LITEX - Building a Consumer-Level Layer 2 Application Framework

Summaries

LITEX is a complete Layer 2 framework for consumer-level blockchain applications. The entire framework is divided into two parts: on-chain contract and off-chain protocol. The on-chain contract is a rule publicity platform that aims to fix the state and logic in the consensus layer, and provides various templates such as payment channel contract and business verification contract, etc. The off-chain protocol is a rule execution platform that aims to process the data organization, transmission and verification of data off the chain and provide data credibility, data protocol and authentication protocol.

LITEX provides developers with a verifiable, low-threshold, user-friendly, free-to-develop solution from end users' perspective. This whitepaper outlines LITEX's design philosophy, system architecture, crypto economic model, and best practices for developing blockchain applications with LITEX framework.

Catalog

Vision

Blockchain industry is a realm of high-recognition threshold. It has triggered many social experiments since its birth, but none of the popular applications appeared in the mainstream users. The reason behind this is that the design goal of the public chain is to reach consensus as broad as possible, and the more consensus nodes, the lower the performance, which makes it unable to support products that serve users of large volumes. In the direction of solving the problem of public chain performance, the idea of layered design gradually takes up the mainstream and derives many Layer 2 solutions but the high-threshold nature of users' participation still cannot support consumer applications.

Consumer-grade products are the most common types of products in our daily lives, and their goal is to reduce the cost of price and use as much as possible on the basis of meeting the needs of mainstream consumers. On the contrary, industrial products generally need to meet more stringent requirements of demand design and pay more attention to performance, but take little consideration in terms of cost and ease of use. For example, consumer routers have small physical volume, low energy consumption, user-friendly configuration, switch and AP capabilities while the price is only tens of yuan; on the other hand, industrial routers have powerful performance, high-level security, but also bulky volume, high energy consumption, complex operation (requires professionals to configure with codes). The price range from tens of thousands to millions of yuan. It is not difficult to find that if there is no evolution of industrial routers to consumer routers, the Internet will be hard to spread as it is today.

Bitcoin - the earliest blockchain application - brings peer-to-peer cryptocurrency payment; Ethereum goes further and provides decentralized smart contract platform services. As bottom-layer public chain, global consensus is their value base. The stronger, the more extensible consensus is, the more nodes around the globe will participate in the synchronization and verification of the data, which will inevitably lead to a reduction in processing efficiency and cannot further support the consumer applications. Paradoxically, the development of the crypto economy is inseparable from the expansion of the basic user community. In order to attract more people to join, the crypto world must constantly expand the scene and lower the threshold, which depends on the emergence of a large number of consumer applications.

The birth of consumer applications relies on high TPS (Transaction Per Second), low transaction fees and low usage thresholds, at the same time we cannot completely abandon the decentralized and secure nature brought by blockchain technology. Then we have encountered the impossible triangle problem often mentioned in the blockchain world: safety, decentralization, efficiency. You can't have them all. At this time, if we still hope to solve the impossible triangle on the same layer by constantly adding new functions and new designs, the whole problem will become quite complicated, which is not conducive to our understanding and analysis of internal laws of things. Moreover, if we put all the steps and functions into the same layer, this layer will become more and more complicated and reach to a high degree of coupling. Additionally, future modifications and upgrades will be very

difficult to implement, which is unacceptable for the blockchain that actually stores value.

For any problem that reached a certain complex stage, if the current method isn't viable, an alternative can often be found with the idea of adding a layer. Layering in computer science is a very common idea. TCP/IP has a four-layer structure, OSI model has a seven-layer structure, and the most-exposed computer storage is, as well, divided into four levels: level 1 cache, level 2 cache, memory, and hard disk.

Whether public chain - the carrier of consensus - can accumulate consensus and become a value storage network depends on two most important factors: security and decentralization. Security determines how much value the public chain can carry, and a public chain cannot precipitate value above its attack cost; Decentralization decides whether the public chain can become a broader value network for anti-censorship. We should let the public chain maintain security and decentralization, the value base of the blockchain and solve the issues related to performance, privacy on the upper level. Only by doing this can we make a consumer product based on blockchain – this is the layering idea of the blockchain.

In order to solve the performance issue of the public chain (Layer 1), developers have designed a series of upper layer (Layer 2) from the perspective of layering.

Solution. Layer 2 is a design pattern that advocates putting business logic that does not require global consensus off the chain and submitting to chain for global consensus only when it needs to be settled or arbitraged. Lightning Network, State Channel and Plasma all belong to the Layer 2 solution.

However, the design of these solutions is very complicated, no matter the developers' implementing difficulty or users' thresholds, which makes them unable to meet the needs of large-scale consumer applications. Through research, we found that the current Layer 2 solution's over-complicated design process strives to achieve comprehensive security, privacy, and complete decentralization while overlook the cost of use. This suggests that their positioning is still on the level of "industrial" solution rather than a "consumer" applications support framework.

We believe that crypto economy requires consumer applications, and the design of the Layer 2 solution also needs to make a trade-off from the perspective of users. Therefore, we designed LITEX and hoped to provide developers with a more "down-to-earth" Layer 2 solution, which greatly reduced the users' cognition and usage threshold, hatched more consumer-level blockchain applications and accelerate the development of crypto economy.

Overview

LITEX is a complete Layer 2 framework for consumer-level blockchain applications. Based on LITEX, developers can easily build user-friendly blockchain applications, allowing users to gain

an easy-to-use experience like Internet products, and benefit from asset security, high liquidity, transparency and other characteristics brought by blockchain technology.

Product-wise, LITEX splits the consumer blockchain application into two parts: encrypted payment and business logic. Encrypted payments involve user assets which require cryptographic level security. LITEX will use the payment channel solution to ensure user asset security, and also provide token aggregation, senseless upgrade, transaction readability, uni/bi-directional channel option, etc. In practice, users will not be able to perceive the difference between encrypted payment and electronic payment In the business logic part, sufficient flexibility and compatibility are needed to feed the complex and various logical needs. LITEX proposes a design pattern of on-chain verification and off-chain arbitration, which greatly reduces the development difficulty and usage threshold.

Tech-wise, LITEX has developed payment channel contracts and business verification contracts for both encrypted payment and business logic. Currently, the development of the contract is mainly based on Ethereum while in the future it can be extended to any other public chains that support smart contracts. Payment channel contract is already supportive of opening the payment channel for both ETH and all ERC-20 tokens in a single contract; Business verification contract gives the design of gaming application templates which show users the results of readable and playback-capable on-chain verification. LITEX will also give out design instances in financial products and dapps subsequently.

Commercial-wise, LITEX has always believed that the data generated by user operation, user activity and money transfer of a consumer application provides both users and developers with great reference value because this data establish positive feedback between users and applications. Therefore, LITEX adopts license chain implemented with the pBFT consensus to carry off-chain data, which makes the original point-to-point, only-known-by-both-parties transaction data gain public credibility and vitalizes the business ecosystem built on top of it.

With the help of LITEX, developers can implement business logic with their familiar technology stack. They can assure transparency, and efficiency and verifiability of the application by only performing a chain declaration in the form of a verification contract.

Payment-wise, users can get the payment experience of “speed increase and fee deduction” powered by Layer 2 technology, as well as close the payment channel at any time and wield your own money ownership, without worrying about unused funds being detained by developers. Blockchain application based on the LITEX framework is on par with Internet application in terms of user experience, and once there is doubt about the off-chain data, users can easily perform on-chain verification, which draws a drastic difference from those “pseudo-blockchain applications” with zero blockchain characteristics.

