Erachain
Blockchain 3.0

Developed for Traditional Businesses with Decentralized Reward Technology

White Paper

08.17.2017

The Chinese Informatization Strategy, published in December 2016, states that block chain will stimulate the evolution of cyberspace from the 'internet for everyone' to the Internet of Everything – digital, network and intelligent services will be everywhere. This is official recognition of the advent of a new digital era in China, which gave a great boost to the development of block chain technology. The Erachain environment has been in development since 2014 and was announced in February 2017.

The backed up by demand from the environment's active participants (business entities, public authorities, private individuals) who use Erachain for their own purposes. Active participants in the environment can purchase COMPU on the internal decentralized exchange of the Erachain environment or directly from forgers. Two factors rule out speculation in COMPU crypto-fuel: the constant emission of COMPU under the Erachain protocol and the reduction in the price of transactions as their number increases. The transaction price falls, but there are more of them, so the forger collects and sells more COMPU. We will leave this possibility open to fans of speculation at the initial stage of launching the main ERA unit on cryptocurrency exchanges. However, according to our calculations, as the Erachain environment develops globally, all the ERA will be bought and distributed around the world for the purpose of making money from COMPU crypto-fuel due to the increased demand for transactions within the Erachain environment.

As was previously the case on the internet as a whole, there are currently not enough new participants in block chain environments. This problem is addressed by the Erachain block chain environment, which has the advantage of identifying users and protecting their privacy, as well as having many different features to work with.

The project team sees its goal as creating an open decentralized platform and proposes using Erachain to build a "bridge" into the world of block chain technology for governments, traditional business and normal citizens.

Our intentions are confirmed by the working technology of the Erachain block chain environment, which allows everyone to work in it and tackle a number of challenges and problems.

All full users of the environment are identified, meaning that each one has their own page with photo ID and personal information. Any transaction in the Erachain environment is certified by the user's Electronic Digital Signature (EDS)[1], which is generated by an algorithm embedded in the Erachain protocol when any action is performed. Using a pThe whole world is now studying the phenomenon of block chain technology and its application in everyday life. So far, no one has created the block chain environment that we really need.

Our project is designed to give the world a tool to work with block chain technology in various spheres of life. A block chain environment from which any user –whether an IT professional, entrepreneur, public servant or specialist in any field – will be able to derive benefit, earn money and optimize their business processes.

The Erachain environment carries the true power of block chain technology and the properties of cryptocurrencies – the possibility of decentralized money distribution.

[1] EDS (Electronic digital Signature) – an element of an electronic document resulting from the cryptographic conversion of information that protects against counterfeiting.

Satoshi Nakamoto (the creator of Bitcoin) understood only one characteristic of cryptocurrencies: the ability to print money, but he did not mention the possibility of distributing this money.

In fact, the second part is the most important. This omission created the main vulnerability of the Bitcoin ecosystem. Instead of spreading money around the world, the system replaced central banks with pools[2] of miners[3].

Miners threw the system into disarray, stopping the development of updates and improvements, as well as threatening to split Bitcoin in order to reduce its value and buy up more coins at a low price.

Dmitry Ermolaev took the vulnerability of Bitcoin into account. He created two units in the Erachain environment: the ERA[4] asset and an internal crypto-fuel for operations within the environment – COMPU, the price of which is unaffected by jumps in the ERA rate on external exchanges.

In this way, he made a Decentralized Reward System (DSO), a distributed structure for user remuneration, the foundation of the environment. By taking part in the ICO[5] or acquiring some capacity in the system – the ERA asset – on an exchange after the ICO, any person can become a miner (forger): supporting the operation of the environment and earning money.

The Erachain environment has the ability to reward users in a decentralized way as commission for distributed mining - forging[6] (in the blacksmith sense of this word). When using your mobile phone or computer, these devices can serve to support the network. As a reward, you can receive some COMPU crypto-fuel just by having the application running on your electronic device.

The liquidity of COMPU crypto-fuel will bersonalized account, the user gains access to the features of the Erachain environment for conducting business processes. In addition, any user can also have an anonymous account that is only intended for operations with digital

[2] Pool – a server that distributes the task of calculating a block signature between all connected participants.
[3] Miner – a specialist in supporting the distributed platform and creating new blocks with the possibility of receiving rewards in the form of new units and commission in various cryptocurrencies, particularly in Bitcoin.
[4] ERA- a legal unit that grants the right to control the environment and create blocks, as well as defining the level of participants' rights.
[5] ICO- the release of tokens, or coins, by any project that are intended to fund the services it will need in the future.
[6] Forging – activities to support the distributed platform and create new blocks with the possibility of obtaining a reward.

assets. In order to prevent the theft of funds, it is not possible to make a transfer from a personalized account to an anonymous one. Erachain makes it possible to create any asset (shares, cryptocurrency, property) and exchange them for another asset without intermediaries, therefore enabling traditional businesses to conduct an ICO. The exchange of assets will be confirmed in the block chain, and the rights of claim are transferred to the appropriate users of the system.

Erachain encourages participants involved in the development of the network. Participants who join the network and contribute to its growth will grow alongside it. Each transaction brought into the system will increase their own reward.

This paper provides a description of the key features and capabilities of the environment, a comparative analysis of major versions of Blockchain environments, the technical characteristics of Erachain and the functional solutions that it presents.

Contents

Part 1. How the Erachain Environment Works

1. Getting Started with the System

By registering a new profile in the Erachain environment and accepting the rules of its license [3], you agree to be bound by its provisions and undertake to provide real data about your identity, which will be stored in the public domain. The system will then automatically generate a unique seed[7] (public[8] and private[9] key) for you.

2. User Registration

User registration consists of two processes: **the new user's personal data is entered into the block chain and a unique ID is assigned, then verification takes place** – their public key is confirmed by other users of the environment according to the KYC[10] principle.

This is necessary not only for financial institutions to better know and understand their customers (including their risk tolerance and investment preferences), but also to know exactly who they are dealing with and whether their client is involved in any illegal activity.

