LEXEL

Chip-Level Digital Identity Authentication Hardware Infrastructure based on Blockchain

White Paper V2.0

www.lexel.io

LEXEL

Provide Comprehensive Security Hedging and Appreciation Solutions for Personal Crypto Assets

www.lexel.io

Abstract

Regarding the current Internet authentication, no matter login passwords, capital passwords, or SMS verification codes are applied, they can be intercepted or even simulated by hackers. Many hardware-level encryptions are just memory-level that can also be intercepted and simulated. There are serious security issues in many areas such as the Internet, the Internet of Things, and Blockchain, and the situation is getting worse.

LEXEL is a digital identity authentication and crypto asset security solutions provider. It provides users with personal identity authentication and chain of trust based on Blockchain, and offers a comprehensive security hedging and appreciation solutions for personal crypto asset. It can be applied in scenarios such as personal trusted digital identities, crypto asset wallets and cryptocurrency exchanges.

Currently, digital authentication (CA) of the Internet and financial industry is widely used. However, the traditional digital authentication is based on centralized enterprises as its certification bodies. It faces various risks such as information abuse and internal control. It also causes the situation that individual certification body conducts business independently, which cannot be completely trusted accordingly.

The Internet of Value led by current Blockchain technology requires a credible personal identification system as the underlying foundation for value exchange. Based on this foundation, we can further expand the exchange of trustworthy values between individuals and organizations, as well as between individuals and individuals. LEXEL is committed to becoming the underlying foundation for value exchange, providing a trusted underlying identity authentication chain of trust for the prosperity of Blockchain application scenarios.

The identity authentication chain of trust based on LEXEL also provides users and organizations with a comprehensive crypto asset security solution, ensuring the security of crypto assets. Furthermore, LEXEL will develop a value-added ecosystem for crypto assets in the future and create smart contracts on the Public Chain, aiming at fully solving the problems of crypto asset exchange, and promoting credit and investment between individuals and individuals as well as between individuals and institutions ecologically.

LEXEL

Catalogue

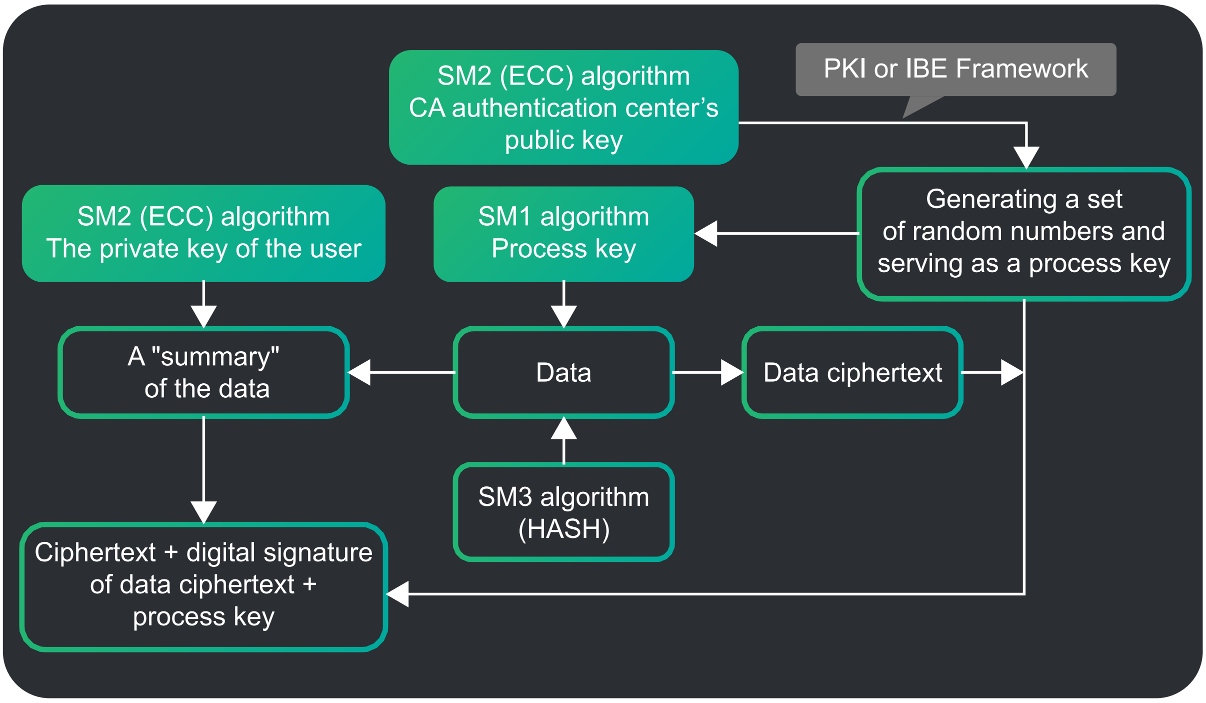
1. Market Overview

1.1 Market Background

In the 1980s, American scholars proposed the concept of PKI (Public Key Infrastructure). In order to promote the application of PKI in the federal government, the United States established the Federal PKI Steering Committee in 1996; in 1999, the PKI Forum was established; in April 2000, the US Department of Defense announced the adoption of the PKI Security Initiative. On June 13, 2001, an international organization that promoted the PKI process in Asia and Oceania was proclaimed. It is the “Asia PKI Forum” and its purpose is to promote PKI standardization in Asia and lay the foundation for global e-commerce.

• What is PKI?

PKI is the abbreviation of Public Key Infrastructure (PKI) and is a generally applicable network security infrastructure. Some American scholars call PKI a collection of infrastructures that provide comprehensive security services, including software, hardware, people, and strategy, but our understanding is focused on public key technologies more.



SM2 (ECC) algorithm CA authentication center’s public key
PKI or IBE Framework
Generating a set of random numbers and serving as a process key
SM2 (ECC) algorithm The private key of the user
SM1 algorithm Process key
A "summary" of the data
Data
Data ciphertext
SM3 algorithm (HASH)
Ciphertext + digital signature of data ciphertext + process key

▲ PKI Authentication architecture logic diagram

Digital certificates are the most basic elements of PKI. All security operations are mainly implemented through certificates. The components of the PKI also include a certification authority (CA) that signs these certificates, a registration authority (RA) that registers and approves the signed certificates, and an electronic catalogue that stores and publishes these certificates. In addition, PKI also includes certificate policies, certification paths, users of certificates, and so on. All of them are the basic components of PKI. They are organically combined to form the PKI.

- **Available Services**

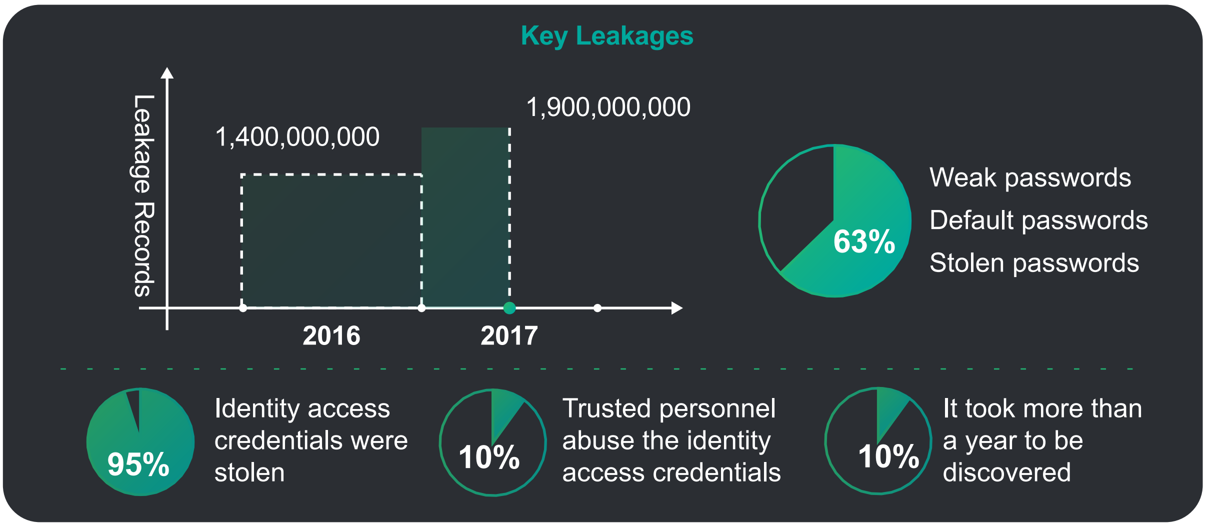
PKI has been widely used in finance, e-government and other fields. For example, online banking uses digital certificates to determine user identities, and enterprise and institution information systems use hardware-based USBKEY or IC cards for identity authentication and other information protection. Among them, applications in secure email, web security applications (SSL/TLS), VPN, IP/sec, and e-commerce are particularly prominent.

1.2 Existing Risks

PKI security includes so many aspects, including device security, operational security, protocol security, and so on. Although PKI has so many application scenarios, there are several fatal problems existing in PKI:

- **Low Security**

As to the present Internet, the main way for servers to authenticate users is the cryptosystem. A user creates a password when using the website for the first time in order to confirm his identity during subsequent visits. Most of the digital signature authentication in the market apply software-level and memory-level encryption, passwords of which can be easily simulated or stolen by hackers, bringing higher risks to user information and funds. To be specific, passwords are either too weak or too complicated. Each website requires a unique password, and it is inconvenient for recovery when users forget their passwords.



- **Insufficient Performance**

The PKI technology is based on the RSA encryption algorithm. It requires the establishment of a CA digital authentication center and adopts a third-party participation mode. The key is distributed and generated in a centralized manner. With the growth of users and the requirements of encryption security, PKI has no choice but to extend the key to RSA algorithm. Accordingly, data stored in database gets larger and the running speed will become slower.

