AKRA NETWORK

White Paper

2021

Contents

Introduction

The emergence of a decentralized financial system based on cryptocurrency is associated with the growing problems of the classical banking system. The central bank is the issuer of money and delegates some of its functions to other organizations (private banks and financial institutions). The presence of these factors affects the privacy and confidentiality of end users. Blockchain-based cryptocurrency offers an alternative to the classical financial system, making it possible to achieve complete decentralization of financial management.

One of the problems of the massive adoption of cryptocurrency in the financial sector is the problem of interaction between blockchains. One of the solutions of this problem could be the creation of an ecosystem to connect multiple blockchains.

AREA Network offers a universal and simple blockchain infrastructure based on Binance Smart Chain (BSC) and Ethereum (ETH). The AKRA project is built in such a way as to become a full-fledged alternative financial system working with cryptocurrency and suitable for both individuals and companies of various capitalization levels.

The intra-network digital economy is represented by the AKRA token and uses the ERC-20 and BEP-20 protocols.

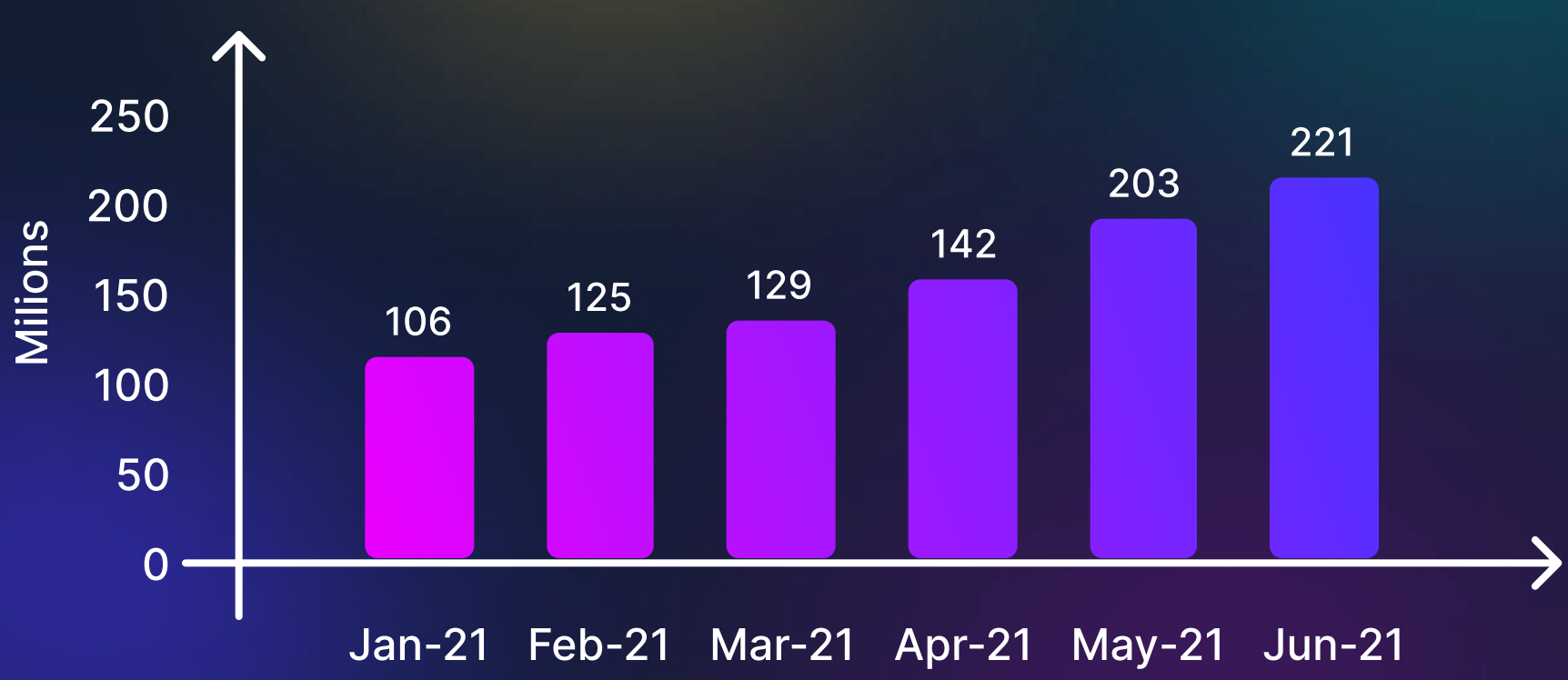
The developers of the AKRA ecosystem offer an effective solution to the problem of interaction between blockchains using blockchain bridges. The technology allows solving the problem of data and financial assets exchange between blockchains, reducing the cost of transfers, and increasing the speed of transactions of digital assets.