Erachain allows the KYC procedure to be used to identify your business partners and guarantees, in case of court proceedings, evidence regarding the subject of dispute linked to their ID. The Erachain environment helps to protect users' reputations by saving a history of all their actions.

2.1. Entering Personal Data

To register with the system, it is necessary to create an account.

To do this, the following personal information should be entered:

- Photograph

[7] Seed – unique code to recover a wallet with private keys.

[8] Public key – a key that can be published and is used to check the authenticity of a signed document.

[9] Private key – the component of a key pair that is kept secret. Used in asymmetric ciphers, which require different keys for encryption and decryption.

[10] KYC (know your customer) principle – a policy by which financial institutions are required to establish the identity of a client prior to conducting transactions with them.

- Full name (as per passport)
- Sex
- Date of birth
- Geographical coordinates of birthplace
- Information about yourself (optional)
- Contact information (optional)

Requirements for the photograph:

- Maximum size of 20 KB and 350 pixels from a computer (the mobile application has automatic compression)
- The face shall occupy more than 80 percent of the total photograph area
- The photo should be in colour
- The background must be light
- The photo should not contain frames, corners or other details
- Straight head position (full face)

After entering this data, it is necessary to send it to be checked by a Registrar (an identified Erachain user), who then adds the information to the block chain. At the same time, a new profile is made in Erachain and a number is assigned that is unique to each user.

The Registrar receives the user profile's byte code and enters it into the program, where it is displayed in a more user-friendly way. The Registrar then verifies the user's personal information and gives them permission to enter data into the block chain. After the personal data is entered, the information is recorded in a block and is confirmed when the block is completed.

2.2. User Verification

Full activation of a new profile takes place when the user completes verification[11].

In order for a user to be verified, a Verifier (an identified user with 100 or more ERA in their account) must confirm their public key and vouch for the user's actions in the block chain and the authenticity of the data entered by the Registrar.

[11] Verification – a procedure for confirming a user's identity.

The user sends this key to the Verifier, who enters it into the system as a special transaction that indicates the public key of the user who is being authenticated. Therefore, this key is linked to a specific user, who becomes verified.

User verification is optional. However, only a verified user can perform legally binding actions in Erachain, as their identity is confirmed and linked to their electronic digital signature.

Consequently, full registration requires the participation of two persons other than the user – a Registrar and a Verifier. It is worth noting that the Registrar and Verifier can be the same person.

Each user is allocated 0.00131072 COMPU, approximately enough for ten transactions, when registering an Erachain account.

2.3. The User's Electronic Digital Signature

An electronic digital signature (EDS) is a special element (public key) of a document based on the ed25519 elliptic-curves algorithm that makes it possible to establish that the information in an electronic document has not been corrupted since the EDS was formed and confirms its ownership.

A new, unique EDS for each user is generated when any transaction is conducted.

The electronic signature meets international encryption standards.

The following function realizes an electronic digital signature based on the ed25519 algorithm:

```
Identity void sign(PrivateKeyAccount creator, boolean asPack)
    {

            boolean withSign = false;
            byte[ ] data = this.toBytes( withSign, null );
            if ( data == null ) return;

            int port = Controller.getInstance().getNetworkPort();
            data = Bytes.concat(data, Ints.toByteArray(port));
```

```
        this.signature = Crypto.getInstance().sign(creator, data);
        if (!asPack)
            this.calcFee();
    }
```

The ed25519 elliptic-curve algorithm makes it possible to sign all actions by verified users electronically and send transactions to the block chain.

3. Anonymous and Verified Accounts

Within the system, the user has the ability to create an unlimited number of both anonymous and verified accounts in the same wallet.

All actions performed from a verified account will be confirmed by an electronic signature. Working with a verified account, the user can use all the features of the environment, performing legally binding actions. In addition, with a view to safeguarding ERA assets, a user may not transfer funds to anonymous accounts.

An anonymous account can also use the functions of the environment and sign actions with an electronic signature, however such actions will not be legally confirmed in Erachain. Similarly, it is not possible to make public statements or create assets from an anonymous account.

4. Decentralized Reward Technology

The Bitcoin and Ethereum networks use currencies that simultaneously serve to ensure the execution of transactions and grant the right to control the environment. This is very good when the network starts operations and the price of the currency itself tends to zero. This situation suits everyone, because transaction costs also tend to zero. However, after a certain amount of time, the value of tokens increased tens of thousands of times, meaning that transaction costs also grew proportionally.

One of the main characteristics of the Erachain environment is the introduction of two accounting units: **ERA** and **COMPU**.

4.1. The Basic Accounting Units of the Erachain Environment

ERA is a legal unit that grants the right to control the environment and create blocks, as well as defining the level of participants' rights. Users with 100 ERA or more in their account have the opportunity to participate in forging and verify newcomers. The total number of coins issued in the environment is 10,000,000 ERA.

COMPU is an internal reward unit that is used to pay commission for making entries and supporting the operation of the environment.

The emission rules for **COMPU** are regulated by the Erachain protocol. Emission is only possible in two cases:

- The creation of a new authenticated user (0,00131072 COMPU).
- The creation of a new block in the block chain (0.00016384 COMPU).

These rules help to prevent deficits or an overissue (inflation) of coins.

The creation of two units makes it possible to **limit the growth in commission charged to users as ERA grows** (as users pay in COMPU within the system). This role differentiation optimizes the environment, provides a flexible and powerful system of rights, as well as an independent payment system for environment services, and gives incentives to the participants who support the processes taking place within it.

Note: In the event that a wallet seed is lost, the ERA units in the user's account are also considered lost.

4.2. Calculating Fees for Sending Transactions

The cost of a transaction (in COMPU) is calculated by Formula 1.1:

$$\sum = \alpha * \beta * 10^{-8} \quad (1.1)$$

where:

α – transaction size (bytes) β – payment coefficient for a transaction

The payment coefficient β = 64.