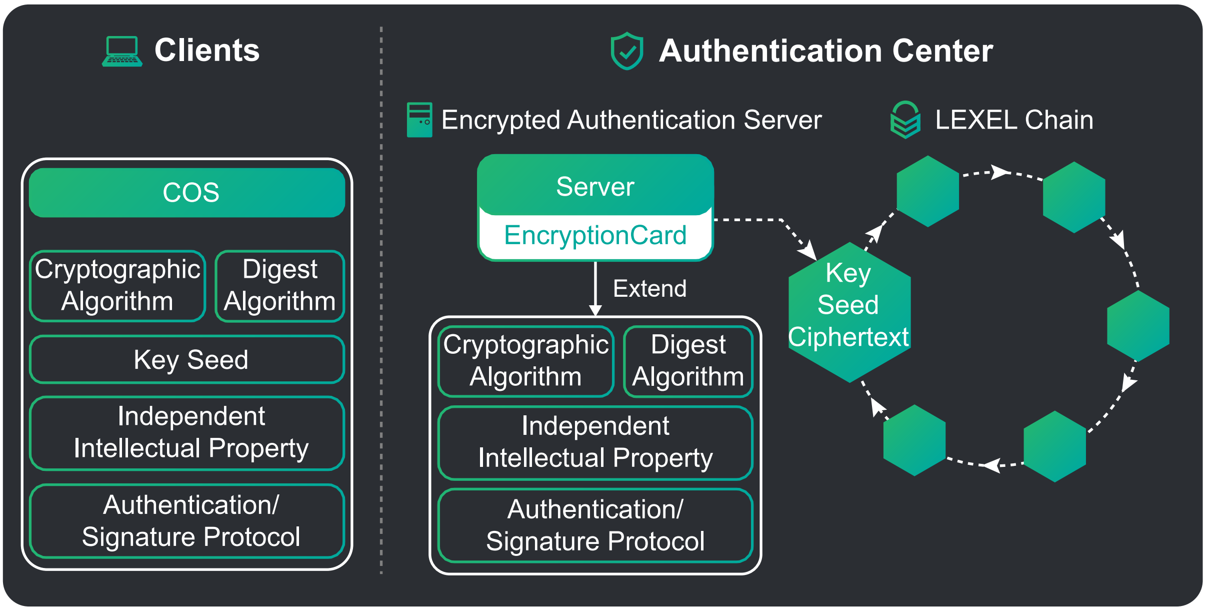
- **Higher Cost**

The PKI authentication process requires a large certificate database for online comparison authentication. For every 1000 users, it is necessary to establish a level 1 CA and a set of databases to store certificates and keys. The speed of database online authentication is low, and the amount of users being managed is small. At the same time, due to the huge database and server architecture, a large number of operation and maintenance personnel are required to ensure the security of the equipment, thus the operation cost is heavy.

2. Key Technical Advantages

2.1 LEXEL Digital Encryption and Security Authentication

The LEXEL system comprises identity authentication, digital signature, key exchange and data encryption protocol. Through the use of symmetric cryptographic algorithms (e.g. cryptographic algorithm, digest algorithm), four functions such as authentication digital signature key exchange and data encryption are completed.



▲ Encryption chip architecture

The key technology lies in how to solve the worldwide problem of key management of single key cryptography. It has the following major characteristics:

2.1.1 Autonomous Controllability

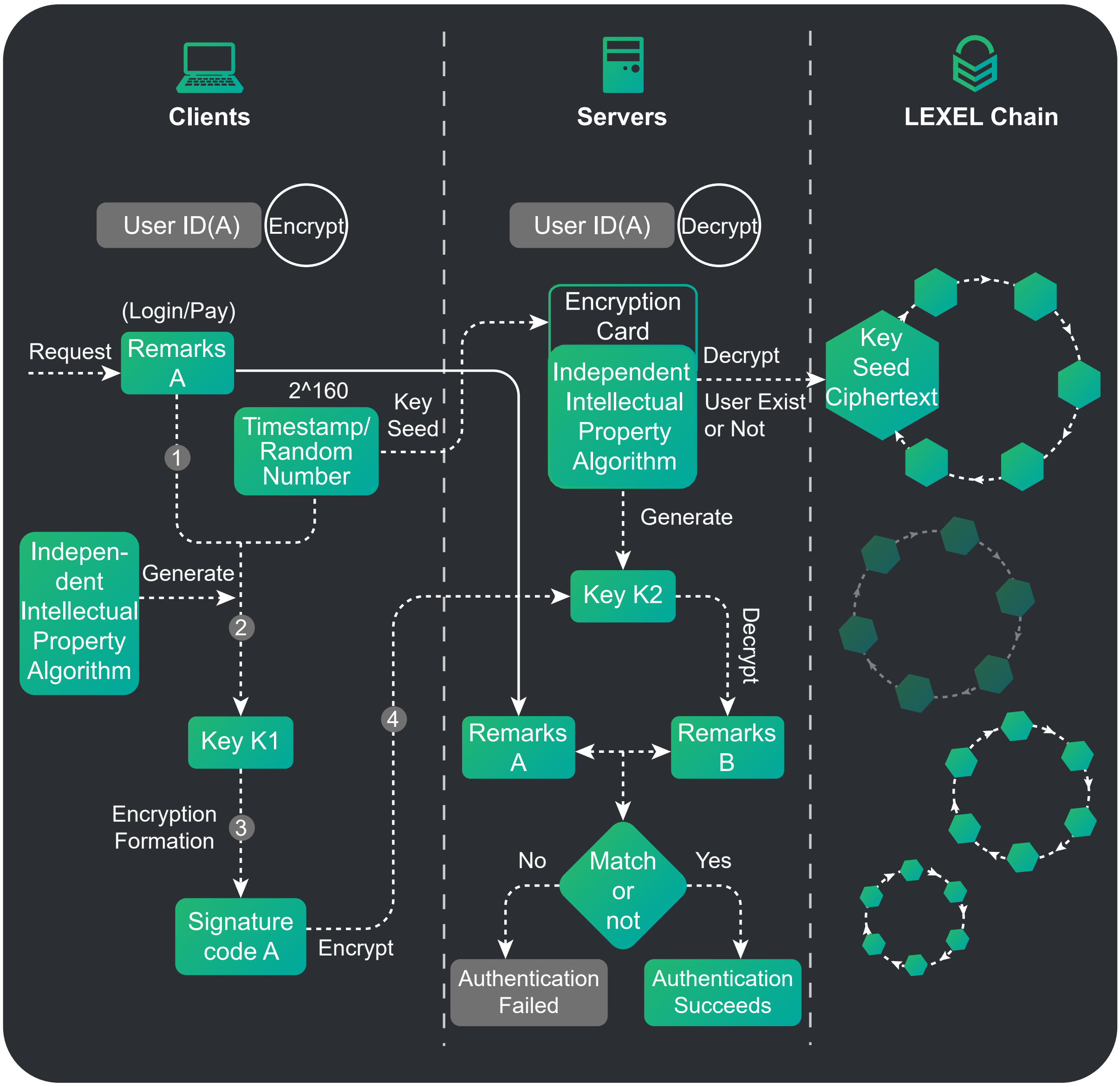
Being autonomous and controllable means to rely on own research and development design, master the core technology of the product, and realize the whole process of self-development, production, upgrade and maintenance of information system from hardware to software. From encryption device to algorithm, from operating system to database, LEXEL 100% uses its self-developed technologies and complies with the national standards, truly ensuring products to be entirely autonomous and controllable from hardware to software.

2.1.2 Advantages Compared with Traditional Authentication Technology

(1) Architecture Comparison

Traditional authentication technologies such as PKI apply two sets of algorithms, 2+3 algorithms and calls to complete the standard authentication process, and the key and device are matched. However, LEXEL calls a single-key algorithm to complete all the authentication procedures. Moreover, key changes once at a time through chip calculation.

LEXEL not only simplifies the authentication process, it also greatly improves the authentication efficiency and the amount of concurrency, better ensuring the security of authentication



(2) Parameter Comparison

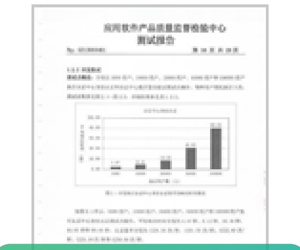
Performance/Authentication Mode	LEXEL	PKI or IBE (Overseas Technologies)
Safety	High (Chip-level authentication)	Low (Memory-level authentication)
Authentication/signature speed	100 -200 times faster than PKI or IBE	slow
Number of users managed by certification center	300 millions in real case, can reach a-billion level theoretically	Cannot guarantee a good operation of more than ten million users
Certification center construction cost	80% lower than PKI or IBE	High
System maintenance personnel	70% lesser than PKI or IBE	More
Core technology	Autonomous & Controllable	Semi-autonomous, non-controllable

(3) International Comparison

In early 2011, the Obama administration allocated 563 million U.S. dollars as new technology R&D funds for the implementation of the "EID" national strategy (more than double the R&D cost of airspace engine in 2015). It was expected that the newly developed technologies would create an EID capable for 300 million users in the United States. However, by present, no new authentication technologies have emerged. As the traditional authentication technologies, representatively known as PKI/CA and IBE systems, cannot meet the requirements for large concurrent commercial applications, the U.S. national strategy failed because of the constraints of weakness of traditional technologies.

With LEXEL technology, a set of LEXEL system is established based on 300 million users. Through the testing by the National Application Software Testing, the system runs well and is sufficient to support 300 million users. The concurrent authentication has reached up to 1228.50 times per second, and the concurrent signature verification has reached to 823.93 times per second. All indexes are better than the upper limits of the traditional authentication center.

Sufficient to support 300 million users



Concurrent authentication 1228.50 times/sec.