Blockchain Layering: Layer 2 Design Ideas

In recent years, the industry has proposed a variety of scaling plans tackling the performance of the public chain. They mainly divides into two categories: on-chain scaling and off-chain scaling. On-chain scaling plan on the chain attempts to achieve the scaling effect by directly modifying the consensus agreement, such as increasing the block capacity, shortening the block interval, altering the consensus algorithm and implementing sharding, etc. This is called the Layer 1 scaling; Off-chain scaling does not seek to upgrade the consensus algorithm of the public chain, but rather complete the operation of the unnecessary global consensus through the cooperation of the on-chain contract and off-chain protocol, and submit to the chain only when it needs to be settled or arbitrated. This is called the Layer 2 scaling.

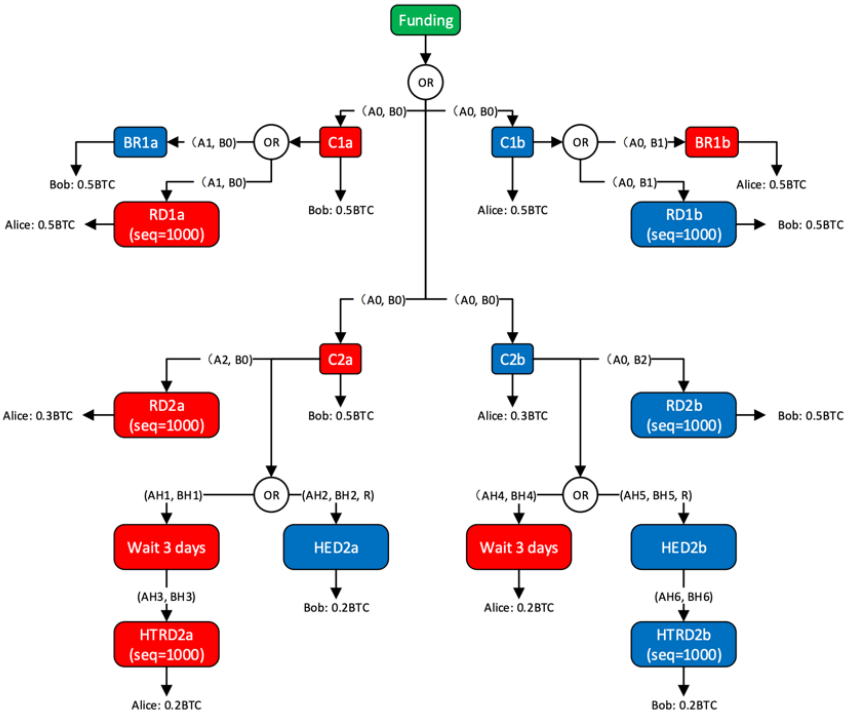
It isn't difficult to imagine that the Layer 1 scaling plan needs to re-establish consensus among all participants, and the new consensus also needs to undergo sufficient long-term inspection. This is undoubtedly very difficult and slow; Even if the final consensus can be reached, the viable improvement at the Layer 1 level is limited: either increasing node throughput or degree of parallelism. Increasing throughput puts a higher requirement on the hardware configuration and network bandwidth of the node, increases the degree of centralization. On the other hand, improving the degree of parallelism relies on the complex sharding technology which is prone to many problems such as high difficulty, high risk, and slow progress in a decentralized architecture.

In comparison, the Layer 2 scaling solution recognizes the global consensus value achieved on Layer 1, does not expect to alter the consensus but rather pursues an optimized way to take advantage of this global consensus. At the same time, people noticed that balance point between security and efficiency varies among different scope of the consensus. Designers of Layer 2 are able to limit the scope of the consensus according to demands in order to achieve the scaling effect that meets them. For example, in the case of micropayment, when two parties reach a consensus on the final fund allocation, the scope of the consensus is limited between these two. Payment channel technology is the solution for this scenario. The current mainstream Layer 2 technologies are as follows:

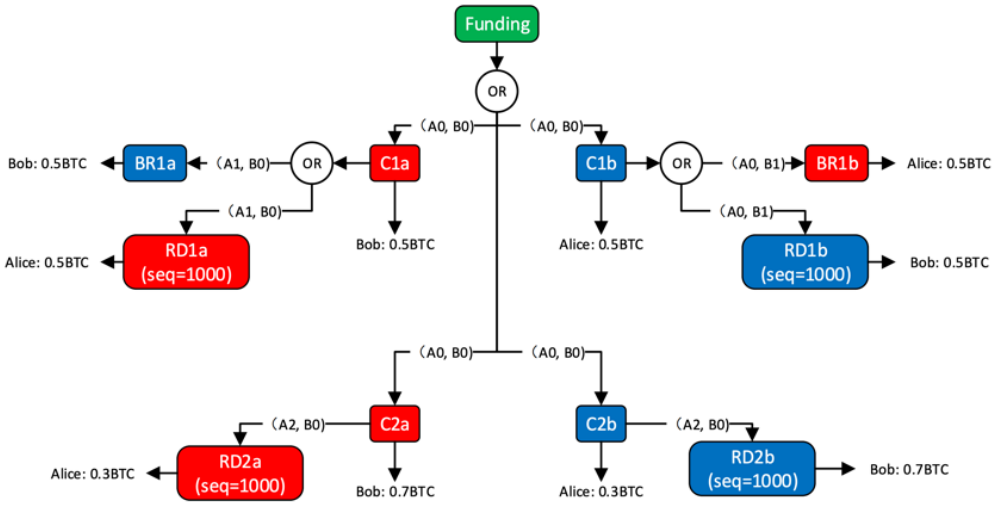
Lightning Network

Lightning Network is a general term for bitcoin off-chain transfer network based on the BOLT protocol. Lightning Network is a distributed network that eliminates the risk of entrusting funds to third parties with smart-contract-supported multi-party instant, high-density micropayments combined with blockchain technology. Essentially, Lightning Networks is a mechanism that utilizes Revocable Sequence Maturity Contract (RSMC) and Hashed Timelock Contract (HTLC) to secure zero-confirmation transactions. Both parties need to open a payment channel to jointly pre-store a portion of the funds into the payment channel. When two parties are transacting, they only need to sign and confirm each transaction without necessarily having to submit each transaction to the

chain. When the payment channel is closed, only the final transaction result needs to be submitted to the blockchain and confirmed. Previous off-chain transactions will no longer occupy blockchain resources, so transactions on Lightning Networks are fast, low-cost, and instantly confirmed.



HTLC（Hashed Timelock Contract）

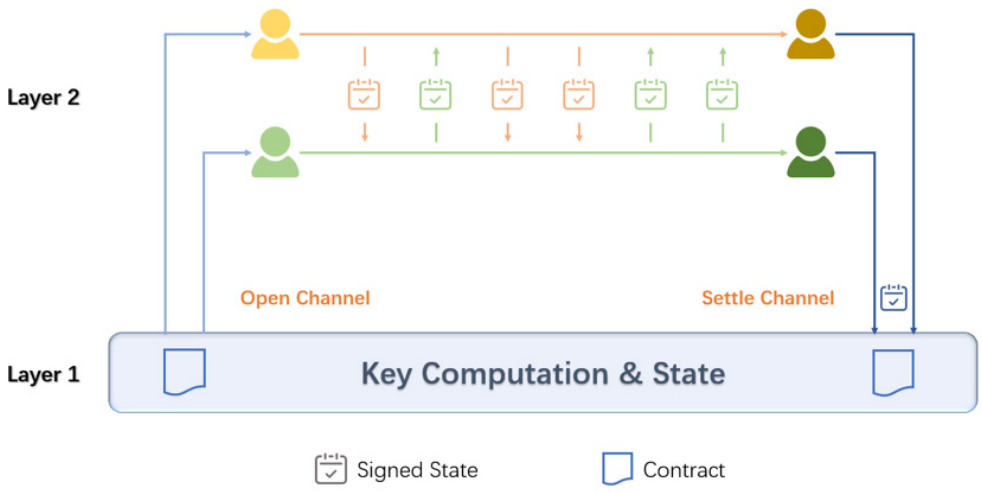


RSMC（Revocable Sequence Maturity Contract）

The Lightning Network is mainly comprised of two parts. The first part is the establishment of the bidirectional payment channel, namely RSMC (Revocable Sequence Maturity Contract). RSMC enables the opening of bidirectional payment channels between two people and secure off-chain transaction that can be terminated at any time without a third party. The second part is HTLC (Hashed Timelock Contract). HTLC enables off-chain transactions by establishing a payment channel through multiple intermediate parties when bidirectional payment channel is unopened. These two types of contracts constitutes the Lightning Network, so that any two people who are both on the Lightning Network function can complete the transaction off-chain.