If a transaction is 200 bytes in size, the transaction cost would be:

$$200 * 64 * 10^{-8} = 0.000128 \mathrm{COMPU}$$

4.3. Calculating Transaction Costs in Real Currency

Here is an example:

Average exchange rate: 1 COMPU = $1000

The cost of a transaction 200 bytes in size: 0.000128 COMPU

Transaction cost:

$$0.000128 * 100 * 10 = \$0.128$$

The average exchange rate is approximate and provided for reference.

4.4. Calculating Forgers' Earnings

The calculation of a forger's earnings depends on the number of ERA units in their account. The more ERA a forger has, the greater their forging power is, and the greater their forging power is, the more rights they have to assemble blocks. For example, with 10% of the ERA in their account, a forger can assemble every 10th block and receive a reward.

However, a forger needs to bear in mind that when they turn off the Erachain program, their forging power stops growing and the process of assembling blocks is also stopped.

The Robin Hood Principle:

When creating an empty block, a forger is paid in such a way: half of the reward is taken from the 10 richest forgers (in ERA units) in the environment, while the remaining half is emitted. This is how a forger receives the full reward for an assembled block.

$$8 \times 128 \times 64 \times 10^{-8} = 0.00065536 \text{ COMPU}$$

When creating a block filled with transactions, a forger receives COMPU in an amount proportional to the size of the assembled block.

The transaction cost is calculated by Formula 1.1.

Maximum number of transactions per block:

Average transaction size is 200 bytes

The maximum amount of information that can be entered into one block is 4,000,000 bytes (4 megabytes).

$$\frac{4000\,000}{200} = 20\,000\text{transactions}$$

The cost of one transaction according to 2.3 is 0.000128 COMPU. The total amount of COMPU is:

$$20000 \,*\, 0.000128 = 2.56 \text{ COMPU}$$

Example 1:

A forger has 100 units of ERA in their account. In 1 month, the forger will assemble 1 block. The maximum number of transactions in one block is 20,000. On average, a forger receives $0.017 for one transaction, which means that in one month (30 days), the forger will earn:

λ – number of transactions in a block

μ – forger's reward for 1 transaction in $

ν – number of assembled blocks

The forger's earnings are calculated by Formula 1.2:

$$I = \lambda * \mu * \nu \quad (1.2)$$

$$20000 * 0.017 * 1 = \$340$$

Example 2:

A forger has 5,000 units of ERA in their account. In 1 month, the forger will assemble 50 blocks. The maximum number of transactions in one block is 20,000. On average, a forger receives $0.017 for one transaction, which means that in one month (30 days), the forger will earn:

$$20000 * 0.017 * 50 = \$17000$$

Example 3:

A forger has 50,000 units of ERA in their account. In 1 month, the forger will assemble 500 blocks. The maximum number of transactions in one block is 20,000. On average, a forger receives $0.017 for one transaction, which means that in one month (30 days), the forger will earn:

$$20000 * 0.017 * 500 = \$170000$$

* Calculations are approximate and depend on the number of forgers in the system and network load.

5. Payment for the Registration of Users

The Erachain environment includes a system that pays a Registrar for entering the details of new users. This feature is implemented through the automatic tracking of registrations.

Consequently, users have the opportunity to earn additional income. The environment automatically pays the Registrar 1.36% of the commission (in COMPU) for each transaction made by a user that they have entered.

6. The Proof of S&P Mechanism

Blockchain 3.0 Erachain is based on the **Proof of Stake and People**[12] algorithm. A block is assembled in 288 seconds 300 times a day, each containing 20,000 transactions. Forgers have the opportunity to participate in the assembly of these blocks. The number of forgers is limited only by the number of ERA units. This enables the best possible distribution and decentralization – around 3,000 nodes should be optimal. In the ERA block chain, the maximum number of nodes can reach 100,000.

COMPU emission is limited by the creation of new verified users.

The genesis[13] block realizes the initial decentralization of ERA units between forgers. The ERA are distributed in such a way that no single forger can have more than 5% of all the issued units, which allows for optimal decentralization from the first block.

The smallest transaction size for a transfer of funds is only 159 bytes. This makes the block chain environment more efficient than others, where transaction length starts at 240 bytes and more – up to 880 bytes. The daily number of transfer transactions is 6,000,000.

[12] Proof of Stake and People - a security method in cryptocurrencies that is based on the requirement to prove that a certain amount of funds is stored in an account (100 ERA). Using this method, the cryptocurrency algorithm is more likely to select a user with a higher amount of funds in their account to confirm the next block in the chain. Unlike classic Proof of Stake, COMPU accounting units are generated when new users register.

[13] Genesis Block – the first block in a block chain.

Part II. The Features and Use of Erachain

The second part of the paper examines the functionality of the Erachain environment, as well as the specific issues that it addresses.

1. Features and Advantages of Erachain

1.1.Environment Features

Let us consider some existing problems that can be solved with the features of the Erachain environment:

Problem 1: The volatility of cryptocurrencies poses risks for their use by traditional companies and banks. The Bitcoin and Ethereum networks use currencies that simultaneously serve to provide liquidity and ensure the execution of transactions. This is very good when the network starts operations and the price of the currency itself tends to zero. This situation suits everyone, because transaction costs also tend to zero. In 2008, a Bitcoin was worth $0.10, but after a certain amount of time, the value of Bitcoin increased tens of thousands of times, meaning that transaction costs also grew proportionally.

In 2017, the value of Bitcoin was $2700, so transaction costs could reach up to $1 or more. Note that this price will no longer suit all users of the system and could eventually lead to its collapse.

It would be advantageous for users of the system if transaction costs were not strictly proportional to the value of the main currency.

Solution: two basic units, ERA and COMPU, have been introduced in Erachain to meet this challenge. The system of charging commission for transactions in the **internal COMPU crypto-fuel of the Erachain environment protects its users against jumps in the ERA rate on external exchanges**. This unique feature of the environment protocol increases the stability of costs and revenue for business solutions based on Erachain and is not effected by speculation on cryptocurrency exchanges.