Concurrent signature authentication 823.93 times/sec.

2.1.3 Technical Evaluation, Technical Awards and Technical Patents

LEXEL technology has obtained 13 invention patents. All of its system test results reach a leading level in the world. Moreover, it is highly appraised by Academician of Chinese Academy of Sciences and highly recognized by experts in cryptography, obtaining the appraisal that "The technology is ahead of Europe and America for at least ten years".

- **Industry International Awards**

Gold crown award

<The Golden Crown of England>

The highest honor for UK international invention exposition

BRONZE AWARD

<Korea International Invention Bronze Award>

The bronze award for Korea international exhibition of inventions

中国国际发明展览会

获奖证书

AWARD CERTIFICATE

<China International Invention Gold Award>

The highest award for China international exhibition of inventions

- **Patent information**

The list of 13 encryption technology invention patents obtained by LEXEL is shown below.

No.	Patent Content	Number of patents
1	Cryptographic algorithm invention patent	2
2	Digital signature invention patent	1
3	Password anti-theft invention patent	2
4	Data transmission invention patent	1
5	Network identity certification invention patent	1
6	Mobile verification invention patent	1
7	The Internet of things certification, Encryption transmission and control invention patents	3
8	Bank card anti-theft encryption invention patent	1
9	VPN encryption invention patent	1

2.2 Core Blockchain Technology of LEXEL

The core Blockchain components of LEXEL include Blockchain infrastructure, Blockchain protocols, and cryptographic algorithms, etc. To be specific, P2P network communication protocols, distributed computing technologies, distributed storage technologies, encryption algorithms and privacy protection algorithms, key management mechanism, consensus mechanism, smart contract, standard token protocol, wallet SDK and other technologies are involved. Hereby, we will further illustrate the following key innovation modules of LEXEL.

2.2.1 Parallel DPOS+BFT

(1) The Underlying Performance of Existing Blockchain Cannot Support Commercial Applications

As a set of decentralized solutions, Blockchain focuses on consensus and governance. Bitcoin was created earlier. It is estimated that the inventor of Bitcoin himself might not even think that the scope of Bitcoin circulation could be worldwide. Therefore, the POW adopted requires each node to participate in competitive bookkeeping (mining). Each bookkeeping node needs to process transactions and maintain system-wide backups, and the nodes are still open without restriction, which leads to a Blockchain bloat.

Blockchain network congestion has caused three obvious consequences. Firstly, throughput is extremely low. It takes Bitcoin 10 minutes to form a block, and it takes ETH about 14 seconds to forms a block. For example, during the peak period of Cryptokitties launch, ETH accumulated millions of unconfirmed transactions. It even could not bear an application with just one smart contract. This is also the main reason why public Blockchain applications have not yet launched. Secondly, the fee is extremely high. Due to the limited processing capacity of the bookkeeping node (miner), it has no choice but to prioritize the transactions that have paid high gas. With competitions, the handling fee for each transaction rises, resulting in the loss of cost advantage for high-frequency applications. Thirdly, financial centralization is formed in essence. As mining becomes more difficult, computing power is gradually concentrated, and energy is largely wasted. Bookkeepers begin to exchange for the power with financial resources. The mining machines concentrate to form the mining pools. Accordingly, the original decentralized Bitcoin has become a tool to monopolize large mining pools.

Therefore, the most critical need for public Blockchain in 2018 is performance improvement. On one hand, it requires that the new generation public Blockchain infrastructure to be able to support thousands or even billions of active users like Google, Facebook and Alibaba, as well as support parallel computing and ensuring high-efficiency and low-latency transactions. It also requires individual users to enjoy the benefits of Blockchain applications at low cost or even for free, thereby helping Dapp develop a larger user scale, increase frequency of utilization, and boost commercial profits. On the other hand, it requires that the creators and participants at the very beginning of the Blockchain ecology to be benefited the most, rather than being easily plundered by wealthy latecomers.

(2) LEXEL Consensus Design

The consensus mechanism is a consistent strategy and method for each node in the Blockchain system, and it is a process of negotiating deterministic transaction order and filtering invalid transactions. In an analogous reality society, the process of the final election of a country or business leader is achieved through the nationwide vote and selection step by step.

At the design level of the consensus mechanism, it is important to consider the balance between fairness and efficiency. Fairness is to ensure that all participants have bookkeeping right. As to efficiency, it does not require all participants to keep accounts from time to time, but allows agent to be chosen by voting. Ultimately, the consensus mechanism needs to meet the requirements for resource utilization, response time, processing time, throughput rate, and maximum limit load capacity of the business scenarios. Therefore, after comparing POW, POS, BFT, DPOS and other mainstream consensus algorithms, LEXEL has chosen to adopt the DPOS consensus.

DPOS, namely Delegated Proof of Stake in full, by introducing the role of "trustee", it reduces the negative impacts of excessive competition and endows professional institutions the bookkeeping capacity. LEXEL confers voting rights on the holder’s holding shares, rather than bookkeeping right for direct mining. The decentralization and democracy of the system can be achieved through the mapping of each person’s cash-holding ratios and their influences. Each holder can give his/her voting right to an bookkeeping representative (at the early stage of the project, the foundation will authenticate and select the bookkeeping representative node), and the top 100 representatives who receive the most votes rotate to generate blocks in accordance with the fixed schedule.

The DPOS consensus algorithm of LEXEL is designed to introduce mainstream decision-making mechanisms (such as the Senate and the National People's Congress system) into the Blockchain system. The advantage is that the number of nodes participating in verification and bookkeeping can be greatly reduced, and consensus can be completed within a few seconds. Meanwhile, efficiency can be improved, energy can be saved and fairness can be ensured.

The operating principles of LEXEL's DPOS are as follows:
Firstly, in normal mode of operation, block producers generate one block every three seconds. Assuming that no one misses their round, it will produce the longest chain. Blocks are invalid at any time if block producers are not dispatched to generate block in the scheduled round.

Secondly, in a few forking scenarios, malicious or faulty nodes that do not exceed one third of the total number of nodes may create a few forks. In this case, a few forks can only generate one block every nine seconds, while most forks can generate two blocks every nine seconds. In this way, the honest 2/3 majority of the chain will always be longer than the minority.

Thirdly, in the multiple production scenario offline, the (offline) minority might attempt to generate an infinite number of forks, but all of their forks will be shorter than the majority's chain, because the generation speed of the minority is deemed to be slower than the majority.

Fourthly, in the case of fragmented networks, not any fork owns most block producers. In this case, the longest chain will be owned by the largest minority group. When network connectivity is restored, smaller minorities will naturally switch to the longest chain, and clear consensus will be restored.

Fifthly, in a few multiple production scenarios online, a few Node B generate two or more alternative blocks within their period of time. The next plan producer (C) can choose to continue to build the chain based on any of the chains generated by B. Once this is done, this choice will become the longest chain, and all nodes that has chosen B1 will switch to fork. It doesn’t matter whether a few bad producers attempt to promote more alternative blocks, as they will never be as part of the longest chain for more than one round.

In addition, in such a low probability that a clear quorum of producers is lacked, a few people can still continue to generate blocks. Stakeholders can change voting transactions in these blocks. These votes can select a group of new producers and restore the participation rate of block generation to 100%. In this case, a few chains will eventually exceed all other chains that operating at a rate of less than 100%.

After all, LEXEL's DPOS is safe even when a number of producers commit frauds, because the community can vote to replace the unqualified producers until 100% participation rate is restored. At the same time, it ensures that the number of honest nodes is continuously optimized so that DPOS is able to confirm the transactions with 99.9% certainty in an average of merely 1.5 seconds.

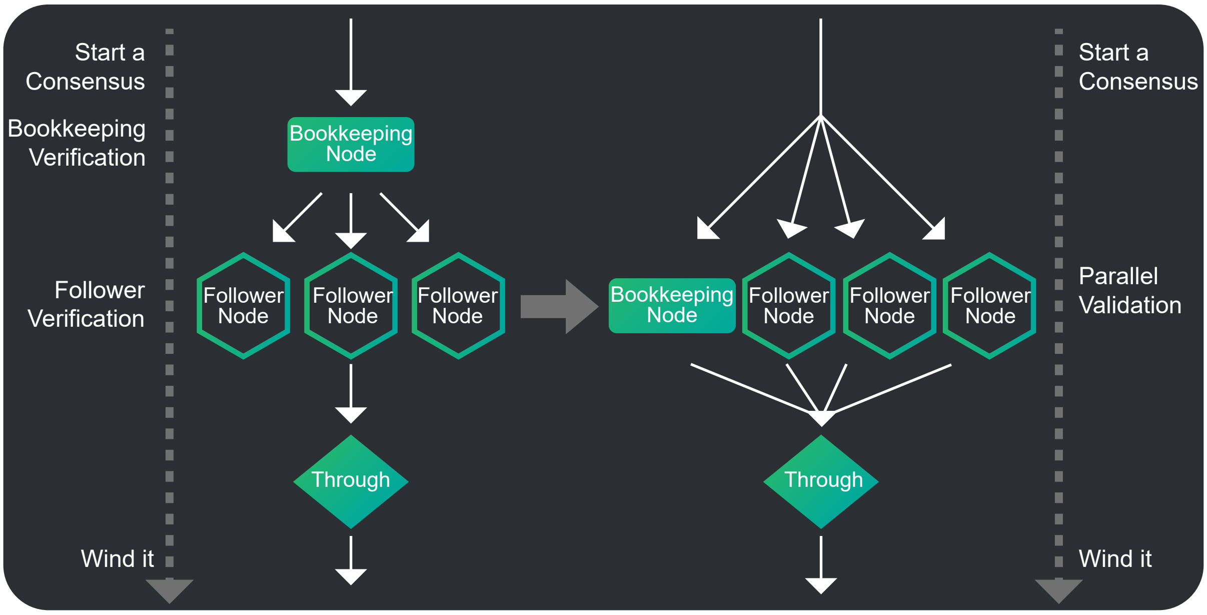
The BFT consensus mechanism of LEXEL is customized to generate blocks within seconds, equipping itself with high consistency, high availability, and strong anti-fraud ability.