1.1 Centralized finance in the global system and existing problems

The first Bitcoin cryptocurrency gave the world a decentralized digital financial system running on the blockchain. Open source code has allowed to explore and discover new perspectives in digital finance, as well as other areas of life that all have made innovations. This has become the main factor in the introduction of cryptocurrencies in many areas of life.

According to data from various analytical sources, the popularity of cryptocurrencies is growing rapidly in various parts of the world. The diagram shows data on the growth of new users of digital finance for the period from January to June 2021, confirming the high interest of users from all over the world.

The growth in the number of cryptocurrency users in 2021



According to: *crypto.com*

The centralized financial system has a number of significant drawbacks, and for this reason, the cryptocurrency is gradually strengthening its position in the financial sector. Among the main problems of the classical financial system, it stands out:

The centralization

Financial flow control is conducted through banks, which can block the funds of the account holder, if it’s necessary.

Emission and inflation control by the regulatory body

Money supply issue is carried out by the central bank depending on various factors and circumstances. This structure also includes the mechanism of keeping inflation low.

Accessibility

For opening a bank account, you must visit a bank branch, and for making payments by bank card at retail outlets requires a payment terminal. These factors may not be available in remote parts of the world,despite the developed banking infrastructure.

High commission

Intermediary functions of banks require significant financial costs. This is reflected in the cost of financial transactions imposed on end users.

2.1 Solutions offered by the AKRA network

The idea of creating the AKRA network is based on the launch of a universal payment instrument available everywhere where there is Internet. At the same time, to ensure maximum outreach of potential customers, providing ease of use, functionality, and low cost of financial services.

The payment system developed in the ecosystem is designed for both individuals and legal entities. There are no restrictions for companies in the place of registration, which allows solving the problem of some legislative prohibitions present in a particular state.

Commissions fees and interaction between blockchains, which are a significant part of the costs, are largely solved by using blockchain bridges.

3.1 Description of the AKRA network

The emergence of a decentralized financial system based on cryptocurrency is related to the growing problems of the classical banking system. The central bank is the issuer of money, delegating part of the functions to other organizations (private banks and financial institutions). The presence of these factors affects the confidentiality and privacy of end users. Blockchain-based cryptocurrency offers an alternative to the classical financial system, allowing full decentralization of financial management.

AKRA network provides a multifunctional payment system that supports both cryptocurrency and traditional finance. The basis of the digital economy is the AKRA token, created on two Ethereum and Binance Smart Chain blockchains with an equal issue of 1,000,000,000 units each.

A wide range of functionalities

When creating a token various parameters and ready-made templates solutions are used to fulfill developers' requests and provide the necessary functions required for the AKRA project.

