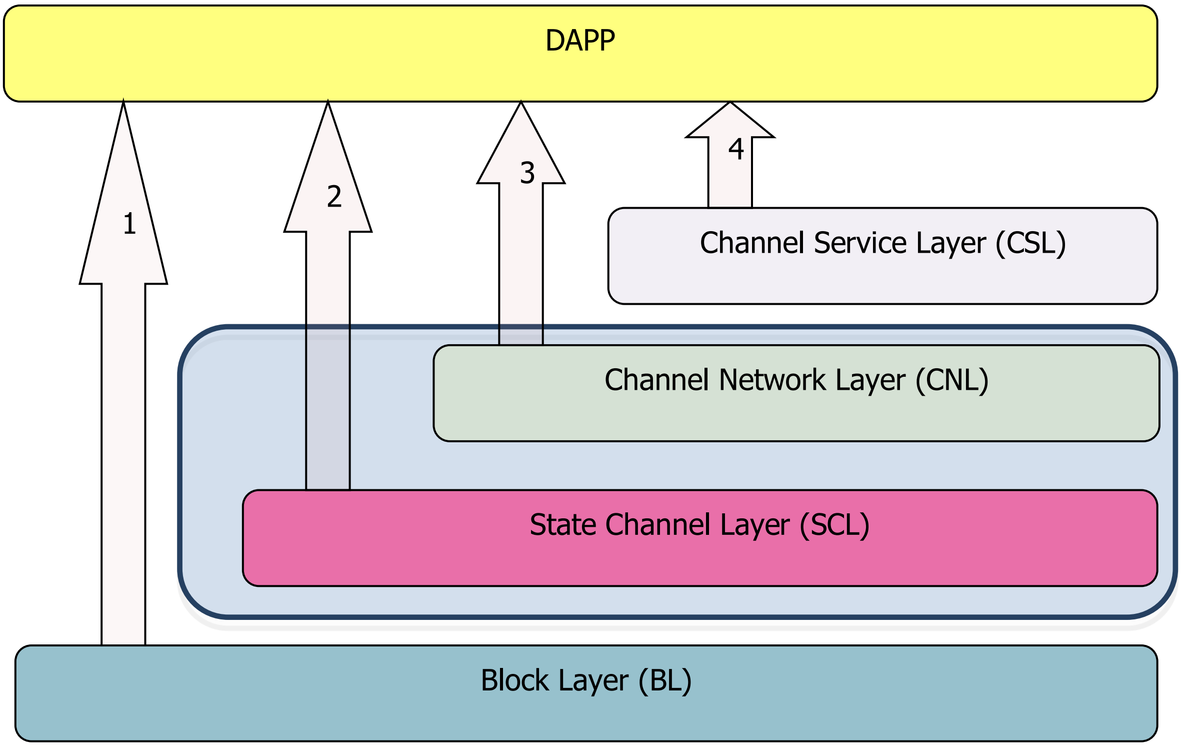
To solve the above problems, the Lightening Network was created for Bitcoin and the Raiden network was created for Etherum. This projects is an universal off-chain scaling solution.

III. Overview

Trinity is an off-chain scaling solution for Neo and is applicable to blockchain transfer of Neo utox and NEP-5 standard tokens. Trinity achieves real-time payments, low transaction fees, scalability, and privacy protection of Neo assets through state channeltechnology.

Trinity aims to provide safe, fast and convenient blockchain services to its users through its fast and safe off-chain payment channels.

Trinity overall framework is as follows:


DAPP
1
2
3
4
Channel Service Layer (CSL)
Channel Network Layer (CNL)
State Channel Layer (SCL)
Block Layer (BL)

Trinity, blockchain and Trinity’s logic layers are completely decoupled from each other. Each of them can serve DAPPs independently. DAPPs deployed on the Trinity network may, according to their business needs, use the API of any of Trinity's logic layers to secure corresponding services available on such layers (as shown in Figures 2, 3, 4), or carry out on-chain transactions without using any Trinity services (as shown in Figure 1).

The State Channel Layer (SCL) provides Trinity with the most fundamental P2P state channel services. State channels are established as transaction parties put up their assets as collaterals on the blockchain and establish a smart contract to endorse subsequent off-chain transactions. The services available on the SCL enable transaction parties to carry out instant transactions with no latency. SCL services are applicable to DAPPs for C2C instant payment, personal high-frequency data collection, among other scenarios.

The Channel Network Layer (CNL) provides Trinity with state channel routing services, i.e. fully automatic intelligent routing for transaction parties without established state channels. All the state channels correspond to a smart contract on the blockchain and an asset collateral. It is not feasible for all users to establish state channels with all their counterparties due to asset collateral costs. Thus, Trinity's routing services are requisite for unperceived state channel routing which allows transaction parties to transact in real time with no latency. CNL services are applicable to DAPPs for B2B/B2C instant payment, network-wide data collection, decentralized exchanges, instant exchange between coins, IoT networking, among other scenarios.