The process of BFT algorithm is combined with one proposal, a few steps of voting and the final confirmation. During this process, there is a maintenance process by a complex state machine, and there are more voting round-trip steps. Part of the process is carried out within the node and between nodes serially. Each step requires waiting time for each other, that is, complete the calculations or network communication data collection at the previous stage, and obtain a periodic confirmation before enter the next phase.

Due to the complexity of the process and the large number of round trips, the consensus process is susceptible to network fluctuations. It is sensitive to network delays and packet loss. In unfavorable networks and computing environments, multiple consensus attempts may be required to achieve the eventual consistency.

The impact of the above technical challenges on the system is that, the parallel processing ability of the system may encounter bottlenecks, or the confirmation rate of transactions may be sporadically prolonged. Therefore, we have conducted an in-depth optimization of the BFT algorithm.

Regarding LEXEL, at first, we has analyzed the consensus process in depth, and decompose it according to the dimensions of computational steps, nodes, etc. We try to make all the nodes' calculations in each phase proceed in parallel. No matter it is a speaker node or a voting node, during the process that a node verifies a batch of transactions, all other nodes are also performing synchronous operations and voting, and do not need to wait for each other.



Parallel BFT Consensus Process

Then, we streamline the computational processes that are time-consuming and redundant, and reduce the time required for each step in the consensus process by optimizing the critical path and caching the repeated calculation results.

At the same time, we test the health of the network and the survival of the nodes. When some bookkeeping nodes are found to be unable to serve, they will quickly switch to the next bookkeeping nodes to avoid the occurrence of invalid wait for all nodes.

Finally, we consider that peak periods and idle periods always exist in financial transactions. When there is no transaction flow during the idle period, the consensus mechanism enters the heartbeat state, only maintaining the health status of the network, and will not generate data including blocks with zero transaction. This can avoid unnecessary waste storage, synchronous traffic and time consumption of empty blocks.

2.2.2 Safer Privacy Protection Algorithm – Zero-Knowledge Proof

(1) Pseudo-anonymity and Leakage of Data Privacy in Existing Public Chain

The biggest selling point of Bitcoin has always been considered as complete anonymity. However, the reality is that under big data and regulatory technology tools, most Bitcoin accounts can also be fully tracked. When the wallet address is not linked to a personal legal currency account, one can always protect his/her privacy. However, when an exchange is made or cashed out on a centralized transaction, the secret will be revealed. At present, the law enforcement agencies in the United States have been able to identify specific Bitcoin users during the investigation process. On the other hand, due to the complete exposure of data in public accounts, some application scenarios that require strong privacy, such as electronic medical records, authentication data, credential management and financial documents, cannot be implemented in the Public Chain network.

Therefore, in the privacy protection technology of the new generation Public Chain, it is necessary to focus on the security needs. It can be started with confidentiality, integrity, non-repudiation, traceability and authenticity. To be specific, confidentiality refers to the extent to which the Blockchain system ensures that its data can only be accessed by authorized users; integrity refers to the Blockchain system's ability to prevent unauthorized access and program/ data tampering; non-repudiation refers to Blockchain system’s ability to be demonstrated and cannot be denied after an activity or event has happened; traceability refers to the degree to which the activity of each user of the Blockchain system can be uniquely traced back to the user's competence; authenticity refers to the ability that Blockchain system can indeed identify the target and resource.

(2) Zero-Knowledge Proof Privacy Protection Algorithm of LEXEL

Zero-knowledge Proof refers to the situation that the certifier does not provide any information to the verifier, but the verifier still believes in their private knowledge. In other words, a program can have a secret input, and the certifier does not reveal anything to the verifier. Zero-knowledge proof provides the basis for privacy protection mechanism construction. The role of zero-knowledge proof in Blockchain privacy protection is increasingly important. At present, zero-knowledge proof is tried to be applied in cryptocurrency to solve the privacy issues for both parties in the transaction. However, as to the application model, the existing zero-knowledge proof scheme is only for Bitcoin's UTXO model, and it is difficult to promote to the new Blockchain based on the account model. Therefore, it also restricts its support for smart contracts. When the existing zero-knowledge solution generates certificates, it first converts the content of certificate into the form of a gate circuit. This process requires a lot of computing resources and time, because this certificate can only be generated on nodes with sufficient computing power (such as mining nodes), which greatly limits its application scenarios.

In order to strengthen anonymous protection and privacy protection, LEXEL intends to introduce ZCASH zero-knowledge proof technology to enhance privacy protection. The zero-knowledge proof protocol contains three algorithms: KeyGen, Prove, and Verify. KeyGen is a random algorithm, inputs common parameters, outputs proof key pk and verification public key vk; Prove algorithm inputs proof public key pk, instance x and proof a, outputs a zero-knowledge proof π; Verify algorithm inputs verification key sk, instance x and proof π, and outputs a decision bit. The zero-knowledge proof protocol can convince everyone in the system that the transaction is correct. However, no transaction address is recorded in the account book. Only the serial number calculated from the address is recorded. In this case, users of the transaction can be hided and their privacy can be protected. Since the serial number is calculated from the transaction address through the hash function, according to the irreversible nature of the hash function, there is no way to reversely deduce the transaction address, thereby the serial number cannot be associated to two or more transactions of the same user.

In addition, as to the asymmetric encryption of the Blockchain itself, LEXEL applies a common hash digest algorithm to record the hash value of the previous block in the block to ensure that the recorded data is tamper resistant and the data integrity is protected. For a given data plaintext and hash, LEXEL can verify whether the data plaintext has been tampered or not. In order to prevent different parties of the Blockchain from repudiating the recorded data, LEXEL has strengthened the digital signature function to confirm the unforgeability of the data unit, that is, to confirm that the message is indeed signed by the issuer. Regarding the process, in the beginning, the signer will process the original text with the private key to generate a digital signature value, then the verifier will verify the signature against the digital signature value and the original text message by applying the public key publicly provided by the signer.

2.2.3 Richer and More Diversified Smart Contract Applications

LEXEL's smart contract takes the ETH design philosophy as a reference and provides a Turing complete smart contract platform that allows developers to write arbitrary logic programs. LEXEL will customize a virtual machine to execute the contract codes. Developers of smart contract can use Solidity language for development. The target addresses of CALL and CALLCODE’s instructions of LEXEL are transmitted through the stack, allowing the contract to dynamically call codes of other contract at run time, making the contract call path non-deterministic. While the data that the smart contract can access is deterministic, all nodes will surely obtain the same target address when they dynamically call the target code, therefore ensuring the consistency of the system.

Regarding the problem that the current smart contract is more difficult to formally verify, on one hand, LEXEL will try to support some easy-to-verify programming languages, such as functional languages Haskell and OCaml. They are more applicable for smart contract codes than imperative programming languages, such as C / C++, Java and

JavaScript, because their structures are easier to be reasoned and formalized. On the one hand, in the sample proposal for smart contracts, using interpreted languages rather than compiled languages, the actual codes are visible on the Blockchain and can be easily checked. Finally, codes are always difficult to be perfect. LEXEL will add certain foundation-level governance mechanisms so as to provide a reasonable mechanism for upgrading, iterating and remedying vulnerabilities in the smart contract.

For the lack of friendly development of ETH smart contract technology, LEXEL will further deepen the development of smart contract manager and add the smart contract naming modules, making it easier for developers concerning upgrading and naming of the smart contract.

2.2.4 SDK Tools

In order to help more eco partners easily access LEXEL, LEXEL will also provide SDK tools and support both Java and node.js development languages. Based on SDK, developers of partners can easily develop DAPP. At that time, the customers of eco partners only need to invoke the functional interfaces of the nodes on the chain, and they can access some or all of the data of the chain on the client side, and initiate transactions to the Blockchain.

Regarding the design of SDK, a simple interface is provided. Developers only needs to pay attention to the data field of the specific DAPP and the result of the call. They don't need to know the specific deployment of the Blockchain node to implement the management, execution and transaction query function of the business contract. In this case, the development threshold and cost of eco partners can be greatly reduced, and the application of various business scenarios can be quickly developed.

2.2.5 Blockchain Technical Advancement of LEXEL

The Blockchain technical advancement of LEXEL can be reflected in different dimensions such as applicability of business scenarios, rationality of architecture design, completeness of computing capability, high-speed consensus efficiency, ultrastrong encryption and privacy security, traceability, and auditability.

Applicability of Business Scenarios: LEXEL will focus on safer infrastructure provision and broader application of nature currency, thoroughly changing the security pain points of the digital currency industry. Unlike the traditional PKI, LEXEL will be oriented according to the needs of real business scenarios to ensure the reliability, efficiency and stability of the business processes.

Rationality of Architecture Design: LEXEL intends to implement disaster recovery for valuable trusted big data on the Blockchain, ensuring redundant backup of the system, data and link, as well as guaranteeing the reliability and availability of the system. Even if the codes of a certain version smart contract or DAPP are flawed, it will not be dissolvingly influenced, hence ensuring high availability of the project.

Completeness of Computing Capability: Programmable value is a significant nature of the block technology, directly determining the ability of technology to demonstrate business logic. The completeness of computing capability is embodied in the "smart contract."

High-speed Consensus Efficiency: Adopts the most advanced high-performance DPOS consensus algorithm currently. It will establish a high standard for the configuration of consensus nodes, ensuring block generation within seconds, supporting up to millions of concurrent transactions.