State Channel

State channel is a off-chain scaling technology for performing transactions and other status updates, an upgraded version of the payment channel. The status channel can not only be used for payment but also for any status update on the blockchain. The nature of the state channel is to provide state maintenance services between different entities by establishing a bidirectional payment channel between either the users or the user and the service.



State Channel

The usage flow of state channel and that of payment channel are relatively consistent, including:

Open the Channel: two or more participants need to agree on the initial state, then two or more parties will store states or a certain amount of tokens in the hosting contract of the state channel, and then the state channel is turned on.

Using the Channel: between two or more participants in an open state channel, users can sign transactions and status off-chain without needing to submit every change of state to the chain.

Close the Channel: When a party needs to close the channel, one needs to submit a valid status update to the chain, and then enter a challenge period. During the challenge period, Participants on

both sides of the status channel can submit status updates with higher serial numbers at any time to prevent users from malicious behaviors. At the end of the challenge period, the valid state with the highest serial number is confirmed as the final state, and is recorded and settled by the main chain.

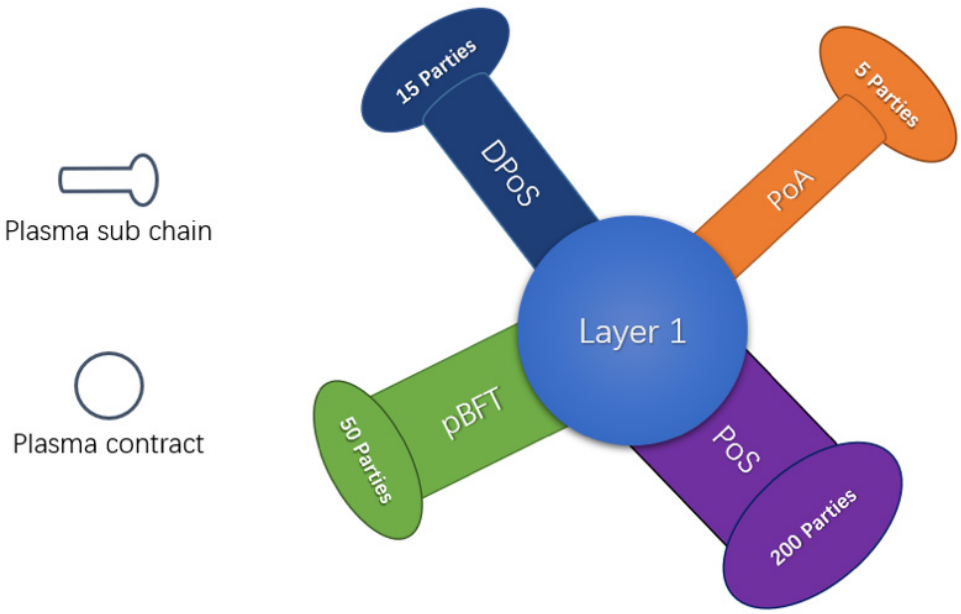
Status Channel allows users to transfer many operations out of the main chain, and users only need to communicate and sign off-chain without waiting for confirmation on-chain. After the completion of the multi-party signature confirmation off-chain, the final status will be submitted to the main chain for settlement.

Plasma

Plasma is an Ethereum-based scaling solution released by Vitalik and Joseph Poon in August 2017. Plasma is a series of automated smart contracts running on the root chain where users can lock their own assets, then map the assets to the corresponding Plasma chain. Plasma chain will be run and maintained by one or more verifiers, the root chain will require the Plasma chain to submit the Merkel Root for each block to the root chain. Only those blocks who completes the proof are valid.

Users on Plasma can verify the validity of Merkel Root with the saved Merkle Proof. To ensure the safety of the sub-chain operations, when users want to quit from the Plasma chain, they only need to submit a contract proof to the root chain, then transfer his assets from Plasma chain back to the root chain. In addition, to ensure that the verifiers on the Plasma chain won’ t behave maliciously, they need to lock a portion of the margin.

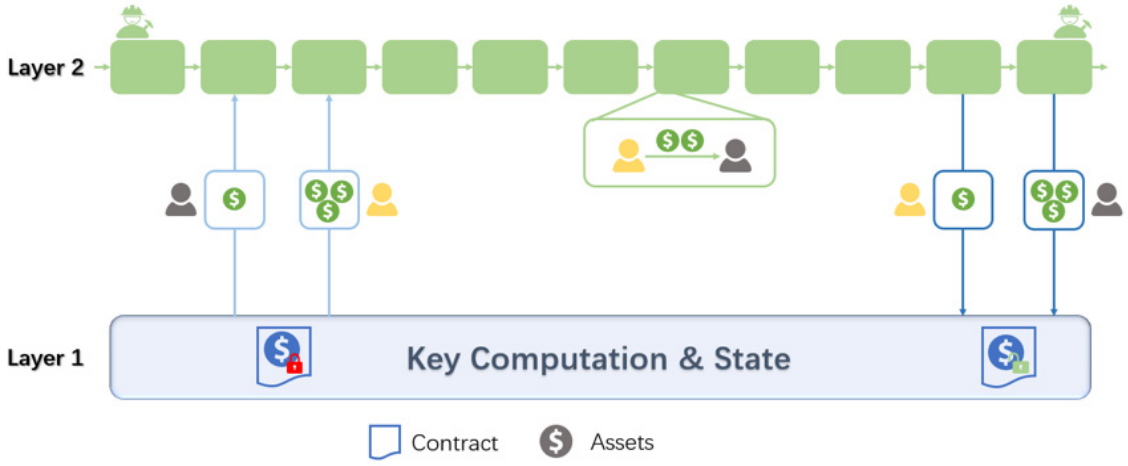
In the smart contract of the root chain, once arbitration occurs on the Plasma, the honest party submits a clear proof of the history of the relevant transaction and the margin of the malicious Plasma verifier will be deducted.



Plasma Overview

Side Chain

The side chain is a separate chain, which allows the asset to be safely transferred from the main chain to the side chain through side chain protocol, completes a series of transactions on the side chain and eventually returns to the main chain. The main difference between the side chain and Plasma is that Plasma is a side chain of no custody. When an error occurs on the Plasma chain, users will detect and submit it for arbitration, then exit the Plasma chain safely and transfer assets back to the main chain. While on the other hand, the safety of the side chain needs to be guaranteed by the side chain itself. Assets transferred to the side chain cannot be safely returned to the main chain when under attacked.



Side Chain

The asset transfer is mainly achieved with 2WP (2-way Peg) between the side chain and the main chain: the user needs to transfer a certain amount of assets on the main chain to a specific address which will be locked, and at the same time, when the evidence of the locked asset is found, the same amount of digital assets will be released on the side chain so that users are free to transfer and transact on the side chain. There are various kinds of 2WP implementations, from centralization to decentralization: Single Custodian, Multi-sig Federation, SPV (Simple Payment Verification).

Summary

These common Layer 2 solutions are rather different, complicated in design and difficult to understand, but if we dig deeper into the design ideas behind them, we can find some commonalities:

First of all, cryptographical fidelity of off-chain data is granted by participants' digital signatures which ensure that no one can forge other people's off-chain data.

