Kreditz Cryptocurrency project

Cryptocurrency 4.0

No need for block chain.
Customizable addresses
Transfer concept.
Ultra fast and light.
Built-in scalability that allows easy improvements to the protocol.
Macro project that incorporates various aspects.

(Translation of the original document)

Definition:

Kreditz is a new generation virtual cryptocurrency, which works through a P2P protocol, incorporating new functions and features, as well as improvements to the ones you can found in current cryptocurrencies. It operates using asymmetric cryptography keys (also called public key cryptography) to guarantee the integrity of transactions.

This project aims to be an improvement of existing cryptographic currencies, whose first and best known exponent is Bitcoin. Before proceeding, it is good that you are documented about the technical concepts of operating a virtual cryptocurrency, so that you can fully understand the points presented here. Anyway, we summarize here the most important terms:

- Block chain: It is the data source to keep the information updated within the protocol. Each block contains all the transactions made in the network from the moment in which the previous block was generated until the moment in which the next one is created. To create a new block, it is necessary to find the solution of the previous block, through a process called "mining".
- Mining: It is the process by which computational effort is dedicated (and therefore, there is an electrical and hardware expense) to find the solution to the cryptographic problem of the previous block. This problem consists on calculating a chain of characters (with a format predefined by the protocol) that has a Hash concordant, in part, with the hash of the file that contains the previous block. In Kreditz, the difficulty will be adjusted automatically based on the calculation power of the network, in order to obtain blocks in a set time interval.

Kreditz operation

Key Generation:

For each new address, the protocol generates a new ECDSA key pair. The private key is stored only in the user's wallet, while the public key, using MD5 and SHA-256 hash functions, yields a valid Kreditz address of the type:

KCE1C52638B5A446AB8AE269AE52908E705

This address has the following qualities:

- Fixed length: 35 characters, all uppercase letters or numbers.
- The first character is always a capital 'K'.
- The remaining 34 characters are hexadecimal, that is: numbers from 0 to 9 or letters from A to F.
- The second and the last character are checksum, which ensures that a given address is valid.

This address is the one that the user must share to receive transactions. You should never share private keys, as these are the ones that guarantee that only he can access the existing funds in your wallet.

Account Summary (Addresses):

The file accsum.dat contains the information of all the existing addresses in the protocol, including the available balance, as well as the current situation of the blockchain. It is updated with each new block that is created, therefore, it is enough to download this file to start operations in the network. This means that a new user does not need to download the whole blockchain to start using their portfolio, mine new blocks or verify new transactions in the network.

Because the size of this file would increase unpredictably if all the addresses created by the users were immediately registered, the protocol only includes in the summary those addresses that have already received a transaction or mined a block. This keeps the file limited to the size of the addresses used. In addition, due to new protocol functionalities, a user will no longer have to create a new address for each transaction (although he can do so if he wishes) thanks to the 'Alias' or 'Personalization' system of the addresses, as well as a new field : The Concept (we will see this in detail later)

For this condition, addresses in Kreditz may have 3 different status:

- Unregistered: The address was created by the user, but has not yet received any transaction. It does not exist in the summary of accounts.

- Pending: It is an address that has received a transaction, therefore appears in the summary of accounts, but has not yet been registered by the owner therefore the public key is unknown. To do this, the owner must send an ACRE (Account Register) application that includes the public key of that address, as well as a phrase (pre-established) signed with his private key to prove that he is the owner of that account. This process is automatic once the address is in the 'Pending' state, as long as the owner is 'Updated'. If not, the wallet will send the ACRE request in the next connection.
- Registered: The account has been registered by the owner, so all the nodes know the public key and can verify transactions.

Additionally, the Kreditz protocol has a unique quality for addresses: Personalized. It consists of assigning an alias to a specific address, so that the user can share this alias, which can be much easier to remember, to receive payments. It is important to note that when you customize an address, it is immediately registered in the summary of accounts, therefore, doing so has a cost, defined by the protocol. There can not be duplicate aliases in the protocol (in the same way that two identical addresses can not exist).