Ultrastrong Encryption and Privacy Security: Data that is important to users' privacy needs to be processed by privacy protection, being classified into privacy sensitive information and public information. Due to the combination of hardware and software encryption technology, users' information privacy protection and assets confirmation are truly ensured. Any unauthorized user cannot decrypt the protected information but only read the public information.

Traceability and Auditability: With the irrevocable and timestamp features of the Blockchain technology, the foundation can supervise and verify all audit records and regard them as evidences in relevant legal disputes.

2.3 Combination of Digital Encryption & Blockchain

Regarding the traditional PKI technology, the CA (Certificate Authority) is the starting point of trust. Only by trusting a certain CA can the digital certificates issued by the CA to the user be trusted. However, in specific applications, the following problems exist in PKI technology:

- **Single Point of Failure:** The CA at the core is vulnerable to be attacked. Once it is controlled, the root CA certificate and the certificate that the CA has already issued are no longer trusted.

- **Multi-CA Mutual Trust:** User certificates can only be verified by the root CA certificate to which they belong. Different CAs cannot mutually authenticate each other. The availability of existing solutions for CA mutual trust is restricted.

LEXEL combines the features of distributed data storage and consensus mechanisms of Blockchain to implement decentralized authentication. Therefore, the combination of LEXEL and Blockchain has created the following advantages:
1) LEXEL will not suffer from system-wide service interruption when the verification node encounters a technical failure or malicious attack. In addition, it is impossible for users to suspend their accounts globally in the event of emergencies of a single organization;
2) When enterprises or individuals use authentication and encryption technologies, they do not need to apply for a certificate from a third-party CA of the traditional PKI or independently deploy a CA system. They only need to join the LEXEL ecology;
3) Combine the DPOS+BFT consensus to ensure security and TPS simultaneously.

Furthermore, as to the Internet currently, the main way for servers to authenticate users is the cryptosystem. A user creates a password when using the website for the first time in order to confirm his identity during subsequent visits. The disadvantages are passwords are either too weak or too complicated. Each website requires a unique password, and it is inconvenient for recovery when users forget their passwords. The most common mechanism to protect network connection is SSL. In addition that the server proves its authenticity, SSL also establishes an encrypted connection between the client and the server. However, if an attacker adds himself to the list of trusted users of the user's browser by using a fake browser root certificate, he can break the secure connection. As to corporate network, administrators can add certificates to the list of trusted users and then perform a "man-in-the-middle" attack on the https connection.

The LEXEL crypto chip is an independent system. Through combining its independent intellectual property algorithm, user identification fields and behavioral remarks information, it can automatically extract user information: fill out user profile on the site, including issuing payment to the designated account of the customer. The distributed algorithm, through allowing the site profile to automatically supplement passwordless logins, ensures one-click login for all account login passwords in a secure environment. Users do not need to record any information: Chip available, site accessible.

3. Business Models and Application Scenarios

3.1 Business Models

As a decentralized solution, LEXEL is led by the LEXEL Foundation for project development and developer community maintenance. It focuses on the development of identity authentication chain of trust, and promotes the launching project based on LEXEL through technical support and investment. .

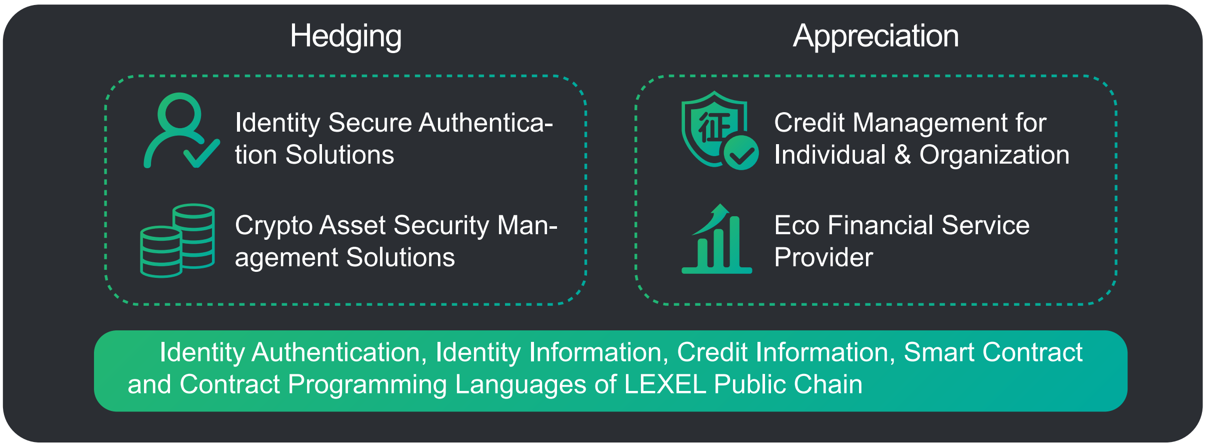
The design of LEXEL identity authentication chain of trust has its own Token. In addition to being used as GAS, Token can be applied to scenarios such as information modification on identity authentication, establishment and maintenance of smart contract, crypto asset pledge, dispute appeal and arbitration on crypto assets, etc. Token consumption will be used as a reward for application developers and miners on the Public Chain to make the trust ecosystem of LEXEL identity authentication healthier.

As a basic Public Chain, it can store complete identity information, credit information, scene-based smart contracts and turning-complete programming languages as well as provide authentication solutions. In addition, as a witness network, a complete decentralized authentication mechanism will be designed to prevent the possibility of network attacks. Based on this, it becomes the foundation for the trust of personal identity authentication in the Internet of Value.

Based on LEXEL identity authentication chain of trust, LEXEL also provides a complete solution for crypto asset security. It uses LEXEL's unique patented digital encryption and security authentication technologies to innovate the private key storage method of traditional crypto asset wallet. Combining hardware and software, it provides more secure solutions for crypto asset storage and transfer.

In addition to assets hedging, LEXEL is committed to building a value-added ecosystem for crypto assets, communicating with developers and service providers (such as crypto asset exchanges, quantified trading teams of crypto assets, P2P financial management teams, etc.) on the chain to build a crypto asset financial ecology that has various modes such as individual-to-individual, individual-to-organization, and organization-to-organization crypto asset lending, investment and financial mutual assistance.

In short, based on LEXEL Public Chain, developers and service provider community, we are committed to becoming the foundation chain of identity authentication trust in the future Internet of Value. Meanwhile, we will provide the best digital financial ecosystem, enabling that crypto assets can lay a solid foundation for and promote the financial development in the future.



Hedging

Identity Secure Authentication Solutions

Crypto Asset Security Management Solutions

Appreciation

Credit Management for Individual & Organization

Eco Financial Service Provider

Identity Authentication, Identity Information, Credit Information, Smart Contract and Contract Programming Languages of LEXEL Public Chain

3.2 Token Design

Token, as a value exchange medium, is an essential link in LEXEL Public Chain. It is directly related to the range of applications on the chain. Besides, as the common currency for LEXEL ecosystem, Token ensures convenient value exchange for users applying LEXEL eco services. The value assurance and application of the Token come from the following aspects:

3.2.1 Cryptocurrency

- Trusted Network Maintenance: Rewards the Witness node in the witness network to ensure the smooth operation of the trusted network;
- Value Exchange on the Chain: Various ecological value exchange scenarios on the service chain.

3.2.2 Application logic

- GAS Consumption: GAS consumption of operations such as network transfers;
- Hardware Consumption: Official recycled token is exchanged into hardware and distributed to users;
- Service Consumption: Organizations/Exchanges that cooperate with LEXEL submit tokens regularly to the official as fees for technical services;
- Consumption of Financial Scenarios: Scenario consumption of various asset transactions in the financial service ecosystem.

3.3 Application Scenarios

3.3.1 Application Scenario 1: Personal Trusted Digital Identity

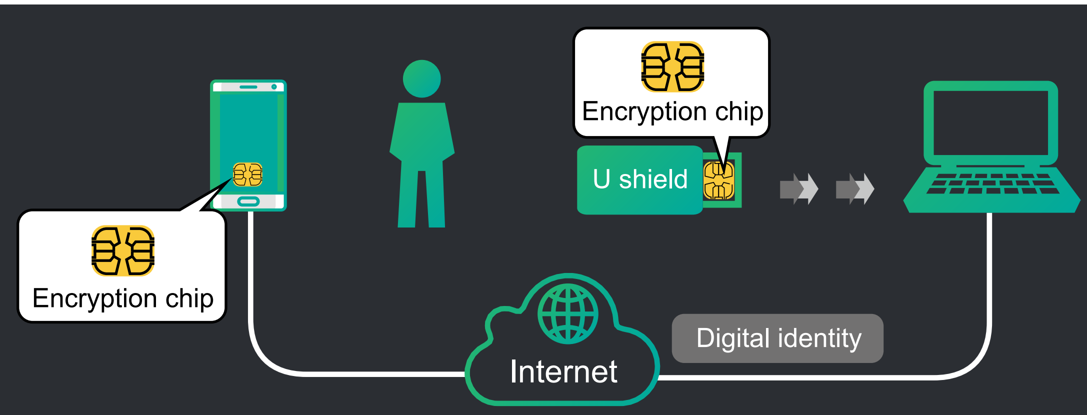
At present, all countries in the world are concerned about personal digital IDs, such as the United States, Germany, Belgium, and some countries even have a unique network identity. However, at present, only Estonia has basically implemented the national EID system and has become the world's most digitalized country. Yet, Estonia is only a small country with a population of 3.4 million. Other countries have encountered a large number of concurrent difficulties during the process of applying personal EID. Throughout the world, there is no EID that can be rapidly tested globally, which means it will be difficult to unify the networking of national ID card issuing authorities and passport issuing agencies around the world.