Second, off-chain data format is defined by on-chain contract which ensures the recognition of the contract when submitted for settlement or arbitration.

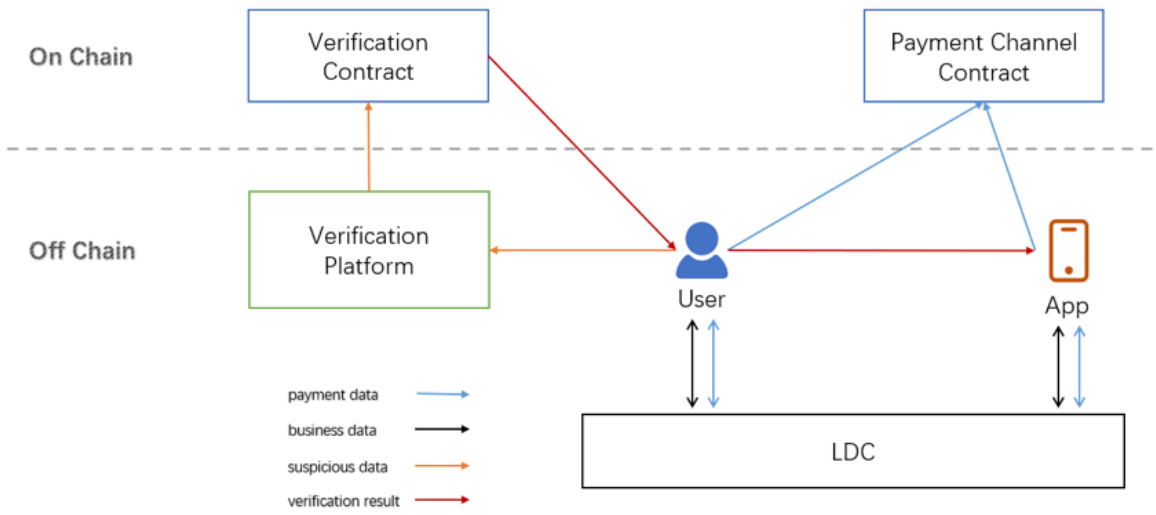
Moreover, Lightning Network, state channels, Plasma and side chains all essentially organize, transmit data of different forms off-chain and aim at different application scenarios.

Finally, when settlement or arbitration is required, they all require users to submit their own off-chain data to the smart contract on-chain for consensus and fixation, completing the return of state and assets.

It is not difficult to conclude from the above commonality analysis that Layer 2 is actually a design pattern. Essentially, these solutions regard public chain as the underlying consensus carrier, and promote the support for the application to the upper layer. This is the idea of blockchain layering. Therefore, we believe that layering is the best path for blockchain technology to reach users' daily life as well as the architecture design that best fits the business logic and user understanding.

LITEX Architecture

The LITEX structure is divided into two major parts: on-chain contract and off-chain protocol. On-chain contract includes the payment channel contract and the business verification contract, fixing state and logic in the consensus layer; off-chain protocol is used to process the organization, delivery, and verification of data off the chain, providing sufficient data credibility. In addition, LITEX provides a set of tools convenient for users to perform data query, submission and chain verification such as Layer 2 transaction browser, business verification platform, process playback tools, etc. The code for these tools and protocols will be open source. Any individual or team can build or reimplement data query and verification tools that suit their needs.



LITEX Overview

LITEX, as a Layer 2 application framework, is adapted to a variety of Layer 1 layer public chains. For better understanding, this whitepaper will use Ethereum as the basic chain to describe LITEX's product and technology solutions.

On-chain Contract

Payment Channel Contract

LITEX's payment channel is a series of channel contract combinations that are highly customized for consumer scenarios on basic of the status channel. Function-wise, in addition to the basic switch channel, deposit and withdrawal and asset preservation, it also provides unique features such as token combination, senseless upgrade, and readable transaction; Type-wise, it is divided into unidirectional channel and bidirectional channel, which better meet the needs of different business scenarios.

Switch Channel / Deposit and Withdrawal / Asset Preservation

For better understanding, we map the asset system of the crypto world to the real world:

First of all, we found that there is no cash in this world where all assets are digital and recorded by a credible bank (public chain). Each person's ID (public chain address) corresponds to an account balance (on-chain assets). At the beginning, money transfer has to go through bank remittance (on-chain transfer) with high fees and low speed. Later on, banks introduce debit card (payment channel), fees caused by transfer between cardholders is extremely low and lightening fast. Users need to pre-deposit some money to the debit card when they try to activate card (open the channel). If the balance is insufficient, users can transfer it from the account to the debit card (deposit). If the balance is over-sufficient, users can transfer it back from the card to the account (withdrawal); User can also cancel the debit card when they no longer need it (closed channel) and the unused funds in the debit card will be returned to the bank account.

So how is asset preservation reflected? In the real world, banks are endorsed by the state with high credibility. They will neither use the funds in your card nor detain the balance when the card is cancelled (except in special circumstances). In crypto world, trust is provided by the public chain, as long as users are able to prove their identities with private key signatures, no third party can stop users from withdrawal or refund. This is forced channel close, which grants the payment channel the ability to secure assets.

Token Aggregation

LITEX is able to use the same contract to carry the payment channels of both ETH and all the ERC-20 tokens. Token aggregation makes LITEX’ s payment channel unique, which is fairly important because users can easily determine whether the target address of the opening channel

points to the official contract or malicious fishing contract, thus ensuring asset security. With the decentralized address mapping service such as ENS, LITEX can also publicize the payment contract address as a more readable and easy-to-remember domain name like pay.litex.eth, further reducing the usage threshold and improving security.

Senseless Upgrade

Non-tamperability of smart contracts provides trust as well as peril. No developer is able to guarantee their own code yield no problems. No product manager dares to assert the design can meet all the future needs. Therefore, maintainability is the basics for consumer products. If the product upgrade requires users' large amount of time and money, even affecting the business operation of the partners, then its design is undoubtedly a failure.

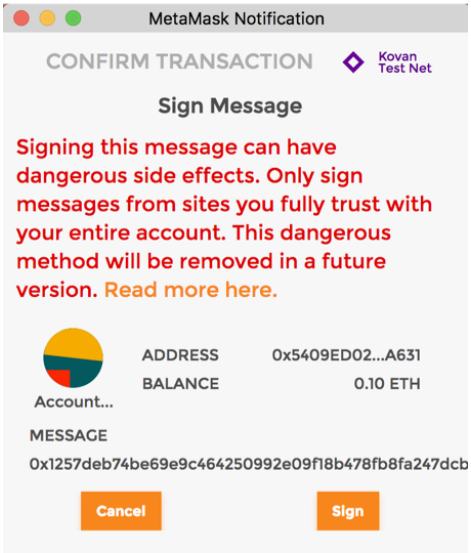
LITEX's payment channel contract uses Delegate Call technology, which enables it to upgrade the contract without changing the contract address. After the upgrade, users with the old version can still use it properly until the business process channel is closed.

When the channel is open next time, the user flow can seamlessly switch to the new contract logic.

The stability of the payment contract address allows developers to worry nothing about business interruptions and user losses caused by contract upgrades and integrate new features into your own products with assurance; seamless switching between new and old contracts provides the user with senseless experience of blockchain technology, and avoid user losses caused by frequently requiring user for cooperation.

Readable Transaction

Blockchain users have long gotten used to meaningless strings — whether public key, private key, or wallet addresses — combined with a bunch of random letters and numbers with the only difference in length, so are digital signatures. If it's just for money transfer, these gibberish is often not a problem at all because it only requires users to double check the transfer amount and the payment address; but when it comes to contract call, users can't acquire the specific content when signing. It's like someone wants to sign a contract with you, but you can't understand the contract. Such operation mode presents a significant risk.