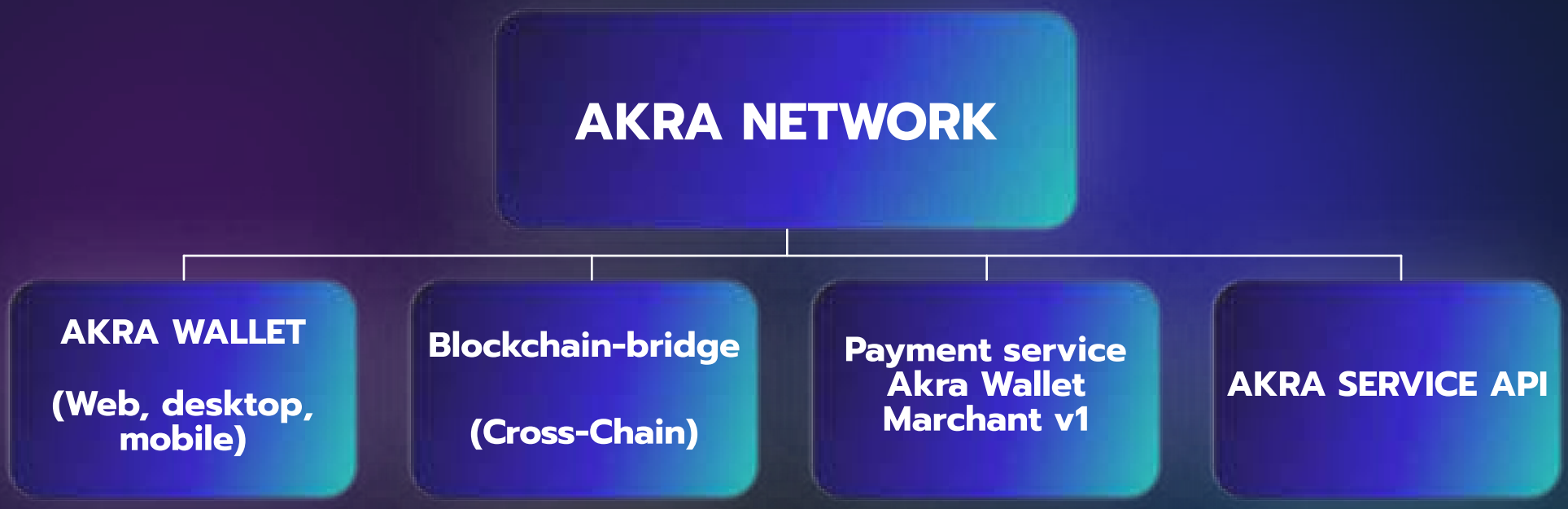
Transparency of Smart-contracts

Operating conditions of the network are prescribed in the smart-contract, which allows to ensure equal conditions for all network members.

Transaction rate

The average transaction processing speed is 2000-4000 operations per second.