Problem 2. Increasing the level of trust in user verification.

Solution: This problem is solved by **identity verification in trust centres** – the Proof of Identity (POI)[14] protocol.

The more trust centres verify a user, the more confidence other users will have in them. Traditional state structures, business corporations and banks, as well as non-traditional business communities (such as Bitcoin or Ethereum), can act as trust centres. Under the Zero-Knowledge Proof (ZKP)[15] protocol, trust centres chosen by the community will be able to confirm the identity of one user on request from another.

Problem 3. The inability of registering a legal entity in the block chain.

Solution: This problem is solved by the **procedure of creating a company** the Digital Blockchain Organization (DBO)[16] .

Real-world organizations can register in the Erachain environment. Users can open and close companies in the Erachain block chain and conduct any type of legally binding activity.

The procedure for creating a legal entity in Erachain (DBO):

1. A legal entity that wishes to perform legally binding actions in the Erachain environment, irrespective of its form of ownership, must issue a power of attorney from the legal entity to an authorized individual that confers the appropriate rights.
2. The individual scans the issued power of attorney.
3. The individual uploads the scan of the power of attorney to the Erachain environment in their own name, signing it with an electronic signature.
4. The individual becomes the legal representative of the legal entity.

[14] Proof of Identity (POI) – a way to verify identities in trust centres.

[15] Zero-Knowledge Proof – a cryptographic protocol that allows one party to verify that any statement is true without having any other information from the second party.

[16] Digital Blockchain Organization (DBO) – a feature that creates a legal entity on the Erachain platform.

Problem 4. The gradual publication of new international regulatory standards on cryptocurrency and the inability of legal entities and private individuals to use digital assets (cryptocurrency) in all spheres of life limits the growth of the cryptocurrency market.

From 26 June 2017, according to EU Directive AML IV, it is illegal for anonymous users to hold more than 250 euros in cryptocurrency. An identified user has the right to exchange any amount of digital and real assets. [12]

Solution: The Erachain environment solves this problem through the **Proof of Identity principle and Identity Gate Protocol.**[17]

The Identity Gate Protocol, a gateway between the digital and real worlds, is set up using Application Programming Interface (API)[18] tools. As a result, it is possible to transfer and exchange digital assets for real ones. Consequently, a user of the Erachain environment has the ability to transfer rights of claim[19], receiving real assets in return and vice versa.

The operating procedure of the Identity Gate Protocol is shown in Figure 1.

[17] Identity Gate Protocol (IGP) – a protocol of the Erachain environment that acts as a gateway between digital and real assets.

[18] API (Application Programming Interface) – an interface between one computer program and another, such as the Erachain block chain and banking systems.

[19] Right of claim – a right derived from a contract to demand performance of obligations under the contract from the second party.

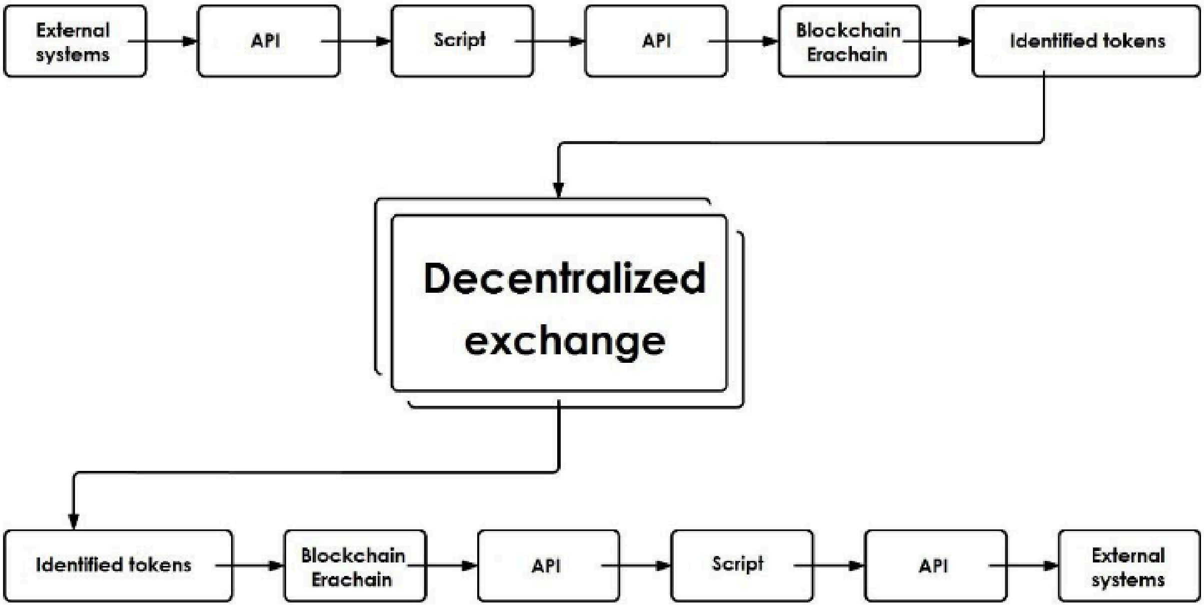

Figure 1: Identity Gate Protocol operating procedure

Data on the movement of cryptocurrencies and traditional currencies (BTC, ETH, USD) is submitted as an input from external environments (cryptocurrency exchanges, banking systems, exchange markets). Through the API, this data is entered into a special script that implements the Identity Gate Protocol. The script connects via API to the Erachain block chain environment, where the program issues identified tokens[20] as an output. The emitter personally guarantees their liquidity.

The algorithm can be implemented identically in the opposite direction. In the Erachain block chain environment, identified tokens are sent through the API to a special script that implements the Identity Gate Protocol. Using the API, this script connects to external systems, where emitters are guaranteed to be able to convert identified tokens into cryptocurrency and fiat currency.