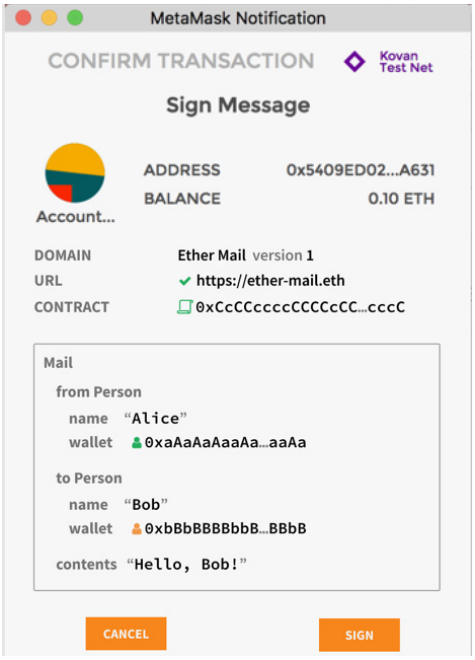


Signing non-typed data

Ethereum's EIP-712 specifies a new signature standard. If the wallet and contracts are signed according to this standard, users may acquire readable fields before signing, further get informed of the specific content to be signed. This operation is called signTypedData.

The LITEX payment contract fully supports the EIP-712 specification. Developers can customize the information that users need to confirm when making a payment request.

(such as currency, amount, order number, product information, etc.), users can fully be aware of which payment request corresponding to the order they are signing when confirming the payment, greatly improving user experiences.



Signing typed data

Unidirectional Channel

In the consumption scenario, merchant provides goods or services to the users, users pay funds to the merchant, and the merchant receives the funds for consumption or production. However, with restriction of the payment channel, the funds received by the merchant are still locked in the channel and submitted to on-chain contracts from payment contract after completing a on-chain transaction. But this operation is relatively complicated to implement because the design of the status channel is bidirectional in default. In a bidirectional channel, two ends are equally capable and free to make transfers. If one wants to withdraw or close the channel, in order to prevent it from malicious behaviors, one has to wait for the other party to sign and authorize this operation; if the other party is off line for a long time or disagrees with this, the one who initiates it has to submit a request to force closing the channel, and get the fund back when the other party submits off-chain transactions or waits over too long. This process is very complicated and time consuming, and also interrupts the channel between the merchant and the user. If the merchant needs to perform the above process with multiple users when initiating a withdraw, both parties will abandon this payment product.

However, the payment behavior in the practical scenario is mostly unidirectional: funds are transferred from the consumer to the merchant. Once we follow the unidirectional idea to redesign the payment channel so that funds can only flow from one end to the other, we will have a solution that fits the practical use case and greatly simplifies the design of the withdrawal process. In a unidirectional channel, only the payment from the user to the merchant needs to be verified, the users do not need to ask the user for approval because the user's payment funds in the channel are owned by the merchant;

merchants cannot forge more user payment credentials because they are unable to grasp the users' private keys. Merchants can unilaterally withdraw funds without disturbing users and only

need to submit an on-chain transaction to complete the withdrawal or even close the reopening channel. Unidirectional channel will greatly increase the merchants' power to control the funds in the channel with the guarantee of the safety of users' funds.

Unidirectional channel is one of the results of LITEX that combines technical solutions with practical scenarios and comprehensive optimization of product solutions.

It simplifies the technical implementation while solving problems and exemplifies LITEX's design philosophy as a consumer blockchain application framework.

Business Verification Contract

Traditional Layer 2 Contract: On-chain Justice + Off-chain Enforcement

If you have researched the current Layer 2 solution, you will find that the most difficult part is the programming of on-chain contract. On-chain contract of Layer 2 is equivalent to an automated court that needs to cover all possible business situations, give out results and execute automatically when an arbitration is requested. The goal of this kind of contract is fairly ideal, but the complexity of implementation in real life is extremely high, especially in the case where public chain has limited support for contracts.

Ideally, business logic can be described as a finite state machine, and all results can be described by a number of determined operations and a global state collection. Each step of the operation changes the current global state through the state machine, and then the participants sign, exchange global state and eventually submit it to the chain as proof. In practice, a complete business logic is difficult for FSM to describe, some of the steps may depend on the intermediate results of the previous steps, and may even require backtracking of the previous input. On the other hand, in order to process multi-step logic, the chain contract needs to have the participants turn the business from off-chain to on-chain at any step, which not only greatly increases the difficulty of development, but also creates a dilemma for users in such situations: either give up the business and bear the corresponding loss of default funds or continue on-chain business and undertake the follow-up transaction costs on-chain.

In the real world, law contains description of logic. For each specific case, the judicial system gives the conclusion and hand it to enforcement department for execution. The open source contract deployed on-chain has a global consensus, and its logic and execution are deterministic. Even contract deployer cannot modify it. This is "Code is Law" advocated by the blockchain industry. It is not difficult to find that smart contract is more than law. Since it is deterministic, it covers the scope of "justice" and "enforcement" as well. For the simple scenarios like payment channel, the "one-stop" process can indeed improve efficiency and achieve the effect of de-trust. But the real use case scenarios are often very complex, and it is difficult for us to consider all the boundaries needed for justice and law enforcement in advance. Even if the rules have been polished to a relatively complete level, putting logic of the judgment and execution with code to on-chain contract is extremely

complicated. Complex code makes the contract's security and readability greatly compromised and hard to be commercially viable.

We believe that in the consumer-level scenario, on-chain contract only needs to be responsible for rules publicity without having to consider "enforcement." This is the
idea of "on-chain verification, off-chain arbitration" demonstrated in business verification contract

Business Verification Contract: On-chain Justice + Off-chain Enforcement

Business verification contract is a unique form of contract in LITEX framework. On one hand, it largely reduces the difficulty of writing a Layer 2 contract while allowing developers to make full use of the public chain consensus value. On the other hand, the cost of using a business verification contract is very low. Without the need of sending on-chain transaction, one can use the full-node query api to get the verification result in real time, which makes users pay no extra cost whether verifying by themselves or verifying by assistant third parties.

From a developer's perspective: developers don't need to implement all business processes in contracts when writing business validation contracts. Rather, they only need to put the most critical business needs and the most reflected logic into the contracts, avoiding extremely complex abnormal process and the handling of on-chain process in the current Layer 2 contract. With this idea, developers can modularize design process with ease. After defining data api with other business processes, they can use any necessary technology stack to finish their business logic. In this way, not only the development efficiency has been improved, but also the maintainability of the product has been greatly enhanced because business logic that was originally implemented in the contract can be implemented with the traditional Internet backend and maintained at any time without the need of redeploying the contract.

From a user's perspective: if the user has any dissent to the result during the use of the application, the user can use data extraction tool provided by the LITEX off-chain protocol, obtain the data corresponding to off-chain query, and select
trusted third-party data platforms (such as etherscan.io, etc.) or their own tools to call the validation contract query, send off-chain data, get clear and easy-to-read verification results, and even play back the entire business process. LITEX Business Verification Contract allows users to easily experience the value of the "verifiable" blockchain features, helping users deepen their understanding of blockchain application and develop a habit of paying attention to the legality of data.

Off-chain Protocol

Off-chain contracts are like anchors that specify what state is legal and how to commit them. With the guarantee of contract, off-chain protocol can be designed flexibly and presented in various forms according to needs. An extreme example will be: two people who understand the contract can reach a simple off-chain

protocol by sending each other an email containing the data off-chain; with the same contract, the other two people can even convert the signature data into a QR code, print it and mail it with an envelope to the other party in order to reach a more primitive under-chain agreement. All in all, as long as the data off-chain meets the requirements of on-chain contract, and can be understood, generated and transferred by involved participants, it should be a qualified off-chain protocol.