3.2 Network structure



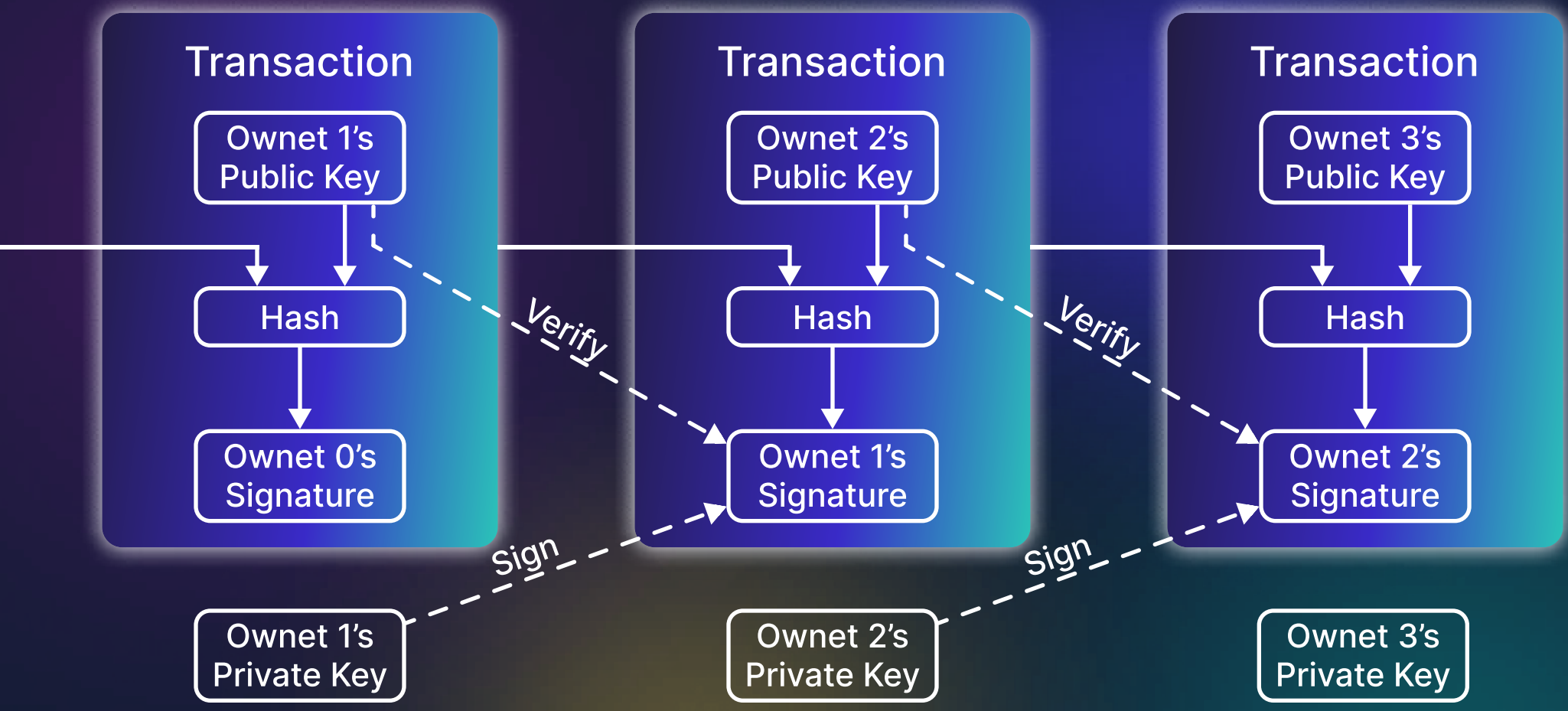
3.3 Blockchain

The blockchain consists of blocks containing data for the operation of the network, linked together by a chain. The connection between the blocks is ensured not only by enumeration, but also each block contains its own hash sum of the previous block. The change of information is transferred to the next block without affecting previous ones. Copies of the blockchain registry are stored on different devices, which greatly increases security in case most of them are disconnected from the network.

The AKRA network is based on the two blockchains Binance Smart Chain and Ethereum. Binance Smart Chain has good functionality and compatibility with the Ethereum Virtual Machine (EVM). Components working in the ecosystem:

1. Full nodes: «standard» fully functional nodes and wallets.
2. Light nodes: SPV nodes and even lighter nodes (e.g., those that just sign transactions)
3. Service nodes: nodes with special functions to provide this service beyond the normal operation of the blockchain.

The scheme of transactions in the blockchain (standard version)



AKRA believes blockchain is one of the foundations for the next generation of information technology, along with emerging trends such as The Internet of Things, smart house, 5G and others. With its tamper-resistant characteristics, blockchain, as an infrastructure technology, is uniquely positioned to provide unprecedented value and data transfer among a wide range of users without trust, enhancing the efficiency and authenticity of the information transfer itself.

3.4 Blockchain information

Functions in the blockchain available for AKRA Tokens (BEP-20):

Transfer	Approve	Increase Allowance
sending tokens	authorize the smart contract dispose of tokens on demand caller.	increasing the number of tokens that can be disposed of using the Approve.

Decrease Allowance

reduction the number of tokens that can be disposed of using the Approve.

Transfer From

transfer of tokens under smart-contract management

Token features available for monitoring in the blockchain registry:

Total Supply

the total number of issued tokens (emission)

Name

token name

Symbol

token symbol

Decimals

the number of digits after comma in the token.