With the creation of Blockchain technology, a variety of consensus mechanisms and governance verification mechanisms have make "Letting people all over the world prove your identity" come true. Even so, the efficiency of Bitcoin, ETH, and other public chains to process transactions was too low. Moreover, asymmetric encryption algorithms such as RSA and ECC were complicated and slow. Therefore, no techniques or applications on personal trusted digital identity for business purpose are really available so far.

Security authentication on identity is to ensure that the right person can correctly access the right resources at the right time and with the right reasons. Management on Account, Authentication, Authorization and Audit is required, that is, taking control of the following aspects, e.g. who can be authorized to use an application or device, how to use this application or device, and knowing who accessed certain applications or devices, etc., ensuring that legitimate users can use IT resources safely and conveniently.

At present, through combining the encryption technology with the brand-new Blockchain technology that adopts the DPOS consensus algorithm, LEXEL is able to solve the concurrency problem of a large amount of transactions perfectly, making three major functions of personal trusted digital identity come true.

1) Realizing the creation of personal digital identity, chain storage, and digital identity query verification.
2) Realizing the binding of personal identity to digital assets with hardware devices, preventing hackers from ripping off identity to creak passwords of digital wallet violently and steal funds from E-Wallet accounts, fully protecting security of digital property.
3) Applications of electronic seal (signature), judicial deposit certificate and preservation of evidence based on trusted personal digital identity.



Take the trillion-dollar-scale market for example, even if the traditional PKI/CA system can break through the problems of massive concurrency and blockchain technology implementation, its cost is five times more than that of LEXEL.

3.3.2 Application Scenario 2: Crypto Asset Wallet

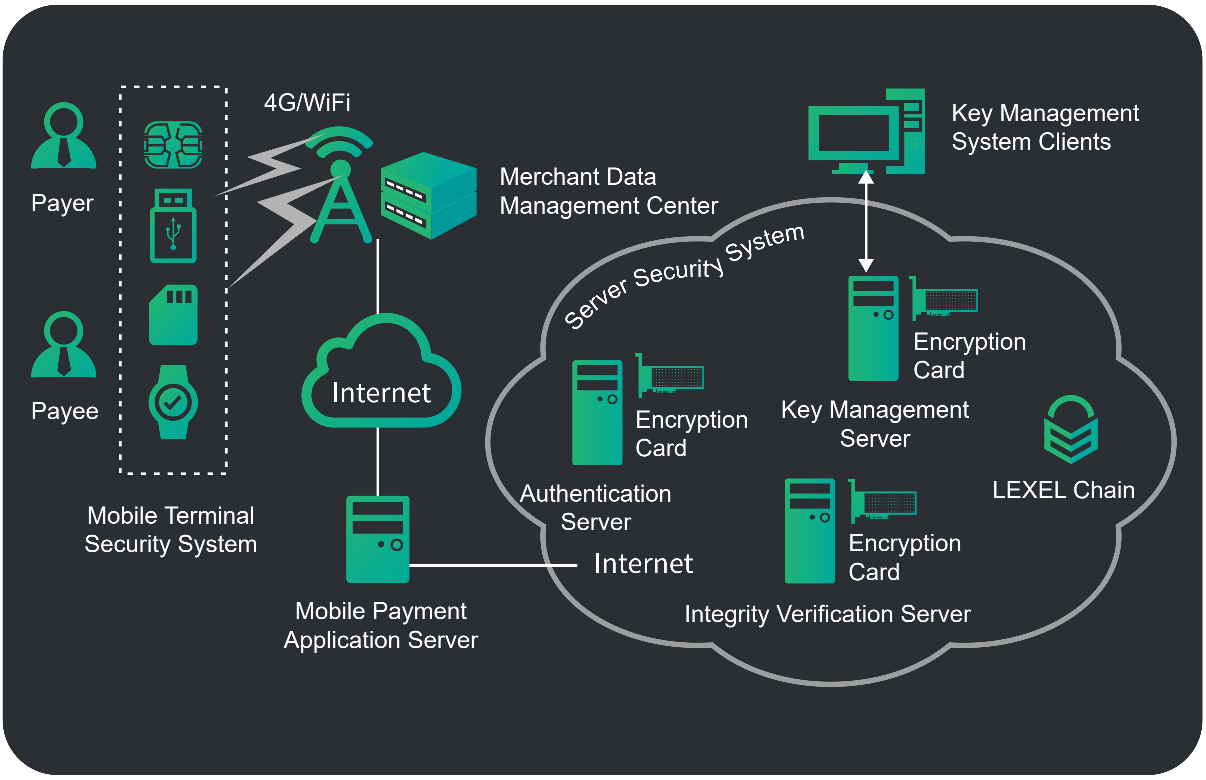
In traditional financial scenario, online banking, mobile banking, mobile payment have vigorously entered into our daily lives. But even so, traditional finance still cannot achieve payment in a high security level, therefore, countries usually limit the amount of payment to control risk. Large-scale transactions still need to be implemented through online banking and hardware devices.

The theory behind it is that, the mobile payment method uses the authentication mode of verification code (dynamic passwords), such as Alipay, WeChat, Apple PAY and so on. Dynamic password authentication mode features fast speed, easy operation with low cost, but it lacks the signature function. Hackers can attack on mobile payment protocol effectively by intercepting and replacing the content on payment slip, and transfer money from user accounts. However, if traditional authentication techniques such as traditional PKI are used to process digital signatures, PKI/CA authentication center' concurrent signature verification procedure will get slower. In addition, since the construction cost of CA authentication center is high, market will not accept them.

In the world of cryptocurrency, users are able to manage tens of millions of crypto assets with a single set of private keys without digital signature not even the procedure for dynamic password authentication. Meanwhile, there are numerous loopholes and back-doors in all kinds of computer and mobile terminals, so it is common that hundreds of millions of assets of cryptocurrency investors are stolen.

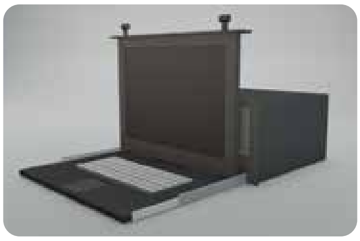
Hence, LEXEL is committed to changing this serious safety pain point of the industry.

The LEXEL technology itself, in the traditional scenario, has implemented a one-time pad system and data encryption to ensure personal information security and fund security. The data encryption transmission speed can satisfy 200~300 million users concurrency without delay. In the digital currency scenario, by combining with the Blockchain technology, the personal trusted digital identity is firstly stored on the Blockchain, and the corresponding key is then regenerated, part of which is stored in the Blockchain ledger and another part of which stored in the special LEXEL hardware (which can support multiple storage devices such as SD card, SIM card, USB disk and intelligent wearable). Users need to verify with hardware devices when making payment and transferring crypto assets, and hackers can't transfer the users' crypto assets even if they has stolen the passwords of the E-Wallet.


Payer
Payee
4G/WiFi
Mobile Terminal Security System
Merchant Data Management Center
Internet
Mobile Payment Application Server
Key Management System Clients
Server Security System
Encryption Card
Key Management Server
Encryption Card
Authentication Server
LEXEL Chain
Internet
Encryption Card
Integrity Verification Server

3.3.3 Application Scenario 3: Cryptocurrency Exchange

Recently, cryptocurrency exchange has been hacked and cryptocurrency assets have been stolen frequently. The main reason is that hackers can steal tokens from the exchanges in “hot wallets” by attacking a large number of users of the exchange. Generally, for major currencies other than Bitcoin and etheric, most of them are not supported by the hardware cold wallet in the market. They are normally protected only through common passwords and multi-signature wallet which can be stolen easily.



LEXEL uses encryption technology to write key password authentication processes into a dedicated hardware. The cryptocurrency exchange that cooperates with LEXEL may require all operations related to the Hot Wallet (including but not limited to the change of administrator login and operation permission, hot wallet user access login, tokens assets extraction, of coin-currency trading, etc.) to go through a further procedure by connecting to the dedicated hardware to verify the key. Because hackers can't obtain the hardware information, they can't move crypto assets away even if they break all the passwords set by the exchange's users.

3.3.4 Application Scenario 4: LEXEL Ecosystem

Based on the basic characteristics of LEXEL, which is high security and massive concurrency, the free ecosystem of LEXEL is formed. Through forming a credit mechanism with smart contract, users are entitled to receive “privileges” (depending on their credits), such as:

1) Use LEXEL Wallet to transfer without Gas Fee
2) The holder's LEXEL will automatically add value (Crypto Asset Banking)
3) Game or application privilege

LEXEL Ecosystem seeks to create a Blockchain ecosystem that not only protects users' crypto assets, but also brings value to users' crypto assets.