However, the design of off-chain protocol in the above example has a fundamental premise - users need to have a strong knowledge of blockchain technology. For long,

blockchain is aimed at tech people instead of general Internet users who barely understand the concepts, not to mention the practical operations. The product structure of Layer 2 is more difficult to comprehend than that of on-chain contract. If the off-chain protocol and products are not optimized, a qualified user must:

Understand the design pattern of Layer 2
Understand the logic of on-chain contract
Be able to discover anomalies of off-chain data
Be able to submit off-chain data to the contract to preserve his or her assets

These requirements go far beyond the capabilities of the general user base and are typical industrial-grade design. To support consumer applications,

LITEX must break the assumption of users' high ability when designing off-chain protocol, and look at the problem from the perspective of users and apply targeted optimization, so that reduce users' perception and usage threshold of blockchain products.

Existing Problem

Users cannot control their own data

Off-chain data is the only evidence that the user protects his or her own rights. In general, users are responsible for managing their own data as well as private key of the crypto account that users have to bear the loss themselves once lost. However, for general users who don't understand what database is, off-chain data is invisible and uncontrollable. Therefore, users can only hope for a user interface to display it. This creates a huge deal of inequality because the developers actually manage the off-chain data of both parties. Once a problem occurs, it is difficult for users to protect their rights – if developers don't provide api, users cannot even export their own off-chain data.

Users cannot handle connection drop

In addition to the data control issue, the Layer 2 system itself has a big problem - connection drop. Suppose there is a channel between Alice and Bob. Under normal circumstances, when Alice wants to close the channel, if Bob is online and agrees with this, they can close it cooperatively. This is the most ideal situation. If Bob disagrees, Alice can submit a mandatory channel close request to the contract, then the contract will give Bob time window long enough to submit his own off-chain

data, in case Alice deliberately submits the data that benefits herself and causes Bob losses. If Alice deliberately submits mandatory channel close request when Bob is offline for a long time, she is likely to rob Bob's assets in the channel, which is how the connection drop problem describes. The current solution to this problem is to set up a "guardian" network users hire that submit off-chain data when connection drop happens. In fact, users are very difficult to be convinced about spending money on this service when they don’t even understand the nature of connection drop, which in turn will make it difficult for the nodes that provide this service to recover the cost and establish such a network.

Insufficient credibility of off-chain data

From a developer's perspective, traditional off-chain protocol has the problem of insufficient data credibility. Off-chain data like chat information is always peer-to-peer, which makes it impossible for anyone other than the developer to grasp the full picture of the data. But in the consumer area, a product’s number of users, level of user activities, income and other information are all extremely important measurement. Good products hope to share this to the market. Therefore, the current situation of low data credibility has also caused great trouble to developers.

In order to solve the problems above, LITEX chose to use the license chain solution as the basis of off-chain protocol which is LITEX Data Chain, as known as LDC. Unlike the side chain approach, LDC only carries the duty of the organization, storage, and delivery of data off chain in the LITEX architecture without involving assets transfer. In other words, LDC is a distributed database shared by all applications and users within LITEX framework. The nodes of the LDC are maintainers of databases, verifiers of off-chain data and guardians of the users. This design solves problems above perfectly.

LDC-LITEX Data Chains

Overview

The LDC is implemented by a license chain cluster. The number of single-chain consensus nodes is no more than 100, and the block generation time is not more than 0.5s. With a TPS of no less than 10,000 and a multi-chain integrated TPS of more than one million, it can suffice the needs of most current commercial products. LDC’s

consensus mechanism, cryptographic primitives, underlying database and virtual machine are all pluggable designs, and are compatible with Ethereum's address format and signature algorithms and all of its development tools. With the development of LITEX on multiple underlying public chains in the future, the support for heterogeneous chains can be continuously added to LDC. LDC can control access based on roles. Its performance and privacy protection capabilities can also be optimized as the technology develops.

Consensus and Nodes

LDC currently uses the pBFT consensus algorithm, in a single-chain consensus network that consists of N nodes, to ensure liveness and safety, while providing fault tolerance of (N - 1) / 3. Considering that performance and latency are greatly affected by the number of nodes, N is set to be no more than 100. LDC is instantly deterministic.

The nodes of the LDC are divided into two types: the consensus node and the verification node. The former is the full node and the latter is the light node. Consensus nodes have the rights to create blocks and participate in the governance, whereas the verification node only has permission to receive transactions. Joining a node requires an access check through the network. If the identity verification failed, and even if it can successfully connect with other nodes at the data network level, no transaction data can be obtained.

The consensus node needs to be selected by voting, and N of nodes with the highest number of votes automatically obtain the block creation permission and the governance permission, and enjoy the block rewards and governance incentives. After the LITEX Token is locked by the voting on the underlying public chain, the corresponding voting rights can be obtained on the LDC, which can be used to vote for one or more nodes. To withdraw the vote, you need to go through the 72-hour unlock period to get the LITEX Token on the underlying chain unlocked. The voting address can receive the governance incentive given by the ecological fund, and the specific incentive method is given in the economic model section.

As a license chain, LDC can dynamically adjust the block weight of the consensus node. Being adjusted once an epoch, it matches block rewards with staking and voting situations through weight adjustment, as well as lower the privilege of unresponsive and unstable nodes. Specific information on the block rewards will be discussed in detail in the economic model section.

Account and Privileges

LDC's accounts are divided into general accounts and contract accounts. The former is an account that has a private key and a public key, and can issue a transaction. The latter is an account that has code logic and data storage. Different from the public chain, the LDC account can be grouped, which makes it easier for privilege management. Groups are achieved by contracts. Each group contains a list of accounts and subgroups, and records the identity of the parent group, which forms a tree structure.

As a license chain, LDC has role-based rights management capabilities. The privilege system is based on contract implementation and can be used for either setting privileges of individual accounts or creating roles for unified management. Common privileges include sending transactions, creating contracts, adding or deleting nodes, etc. One can customize other privileges based on your business needs.

By default, LDC has a superAdmin - super administrator account that can perform operations of the highest privileges on LDC, such as addition and deletion of consensus nodes, managing role

permissions, etc. However, as an underlying facility for an application framework, LDC’ s data needs to be credible and governance authority also need to be implemented by ecology, so on-chain governance mechanism becomes an essential functional module.

On-chain Governance

On-chain governance refers to management rules that can be automatically executed according to conditions during the operation of the blockchain, such as the granting and withdrawal of node permissions, dynamic adjustment of gas rates, etc. In contrast, off-chain governance refers to the process of making decisions through the management committee, and then adjusting the rules on chain through administrator privilege. It is self-evident that on-chain governance, without the risk of centralized governance, is more transparent and more efficient. It is therefore the preferred way of governance in blockchain.

The LDC decentralizes super admin privileges into multiple sub-rights, each of which can be controlled by one or more governance contracts. This mechanism makes the implementation of on-chain governance transparent: the voting result of the consensus node can automatically take effect and the synchronization between the voting result and the data of the underlying public chain can also be verified automatically. As the business develops, on-chain governance can be constantly revised and supplemented, just like laws in the real world, which helps to ensure the security of the LITEX crypto economy in light of evolving challenges.

Privacy Protection

The credibility of off-chain data is of great significance to developers, but the privacy of payment data is also extremely important to users. Compared to the services of centralized architecture, LDC's data does not rely on the storage of the central server, so it can avoid data loss or data leakage from a single point of failure. P2P networking can minimize the exposure of information like IP address; user accounts are created based on cryptography, which does not need to correspond to the actual identity. These are the advantages of LDC as a blockchain architecture for data privacy protection.

However, blockchain still has privacy disadvantages. In order to quickly reach consensus and trace transactions, on-chain data is open and transparent.