Balance Of

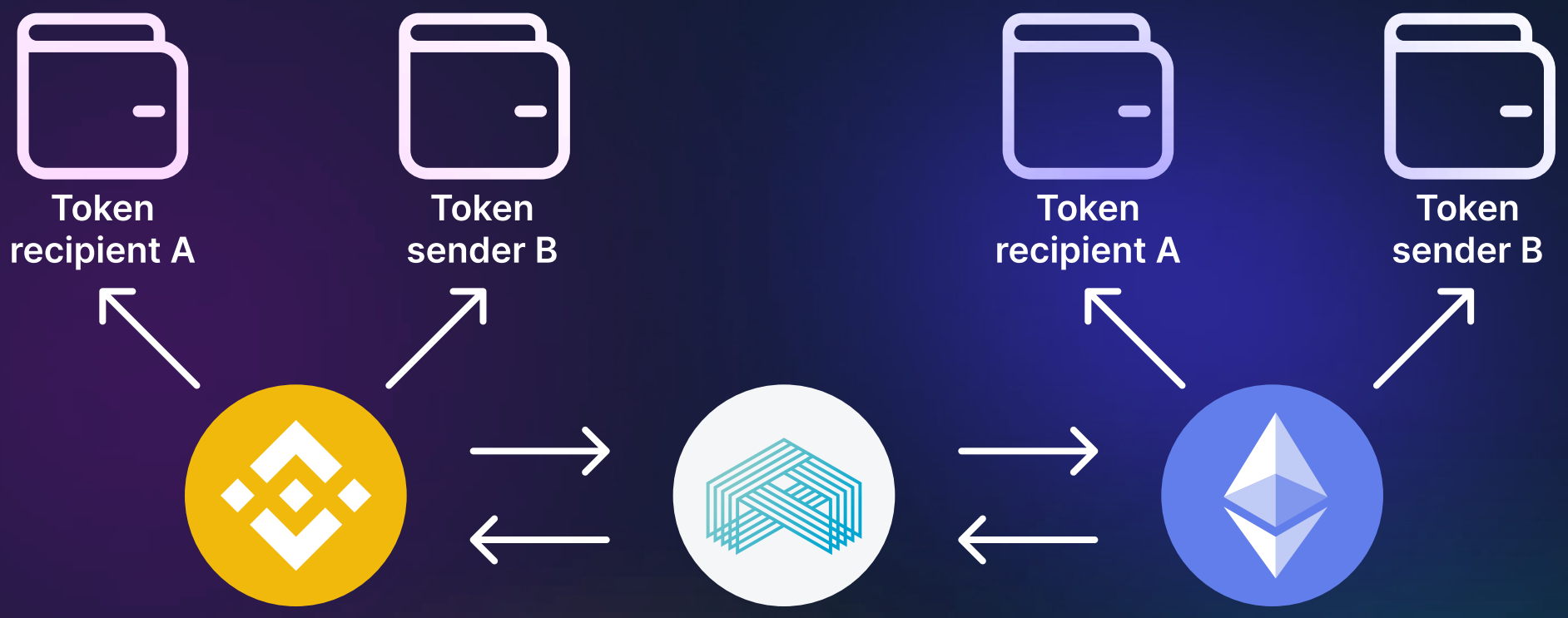
balance check tokens on wallets.

Allowance

check for available tokens, which the smart-contract will be able to dispose of after Approve function call, Increase Allowance.

4.1 Blockchain Bridge (Cross-Chain)

Blockchain bridge or cross-chain is used to solve problems related to the transfer of digital funds between different blockchain networks. Without using this function, it is possible to transfer coins using cryptocurrency exchanges or P2P exchanges, which significantly increases the time spent on the transaction and the cost of commission. The exchange method involves the use of internal liquidity pools and internal wallets. This method is not decentralized. Using blockchain bridge technology, the entire process is fully decentralized, operating at the blockchain level. Smart contracts are responsible for ensuring compliance with the conditions in the process.



The principle of operation is to transfer a digital asset from a base chain to a secondary chain and vice versa. Practically there is a blocking of funds in one chain and unblocking of the same amount of assets in the other, acting on the principle of double pegging (2WP).

Problems solved by blockchain-bridge technology:

Scaling up and reducing the load on the network

Working in L1 and L2 chains distributes the network load more effectively, which is especially important with a large number of transactions.

Reducing the cost of commission

It is achieved through direct interaction between blockchains without involving centralized intermediaries.

Safety

In the exchange the entire sequence of operations is controlled by smart-contracts, which eliminates the risks of third-party interference.

Interactive

The technology allows to support work with different blockchains, that are connected to AKRA blockchain bridge.