Problem 5. Doing business: the conclusion of contracts and exchange of legally important information is a long process that involves a number of intermediaries and requires considerable expense.

[20] Identified tokens – digitized tokens that can be exchanged for goods and services.

Solution: This problem is solved by the **Blockchain Business Application Designer**.

The Erachain environment offers the possibility of creating applications to do business more easily and efficiently that integrate your current branding (white label). The source code of the Blockchain Business Application Designer is available in the public domain

An organization can create a user-friendly application (for mobile phone or PC) under its brand name with the functionality that it needs, linked to the Erachain environment through API. When using the business applications and performing actions, all transactions are automatically sent from the application to the block chain environment.

Erachain environment features that can be integrated with a business application:

- Document management
- Signing and approving contracts with a EDS
- Creating document templates
- Business correspondence
- Sending registered letters
- Conducting votes and multiple-choice surveys

Problem 6. The absence of a regulated process for issuing debt assets that guarantees their return in 100 percent of cases.

Solution: The problem is solved by the **feature** of the Erachain environment that **issues ERA assets on credit with a guarantee of their return.** A user can give ERA to another user for a limited time to earn money through forging and can guarantee its return by pressing a single key. These actions will be confirmed in the block chain, which eliminates the possibility of fraud on the part of the debtor.

It is worth noting that this function is also used to optimize the operation of Erachain: the genesis block of the environment transfers control over the basic legal units to many independent forgers in order to improve the decentralization of the environment.

Problem 7: There is a risk of losing all assets when trading on cryptocurrency exchanges. There is no mechanism for the safe, quick and simple exchange of any asset for another one on the exchange.

Solution: The Erachain environment has its **own decentralized exchange** designed for the direct exchange of any assets without first exchanging them for ERA units. A minimal commission is paid for carrying out the transaction (execution of a purchase or sale order) in COMPU units. The exchange is protected from hacking and fund freezes by decentralization – one of the basic properties of block chain technology.

Problem 8. The issue of privacy when sending messages and documents over the internet.

Solution: The Erachain environment addresses this problem with its **public and private document-signing feature**. Users can conclude a contract and sign it with an EDS, and the contract and its contents will be hidden from other users in the environment. The terms of the contract are stored in the block chain and are considered to be legally binding, but can only be decrypted by the parties to the agreement.

Problem 9. The problem of bureaucratic inefficiency: keeping records of citizenship, designations and social statuses is a long and complex process. It is necessary to visit a number of organizations in order to collect the required documents.

Solution: This problem is solved through the Erachain environment's **function to keep records on designations, employment, social status, citizenship, diplomas and certificates**. The data will be confirmed by an EDS in the block chain. As a result, it will be possible to see who and when assigned a status, was awarded a diploma or received citizenship

Problem 10. The lengthy process of obtaining patents.

Solution: This problem is solved by Erachain's **possibility of creating public statements, articles, charters, memoranda, consortia, pacts and other original documents,**

registering inventions and discoveries, and keeping record of patents. Information on who created a document and when is recorded in the block chain and, if necessary, can be decrypted for all users by the owner.

Problem 11. The problem of finding investments for the development of projects and a low level of investor confidence.

Solution: Erachain addresses this issue with its **feature of creating original digital assets and the ability to distribute them among investors within the environment**. For greater security and trust, Erachain provides an escrow agent function.

The Creation of Digital Assets and Holding an ICO

In order to create digital assets and hold an ICO, a user must:

1. Register on the Erachain platform as a private individual or legal entity
2. Specify the asset name, add a logo and write a description in the Create Asset section. Specify the number of units to be issued and their type (movable or immovable, divisible or indivisible).
3. Click the Create button
4. Describe their idea for an ICO and set up its terms
5. Officially take responsibility for the project by publishing expense reports for the collected funds

The whole world can monitor the progress of your ICO in detail with greater confidence in the reliability of the data provided, as it is linked to your profile in the block chain and signed with your electronic digital signature. Consequently, the Erachain environment can be used as an escrow agent in various projects requiring investments.

1.2. Example Use of the Erachain Environment

1.2.1. For Business

Holding an ICO for a Start-up

Let us look at an example. A doctor/inventor (bioengineer) has an idea to create a high-tech implant. First, he must design a 3D model, then construct a prototype of the implant and test it, after which it will be possible to manufacture and release the implants for medical treatment.

Investment is essential to successfully develop this idea. For the first phase of a project, $5,000 of funding is required to construct a 3D model. For the second stage – $20,000 to create a prototype (materials and equipment) and conduct tests. The third phase requires $35,000 to receive a patent, register the company and purchase materials.

In the Erachain environment, the inventor issues 100,000 tokens of an asset, ToothPro, on the internal exchange, specifying his terms in the description.

For the first stage of crowdfunding, the required investment amount is $5,000. Investors wishing to participate in crowdfunding change their real money into digital funds through the Identity Gate Protocol. In turn, the inventor puts 7,000 tokens up for sale on the internal Erachain exchange, representing 7% of their total number. Buying tokens on the exchange for digital money, investors will receive ToothPro assets depending on the amount they invest in the project. If all the funds are raised, the crowdfunding ends successfully and investors receive 7% of all issued ToothPro digital assets. The doctor/inventor, on the other hand, gets the money to construct his 3D model. In the block chain, investors can keep track of what the inventor is spending their digital money on. The designer can exchange digital money for the required materials and pay for the work of contractors. If he has to pay for this work in fiat money, he can transfer digital money into fiat currency through the IGP. After producing the 3D model, the inventor will proceed to the second stage.

The second phase requires an investment of $20,000 for the design of a prototype and testing. Similar to the first phase, the inventor puts another 15% of his ToothPro assets up for sale. The doctor receives the investment in digital currency and spends it on materials, equipment and contractors in the Erachain block chain. The entire business process is conducted in the block chain: contracts are concluded and signed, and bills, delivery documents and invoices are drawn up directly in the Erachain environment – the information is open and accessible to all investors, so that each of them can trace the full path of their investments. At the end of the second phase, the doctor/inventor has a prototype of a high-tech implant that has passed all the tests and he is ready to scale up production.