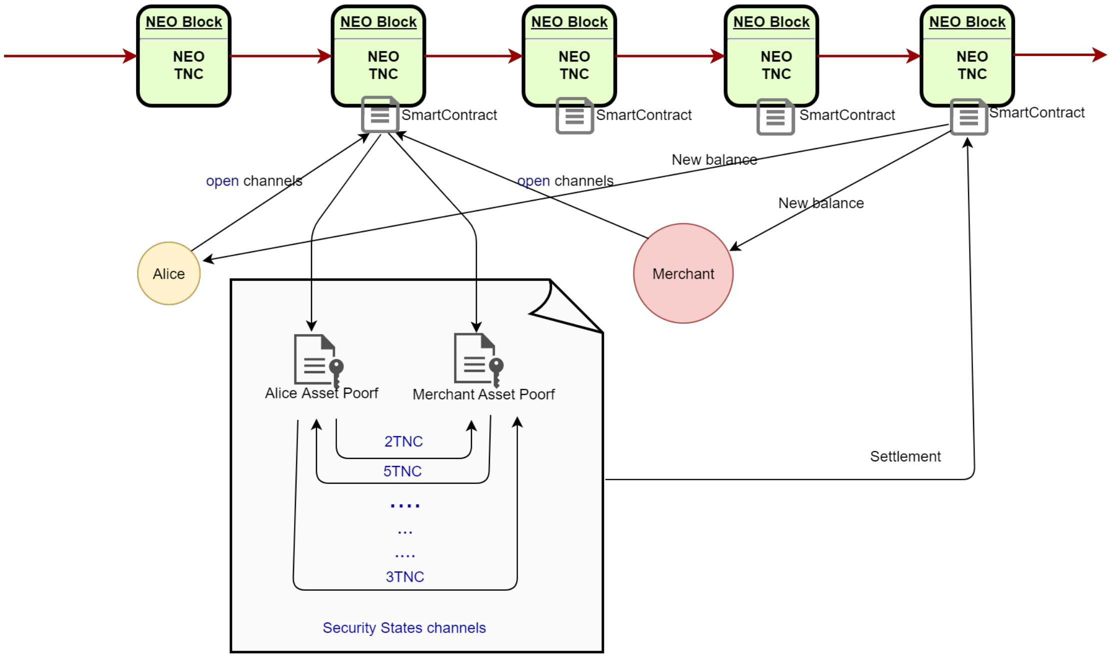
The Channel Service Layer (CSL) provides Trinity with plug-in customizable off-chain transaction services. The channel atomic layer (CAL) and the CNL function jointly to make on-chain assets flow fast off chain as Trinity aims to be "good and fast". The CSL is designed to improve users' transaction experience. DAPPs may acquire personalized services through custom implementation by themselves or customization by Trinity on the CSL as transaction needs vary per industry, asset and stake. Common services available on the CSL include: gateway services for light clients, mix-coin transaction services with privacy protection, high-priority quality of service (QoS) routing for state channels, peer-to-peer connection-oriented state channel routing, channel detection proxy service, etc.

That Trinity and the blockchain layers are completely decoupled from each other lays a solid foundation for Trinity's subsequent moves - blockchain transplants and cross-chain transaction services.

IV. Technical Implementation

4.1 Proof of Assets(PoA)

PoA, equivalent to settlement reserve fund, is a key factor in off-chain scaling solutions. It is achieved through digital signature and hash lock, that's to say, transactions are performed with mainnet digital assets as collaterals.



The graph shows two traders: Alice and Merchant. PoA means they lock their mainnet tokens as collaterals to form PoA. For example, Alice has 1000 NEO NEP-5 and Merchant has 1000 NEO NEP-5. Before off-chain transfers, Alice and Merchant lock certain number of tokens as proof of assets. Without PoA, token transfers cannot be performed. PoA is a binding protocol implemented by the NEO blockchain. Digital signature ensures that Alice and Merchant stay in the value transfer. Also, as only Alice and Merchant have access to tokens of the smart contracts in the payment channel, Trinity PoA is as binding as mainnet transactions.

Once mainnet tokens are locked, PoA is formed. Then A and B can conduct off-chain transactions immediately through payment channels without time limits. When the transactions are finished, assets can be transferred back to the mainnet and the balance is registered on the mainnet. However, off-chain transactions will not be recorded. To put in other words, the number of transactions and the amount of each transaction will not be broadcast to the entire network so as to protect user privacy.

4.2 Smart Contract

On-chain smart contracts have the following main functions:

1) determining transaction rules agreed and shared between transaction participants

2) issuing transaction tokens as a guarantee of off-chain payment

3) smart arbitration: In case of breach by either party, the smart contract can function to impose fair punishment on the breaching party.

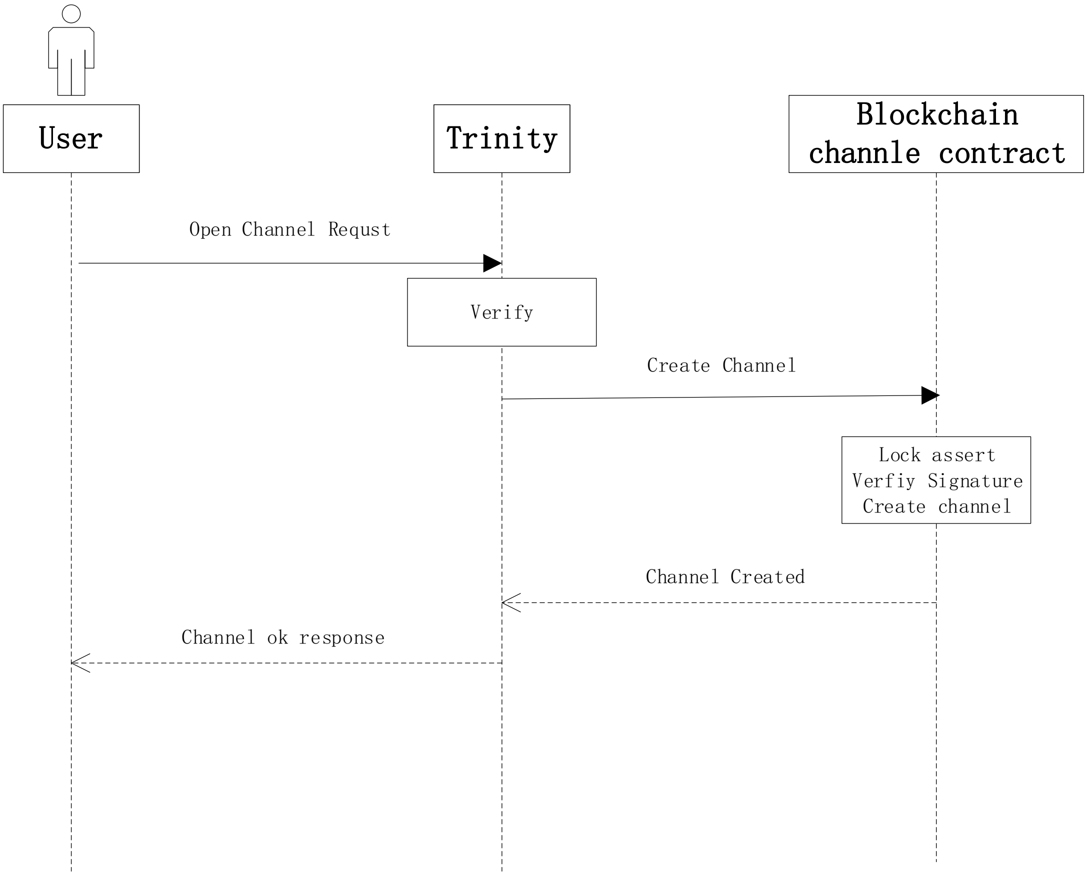
4) channel management and closure of channels: Transactions are executed off chain, but the balance is recorded on chain.