Therefore, anyone can see all the data from the genesis block to current block and track all transactions. Although the address information within the transaction does not

correspond to any real information, in reality, the information of the user in real life will inevitably be exposed. As a result, it creates a possibility that the address on the chain can be matched to the identity off the chain; coupled with the traceability of the blockchain transaction, it is more likely to cause privacy leakage.

In response to this problem, LDC has prepared two solutions. The first is a cryptography solution that can use zero-knowledge proof technology to protect the privacy of transactional data. Once it starts, it does not need to know the address information and transaction content of the sender, only need to provide relevant

proof. This solution can effectively protect the address information and transaction details of the sender and receiver. However, it may put a bottleneck on performance, and is therefore suitable for use in more critical business scenarios such as payment scenarios. The other solution is data isolation that separates sensitive data through side chain or even outside the chain, and put the witness information that needs to participate in the consensus on the LDC. This solution is better in performance, and easier to combine with existing scenarios.

Connection Drop Prevention

LDC can effectively solve the problem of connection drop in the Layer 2 solution. LDC nodes are ecological maintainers and beneficiaries. Because each transaction will be processed by the nodes, the nodes will get the transaction fee benefits and have the responsibility and ability to help users submit evidence on chain in case of connection drop. In addition, to incentivize nodes, a portion of the fee income will be set aside to reward nodes that have successfully helped users submit off-chain data.

When the user signs the off-chain data, an authorization is automatically issued, so that all nodes that obtain this data can submit data to the contract. On the other hand, the applicant must apply to force the closing of the channel according to on-chain contract by oneself, not by other addresses. With this mechanism, the node cannot maliciously replace the user to perform the forced closing operation, and can only help the user to submit off-chain data when the opponent initiates the forced closing operation, which fully guarantees the security of the user's assets.

Advantages of LDC

Improved Data Credibility

As a license chain, the off-chain data stored on LDC is public and non-tamperable. Developers are free to change the data on LDC. Since off-chain data is based on the information queried on the LDC, the developers cannot falsely report data numbers as in other Layer 2 scenarios. Because developers cannot obtain user's private key, they cannot forge the off-chain data (ie, payment data) signed by the user's main address. Therefore, the data on LDC largely reflects the actual operation of the user, and is therefore credible statistics, which in the future can be used as a measurement for applications in the LITEX ecosystem.

In addition, LDC is also resistant to sybil attacks. Since LITEX's payment channel is a unidirectional channel, developers can’ t falsify transaction volume by creating multiple accounts and transfer between them. Once the funds in the channel are exhausted, funds can only be traced through on-chain transactions or new open channel. This method costs the same amount of money and time as directly forging the transaction volume with on-chain contract. As for other Layer 2 solution that uses P2P or bidirectional channel, falsifying trading volume is very easy. But because their off-chain data has no credibility, directly reporting falsified data can be a more cost-efficient method.

Secure Data

Off-chain data is the most important part of the Layer 2 application. The user's asset security is completely dependent on the preservation and management of off-chain data. LDC, via license chain, manages the off-chain data in a more secure way. There will be no data loss caused by users clearing the cache or accidentally deleting the application, and the application data will not corrupt due to a single point of failure in developer’ s server.

User-Friendly Experience

Under the traditional Layer 2 application model, due to lack of tech knowledge, users do not know where their own off-chain data is located. It is also impossible for them to extract such data for on-chain arbitration. They can only rely on developers to provide corresponding user interface in order to query and extract off-chain data. Essentially, one party control off-chain data of both sides, which makes users very vulnerable and passive.

Off-chain data stored on LDC is completely transparent, and users can query data with the official blockchain browser. They can also filter and group the data according to the type of application, interaction process, usage time so that users can quickly identify what off-chain data they want to arbitrate or verify and submit the data with just one click. LDC's blockchain browser, verification platform and other technologies will be completely open source. Any third party can build and customize the data query and verification platform that conforms with the LDC data protocol, and then serve corresponding users.

LITEX Economic Model

As a multi-role Layer 2 ecosystem, LITEX needs a set of incentive rules to ensure its health and growth, and return the value of the ecology to all participants. Thus, LITEX issued LITEX Token (The symbol is LXT) to implement this idea.

LXT is an ERC-20 token issued on Ethereum with a total number of 2 billion. It can neither be minted nor destroyed. As LITEX supports more public chains, LXT has the ability to perform partial cross-chain migration on demand, and the total number of LXT in the network will not increase in the process of migration. The distribution of LXT is shown in Appendix 1.

Value Capture

LXT, as a token in the LITEX ecosystem, is required to have the ability of capturing the entire ecological value. LITEX’ s main product is divided into two parts: cryptographic payment and business logic. Since the resource consumption involved in these two parts is different from that of

the main participants, it is necessary to develop a corresponding value capture method, taking into account the various roles in the LITEX ecosystem and striving to ensure the consistency of interests of all parties. In addition, in order to encourage the nodes to join in the early stage of ecology, LITEX will also take some of the tokens as block rewards, and assign to all consensus nodes according to block creations.

Cryptographic Payment

The endeavor of LDC consensus node makes users securely and quickly pay through the payment channel in the LITEX network. In order to maintain the security, stability and processing efficiency of the LITEX network, the consensus nodes need to invest a lot of money and energy to facilitate the operation of the node software. Therefore, it is reasonable for the consensus nodes to get a certain percentage of the fee from the total amount paid. As the last guardian of user transaction security, the verification node of the LITEX network monitors each transaction on the chain, ensuring that the network consensus node is not working maliciously. Therefore, the verification nodes should also get a portion of the transaction fee income.

When a user makes a payment in the LITEX network, he/she needs to pay a certain percentage of the transaction fee according to the type of token actually used. The transaction fee will be first distributed in accordance to the consensus node and the verification node, and then to the proportion of the number of LXTs staked by their respective types of nodes. Specific allocation rules will be described in the Value Assignment section.

Business Logic

When developers are building on LITEX, they need to pay a certain amount of fees for occupying LDC’ s resources, which mainly include: computing resources, network bandwidth resources, storage resources, etc., wherein computing resources and network bandwidth resources are short-term consumption resources that will be refreshed in real time, and storage resources are long-term consuming resources, which require long-term storage costs for consensus nodes. Therefore the economic model does not calculate the developer’ s consumption of computing resources and network bandwidth in the early stage, which has been subsidized in block rewards to the consensus nodes. But developers need to pay a certain amount of cost for non-renewable storage resources.

LDC will give developers some initial storage space, which is free. Nevertheless, as the data grows, if these spaces have not been updated for a considerable period of time, they may be recycled after a snapshot, and its contents are stored in read-only form in the archive server. In order to get more available storage space, developers need to stake LXT, according to the actual situation of the application, to get storage space in the LDC network. Because LXT is a non-inflation model, developers will not have actual financial loss. They are just locking the LXT liquidity to obtain limited storage space from the LDC network.

Block Rewards

The values described above depend on the development of the LITEX ecosystem. If the ecology prospers, these values can bring considerable benefits to all nodes. In the early stage, however, it is difficult to cover the cost of maintaining the network. Therefore, LITEX will come up with a portion of LXT as block creation incentives for the consensus node that participates in the network construction in the early stage.

Value Distribution

LXT, as a token in the LITEX ecosystem, is required to have the ability of capturing the entire ecological value. LITEX' s main product is divided into two parts: cryptographic payment and business logic. Since the resource consumption involved in these two parts is different from that of the main participants, it is necessary to develop a corresponding value capture method, taking into account the various roles in the LITEX ecosystem and striving to ensure the consistency of interests of all parties. In addition, in order to encourage the nodes to join in the early stage of ecology, LITEX will also take some of the tokens as block rewards, and assign to all consensus nodes according to block creations.