5.1 Cryptographic primitives

Shamir's secret sharing scheme is used in cryptography and is implemented in the AKRA network. The principle is to partition the secret ***(t, n)*** between participants ***Pn, ... Pn*** such that any number of participants ***t*** can recover the secret ***s***. At the same time, a smaller group of participants receives no information about the secret ***s***.

- The offeror selects $\in$ ***R Zq*** (when ***n*** < ***q***).
- The offeror selects random participants ***f*** (.) over ***Zq*** of degree at most ***t-1*** satisfying ***f(0) = s***.
- Each punter ***Pi*** gets ***si = f(i)*** as his share.
- The offeror calculates the public key of the participants as ***P = s.G***.
- The public key and the private key are divided into: ***(pk,(sk1, ... , skn)) = (P,(s1, ... , sn))***.

5.2 Secret construction

An arbitrary group ***P*** of ***t*** participants can reconstruct the polynomial ***f(.)*** by the Lagrange formula as follows:

$$f(u) = \sum f(i)\omega(u)_{\text{, when}} \omega_i(u) = \prod_{i\in\rho, j\neq i} \frac{u-i}{i-j} \ mod\ q$$

5.3 Secret key exchange

The elliptic curve notation for the discrete logarithm problem is used. Assume that ***q*** — is a large prime number, and ***G,H*** — are generating subgroups of order ***q*** of elliptic curve ***E***. Assume that ***E*** is chosen in such a way that the discrete logarithm problem in the subgroup generated by ***G***, is difficult, so it is impossible to compute an integer ***d*** such that ***G = dH***.

5.4 Secret key exchange scheme to prevent fraud

The secret exchange verification scheme (VSS) implemented in the AKRA network, prevents possible fraud by participants. In a VSS, each user can confirm his share, if someone spreads uncoordinated transactions, he will be detected.

Assume a participant has a secret ***s0*** $\in$ ***Zq*** and a random number ***s0*** $\in$ ***Zq***, and it is bound to the pair ***(s,s0)*** via the public information ***C0 = sG + s0H***. The secret ***s*** can be shared between ***P1,⋯ ,Pn*** as follows.

The participant obeys the following:

1. Random polynomials $f(u) = s + t_1u + \ldots + f_{t-1}u^{t-1}$, when $s, s', f_k, f'_k \in \mathbb{Z}_q$ for $k \in \{1, \ldots, t-1\}$
2. Compute $(s_i, s'_i) = (f(i), f'(i))$ for $i \in \{1, \ldots, n\}$
3. Send $\left(s_i, s'_i\right)$, a secret for participant Pi for $i \in \{1, \ldots, n\}$
4. Translating the valuations $C_k = f_kG + f'_kH$ for $k \in \{1, \ldots, t-1\}$

5.5 Formulas

Keys

- Secret key: $s = x \in \mathbb{Z}_n^*$
- Public key: ***P = x.G***

Signature

1. $k \leftarrow \$\mathbb{Z}_n^*$
2. ***(x1,y1) = k.G***
3. ***q = x1 mod n.*** when ***q = 0***, return to step 1
4. ***r = k–1(h + qs) mod n.*** when ***r = 0***, return to step 1
5. Backtrack ***(q,r)***

Signature

1. $w = r^{-1}\ mod\ n$
2. $u_1 = hw\ mod\ n$
3. $u_2 = qw\ mod\ n$
4. ***(x1,y1) = u1.G + u2.P***. when ***(x1,y1)*** equal to an identity, the signature is invalid

Signature is valid, when $q = x_1\ mod\ n$,**Invalid in other cases**

6.1 Safety

The AKRA network implements a crypto-encryption mechanism, providing a high degree of security for cryptocurrency transactions. The detailed principle of functioning is described above. Storage of tokens is carried out both on "cold" and "hot" types of wallets. For the highest degree of reliability AKRA developers have created their own line of crypto-wallets.