Each new address added to the account summary will also have assigned the corresponding account number, which will coincide with its relative position in the file; therefore, this number will increase to the same extent that accounts are recorded. This account number may also be used to receive transactions.

Optimization of the accounts summary:

As already mentioned, the accounts summary contains all the necessary information for the nodes and is, therefore, the crucial part of the Kreditz protocol, so keeping it efficient is a fundamental part of the project. To achieve this, certain measures are included:

- Registration cost per account. (explained in the previous paragraph)
- Cost for account customization (explained in the previous paragraph)
- Verification of abandoned accounts: every 105120 blocks (1 year) the protocol will review the last operation of all the accounts in the summary, and deduct a commission (established by the protocol) to all those accounts that have not presented activity since the last revision. The discounted commissions will be added as a reward to the miner of the next block. If the remaining amount in one address is less than the maintenance cost, the account will be deleted and its space in the account summary can be reused for a new account.
- There will be a minimum amount per transaction, established by the protocol, to avoid saturation of the network with micro transactions.

The concept:

The concept is an alphanumeric chain added in each transfer, which can contain any type of information that the payer can include for the receiver of the transfer. The concept is included in the digital signature to avoid double-spending situations. The length of the concept has a maximum of 40 characters and is not case sensitive.

Blocks:

In the Kreditz protocol, the blocks serves to order the transactions correlatively and keep the account summary updated, so once a block is created and its information added, its utility lies only in consulting the transaction history. This is why Kreditz is independent of the block chain once the user updates to the network. Only as a safety measure will the last twenty generated blocks always be downloaded, which also serve as reference for the calculation of the mining difficulty.

The user can choose between running a complete node, in which case he will download the entire blockchain before updating, or not; if you do not do it, just download the last twenty blocks.

The structure of a block is the following:

- Header: Contains all the information of the block, including: start time, end, duration, direction that performed the mining, reward, commissions, problem for mining, difficulty, etc.
- List of transactions: A list of all transactions included in the block.
- Solution: the string of characters that represents the solution that validates the problem of mining raised in the header.

Double spent control:

In the Kreditz protocol, double-spending control is carried out by verificating the transaction hash. Since all transactions have a timestamp incorporated (with milli seconds precision), a signed transaction will only be valid for the current block or the next one (we will explain later why). Unlike other cryptocurrencies, this means not being able to perform offline transactions, but it allows faster calculation and verification of transactions, as well as the virtual elimination of orphan blocks. A transaction can not be duplicated in the same block, nor exist in the previous block, in order to be accepted, since if its creation timestamp were lower than the start of block X-1, it would be automatically discarded.

Network time:

Given the nature of the Kreditz algorithm, the precision in the synchronization of the nodes is very important. Although it does not require absolute accuracy, if it is necessary that they handle very similar times. This is why version 0.2 will use known public servers to set the time of the node before comparing it with the other members of the network. Although the difference by latency should in no case exceed two seconds, the protocol establishes as three seconds the maximum time allowed to

accept transactions from a pair; this prevents late and malicious retransmission of duplicate operations.

All operations within the network use the UTC reference time.

Orphan Blocks:

The Kreditz protocol is designed to prevent the creation of orphaned blocks, and if one is created, prevent its propagation through the network. This is achieved by keeping all pending transactions uniform, modifying their structure only if a modification will not be included in the next block, in order to give time to re-verify all subsequent transactions. This means that if one or more transactions are generated shortly before the creation of a block, those transactions will be included in the subsequent block.

Kreditz Project objectives

The Kreditz project aims to facilitate the payment of goods and services online, without the need for third parties and in an effective time for both consumers and merchants. To achieve this goal, the project includes the development not only of the protocol and the portfolio, but also of other applications that will allow this functionality.