Payment Fee Allocation

Type of Node	Distribution Ratio	Distribution Method
Consensus Node	70%	Distributed according to votes received
Verification Node	30%	Distributed according to votes offered

LDC Space Staking Rate

Type of Space	Space Volume	Staking Ratio	Is Permanent Storage
Initial Space	100 MB / Contract	0	No
Produced Space	10 TB in total	10 LXT / MB	Yes

Block Rewards

Total	Rewards / Block	Block Creation Rule	Rewards From
300 million LXT	2 LXT	Halving per 2 years	Reservation of Ecosystem Construction

Unified Value

Consensus Node

As the main resource cost payer of the network, the consensus node obtains the ecological reward from the ecosystem as well as transaction fees paid by a portion of users; since developers need to stake a certain amount of LXT to get a certain percentage of storage space, it guarantees that the consensus node does not need to increase the hardware cost without an upper limit.

Verification Node

As a security guardian for the entire network, the verification node can get some of the ecological rewards from the system. It can also obtain a portion of the transaction fees through staking LXT. In addition, when the verification node finds a transaction error in the network or the consensus node behaves maliciously, the verification node can submit for arbitration. If the transaction is confirmed to be wrong or the behavior is malicious, the verification node can also get additional verification rewards.

Users

Users mainly want to obtain secure and efficient transaction transfer services. The 100 consensus nodes on LDC' s single chain, to a certain extent, ensure the decentralized characteristics, reduce the possibility of the consensus node behaving maliciously, and adopt an efficient payment channel. Provided with more than 10,000 TPS capabilities, users can get a secure, efficient and low-cost transaction transfer experience.

Developers

LITEX provides developers with complete technical solutions to help traditional developers conveniently utilize blockchain technology to build their own blockchain applications. It will also

facilitate the growth of products by taking advantage of the ecological infrastructure within the blockchain.

LITEX Ecology

In the entire LITEX ecosystem, consensus nodes, verification nodes, and developers all need to freeze a certain amount of LXT to get the dividend rights of the corresponding transaction fees or the required development resources. The entire economic model fully balances the interests of all parties in the ecosystem to ensure the consistency of the interests of all parties.

Organization

LITEX Community Foundation

The LITEX Community Foundation is based in Singapore and is the legal body of the LITEX community. It is responsible for LITEX's technology development, business operation and marketing, as well as all legal responsibilities of LITEX.

The LITEX Foundation has a highest decision-making committee that utilizes its power to manage and constrain the various other agencies within the Foundation. The decision-making committee has a three-year term and will be elected by the LITEX community upon expiration.

Subordinate Executive Departments:

Technical Department : Mainly responsible for developing technical route, tech solution selection, architecture design, project development and management, and Github repo update and maintenance for the LITEX community open source project.

Operations : Mainly responsible for the operation and management of the LITEX community, including community event planning, event execution and implementation of community incentive programs.

Marketing : Mainly responsible for community branding and marketing, business development, and construction of community ecological.

HR & Finance Department : Mainly responsible for the recruitment of LITEX Foundation volunteers, the management of Foundation members' financial related business.

LITEX Lab

Guanghong Xu - CEO

Guanghong graduated from the Department of Mathematics majoring in Cryptography at Peking and received a Master's degree from Illinois Institute of Technology majoring in Applied Mathematics and Computer Science with research interest in PKI encryption system. He once worked at VeriSign and served as a risk strategy and security consultant at Deloitte. He also participated in the work of payment information encryption certification during VISA’s IPO in New York Stock Exchange as well as the work of top global programs and companies in information encryption and digital certification such as Apple, Electronic Arts (EA), and Broadcom. He has extensive experience in cryptography and business applications, and currently serves as the Director of Corporate Risk Strategy at Kaiser.

Leo Wang - COO

Leo received his degree of Bachelor of Science (2003-2007) and Master of Science (2007-2010) from the Department of Computer Science at Peking University. He served as operation manager in "Non-bank card payment" department at Yeepay, the world's largest decentralized payment product. He is a serial entrepreneur, executive director of Peking University CEO Club, and blockchain technology evangelist and practitioners.

Johnson Zhang - CTO

Johnson received his degree of Bachelor of Science (2003-2007) and Master of Science (2007-2010) from the Department of Computer Science at Peking University. He is a blockchain expert, network security expert, full stack developer, LTXN designer. He served as senior R&D engineer at IBM and Sina Weibo.

Frank Lou - CPO

Frank received his degree of Bachelor of Science (2007-2011) and Master of Science (2011-2014) from the Department of Computer Science at Peking University. He is a blockchain expert, project architect, full stack developer. He has extensive experience in combining product requirements and cutting-edge technology design solutions.

Teddy Chu

Founding Partner and Vice President of Duolabao, former Senior Product Operation of non-bank card projects at Yeepay. He also worked as the product manager of Baidu Shenbian team. He received a Bachelor's degree and a Master’s degree in Computer Science and Technology from Beihang University. Duolabao was once China’s leading marketing and sales company in offline payment, top three WeChat payment service providers and serving more than 2 million transactions every day.

Cornerstone Investors and Consultants

Chen Yu - Investor

Co-founder and President of Yeepay. He graduated from the Department of Computer Science at Peking University and gained 20 years’ experience in the Internet, e-commerce and software fields.

He was in the honor list of "100 people in China Mobile Influence Gold Award" and awarded eWorld 2013 e-commerce world "2013 EC100 China e-commerce marketing hundred people" . He is the author of the best-selling book "Seeing the Future: People Changing the Internet World."

Dawei Chang - Investor

Founder and CEO of Duolabao, founder and former CTO of Yeepay, and a senior software engineer at Riverside in Silicon Valley. He received a Bachelor of Science degree in Computer Science from Peking University and a Master of Computer Engineering from the University of Maryland. He was also a member of the Chinese Engineers Association in Silicon Valley.

Jeffrey Wernick - Consultant

Ph.D. in Economics and Finance from the University of Chicago, an early participant in Bitcoin, an early investor in Uber and airbnb.

Lin Cong - Consultant

Member of the Wall Street Blockchain Alliance, String Labs Consultant, He is currently a professor of finance at the University of Chicago, a doctoral tutor, and a professor at East Asian Studies Center, Summa Cum Laude and Phi Beta Kappa award winner.

Bin Chen - Consultant

Former PayPal Senior Architect. He received a master's degree from Jilin University in 1989. He was the Director of System Integration at Hitachi USA and the chief architect of Abacus, Chief Engineer of Internet Applications at Nokia, having a wealth of overseas experience, years of experience in the payment industry. He translated and published "Architecture and the Future", "Architectural Truth" and "Data is the Future - The Road to Big Data". He is the practitioner and preacher of cutting-edge technologies.

Token Fund Investors

Appendix I: LITEX Token (LXT) Distribution

Quantity	Ratio	Used For	Specification
700,000,000	35%	Pre-sale	Targeted at token funds, used for development, recruiting and marketing. The usage of part will be shown to the public regularly.
300,000,000	15%	Ecosystem Construction	Used for ecosystem initialization such as airdrop, block rewards, etc
600,000,000	30%	Development Fund	Used for developing business partners and building teams. The usage of this part is determined by LITEX foundation and will be shown to the public in advance.
300,000,000	15%	Team	Rewarding the team for exploring the crypto world, developing and maintaining the product and operation of LITEX. This part will be frozen in smart contract when issued and unfrozen 1/36 every month afterwards. It takes 36 months to finish the entire process.
100,000,000	5%	Consultants and Business Partners	Targeted at business partners and consultants.

Appendix II: LDC Consensus Node Configuration Reference

Type	CPU	RAM	Storage	Bandwidth	Average Latency
Onboard	2 Cores	4G	30G	10M	≦ 10ms
Production	4 Cores	8G	200G	100M	≦ 10ms
Recommended	16 Cores	64G	500G	100M	≦ 10ms