The main decision to the AKRA network's security problem is the two-way binding mechanism (2WP), allowing the transfer of an asset from the underlying blockchain to the secondary blockchain and conversely. The principle is the temporary interlock the required number of coins in the underlying blockchain. At that moment, the same number of tokens is unlocked, in the secondary blockchain. The base layer assets can be unblocked when the equivalent number of tokens in the secondary blockchain is locked again. The mechanism of 2WP security is based on the honesty of the majority of participants in the network involved in 2WP.

When funds are sent to the AKRA network wallet address, an external transaction within the smart contract is verified. Then it is possible to check the inclusion of the transaction in the block, and then calculating the level of complexity along the chain, minimizing the possibility of fraud.

7.1 Tokenomics

The basis of the digital economy is the AKRA Token running on the BEP-20 (Binance Smart Chain) and ERC-20 (Ethereum) protocols. The emission of each protocol is 1,000,000,000 tokens (a total of 2,000,000,000 units). After the launch of the coin AKRA blockchain on its own blockchain, existing tokens will be exchanged for the coin at a rate of 1:1.

AKRA token distribution graph

7.2 BEP-20 and ERC-20 technical token standard

AKRA token development is based on BEP-20 (Binance Smart Chain) and ERC-20 (Ethereum) standards. Both platforms run on the same virtual machine EVM (Ethereum Virtual Machine). The cryptocurrency addresses in BEP-20 (BSC) and ERC-20 (Ethereum) are identical, allowing transactions between each other.

The use of two blockchains allows the AKRA network to expand its capabilities and thereby increase the number of potential users. The use of tokens based on BEP-20 solves the problem of high transfer fees, and the ERC-20 standard increases the security and scalability of the network.

BEP-20 и ERC technical specifications

Specifications	BEP-20	ERC-20
Blockchain	Binance Smart Chain	Ethereum
Block creation time	3 seconds	13 seconds
Average fee	$ 0,05 – 0,20	$ 5 – 20
Network capacity	300+ TBs	15 TBs
Transaction Rate	Up to 4000/sec	25/sec
Mining/staking	+	+

7.3 Commission fees

Transaction fees in the AKRA network (ERC-20) are paid in GAS, just like in the Ethereum network. Using the ERC-20 protocol, the pricing mechanism changes depending on transaction demand. Note that the transaction costs in Ethereum are higher than in BSC. If set a lower fee, the transfer will take longer in this case.

GAS prices for commission payments fluctuate depending on market factors. When transferring AKRA token to BEP-20 (BSC), the transfer fee mechanism is similar to the Ethereum network. Transactions are calculated using the computing power required to execute the transactions.

7.4 Storing tokens

In order to provide maximum convenience when using tokens, several types of cryptocurrency wallets and Web Akra Wallet v1 payment system working not only with cryptocurrency, but also with fiat money are being developed. Presented options have their own characteristics depending on the specific purposes of their use.

Storing digital assets on an exchange is not the most reliable option because the keys to the wallet are kept by the administration of the exchange. In the case of failure or hacking, there is a high probability of losing funds.

Cryptocurrency Wallet Development

1 Akra Wallet mobile
Mobile cryptocurrency wallet app for working on IOS and Android

2 Web Akra Wallet v1
Fiat payment system for Individuals and legal entities

3 Akra Wallet Plagin
Browser version of Crypto Wallet

4 Akra Wallet desktop
Cryptocurrency wallet for desktop versions

AKRA tokens also work with other types of wallets supporting ERC-20 and BEP-20 protocols. These include MetaMask, TrustWallet and other multi-currency crypto-purses on the market. Correct and safe work with AKRA tokens can be guaranteed only from the line of own developments.

7.5 Pricing. Market regulation

A unique system using two protocols for tokens (BEP-20 and ERC-20) greatly helps separate the value of using blockchain from market speculation. Because of the correlation with blockchain resource usage, the value is more predictable when monitoring AKRA token supply and demand. In addition, the Fund's governance mechanism further stabilizes the value. The estimated value of the token in the markets will be $2.