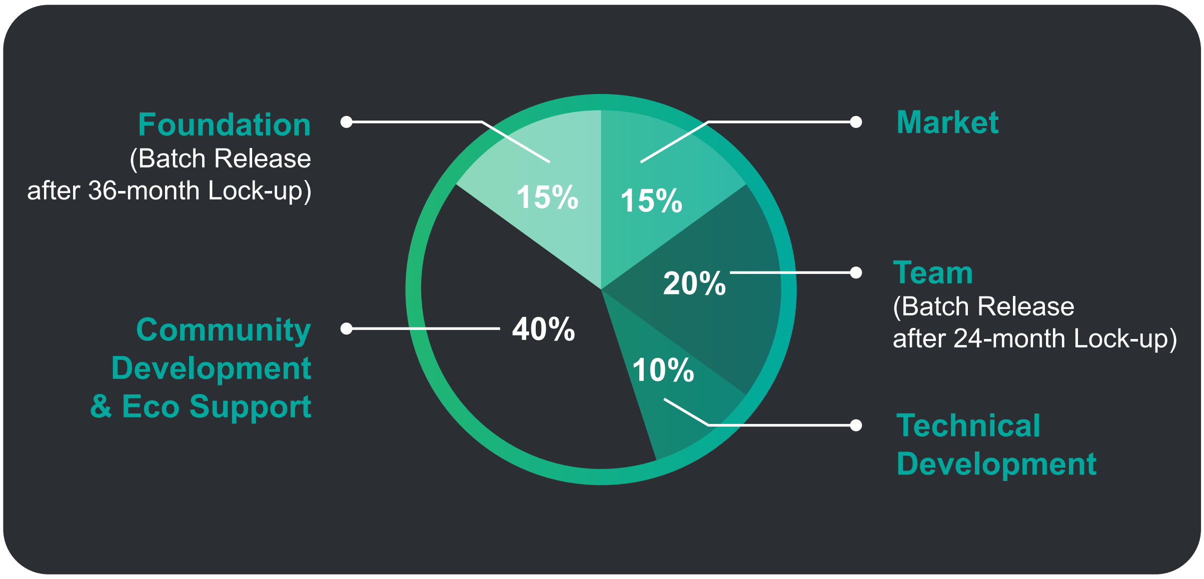
4. Token Distribution

a). Total Amount of Tokens: 10,000,000,000 LEXT (Never additional issuing)

b). Token generation time: Mid February, 2018.

c). Time to Launch on the Exchange: Mid June, 2018.

LEXEL will not have any form of public offerings or private placements. All tokens are only presented to strategic investors, community ecology contributors and business partners, as well as kept and held by the Foundation and the Technology Development Team. Chinese and Americans are prohibited from buying and holding LEXT in any way. Otherwise, all legal consequences incurred should be borne by yourself.



At that time, LEXT will circulate in the LEXEL ecosystem, including but not limited to bookkeeping and consumption (GAS) of transaction (business), creation of personal digital identity and bill query, security encryption storage and related service charges payment, trusted browser advertising revenue, and service fees for other digital authentication scenarios.

5. Roadmap

2011~2017

Early 2011 to Nov. 2017	R&D of Encryption Authentication Technology

2018

Mid Feb 2018	Generate Tokens
Mid June 2018	Launch Tokens in the Exchange
Late June 2018	Develop Mainnet
July to Aug, 2018	R&D of Key Hardware
Sept 2018	R&D of Key Modules, Basically Complete Mainnet
Dec 2018	Accomplish & Launch Mainnet and Wallet

2019

Mar 2019	Release the Application Template of Smart Contract
June 2019	Connect Hardware to Mainnet and Further Develop
Aug 2019	Finish Connecting Hardware to Mainnet
Dec 2019	Trial Operation of the First DApp

From 2020 on

Continuous Promotion	Expand the Scope of Application for Hardware and Mainnet, Establish the Mainnet Ecology

6. Core Team

6.1 Team Members

Lewis Lo

CEO CTO

More than 10 years' experience in IT development, responsible for the overall coordination and management of LEXEL, focus on launching and application of Blockchain in recent years, successfully developed a sales and anti-counterfeiting traceability platform for a jewelry company based on the alliance chain technique (namely PBFT consensus mechanism).

Evangelos Rekleitis

CSO

Graduated from Imperial College London with a Master's degree in Computer Science; has been an ICT engineer and risk analyst since 2007; involved in the revision of the cyber security strategy and cloud security strategy of the Cyprus government; carried out many security researches and risk analysis and management projects; engaged in the EU Agency for Network and Information Security in 2015, participated in projects such as Big Data Security, Cyber Threats, Security Standardization and Cryptography.

Christine He

COO

Graduated from North Carolina State University, served at the world's largest video e-commerce company Cinsay Inc. and led teams in cross-border businesses, assisted Formula E team Andretti Autosport in developing and operating customized webgame, proficient in multiple languages, good at community operations and public relations.

Alog Rana

Graduated from Imperial College London, rich experience in secure transactions, AML and fraud detection solutions, practical experience in low latency, scalability and HA system design, professional knowledge on financial IT throughout the entire project.

Soumil Verma

Graduated from North Carolina State University with double degrees in Computer Engineering and Electronic Engineering, served as a researcher at the University of Connecticut and worked as a data analyst for the USDA Food Safety Inspection Agency, participated in the ArcGIS project.

Anuj Sanghavi

Currently working as a project engineer at Caterpillar Inc./EASi LLC, responsible for the automation testing project, served at Albright Entrepreneurs Village, used to be the co-chairman of the Electron and Electronic Engineers Association in North Carolina State University and cashier in the Carrom Club.

Todd Downing

Graduated from Baylor University and has more than 20 years' experience in IT industry with a wide range of business knowledge, used to serve at well-known companies such as Dell, Nexstar Broadcasting and Cinsay, participated in the formulation of corporate development strategies, unique insights in technology and business development.

James Kersbergen

More than 20 years' experience in technical development, served at Belo, Nexstar Broadcasting, and Cinsay, responsible for technical development and team management, conducted in-depth researches on streaming media, cloud computing and database technology.

Serge Kononov

More than 15 years' experience in IT testing, having in-depth knowledge on test technology, good at automated testing, responsible for the design and construction for enterprise automation framework to ensure rapid iteration of product reliability.

Fadi el Hamdi

Graduated from Department of International Business Finance, University of Amsterdam, served at IT Department of ABN AMRO Bank N.V., responsible for financial security vulnerability analysis on internet banking, provided network security work environment and dealt with virus Trojan invasion.

6.2 Advisors

Richard Zhang

Graduated from Department of Electrical Engineering and Computer Science of University of California, Berkeley, served at BigFix and IBM as a senior software engineer, currently working at AppDynamics as an advanced software engineer, created a network graphics calculator engine and participated in an open source project of file encryption software TrueCrypt, focusing on network technologies such as user experience, single page applications, encryption technology, application security transmission, application security performance management.

Riad Elmnebhi

Graduated from Institut National des Sciences Appliquées (INSA), majoring in Information Systems Architecture, served at BNP Paribas for 11 years, currently working as director of Blockchain program at the bank, responsible for creating private Blockchain system for BNP Paribas.

Khalil Najjar

Senior Advisor on Cloud Technology, Enterprise ERP and Enterprise Digitalization;
Expert and architect in Internet of Things, Blockchain, micros-ervices, AI and other fields.

6.3 Partners

Genesis Capital

JD Foundation

BCFOF

Juhe Capital

Blockchain Lab,
Purdue University

TriChain Capital

Africoin

Gravity Capital

7star Exch

6.4 Media Partners

Jinse.com

Huoxun.com

ITerduo.com

Tokenpapa.com

TokenBook

NIU.XXX

One Top

Sandianzhong.com

7. Risk Disclosure

LEXEL team solemnly remind you: Participants should be aware that all Blockchain projects carry risks. The value of Blockchain projects is closely related to project development and expectations of market participants. Participants should not blindly believe in any profit guarantees made by the Blockchain team, nor should they follow the trend of participation blindly. Participants should judge the technology and application development potential of the projects, their own economic affordability as well as psychological endurance objectively. All responsibilities, benefits and losses are ultimately borne by the participants.

To be specific, the following risks may exist in LEXEL and LEXT.

1) Risk of Insufficient Information Disclosure

As of the date of the Whitepaper, LEXEL is still under development. Its philosophy, consensus mechanisms, algorithms, codes and other specifications, and parameters may constantly update and change. Although the White Paper contains specific information about LEXEL, it is not absolutely complete and the seller may make adjustments and updates from time to time for particular purposes. The seller is unable and has no obligation to keep the participants informed of every detail (including their progress and expected milestones, whether postponed or not) during the development process of LEXEL. Therefore, the seller does not necessarily ensure participants to fully and promptly understand the generated Information. Insufficient information disclosure is inevitable and reasonable.

2) Regulatory Risk

Cryptocurrencies are being or may be supervised by regulators in many countries. The seller may receive inquiries, notices, warnings, orders or rulings from time to time from one or more regulators, and may even be ordered to suspend or terminate any action related to sales and development of LEXEL or LEXT Token. The development, marketing, promotion or other aspects, and sales may be seriously affected, hindered or terminated. As the regulatory policies may change from time to time, the existing regulatory permission or tolerance for LEXEL or its sales in any country may only be temporary. In different countries, LEXT Token may be defined as virtual goods, crypto assets or even securities or currencies at any time. Therefore, according to local regulatory requirements in some countries, LEXT Token may be prohibited for trade or possession.

3) Risk of Accelerated Development of Cryptography

Cryptography is evolving constantly. It cannot guarantee absolute security at any time. The progress of cryptography (such as password cracking) or technical progress (such as the invention/improvement of quantum computers) can put cryptography-based systems (including LEXEL) at risk. This may result in anyone's LEXT Token being stolen, stolen by theft, vanished, destroyed or devalued. To some reasonable extent, the project side will get ready to take precautions or remedies, upgrade the underlying protocol on LEXEL to deal with any progress in cryptography, and wherever appropriate, incorporate new and reasonable security measures. The future of cryptography and security innovations is unpredictable, the project side will work with other members from the LEXEL community to adapt to the constant changes in the field of cryptography and security.

4) Risk of Project Failure or Suspension

LEXEL is still under development. It is not a finished product to be launched. Due to the technical complexity of LEXEL system, the seller may encounter unpredictable and/or insurmountable difficulties from time to time. Therefore, the development of LEXEL may fail or suspend at any time for any reason (for example, lack of funds). Failure or suspension in development will result in LEXT Token being unable to be delivered to any participants for sale.

5) Risk of Income Being Stolen

Someone may attempt to steal funds raised by the seller (including those converted into legal tender). Such theft or attempted theft may affect the seller's ability to provide fund for the development of LEXEL. Although the seller will apply the most advanced technology to protect the safety of funds raised, some cyber theft can hardly be stopped completely.