Channel smart contracts are an executable code incorporating shared rules for operating an off-chain payment channel. When using the channels, each participant agrees on those rules implicitly. The channels allow:

1) large volume of two-way value transmission between participants

2) conditional value transmission with expiration and pre-defined rules

3) rules that determine the sequence of transfer



Each channel supports two-way off-chain payment channels and has their own settlement cycles. Both participants in a transaction can store any amount of deposits for any number of times.

Transactions may be completed under certain conditions, meaning there might be several fast transactions waiting for completion at any time point. The transactions are represented by a lock structure that includes numerical values, expiration time and hash lock. A set of all unimplemented transactions is encoded by a Merkle Tree and represented by its root in each transaction.

Channel capacity is the total amount of deposits of the two participants in a transaction. The capacity represents the maximum amount of transactions and the total amount of assets involved in unimplemented transactions. The capacity is divided into two parts: disposable balance and locked balance of each participant. The disposable balance is changing with the direction and value of completed transactions during the life span of the channels, and will increase with deposits by the corresponding participant or payments by the counterparty. The amount of the locked balance depends on the direction and value of locked transfers of unimplemented transactions, increasing with each locked transfer and decreasing as transfer and payment succeed or by other means.

Participant's balance= deposit + received amount − paid amount

$$Bn=Pd+Pr-Ps$$

Locked balance = total amount of unimplemented transactions

$$Bl=\Sigma_{K=O}^{n-1}Tp$$

After development, the channels are likely to receive multiple deposits from any participant. Once confirmed by the counterparty, the depositor can carry out transfers with the disposable balance.

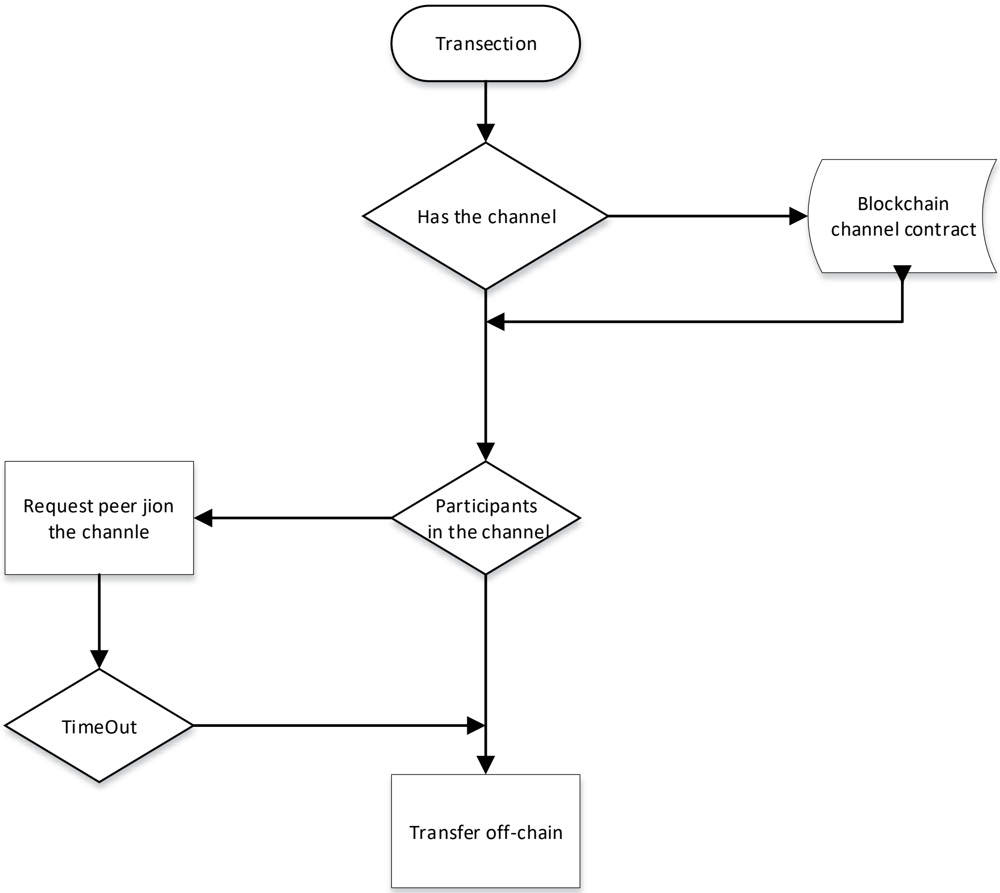
Channels are subject to closure in case either participant intends to cancel the transaction or any disputes arise, after which the settlement window opens for the corresponding participant to update the status of the counterparty and revoke the unlocked lock. Neither participant is allowed to carry out partial revocation.