- WalletLite: Implementation of the wallet for the user who only wants to buy and sell. It will not act as a node, nor validate operations, it will only keep the summary of accounts and the user's own portfolio updated. It will allow you to make instant payments with a single click at the places that accept payments at Kreditz, as well as verify the balance of your portfolio at all times.
- Web explorer: will keep the status of the Kreditz network up-to-date at all times, to serve as a source of information to those who wish to consult it.
- Web exchange: Similar to the existing one for Bitcoin, a web platform that allows Kreditz owners to exchange their balance to FIAT, quickly, efficiently and reliably, directly with other users.
- Web tools: This part includes the development of tools for programmers, in different languages (PHP, Phyton, Java, etc) to facilitate the incorporation of Kreditz payment procedures in websites that wish to join the network.
- Wallet: Constant improvement of the desktop wallet, since as the main support of the network, it requires continuous updating to incorporate new functionalities to the protocol.

Another objective of Kreditz is to create a community of users as large as possible, avoiding the action of whales and speculators. This is why the initial code does not include any type of function that facilitates mining by the pools dedicated to it; On the contrary, our idea is that in the first months, mining is done directly by the users, since in this way more people will be participating in the project.

Operability and business model.

The following box shows the Kreditz production schedule over time.

Kreditz Block Reward Schedule							
Weeks	Aprox. Time	From	To	Blocks	Reward/Block	Coins/Period	Total Coins
Contrib	...	0	0	1	1.420.544.000	1.420.544.000	1.420.544.000
1	1 week	1	2.016	2.016	1.024.000	2.064.384.000	3.484.928.000
2	3 weeks	2.017	6.048	4.032	512.000	2.064.384.000	5.549.312.000
4	1 month, 3 weeks	6.049	14.112	8.064	256.000	2.064.384.000	7.613.696.000
8	3 months, 3 weeks	14.113	30.240	16.128	128.000	2.064.384.000	9.678.080.000
16	7 months, 3 weeks	30.241	62.496	32.256	64.000	2.064.384.000	11.742.464.000
32	1 year, 3 months	62.497	127.008	64.512	32.000	2.064.384.000	13.806.848.000
64	2 years, 6 months	127.009	256.032	129.024	16.000	2.064.384.000	15.871.232.000
128	5 years	256.033	514.080	258.048	8.000	2.064.384.000	17.935.616.000
256	10 years	514.081	1.030.176	516.096	4.000	2.064.384.000	20.000.000.000
...	Forever	1.030.177	...	...	0	0	20.000.000.000

7% of the total Kreditz to be produced will be premined in block zero; of this amount, 5% (1,000,000,000.00 KDZ) will be to the promotion of the project through gifts, prizes, contests and activities through the different channels and social networks (blog, facebook, twitter, etc.) achieve maximum diffusion and reach the largest number of users. The detailed accounting of this amount will be reflected on the website in an updated and transparent manner.

The remaining 420,544,000.00 KDZ will be used as follows:

Initial Auction for Project Contributors (IAPC)

200,000,000.00 KDZ will be allocated to a first offer for project contributors, at a conversion rate of 1.00 KDZ = 0.00000001 BTC. The objective of this auction will be to raise funds to continue with the following steps of the project:

- Business hosting of the web pages that are part of the project.
- Translation of all the components of the project to the most outstanding languages: Russian, Mandarin Chinese, Korean and Japanese.
- Physical installation of a minimum of two master nodes to guarantee the operation of the network at all times once started. These nodes will also serve the websites related to Kreditz, and will be located in different countries.
- In general, any remnant in the proceeds of this auction will be used to improve the protocol and related services.

Initial promotion for incorporation to exchange webs:

100,000,000.00 KDZ will be dedicated to promoting the project with different exchange pages to incorporate Kreditz in its list of currencies. This will allow a rapid re-valuation of the project, increasing the global interest for the currency and at the same time provide early benefits to the initial contributors.

Accumulated for improvements in the protocol:

Finally, a total of 100,544,000.00 KDZ will be dedicated to reward those members of the community who offer improvements to the Kreditz protocol; The rewards in these cases will be according to the impact that these improvements represent for the protocol, but they must not exceed 1% of this amount in any case. The development group may offer rewards to whoever manages to improve certain aspect, including the amount of said specific reward.

The following points are considered foundational values of the project:

- It will not be invested in paid advertising
- The anonymity of the development team will be maintained as far as possible, following the ideal of the creator of Bitcoin.
- Any benefits obtained through the additional services of the project will be fully re-invested in it.
- The deadlines set as the highest priority will be met.