Having studied the economic models of most public blockchain networks and conducting analytics, the biggest obstacle to the adoption of blockchain-based mass applications was discovered: the cost of using blockchain is directly related to the valuation of tokens. While token valuation typically increases as blockchain usage grows, the cost of using blockchain varies depending on whether a party wants to conduct payment transactions or smart contract transactions. This doesn't even mention speculation by investors and traders as a contributor to the value of blockchain. No business owner would run an app or business on blockchain or anywhere else with unpredictable and unstable value.

8.1 Guidelines for safe working

For safe working in the AKRA network and cryptocurrency, in general, should adhere to some recommendations outlined below.

Do not disclose your wallet password

Under no circumstances disclose the password to cryptocurrency wallet. Responsibility for the safety of funds lies only on its owner. Decentralized management does not allow to freeze or block digital assets, as well as return it back to the sender in case of need.

Check the transaction address before sending

Providing an incorrect wallet address may result in losing funds without the ability to recovery process. You should carefully check the address, to which the transaction will be made.

Transaction has no retroactive effect

Decentralized cryptocurrency system built so that transactions cannot be reversed or returned to the sender

Secure connection

When conducting cryptocurrency transactions, it should be used a secure connection to avoid intercepting passwords by hackers, which subsequently can lead to unauthorized access to wallet. Particular attention should be paid to connection via public Wi-Fi networks and VPN-services.

ROAD MAP

- Q3 2021 — Foundation of the AKRA project as a universal monetary instrument, (ecosystem logic development, database development). Launched
- Q4 2021 — Creation of AKRA. Launched
- Q4 2021 — Development of web AKRA Wallet v1 payment system for individuals and legal entities. Launched
- Q4 2021 — Launch of strategic partner programs. Launched
- Q4 2021 — AKRA Futures robots creation of a terminal for automatic cryptocurrency futures trading service. Launched
- Q3 2022 — AKRA Mining using Proof of Stake Staking. 80% readiness
- Q3 2022 — AKRA Futures robots creation of a service for automatic cryptocurrency futures trading. 50% readiness
- Q4 2022 — Partial sale of AKRA BEP-20 tokens. Collaborations with opinion leaders, targeted community building. 80% readiness
- Q4 2022 — Listing on the exchange. 20% readiness
- Q1 2023 — Partial sale of AKRA ERC-20 tokens. Collaborations with opinion leaders, targeted community building. 20% readiness
- Q1 2023 — Listing on the exchange. Preparation
- Q1 2023 — Updating the AKRA Futures robots terminal using artificial intelligence technology.
- Q1 2023 — Bridges between Binance Smart Chain blockchain and Ethereum. Preparation
- Q2 2023 — Implementation of a fiat payment system for individuals and legal entities through invoicing. Preparation
- Q3 2023 — Token listing on Coinmarketcap, Coingecko. 40% readiness
- Q4 2023 — Mobile app development for IOS and Android. Preparation
- Q1 2024 — Development of AKRA Wallet desktop for Windows, Mac, Linux. Preparation
- Q2 2024 — Development of AKRA Wallet web browser plugin. Preparation

Glossary

- Block: a recordset of cryptocurrency transactions, combined into a block and connected by chains.
- Blockchain: the technology for decentralized network registry management, based on a cryptographic method of information protection, which excludes interference in the network.
- Validators: nodes in the blockchain system that take on the tasks of maintaining the cryptocurrency network.
- Private key: password for access to confidential information.
- Key: the encryption setting, determining the choice of a particular transformation of a given text.
- Cross-Chain: a technology, ensuring the transfer of data and transactions between different blockchains.
- Public key: non-encrypted data transmitted in words.
- Digital signatures: are used to authenticate the document, its origin and authorship. It eliminates the distortion of information in an electronic document.
- API: a special protocol for the interaction of computer programs, which allows to use the functions of one application within another.
- Ethereum Virtual Machine (EVM): it’s a computing machine that acts as a decentralized computer with millions of executable projects.
- SPV: light nodes in the blockchain that sign transactions.

Sources

- Information security – Wikipedia (wikipedia.org)
- Cryptography. Cryptography - Wikipedia (wikipedia.org)
- Berry Schoenmakers, Lecture notes on cryptographic protocols, 2021.
- Mastering Bitcoin: Programming the Open Blockchain. M. Antonopoulos