The operation of transaction update receives a signed PoA which includes a data packet with channel specific like Merkel Tree root, transaction amount, and a transaction sequence. As the node can only provide information about the signature of the counterparty, we know the data is not tampered, and is valid. To prevent the node from providing outdated information, the amount withdrawn is deducted from the amount transmitted, which is a monotonic increasing value. Therefore, there should be no transaction carrying a negative value; any participant providing outdated information will see his/her net balance decrease.

Another channel operation is revoking the lock, i.e. receiving the proof of unlocking that is made of a lock data structure and proves that the lock is included in the Merkel Tree and there is an available password to unlock it. The channel recalculates Merkel Tree root and verify the password to verify the lock. If all such verifications are passed, the amount transferrable by the counterparty will increase.

4.3 State Channels

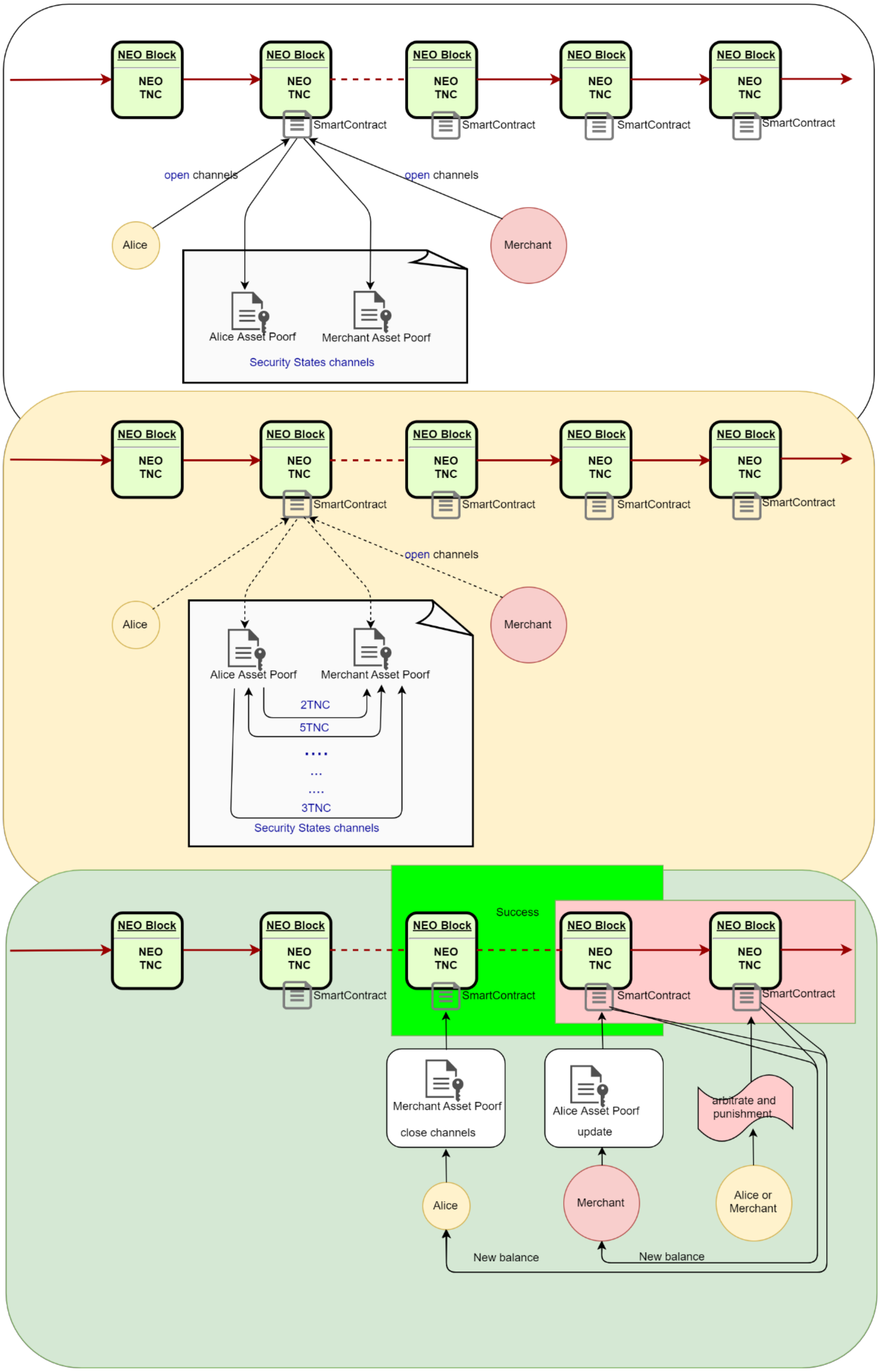
Trinity uses on-chain smart contracts to authenticate participants, lock/unlock deposits and resolve disputes for state channels management. Off-chain transactions are made possible through Trinity's off-chain protocol.


Transection
Has the channel
Blockchain channel contract
Request peer jion the channle
Participants in the channel
TimeOut
Transfer off-chain

4.3.1 Life Cycle of the Channel

During the life cycle, tokens are locked to ensure they can only be sent and received in the channel until it is closed so as to avoid double-spending. Once the channel is developed, participants can check and verify its existence. Each counterparty does not need to check all records, but only track the updates. PoA includes the final total amount of transfer in the Trinity network sent to the participants, and is signed digitally by the sender.