In the third stage, the inventor needs to raise $35,000 to formally register the company and launch the new-generation implants. He puts another 27% of the ToothPro digital assets up for sale. The inventor will receive the collected investments in digital currency, register the company and continue to develop his high-tech business. While the investors will in total receive 49% of the shares, in proportion to all of their investments.

Signing Contracts

The Erachain environment offers the possibility to sign contracts, agreements and other documents, both openly and privately. When the signature is open, all users can see who has made a deal, how and what exactly it is. With an encrypted signature, users can only see who has concluded the contract but cannot see its contents.

Businessman A wants to buy a yacht from Businessman B, but they do not want information about the transaction to be common knowledge. Businessman A draws up a contract in the block chain, encrypts it and sends it to Businessman B. Both sign the contract with an EDS in the block chain, after which the transaction is considered complete.

The signed contract is considered to be legally binding and the parties may sue if it is not complied with.

Holding an ICO for a Real-World Business

The owner of the old MetalCorp factory wants to renovate his facilities. Previously, in order to carry out full repairs, the owner would have had to borrow money from the bank, which is not economically beneficial and leads to risks.

Now, the factory owner can create an asset in Erachain – MCcoin. The value of the asset is proportional to the value of the factory and its potential performance (as assessed by a specialist, which can be confirmed by a special block chain entry). The value of the MCcoin digital asset will grow directly in proportion with the progress of renovation from the time the asset is released until the full modernization of the factory is completed. The owner holds an ICO on the Erachain platform and, as a result, raises money for the renovation. Asset holders can monitor what the owner spends on their investment on, while the owner gets a more powerful factory thanks to the received funds.

Doing Business Anywhere in the World

Company A from Switzerland is working with Company B from Japan. Previously to do business, they had to travel and send documents by post, which slowed business processes.

Now, using the Erachain platform, doing business becomes simpler and several times quicker! In Erachain, it is possible to generate document templates, create new ones, write registered letters, hold votes, keep records and manage the company's entire document flow. And most importantly: in Erachain it is possible to approve decisions in just 1 click using an EDS.

1.2.2. For Public Authorities and Citizens

Voting in the Blockchain

Every citizen can be assured of the fairness of voting conducted in the Erachain environment. A vote can be of any type and include any number of participants. The votes will be genuine as long as the strict voting algorithm is observed: 1 vote = 1 user ID. Votes are created in the Erachain environment in the same way as any other asset. It is worth pointing out that, as with assets, it will be possible to see who voted and for whom.

Marriage Registration

Bob wants to marry Alice. Previously, in order to do this officially, they had to file an application at the registry office with a receipt for payment of the state duty, wait for the specified period, and only then could Bob and Alice become a family.

Now, with the Erachain platform, there is no need to even leave the house! The necessary documents can be drawn up in one click. Relationships are registered and stored in the block chain, and Bob and Alice can become a happy family.

Maintaining Global Databases, Civil Records and Government Documentation

Country A wants to switch to an electronic system of recording social status. By choosing the Erachain platform, Country A gets a quick and open tool to keep record of licenses, citizenship, passports, driving permits and education documents. This enables all state and non-state bodies to have access to the open information.

Part III. Analysis of Blockchain Versions

1. Analysis of Blockchain Versions

The third part of the paper is devoted to a comparative analysis of all currently existing block chain versions (Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0, implemented by the Erachain block chain environment), highlighting their distinctive features, advantages and disadvantages, assessing the potential for their wide application in all sectors of society and drawing a conclusion on the main benefits of the newest version of block chain technology.

Blockchain is a decentralized database consisting of a chain of transaction blocks, each of which contains a reference to the previous block. The distributed data technology makes it possible to confirm the information in the blocks using remote nodes while ensuring a high level of security for all data. Therefore, the technology's protocol is capable of solving absolutely any government or business task. The goal of this comparative analysis is to answer the question: which version of the block chain environment best solves business efficiency issues?

1.1. Blockchain 1.0

The block chain technology in Blockchain 1.0 was first implemented in the Bitcoin environment. The recording protocol does not contain smart contracts[21]. There is also a variety – multichain – that breaks the chain down into smaller pieces. This feature reduces the cost of storing data with individual nodes in the environment. In addition, this version supports block chain protocol extensions that make allowance for various digital units (coloured coins, painted tokens).

Disadvantages of Blockchain 1.0:

- The large size of entries – about 800 bytes. This is because each entry references previous ones and contains a data-processing script for each output of the resource and a link for change.

[21] Smart contracts – an electronic algorithm describing a set of conditions that trigger certain events in the real world or digital systems when they are fulfilled.

- There is only one accounting unit.

1.2. Blockchain 2.0

The main advantage of this version of Blockchain is the "soft" (programmable) protocol, which allows entire programs – smart contracts – to be added to an entry. Blockchain environments based on Blockchain 2.0 are very convenient for developers – it is possible to quickly create a new kind of protocol or entry without conflicting with the underlying block chain environment.

Disadvantages of Blockchain 2.0:

- The size of entries with smart contracts is very large – the entries store entire programs
- Very slow operation – a smart contract must be fully compiled each time to obtain any sort of result
- The size of the database is very large, because it stores data about the current state of all participants' accounts and other information that is required for the program to work.

1.3. Blockchain 3.0

Blockchain 3.0 is the next step in the evolution of block chain technology with a small entry size (159 bytes) and a rigid protocol with superfast transactions that can be updated by the decision of environment participants and can specify user rights at protocol level. The block number is associated with the current time, which makes it easy to link Blockchain 3.0 to the Internet of Things and automated control systems, which require high processing speed and a constant turnaround time.