6) Risk of Source Code Vulnerability

No one can guarantee that the source codes of LEXEL are completely flawless. Codes may have certain flaws, errors, bugs, and loopholes that may prevent users from using certain features, expose users' information, or cause other problems. If such defects exist, the usability, stability and/or safety of LEXEL will be impaired. As a result, the value of the LEXT Token will be adversely affected.

7) Risk of Permission-free Access and Decentralized & Self-control Ledger

The distributed ledger underlying LEXEL is permission-free, which means it can be accessed and applied by everyone freely without any restrictions on access. Although

LEXEL was initially developed by the seller, it is not owned, operated or controlled by the seller. The spontaneously formed LEXEL community is completely open, decentralized and permission-free. It is made up of users, fans, developers, LEXT Token holders and other participants worldwide, most of whom have no relationship with the seller at all. Regarding the maintenance, governance and evolution of LEXEL, the community is decentralized and autonomous. The seller, regardless of its previous efforts and contributions to LEXEL, is merely an active member in the community as equal as others, having no supremacy or arbitrariness. Therefore, after LEXEL launches, its governance and even evolution will no longer be dominated by the seller.

8) Risk of Source Code Upgrade

The source codes of LEXEL will be gradually broadened and may be upgraded, amended, modified or changed by any member of LEXEL community from time to time. No one can predict or guarantee the exact result caused by such upgrade, amendment, modification or change. As a result, any upgrade, amendment, modification or alteration may result in unpredictable or unexpected outcomes that could have a material adverse effect on the operation of the LEXEL or the value of LEXT Token.

9) Risk of Security Vulnerability

LEXEL Blockchain is based on open source software and is a distributed ledger with no permission required. Despite the seller's efforts to maintain the security of LEXEL system, it is possible for anyone to intentionally or unintentionally bring weaknesses or defects to the core infrastructure elements of LEXEL, and the seller may not be able to prevent or remedy these problems with its security measures. This may eventually result in the losses of participants' LEXT Token or other digital tokens.

10) Risk of “Distributed DoS” Attack

LEXEL is designed as an open and permission-free ledger. Therefore, LEXEL may suffer from "Distributed Denial of Service (DoS)" attacks from time to time. Such attacks would negatively affect, stall or paralyze the LEXEL system. As a result, transactions will be delayed to be written into the blocks of LEXEL Blockchain, or even cannot be implemented temporarily.

11) Risk of Insufficient Processing Capabilities for Nodes

The rapid development of LEXEL will be accompanied by a sharp increase in trading volume and the demand for processing capacities. If the demand for processing capabilities exceeds the load that the nodes can provide in the LEXEL Blockchain network, the

LEXEL network may be paralyzed and/or stalled, and fraud or fake transactions such as "double spend" may occur. In the worst-case scenario, LEXT Token held by anyone may be lost, and a rollback Blockchain or even a hard fork may be triggered. The consequences of these events will undermine the usability, stability and security of LEXEL Blockchain as well as the value of the LEXT Token.

12) Risk of Unauthorized LEXT Token to be Claimed

Any person who obtains the buyer's registered email or registered account access by decrypting or cracking the LEXT Token purchaser's password will be able to maliciously claim the purchased LEXT Token. Accordingly, the LEXT Token purchased by the purchaser during the sale may be mistakenly sent to any person who claims LEXT Token through the registered email or registered account of the purchaser, and such sending is irrevocable and irreversible. Each purchaser should take measures as follows to properly maintain the security of his/her registered email or registered account: use a high security password; do not open or respond to any fraudulent email; and strictly protect his/her confidential or personal information.

13) Risk of Loss of Private Key for LEXT Token Wallet

It may be irreversible if the private key necessary to access the LEXT Token is lost or destroyed. LEXT Token can only be manipulated if the relevant unique public and private keys are possessed through local or online LEXT Token Wallet. Each purchaser should properly keep the private key to his/her LEXT Token Wallet. If the private key to a LEXT Token purchaser is missing, lost, leaked, damaged or compromised, neither the seller nor any other person can help the purchaser access or retrieve the relevant LEXT Token.

14) Risk of System Forking

LEXEL is an open-source project initiated by the seller and supported by the community. Although the seller has influences on the LEXEL community, he/she does not and cannot arrogate the development, marketing, operation or other aspects of LEXEL. Anyone can develop a patch for LEXEL codes or upgrade them without the authorization of any other person. Once part of the LEXEL Blockchain verifiers accept the patch or the upgrade, it may cause the LEXEL Blockchain to “fork”, and thus two forked networks will generate until the forked Blockchains merge or one of them terminates to generate new block (both cases might never occur). Each branch of the LEXEL Blockchain will have its own cryptocurrency due to the forking. Therefore, LEXT Token with almost the same technical features and functions will exist on two forked branches. The LEXEL community may be split into two groups, supporting two branches respectively. In addition, the forked branches of LEXEL Blockchain can theoretically further forked infinitely. The temporary or permanent existence of a forked Blockchain may adversely affect the value of LEXT Token. At worst, it may destroy the sustainability of the LEXEL system. Although the forking of LEXEL Blockchain may be resolved through combining the two branches by the community with efforts, success cannot be guaranteed and it may take a long time.

15) Risk of Platform Consolidation

Technically speaking, LEXEL may consolidate with other Blockchain projects to achieve synergies or other valuable considerations under certain circumstances. This form of consolidation may result in LEXEL Blockchain to be abandoned or discarded in exchange for a certain number of cryptocurrencies on other newly created Blockchains. The new cryptocurrencies will be distributed and delivered to the LEXT Token holders before the consolidation. Under certain valuation models, LEXT Token holders may receive insufficient compensation in such consolidation.

16) Risk of Insufficient Attention to the Application

The value of LEXT Token largely depends on the popularity of the LEXEL platform. It is not expected that LEXEL will be well known, popular, or commonly used within a short period of time after release. At worst, LEXEL may even be marginalized for long, attracting only a small sum of users. Comparatively, a large demand for LEXT Token may be speculative. Insufficient users may lead to an increase in price fluctuation of the LEXT Token in the market and affect the long-term development of LEXEL. When such price fluctuation occurs, the seller will not (and has no responsibility) to stabilize or affect the market price of LEXT Token.

17) Risk of Lack of Liquidity

LEXT Token is neither a currency issued by any individual, entity, central bank or a national, supranational or quasi-national organization, nor is it supported by any hard assets or other credits. The circulation and transaction of LEXT Token in the market is not the seller's responsibility or pursuit. Transactions of LEXT Token are based only on the consensus reached by the relevant market participants concerning the value of the token. No one is obliged to purchase any LEXT Token from a LEXT Token holder, nor is any person able to guarantee the liquidity or market price of LEXT Token at any time. If a LEXT Token holder wants to transfer the LEXT Token, the LEXT Token holder needs to look for one or more buyers who want to buy the token at an agreed price. This process may be very costly, time consuming, and ultimately unsuccessful. In addition, LEXT Token may not be available for public transactions on cryptocurrency exchanges or other markets.

18) Risk of Token Price Fluctuation

Cryptocurrencies usually fluctuate greatly in price in the open market. In the short term, price shocks often occur and the price may be denominated in Bitcoin, ETH, U.S. dollars or other legal tender. The price fluctuation may be caused by market forces (including speculative trading), changes in regulatory policies, technical innovations, availability of exchanges, and other objective factors. This fluctuation also reflects changes in the supply-demand balance. Regardless of whether there is a secondary market for LEXT Token transactions or not, the seller is not liable for any LEXT Token transactions in the secondary market. Therefore, the seller is not obligated to stabilize the price fluctuation of the LEXT Token and is not concerned about it. The risk involved in the LEXT Token transaction price should be borne by the LEXT Token traders themselves.

19) Risk of Competitions

The underlying protocol of LEXEL is based on open-source computer software and no one claims copyright or other intellectual property rights over the source code. Therefore, anyone can legally replicate, copy, reproduce, design, modify, upgrade, improve, recode, reprogram, or use the source code and/or the underlying protocol of LEXEL in other ways in an attempt to develop a competitive protocol, software, systems, virtual platforms, or virtual machines to compete with, or even catch up with or replace LEXEL. The seller cannot control this. In addition, many Blockchain-based platforms have already existed and there will be more to compete with LEXEL. It is impossible for the seller to eliminate, prevent, limit or reduce such competitive efforts aiming at competing with or replacing LEXEL under any circumstances.

20) Risk of the Third-party Developers

LEXEL will provide an open platform for any type of distributed applications and smart contract programs developed by third parties (especially members of LEXEL community). All applications and smart contract procedures can be accessed to or built on LEXEL Blockchain without being limited by censorship, restrictions, controls, prequalification or access requirements. The seller is neither intended nor able to act as an auditor to review any program that will be developed on LEXEL system or related to LEXEL system to any extent. Therefore, programs that are banned or restricted in specific jurisdictions, such as those involving gambling, betting, lottery, lotto, pornography, etc., may be developed, accelerated, promoted, or operated by making use of the permission-free requirement. Regulatory authorities in certain jurisdictions may take appropriate administrative or judicial measures against specific programs or even their developers or users. Any governmental punishments, penalties, sanctions, repressions, or other regulatory measures will more or less frighten or deter the existing or potential LEXEL users from applying the LEXEL system and hold the LEXT Token, which will have significant negative effects on the prospects of LEXEL.

21) Risk of Other Encryption Assets

LEXEL will create or produce and circulate various encryption assets. Some of these encryption assets may be issued by specific individuals, and the issuers will have specific commitments or obligations to the holders. Other encryption assets may be created by smart contracts within LEXEL. None of these encryption assets have the same or similar features as LEXT Token. These encryption assets are not sold or offered by the sellers, and the sellers will not be responsible for them, unless the seller otherwise specified.

LEXEL

www.lexel.io