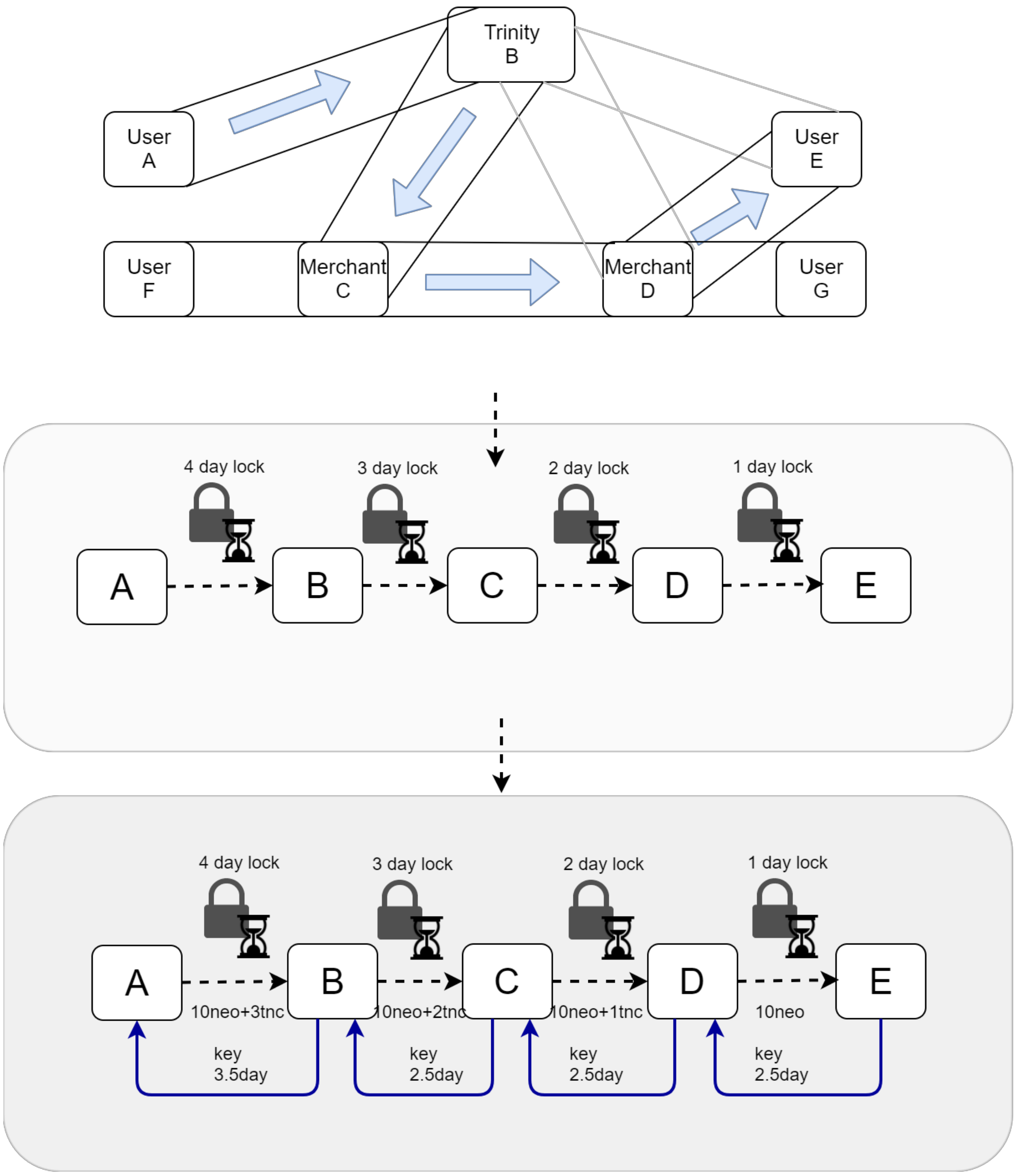
If one participant decides to settle the assets on the blockchain, he/she can require the payment of the other participant or pay the unpaid assets. The participant can submit transaction request through smart contracts to select PoA and close the payment channels. The other participant who hasn't closed the channels must provide the PoA. If no transfer occurs, the operation is not needed. After PoA submission by the participants, they can withdraw their tokens. If one of them hasn't submitted the PoA on time, the assets will be determined by the PoA of the participant who requests closure.



The above graph shows the entire lifecycle of Trinity network payment channels.

4.3.2 Channel Network

The development and settlement of payment channels must be conducted on the blockchain. Therefore, it is impossible to create new channels for each potential target. Trinity solves the problem through the development of payment channel network where participants are connected with each other.



As shown in the graph above, A wants to send cryptocurrency to E. A must find a network channel to connect E. Each participant on the route needs to cooperate with each other so that A can transfer tokens to E. The participants transfer tokens to the next node through payment and rent the channels to A. Encrypted hash lock prevents crediting of the intermediary transfers until E confirms receipt of A’s tokens. Once A decides to unlock and pay, she sends the key to E.

As each participant on the route who unlocks their payment gets incentives, the private key will be returned to Alice through the channels. All locked transfers can be traded on the mainnet through Alice’s private key. However, the participants had better integrate the locked transfer value to form a standard PoA. PoA that includes locked transfer value and invalid lock can be synched on the state channels. In this way, transfer among multiple participants can be done.

Counterparties in the network will not open their channels for free. After all, transfer will result in extra network traffic and imbalance of payment channel. Therefore, participants of the Trinity network pay for renting the channels, and the fees they pay will encourage the payment channels to be more balanced.

4.4 Off-chain Transactions

All off-chain transactions need to be programmed based on the format of the PoA to ensure consistency and safety of channel communications. The information includes:

1) transaction sequence

2) the number of transfers

3) suspend

4) Merkle Tree root node

5) signatures that include the above information

Trinity provides the following two off-chain transactions:

1）Direct Transaction

2）Router Transaction

4.4.1 Direct Transaction

Direct transaction doesn't rely on locks, as it is completed automatically after successful sending of network data package. As the transmission runs on asynchronous network, it cannot be completed in an atomic manner. The keysto direct transaction are as follows:

1) Unlocked information means that the number of messagesconveying information will continue to increase, and there may be messages of

transaction cancelation. That’s to say, the payer will pay for the transaction unconditionally regardless of whether services are received.

2) The payer must assume that the transaction is completed when messages are sent to the network.

A successful direct transaction only needs 2 messages: transaction message and confirmation message. For example,
Alice wants to pay n assets to Bob. First, Alice creates a new transaction message. Alice signs the transaction and sends it to Bob, and the transaction is completed.

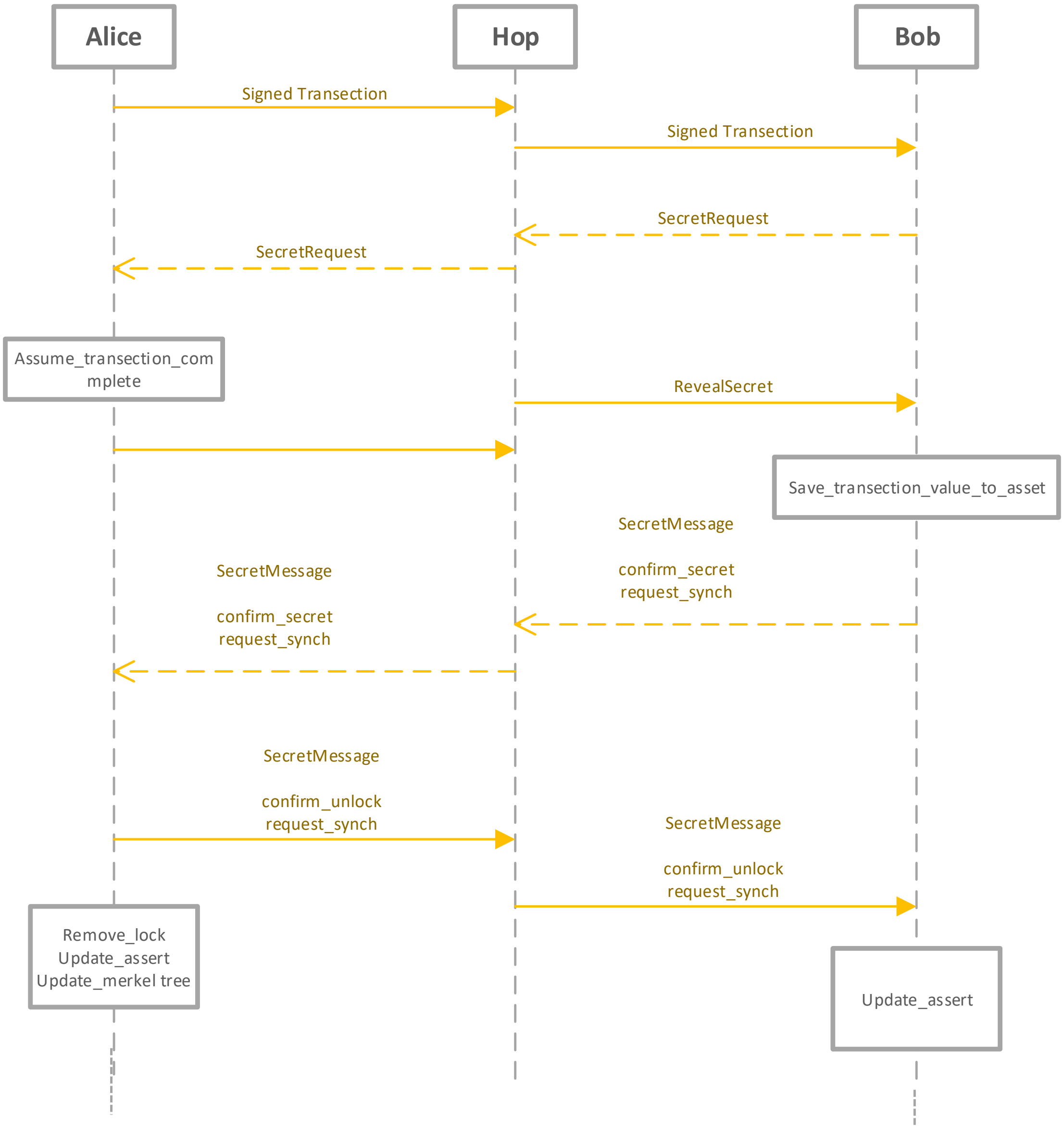
4.4.2 Router Transaction

Router transaction is usually used in channel network with an initiator, a trader and many intermediate nodes. To ensure privacy and immutability of transactions, the intermediate transaction is designed to be a transaction with a hash lock which contains transaction figures. The lock is also used to verify the cipher text to unlock it and its maturity.

Another example of Alice and Bob.

Alice wants to pay n assets to Bob. First, Alice creates a new transaction message.

1. Alice signs the transaction and sends it to Bob.
2. Bob sends secret request message to Alice as a request to cancel the transaction.
3. Alice sends the cipher text to Bob and assumes the transaction is completed then.
4. Bob receives the cipher text and has n assets transacted to him.
5. Bob sends a message with the cipher text to Alice, stating he is aware of the codes and request off-chain synch.
6. Alice sends a cipher text to Bob to notify him that the lock will be removed from the Merkel Tree, and that the amount of transaction and tree root will be updated.



V. Token Introduction

The core of the tokenized economy is to incentivize the ecosystem with tokens. Trinity also needs an incentive system to achieve high efficiency. TNC (Trinity Network Credit) is used as credits to balance state channels of Trinity network.

5.1 Function and Value of TNC

The core of Trinity is the state channels. In order to involve more users and form a micropayment eco-habit, state channel itself is free, that is, Trinity is available for users without TNC.

The feasibility of Trinity requires cooperation with many participants, while TNC serves as an incentive and a balance.

TNC Use Cases:

1. Unified asset for network settlement

   TNC can be but is not required to be used as a mortgaged asset during channel establishment, so as to provide a unified settlement method. As such, the TNC could be the most direct and convenient way to those small and medium sized nodes or users unwilling or unable to synchronize resources on the entire chain. This unified settlement mechanism helps reduce unnecessary exchange costs for on-chain and off-chain transactions.

2. Trinity network contribution reward

   Trinity provides channel routing to improve transaction convenience throughout the entire network. The channel routing enables effective state interactions and value transfers between users/nodes through the channel, which makes the Trinity network more flexible and convenient. The TNC can reward the channel routing providers in an effective manner, which encourages more nodes/users to participate in the network channel and enables more efficient asset flows.

3. Trinity network value-added services

   As a privacy-conscious network, Trinity adopts multiple technologies like zero-knowledge proof and CoinJoin to protect data security and enhance privacy protection for users. Moreover, the Trinity network can provide further privacy protections which can be acquired through TNC payment.

   Other services provided by Trinity include QoS, connection-oriented channel routing, thin client gateway services, proxy services on state channel testing and monitoring among other value-added services.

   Dapp developers are able to customize value-added services on Trinity's channel service layer. These services will be available for all Trinity users by paying TNC to developers.

4. Network ServiceFees

   The Trinity network is devoted to providing digital asset services for small and medium sized businesses. Small and medium sized businesses using the Trinity network to distribute or manage digital assets can use TNC to pay for the needed services.

5. Enterprise customization servicefee

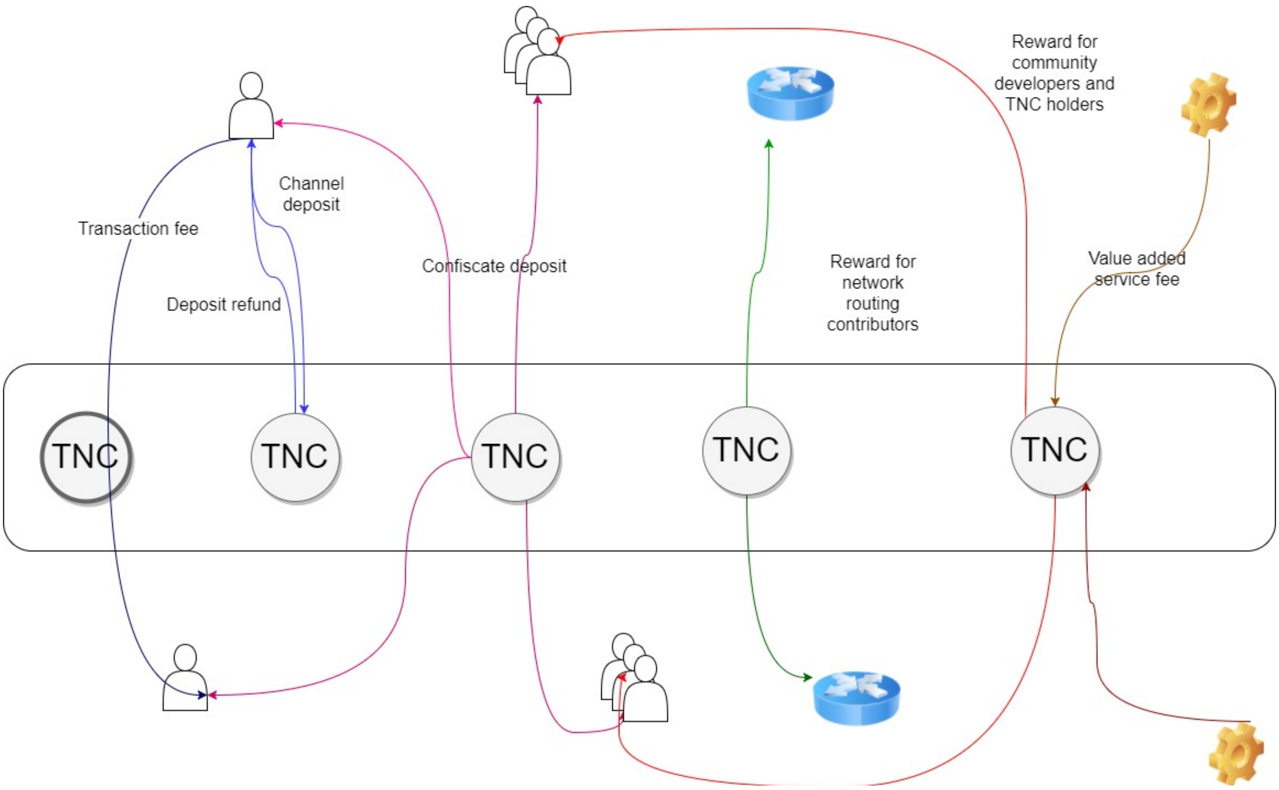
Businesses requiring customized services like independent state channel modes and highly customized wallets shall pay for those customized services in TNC.

6. Incentives for TNC holders and community developers

For developers who are constantly concerned about and supporting the Trinity community, Trinity is to reward them with TNC tokens. Such incentives aim encourage more talents to develop the Trinity community and keep improving Trinity protocols.

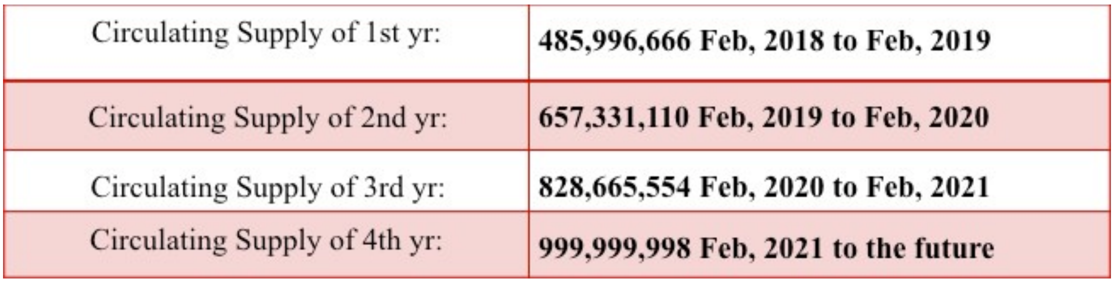
TNC holders will be rewarded as set in the following chart, in a bid to motivate more to contribute to Trinity network development.