The main difference between the new version and Blockchain 2.0 is the presence of a Proof of Identity protocol. In Blockchain 3.0, legal issues are being addressed regarding the regulation of activities in the block chain environment – we aspire to meet the norms of international law (Electronic IDentification in the EU, Digital Signature Algorithm (DSA) in the USA and Federal Law No. 63 in Russia). All users of the platform are identified.

Identity Gate Protocol (IGP) technology, one of the elements of the Erachain environment, makes it possible to exchange real assets for digital ones and vice versa.

Another key feature that sets the Erachain block chain environment apart is the introduction of several basic accounting units that are responsible for different aspects of the environment. The main legal unit (ERA) grants the basic right to control the environment and create blocks, as well as defining the level of participants' rights. The second, COMPU, is a payment and reward unit that is used to pay commission for adding entries and gives an incentive to forgers to support the environment.

This role differentiation makes it possible to build a well-defined system of rights and an independent payment system for environment services while encouraging participants that support the environment. In addition, the distinction between accounting units protects users against speculation in the ERA unit on exchanges.

1.4. Comparison Table of Blockchain Versions

Table 1 compares the characteristics of different block chain environments:

Table 1. Comparison of Blockchain Versions

Blockchain environment version	Features					
	Interaction with traditional businesses	Interaction with traditional businesses	Interaction with traditional businesses	Interaction with traditional businesses	Interaction with traditional businesses	Compliance with the KYC principle
Blockchain 1.0	✓	-	✓✓	-	-	-
Blockchain 2.0	✓✓	✓✓✓	✓	✓✓✓	-	-
Blockchain 3.0	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓

“-”   - feature is not present

“✓”   - feature is poorly implemented

“✓✓”   - feature is well implemented

“✓✓✓”- feature is implemented very well

Part IV. Positioning the Environment

1. The History of Erachain

Dmitry Ermolaev is the founder and chief developer of the Erachain block chain environment. In 2014, Dmitry began to create Erachain alongside his brother Alexander. In February 2017, they launched the genesis block of the environment.

The first 200 users of the Erachain environment are Dmitry and Alexander's Russian friends and acquaintances. These users started using the Erachain environment and people from other countries (such as China, India and Korea) gradually began to show an interest in it. Dmitry has created the first block chain with the ability to register identified users and wants people around the world to use it. All funds raised by the ICO will be transferred to a Swiss foundation, the charter of which will state all the requirements for their expenditure, the main one being the improvement of the Erachain environment for the convenience of its users. The main language of the program is English. The Erachain environment is programmed in Java. [1]

2. Comparing the Ethereum and Erachain Platforms for an ICO

Let us look at a vivid example of a project built on block chain technology, the Ethereum environment. One of the factors that influenced the growth of Ethereum's capitalization and popularity was the implementation of ICOs.

The Ethereum project was created on 30 July 2015, and one of the first successful ICOs in Ethereum was the Augur project (the first decentralized prediction platform).

In total, more than 100 projects have been created on Ethereum and the most successful are considered to be Golem, EOS, Aragon, Gnosis, DAO and Lisk.

Beginning in spring 2017, the capitalization of Ethereum grew largely due to the ICO feature, which also contributed to the popularization of the platform. The capitalization of Ethereum is now more than $20 billion.

If we analyse the Erachain environment from the perspective of a platform for ICOs, an important feature is the ability to create assets and conduct ICOs in a completely lawful manner thanks to user verification. All purchases of shares at the ICO and subsequent expenses paid by the startup are fully transparent, which puts the ICO on a more serious level. The process of creating an asset is also very simple and faster than in the Ethereum environment. This primarily attracts companies from the real sector of the economy that want to have an ICO.

All this together makes the ICO more transparent and allows verified users, individuals or legal entities to invest in any ICO on the Erachain platform. A larger part of the market is involved in the ICO and investments are made more often by companies, not just by individuals. All these factors combined will lead to an increase in the value of the ERA unit.

Looking at the capitalization of Ethereum and bearing in mind that only anonymous private individuals can invest in their project, we can predict that involving companies in the ICO investment process will cause a significant increase in the capitalization of ERA.

3. Analysis of Business Technology in Other Environments

There are other block chain environments that have been created for doing business:

Clause is an open platform based on block chain technology that is designed solely for the purpose of doing business and managing document flow.

Block notary is a mobile application that allows users to share video messages and documents, speeding up business processes. A demo version of the product has already been created.

The Ascribe platform is designed for artists and designers. It gives them the opportunity to patent their products instantly. Registration is standard and a confirmation message is sent by email.

Boardroom is a platform for creating tables and holding votes based on block chain technology with smart contracts for doing business and generating document templates.

Dot Blockchain Music is a platform for musicians and music lovers. Musicians can patent their works.

Erachain is an innovative block chain environment that combines all the main functions for doing business with solutions for governmental organizations and private individuals, possibility of notarizing documents and assets, in addition to having a decentralized exchange and the ability to issue new assets quickly and conveniently.

Conclusion

Blockchain technology is the future of international processes. The project team sees its main objective as developing the environment to a level that involves the maximum number of participants and perfecting it so that each one of them finds it a convenient and secure place to work. Erachain is an environment that will grow exponentially as new users are registered. The more participants enter it, the more efficient and valuable the network becomes for all existing users.

Table 2 shows the development plan for the environment from 2018 onwards. It includes items on both improvements to the technology itself and its development within the global community. Starting in 2018, each item in the plan will be elaborated and published in the Erachain environment for public voting by verified users with a view to involving them in making important decisions regarding the environment's development and approving the completion of each item in the plan. Legally relevant documentation, financial reports and any other important documents relating to the development of the project will be uploaded onto the Erachain environment as they become available.

Table 2. Erachain Environment Development Plan

Year	Development Plan
2018	Stress tests and increasing the capacity of the Erachain environment (if necessary) before a large number of users register. Funding for promising start-ups and support for their ICO campaigns. *Information on investor cash flows and reports on work performed by start-ups will be opened up and stored in the block chain* Creating an exchange and Telegram bot for buying and selling tokens. Enhancement of the notification system. The user will get notifications when documents are signed.