With the evolvement of the Trinity network and more participation, TNC will show more values in an increasing use cases.



5.2 Token Distribution

Total designated unit	**1 Billion**
Part#1 Private donation	**111,111,111**
Part#2 Public donation	**222,222,222**
Part#3 Operational allocation	**152,663,333**
Part#4 ESOP (3 yr locking, 1 yr cliff with 33% vested; 1st vesting by Feb. 2019)	**180,670,000**
Part#5 Main lock (3 yr locking, 1yr cliff with 33% unlocked; 1st unlocking by Feb, 2019; decided collectively by directors of the Foundation)	**333,333,333**



Circulating Supply of 1st yr:	**485,996,666 Feb, 2018 to Feb, 2019**
Circulating Supply of 2nd yr:	**657,331,110 Feb, 2019 to Feb, 2020**
Circulating Supply of 3rd yr:	**828,665,554 Feb, 2020 to Feb, 2021**
Circulating Supply of 4th yr:	**999,999,998 Feb, 2021 to the future**

Note 1: By the first time TNC is distributed to its donors, Part#4 and Part#5 will be available on the TNC Neo Smart Contract Rich List for supervision by the community.

Note2: All donors, either through private or public round, will be donating based on the SAME exchange rate as NEO. There is no discount for private donors.

Note3: Distribution of Part#5 will be explained in great detail in future documentations. As of this moment, the Trinity Foundation is considering the option of setting up an automated distribution of these TNC to State Channel operators, promoters and community contributors. But it is for sure in no means will Part#5 be distributed to all of the incumbent Trinity Foundation directors or team members.

IV. Team

6.1 Team members

David Yiling Li

Founder

The former NEO overseas manager, responsible for the Neo token global sales, community building, commercial cooperation and ecological construction， etc. in 2016.
The Co-founder of Fourier PR, which is one of the top crypto-economy project and consultancy enterprise in China. Fourier is also cooperate with FBG and its clients dominate the top 100 list of coinmarketcap. The founder of Rai Stone.

Guangfeng Zhang

Co-founder

Expert of security and blockchain. Guangfeng has more than 15 years of experience in technology development. He has worked in the Giesecke+Devrient (China) and CBPM (China Banknote Printing and Minting Corp) Blockchain Research Institute, engaged in the formulation and promotion of the PBoC 2.0 / 3.0 specification, the design of the digital ticket trading platform based on digital currency and blockchain technology.

Fengping Yi

Co-founder

Government Affairs Specialist on Blockchain, rich experience in public sector and blockchain business development. Joined China Ethereum community in 2015 and had been working on blockchain industry's affairs with the Government. Former government official responsible for business development. Former Director of Government Affairs at Shanghai Onchain Technologies Ltd. Former Vice Director of Tongji University Fintech and Blockchain Research Institute. Responsible for helping the company join the MIIT blockchain reference architecture building and policy-making. Participation in Guiyang municipal government's Credit Farmer project, which is seen as the very first government-sponsored blockchain application nationwide.

Will Wei Wu

Core Dev

SW and I&V specialist, 10 years' experience in technology development. Software Development, I&V Specialist and Test Automation Coach in Nokia. Initiator of Grooming2robot project (A Natural Language Processing Based Automation Testing Tool) Blockchain fan, Hyperledger Fabric technology document translation in gitbook.

6.2 Advisors

JC XU

Co-founder of Badwater Capital (a digital currency fund), early supporter of RPX, CPX, VEN, REQ, ZRX, etc. He worked for DFJ Dragon Fund (a well-known venture capital fund in Silicon Valley and China) on TMT venture capital. His startup projects were invested by IDG and were purchased in 2016. Studied in Indiana University-Kelley School of Business and Draper University in Silicon Valley.

Zhoudong Ji

Blockchain expert Former blockchain expert of a Fortune 500 company (Wanda), Deputy Secretary-General of Blockchain Industry Development Forum of MIIT. He participated in the draft of MIIT White Paper and the development of relevant standards. He wrote Blockchain Development Guide and other professional books.

Yanbo Li

Former senior R&D engineer and technical director of Qualcomm and Redpoint Positioning Linux kernel network subsystem code contributor, specializing in architecture design of distributed network system and implementation of Mesh network protocol. Currently in charge of management of Onchain Beijing office and development of an open source blockchain platform--Distributed Network Architecture. He studied under Dan Boneh in Standford and has an outstanding background in cryptography

VI. Risks and Disclaimer

1) This document is only for sharing relevant information to specific readers asking for information of the project, and shall not be construed as either a guidance for future investments or a contract/warrant of any kind.

2) Those who choose to participate in the TOKEN Distribution Plan shall be deemed to have understood and accepted the risks associated with the Project and have agreed to take full responsibility for their participation.

3) The Project Team explicitly claims that it neither provides guarantee of returns nor takes responsibility for any direct or indirect losses arising from the Project.

4) The TOKEN involved in the Project is an encrypted code to be used in transaction process, rather than a representation of any equity, right to earnings or right of control relevant to the Project.

5) Digital currencies carry high uncertainties, including but not limited to different regulatory regimes in various nations, industrial incentives/competitions, and technical flaws of digital currencies. As such, we provide no guarantee for the success of the Project. In fact, the Project involves risk of failure, and even nullification of the TOKEN.

6) The Project Team will make efforts to fix the problems that likely to occur in its development. Nevertheless, the Project is still under policy uncertainties. Thus, you are advised to have a comprehensive understanding of the Blockchain and the associated risks before making investments.

VIII Contact us

Website：https://trinity.tech/

Email: support@trinity.tech

Telegram: https://t.me/TrinityStateChannels