	Implementing a function to cancel verification through the Proof of Identity protocol. Implementation of the Zero-Knowledge Proof protocol. Creating an ERA inheritance mechanism. A user will be able to transfer their coins and assets to their successors. The beginning of work to create a credit, insurance and business accounting process. Implementation at the national level of a recording system for statuses, education documents (certificates and diplomas), citizenship, censuses and passport control in Europe, Asia, etc. Goods turnover in large corporations based on block chain. Implementation of document management in different countries. Introduction of remote banking, as well as the recording of bank guarantees and bills of exchange. Recording of off-exchange bank transactions.
2019	Highly efficient image compression technology to reduce the cost of entering different types of multimedia files into the block chain. Text and photo recognition technology (faceted classification). Development of biohardware devices for storing secret keys that cannot be lost or stolen. Creation and implementation of a function to automatically generate a personal index of business reputation and activity in Erachain. The creation of forging pools for users with less than 100 ERA. Entry into the P2P lending and insurance market. Introduction of automatic accounting based on source documents into the block chain. Implementation at state level in various countries.

	Establishment of a banking services marketplace based on block chain for banks and large financial corporations.
2020	The possibility of forging with a mobile phone. Creating software to integrate all existing block chain environments with Erachain. The implementation of quantum cryptography into the Erachain protocol to enhance the security of information. Implementation of Erachain at the UN level.
2021	The introduction of artificial intelligence into the Erachain protocol in order to support the protocol. Further development of the ways to use Erachain in accordance with the invention of new technology in various spheres of human activity.

Additions can be made to the Erachain Environment Development Plan. By registering their personal account on Erachain.org and entering their suggestion for the development of Erachain in a special form, a user can send it to the project team for consideration. The best ideas will be published on the site, be included in weekly news updates about the project and starting in 2018 will be put to public vote in the Erachain environment for approval and inclusion in the development plan.

List of Terms and Abbreviations

API (Application Programming Interface) – an interface between one computer program and another, such as the Erachain block chain and banking systems.

Blockchain Designer – the ability of the Erachain environment to create applications for doing business easily and conveniently.

COMPU – a reward payment unit that is used to pay commission for making entries and supporting the environment.

Decentralized exchange – an exchange based on block chain technology.

Digital assets – assets existing in binary format that offer ownership rights.

Digital Blockchain Organization (DBO) – a feature that creates a legal entity on the Erachain platform.

EDS (Electronic digital Signature) – an element of an electronic document resulting from the cryptographic conversion of information that protects against counterfeiting.

ERA – a legal unit that grants the right to control the environment and create blocks, as well as defining the level of participants' rights.

Forging – activities to support the distributed platform and create new blocks with the possibility of obtaining a reward.

Genesis Block – the first block in a block chain.

Identified tokens- digitized tokens that can be exchanged for goods and services.

Identity Gate Protocol (IGP) – a protocol of the Erachain environment that acts as a gateway between digital and real assets.

ICO (Initial coin offering) – the release of tokens, or coins, by any project that are intended to fund the services it will need in the future.

Legitimacy – recognized by law, in accordance with the law.

Miner – a specialist in supporting the distributed platform and creating new blocks with the possibility of receiving rewards in the form of new units and commission in various cryptocurrencies, particularly in Bitcoin.

Registration – the procedure of adding a user to the Erachain block chain.

Registrar – an identified Erachain user.

Right of claim – a right derived from a contract to demand performance of obligations under the contract from the second party.

Seed – unique code to recover a wallet with private keys.

Smart contract – an electronic algorithm describing a set of conditions that trigger certain events in the real world or digital systems when they are fulfilled.

Pool – a server that distributes the task of calculating a block signature between all connected participants.

Proof of Identity (POI) – a way to verify identities in trust centres.

Proof of Stake and People - a security method in cryptocurrencies that is based on the requirement to prove that a certain amount of funds is stored in an account (100 ERA). Using this method, the cryptocurrency algorithm is more likely to select a user with a higher amount of funds in their account to confirm the next block in the chain. Unlike classic Proof of Stake, COMPU accounting units are generated when new users register.

Private key – the component of a key pair that is kept secret. Used in asymmetric ciphers, which require different keys for encryption and decryption.

Public key – a key that can be published and is used to check the authenticity of a signed document.

Verification – a procedure for confirming a user's identity

Verifier – an identified Erachain user with 100 ERA in their account.

Zero-Knowledge Proof – a cryptographic protocol that allows one party to verify that any statement is true without having any other information from the second party.

Sources and Materials

[1] – Genesis block info: 23.02.2017, 10:13:13 GMT (time stamp 1487844793333), HASH — block 1

(V5RkNcBrDi88Tbkm71DN1Po7M7yEop9kpu95gxHjPvR7MDa3uMkYotvGJ8awRTmz2abBEGXShZptrVdzmwuMsag)

(Java language, 170,000 lines of code available on GitHub – https://github.com/Icreator/)

[2] https://www.sec.gov/news/press-release/2017-131

[3] The license is available on the website.

[4] https://bitcoin.org

[5] https://99bitcoins.com/know-problems-with-bitcoin

[6] https://www.ethereum.org/

[7] https://angel.co/clause

[8] https://www.blocknotary.com/interview.html

[9] https://www.ascribe.io/

[10] http://boardroom.to/

[11] http://dotblock chainmusic.com/about/

[12] https://www.coindesk.com/information/ethereum-smart-contracts-work/

[13] https://www.cbr.ru/today/anti_legalisation/eu/EUGuidanceCDD062617.pdf

[14] www.europa.eu

[15] https://ed25519.cr.yp.to/index.html

[16] https://en.wikipedia.org/wiki/Know_your_customer

[17] https://www.bitcoinmining.com/

[18] https://bitcoinmagazine.com/articles/chinas-block chain-invasion/

[19] http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm