

# KALKULUS

WHITE PAPER

v 1.0



# TABLE OF CONTENTS

<b>Abstract</b> .....	01
<b>Acknowledgements</b> .....	01
<b>Contributors welcome</b> .....	01
<b>Disclaimer</b> .....	02
<b>Abbreviations</b> .....	04
<b>1. About Kalkulus</b>	
1.1. Overview.....	05
1.2. History.....	06
1.3. Kalkulus Ecosystem Outline .....	07
<b>2. Kalkulus Blockchain</b>	
2.1. PoS (Proof-of-Stake).....	08
2.2. Masternodes .....	09
2.3. See-Saw Mechanism .....	10
2.4. Planned Reward Distribution (by block height) .....	11
2.5. SwiftTX and Instant Transaction.....	12
2.6. Obfuscation Protocol.....	12
2.7. Governance by Voting On Network .....	13
2.8. Specs Table.....	14
<b>3. Kalkulus Decentralized Applications Technology</b>	
3.1. KLKS dApps Architecture Overview .....	15
3.2. KLKS-dAPI .....	17
3.3. KLKS-Storage .....	19

## 4. Early Stage Kalkulus dApp

4.1. Kalkulus dAPPStore & KLKS-ID.....	20
4.2. KLKS-PoE.....	21
4.3. KLKS-DFS.....	22
4.4. KLK-KYC.....	23
4.5. KLKS-MSG.....	24

## 5. The Hub

5.1. The Hub Overview.....	25
5.2. Staking V-Box.....	26
5.3. Easy Masternode Deployment.....	28
5.4. COMA Nodes.....	28
5.5. The Hub 2.0.....	30

## 6. KLKS-PAY

6.1. Cryptocurrencies Payment Gateway.....	31
--	----

Appendix.....	32
---------------	----

References.....	32
-----------------	----

List of Sources.....	32
----------------------	----

## Abstract

This document is intended for those who do not have specific technical skills in blockchain technology or for those more experienced in the field in question, provided the reader has at least a general understanding of what a blockchain is.

The Kalkulus's architecture will be introduced with the aid of graphics, and through a gradual exposition of how Kalkulus ecosystem is composed.

We want to communicate our vision because we believe that, in a project such as this, it is of primary importance to engage those who would use day by day our technology and we stand to gain enormously from people's engagement with it. Its very important to gain insights on our work from multiple viewpoints. Furthermore, we publish this document in order to be consultable by our current partners and by those who want to join our project in future.

## Acknowledgements

Kalkulus would never have been born without the work of those who have developed projects such as Bitcoin, Peercoin, Dash and PIVX. Open source software is constantly paving the way for exciting innovations and we are deeply grateful to our predecessors who pioneered the opportunities offered by this technological language. Also thank you for all the people who try to make open source even more open! Freaking awesome! When information and knowledge are free, society can only benefit from it.

## Contributors welcome

Kalkulus is a project in continuous development and this document have not be intended as final. Blockchain code of Kalkulus is open source, all contributions and discussion to this document are absolutely welcome, and anyone may contribute to this project.

We welcome collaboration in many forms, and there's always plenty to do! If you aim to contribute to the project, contact the team at [kalkulusteam@gmail.com](mailto:kalkulusteam@gmail.com) or follow our Official Github <https://github.com/kalkulusteam/klks>

## Disclaimer

This document have the solely purpose of describe and illustrate technical development of Kalkulus as project and describe targets set by the development team. The introduction and description of the basic conditions of the project in this document is an invitation to the general public. The information provided on this document does not constitute in any way an investment advice, financial advice, trading advice, or any other sort of advice, and you should not treat any of the content as such.

Nothing on this document should be taken as an offer to buy any digital asset. Do conduct your own due diligence and consult your financial advisory before making any investment decision. Kalkulus will not be held responsible for the investment decisions you make based on the information provided on this technical document.

Those who have the intention to participate, invest, and cooperate in this project must clearly understand the full risks of this project, that is not and cannot be regarded as an investment or declaration of commitment to any specific or unspecified subject, is not a commitment nor a guarantee of accomplishment of all described development targets.

The digital asset “Kalkulus” or “KLKS” referred on this project, has a complete and independent value separate from the project team. The trading behavior on different digital assets trading platform, market environment and the degree of acceptance of market entities will determine and change the value of KLKS as digital asset. This value is determined by the recognition of the value and exchange value of the relevant market participants.

Digital assets markets could have larger price volatility caused by unstable policies on blockchains in countries and regions around the world. It is common for prices to face drastic fluctuations and value of your holdings could increase or decrease by over 100% in a single day. Although this could mean potential huge profits, this also could mean potential huge losses.

The team cannot guarantee the value of KLKS as digital asset over time , also the ROI of masternodes can depends from several conditions and cannot be considered as a guarantee of financial return. KLKS as digital assets cannot be regarded as bonds or any form of securities, nor is it a project team’s, company’s equity, shares, ownership or control.

For this reason, you should **DO NOT INVEST ALL YOUR MONEY IN ANY DIGITAL ASSETS**. Only invest money which you are willing to lose. Cryptocurrency trading may not be suitable for all users of this website. Anyone looking to invest in cryptocurrencies should consult a fully qualified independent professional financial adviser.

Kalkulus team and the project itself faces many risks, including but not limited to the world economy and environment, blockchain development, corporate operations, and other unpredictable events that could happen anytime or force the project to terminate development operations.

The project team cannot and will not be liable for any loss or damage caused by your own actions, you are the solely responsible of your digital holdings and custody of your private keys. The project team also cannot guarantee the storage, retrieval, and modification of the relevant virtual property of your digital assets. You are the solely responsible of holding Kalkulus in trading exchange or digital asset portfolio, also those provided by the team, represents an understanding and willingness to accept its risks.

In view of changes in the ongoing regulation of blockchain technology, cryptocurrency or intangible assets by governments around the world, Kalkulus team reserves all rights to modify, delete, add, revoke, abrogate, and interpret related behaviors of some or all of the contents of this document at any time, in accordance with the laws regulations, and actual conditions of each region.

You confirm that you are free to judge the content of the project team and the project services, and bear all risks arising from the use of the contents of this document, including the risks arising from the reliance on the correctness, completeness or practicality of the contents of this document.

## Abbreviations

<b>2FA</b>	<b>Two Factor Authentication</b>
<b>API</b>	<b>Application Program Interface</b>
<b>App</b>	<b>Application</b>
<b>ASIC</b>	<b>Application-Specific Integrated Circuit</b>
<b>BR</b>	<b>Block Reward</b>
<b>COMA (nodes)</b>	<b>Clientless Onsite Masternodes</b>
<b>DFS</b>	<b>Distributed File Storage</b>
<b>DIN (nodes)</b>	<b>Dapps Infrastructure Network</b>
<b>CSS</b>	<b>Cascade Style Sheets</b>
<b>CPU</b>	<b>Central Processing Unit</b>
<b>dApp</b>	<b>Decentralized Application</b>
<b>GUI</b>	<b>Graphic User Interface</b>
<b>ID</b>	<b>Identification</b>
<b>KLKS</b>	<b>Kalkulus digital asset ticker</b>
<b>KYC</b>	<b>Know Your Customer</b>
<b>MN</b>	<b>Masternode</b>
<b>MSG</b>	<b>Messenger</b>
<b>PoE</b>	<b>Proof of Existence</b>
<b>PoW</b>	<b>Proof-of-Work</b>
<b>PoS</b>	<b>Proof-of-Stake</b>
<b>P2P</b>	<b>Peer-to-Peer</b>
<b>REFID</b>	<b>Reference code Identifying</b>
<b>RPC</b>	<b>Remote Procedure Call</b>
<b>UI</b>	<b>User Interface</b>
<b>UUID</b>	<b>Universally Unique Identifier</b>
<b>UX</b>	<b>User Experience</b>
<b>VPS</b>	<b>Virtual Private Server</b>

### Overview

Kalkulus is a blockchain project based on its own open source and decentralized digital asset, identified through the ticker \$KLKS, that enables instant transactions to anyone, anywhere in the world. The process of minting new coins for Kalkulus is based on Proof-of-Stake (PoS), an algorithm to achieve consensus by requiring users to stake an amount of their digital holdings having a chance of being selected to validate blocks of transactions, and get rewarded for doing so.

The network of Kalkulus is secured by masternodes, that are crypto full nodes running a client that supports the network by hosting an entire copy of the coin's ledger in real time. Every masternode running on the network is periodically rewarded, according to conditions of the network and the number of active masternodes, for the whole set of special operations and task that they execute on the blockchain.

Kalkulus offers a perfectly balanced passive income for stakers and masternodes holders, that contribute to maintain the Kalkulus blockchain reliable, fast, stable and secure.

In our opinion, for any crypto-oriented project, it is very important to look at other use-cases that are not mere “financial trading instrument” applications. Through “The Hub”, “KLKS-dAPI”, “KLKS-Storage” and other planned developments, Kalkulus aim to be a long-term project offering services related to blockchain technologies characterized by ease of use. The purpose is to allow all customers to safely experience the potential benefits of a digital currency from different point of view.

Decentralized Applications based on Kalkulus blockchain are the final elements that we are working on, with the purpose of create a complete ecosystem that aspire to bring cryptocurrencies to everyday business and commerce for a smart economy era.



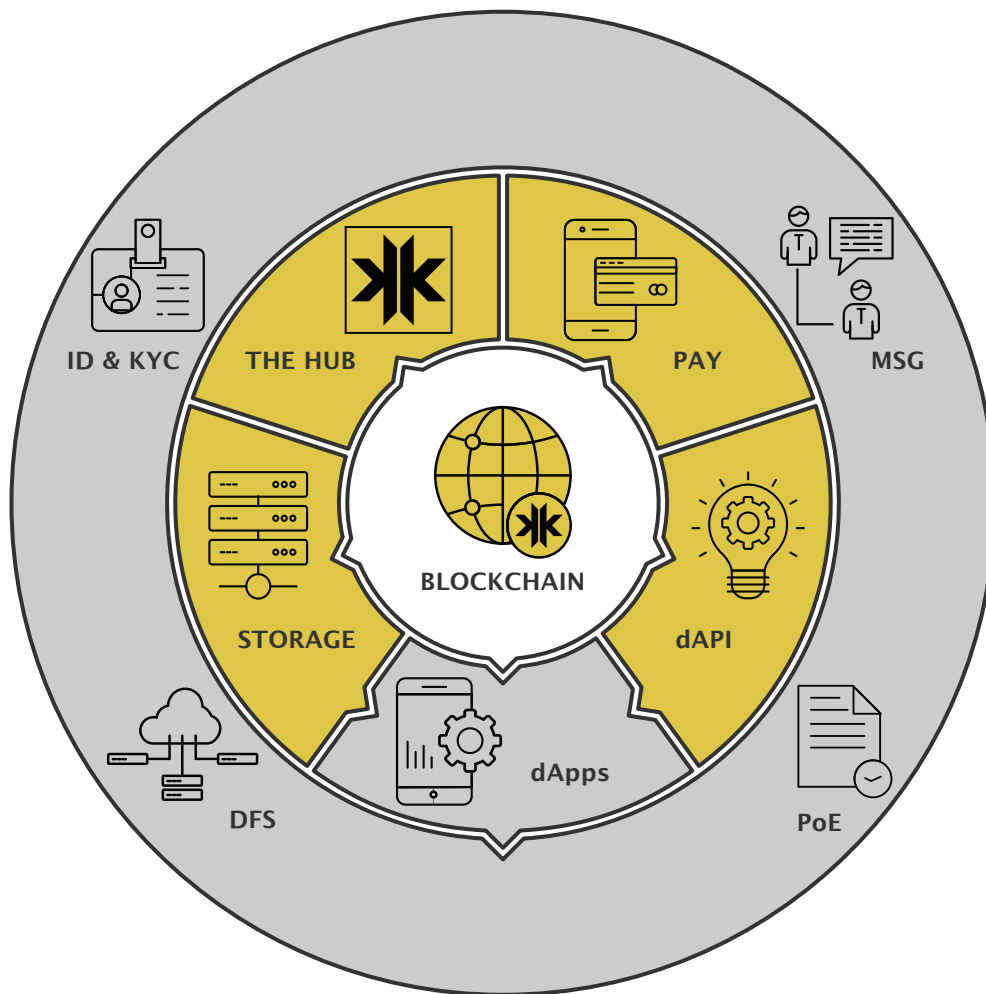
Kalkulus genesis block was mined in November 2017. Based on Proof-of-Work consensus protocol and algorithm Scrypt, Kalkulus ticker and different ambitions, Kalkulus is indeed the result of previous trials conceived exclusively for study and research purposes. The initial exclusive work of the Core team was started by a single person. Currently composed of three elements, the Kalkulus project and team have grown by several collaborators, counting now over 10 peoples that actively put their effort on the project. Kalkulus has experienced constant and ambitious developments that have naturally resulted in an expansion of the team with members that cover different areas of expertise: from blockchain development to back-end developing; from web design to marketing; from specific roles of community managers up to technical support.

In April 2018, the consensus protocol was changed from Proof-of-Work to Proof-of-Stake. The Quark algorithm (Dash/Pivx fork) implemented PoS/Masternode consensus method, with See-Saw Mechanism to balance rewards between masternodes holders and stakers. Also the ticker was changed from KLK to KLKS.

In May 2018 Kalkulus team, according with the community, instituted a “Kalkulus Treasury Fund” that consists of 10 active masternodes (200K KLKS locked) that produced rewards until 1st January 2019. In months to come we will discuss with our community on how to invest all unlocked funds: marketing, promotion and advertising, new exchanges and team expansion are only few of development area where all collected funds could be invested.

In July 2018, Kalkulus launched his first product, giving to KLKS a true and tangible use case: The Hub. The platform is a proprietary set of web-tools aimed to favour and increase the adoption of Kalkulus and other digital assets that are implemented on the platform over time. The Hub main purpose is to be a multi-currencies masternodes deployment and hosting service. The platform offers also other services like a multi currencies “virtual” staking hosting, a cloud full node hosting system that allow user to deploy masternode without needs of desktop client directly from inside the platform, an online wallet with KLKS onsite buy option, as well as advanced monitoring tools to keep track of investments.

Future plans are most focused in developing the decentralized infrastructure for a smart economy based on the Kalkulus Blockchain. We will take a closer look at this topic in the chapters: “Kalkulus Decentralized Applications Technology”.



- 1. KLKS Blockchain:** PoS/Masternodes technology with reliable user desktop wallet on multiple platform (Win/Ubuntu/Mac).
- 2. KLKS-dAPI:** Decentralized Application Building Architecture with symmetrical encryption and secret key option for any central point-of-failure system.
- 3. KLKS Storage:** Decentralized data center with IPFS storage, smart sync and file persistence based on KLKS Blockchain and The Hub VPS.
- 4. KLKS Early Stage dApps:**
  - 4.1. KLKS-PoE:** Validate and store your documents and files over the blockchain.
  - 4.2. KLKS-DFS:** Encrypted file hosting service with cloud storage via IPFS technology.
  - 4.3. KLKS-ID & KYC:** On-line identity verification technology via KLKS Blockchain.
  - 4.4. KLKS-MSG:** Decentralized and permanent message service with instant chat.
- 5. The Hub:** Staking V-Box, Easy Masternode Deployment, COMA (Clientless Onsite Masternodes) Nodes, Web Wallet, interconnected to KLKS-Storage IPFS Technology.
- 6. KLKS-PAY:** Digital Payment Technology Service with physical Point-of-Sale system for local store and plug-in integration for e-commerce.

## PoS (Proof-of-Stake)

In chain-based Proof-of-Work ("PoW"), consensus is reached by nodes called "miners" competing to solve cryptographic puzzles; the miner dedicating the greatest computational resources has the highest chance of producing the next block.

The Kalkulus Proof-of-Stake ("PoS") consensus algorithm selects a validator every period of 60 seconds according to the amount of coins that the potential validator allocate for staking, in proportion to circulating supply, and assigns to that validator the right to create a single block.

Every new found block is linked to the previous block, and so over time all found blocks converge into a single constantly growing blockchain that relies on nodes incentivized to maintain an economic participation in the network.

In other words, Proof-of-Stake means that all clients connected to the network and unlocked for staking (or still not encrypted) mint new coins and ensure a passive income according to the amount of available staking power.

Kalkulus's Proof-of-Stake system by Peercoin combines randomization with the concept of "coin age", a number derived from the product of the number of coins multiplied by the number of minutes the coins have been held.

Coins that have been unspent for at least 1 hour begin competing for the next block. Older and larger sets of coins have a greater probability of signing the next block. However, once a stake of coins has been used to sign a block, it must start over with zero "coin age" and thus wait at least 1 hour before signing another block.

PoS provides several benefits over PoW:

1. PoS block generation requires less power consumption than PoW. This process secures the network and gradually produces new coins over time and requires very minimal energy consumption; it only requires the energy to run the KLKS client software on a computer or a VPS, as opposed to running resource-intensive cryptographic hashing functions.

2. The Proof-of-Stake method of generating coins reduce centralization risk, exponentially increasing cost for the stakeholders to establish a monopoly. All new coins are generated according to the original amount of holdings of each individual validator. In other words, someone holding 1% of the currency, if this amount is “mintable” and effectively put in staking, will generate 1% of all Proof-of-Stake coin blocks.

## Masternodes

A masternode is a full node, running on its own server, that ensure decentralization and improve stability of the network.

Masternode servers, that must be online and functioning 24/7, store and distribute in real-time a full copy of the blockchain, verify that blocks and transactions are valid, and perform other additional task like SwiftTX, obfuscation and governance.

Operating as a masternode validator requires the ownership of 20000 KLKS as collateral. To incentivize their operations, masternodes are rewarded with a portion of all newly created KLKS, according to a pre-determined mechanism of rewards allocation among all stakers.

## See-Saw Mechanism

In order to allocate rewards distribution more efficiently, Kalkulus adopt a system that dynamically change the ratio of rewards between masternodes and stakers, preventing centralization of the network from masternode holders.

See-Saw Reward Mechanism” automatically modify ratio between masternodes and staking rewards and re-balance amount of distributed shares, according to the percentage of coins locked in masternodes.

The more coins are locked in masternodes as collateral, the less rewards are distributed to masternode holders: as consequence, masternode became less profitable and ROI for investors became longer. As consequence, profitability for staking increase of the same percentage.

When number of active masternode is less or equal to 1% of total circulation, the reward is 90% of the total block reward, and the staking wallet receives 10%. At 10% of masternode saturation, the share is split to ~80% for masternodes ~20% for stakers. At 25% of total circulating coins locked in masternodes, the ratio became 65/35.

Equilibrium point, where the block reward is split evenly between masternodes and stakers, is reached when ~41.5% of coins are locked in masternodes.

The number of active masternodes needed for equilibrium is always variable over time, being based on the number of coins locked in masternodes over amount of total supply.

Going over the 41,5% of coins locked on masternodes, the share for masternodes start to decrease, favouring stakers. The See-Saw Reward Balance System, created by PIVX and adopted by KLKS, provides numerous benefits over reward split methods used by other PoS/MN cryptocurrencies:

1. It can indirectly affect the total count of masternodes in the network by varying reward size of masternodes versus staking.
2. Promotes staking by increasing its reward payment portion when masternode count is high, thus maintaining a high level of network security.
3. Allows all coins owners to be rewarded for holding coins rather than just the masternode owners, resulting in a fairer and less centralized system.

## Planned Reward Distribution (by block height)

Block Eight	Block Rewards	PoS/MN Ratio
From block 1 to 4999		Proof-of-Work
4999 > 380711	15	Dynamic Ratio*
380712 > 423913	12	
423914 > 467114	9.6	
467115 > 510315	7.7	
510316 > 553516	6.15	
553517 > 639917	5.25	
639918 > 726318	4.45	
726319 > 812719	3.8	
812720 > 899120	3.2	
899121 > 1028721	2.75	
1028722 > 1158322	2.45	
1158323 > 1287923	2.2	
1287924 to total supply	2	

(\*) The ratio allocation of block rewards between MN and PoS is dynamically balanced through the See-Saw Rewards Mechanism and will change according to different factors, in primis the shares of total coins locked on masternodes over the total supply.

## SwiftTX and Instant Transactions

SwiftTX technology, introduced by PIVX, is operated and secured through the masternode network, and allows transactions to be confirmed and validated also with zero-confirmations.

This function takes place via a deterministic selection of a masternodes for each input spent in a SwiftTX transaction. The masternode examines the input via ZeroMQ Library (a high-performance asynchronous messaging language) over the masternodes network, near-instantly achieving consensus and eliminating the need to await confirmations and the risk of a double-spend.

This differs from inputs used in normal transactions, which can be spent after just one confirmation regardless of whether the blockchain was received using SwiftTX or not. Adopting SwiftTX technology, Kalkulus is able to provide near-zero confirmation transaction competing with other high-speed cryptocurrencies.

## Obfuscation Protocol

Obfuscation Protocol is a privacy function that, when activated, start a process of mixing a portion of available balance, making harder the tracking process of those coins when sent or received on the network. Activating the Obfuscation Protocol, the wallet start to fragment a pre-set amount of coins in small parts, then send this coins to masternodes for anonymization.

When received from masternodes, coins sent for obfuscation are mixed and swapped with other coins coming from other obfuscation request, and are sent back to the original owners, in the same amount but from different and unknown address, making harder the tracking process when sent again.

Activating Obfuscation Protocol, there is no way to relate input and outputs in one transaction and thus the exact direction of money movement remains unknown to third parties. Obfuscation coin-mixing methods increase privacy for users because inputs to a transaction cannot longer be reliably associated to a single user.

## Governance by Voting On Network

In many public blockchains, governance is informal, and “rules” are community based. With Kalkulus, governance can be achieved by hard coding rules explicitly into the blockchain code directly. Kalkulus masternodes form a distributed, decentralized, management governance system that votes on-network on proposals created and submitted from community members.

Through the Governance Budgeting System, anyone can submit a description of proposal for development, requesting a budget and a deadline for the proposal. When a proposal is submitted, all masternodes owners have the right to vote the proposal by signing a message from the masternode collateral address. The votes can be submitted at any time, and can also be changed, and this is possible to be done prior to the emission of “superblock”, that are special blocks minted each month. When voting sessions are closed, the blockchain executes a decentralized tally and validates all votes, broadcasting results of votes and allocating the budget in the next superblock.

We will utilize a multi-step process for creating and submitting proposals. Each phase will need to be fully completed:

1. Start in our Discord chat, and talk with the community about your idea. Gauge interest and if the response is positive, move to the next phase.
2. Be open to suggestions from the community and developers. Be flexible and willing to incorporate external ideas and suggestions into your proposal.
3. Utilize multiple social media platforms to discuss and receive feedback. Remember that reaching a consistent portion of the Kalkulus’s user base will often require some footwork.
4. Create a formal pre-proposal on the specific Governance Pre-Proposal room of our Discord.
5. Upon completion of these steps, you will submit your proposal to the blockchain. Be prepared for a one time fee of submission. The submission fee is non-refundable.
6. Be sure to get back in touch with everyone you spoke with so your idea will be voted on. For a proposal to be paid out, 10% of the eligible masternodes must vote ‘yes’ on your proposal.

At the moment, the Governance Budgeting System is disabled on Kalkulus blockchain, and will be enabled when it will be effectively needed.



Coin Name <b>KALKULUS</b>	Ticker <b>KLKS</b>
Coin Type <b>PoS/MASTERNODE</b>	Hashing Algorithm <b>QUARK</b>
Block Time <b>60 sec.</b>	Block Size <b>1 MB</b>
Coin Name <b>KALKULUS</b>	Premined <b>9,000,000</b> (to perform swap from old KLK)
Reward Method <b>SEE SAW MECHANISM</b>	RPC & P2P ports <b>51122/51121</b>
Minimum Stake Age <b>60 min.</b>	Masternode Collateral <b>20000 KLKS</b>

### Kalkulus dApps Architecture Overview

When the Internet reached the general public in the early 1990's, it brought with it the hopes of a new democratic world based on a decentralized network. The utopia of that vision is today quite clear, since we find ourselves living, working, relating and communicating in a centralized "pyramidal" internet where the big web companies dictate the "rules of the game". Centralized systems are currently the most widespread model for software applications. A standard web app, such as Uber or Twitter, runs on a computer system which is owned and operated by an organization giving it full authority over the app and its workings. There may be multiple users on one side, but the backend is controlled by one single organization. All individuals are directly dependent on the central power to send and receive information. Facebook, Amazon, Google, and every other mainstream service we use on the Internet uses this model.

Yet, the idea of a decentralized and distributed Internet, where in essence no single entity owns or controls the IT infrastructure, is still alive and finds with the Blockchain a new lifeblood through which we can create an environment where resources are shared among the participants, where people (not the big giants of the Internet) have control over their information, their personal data, what they create and share. "Distributed" means computation is spread across multiple nodes instead of just one. "Decentralized" means no node is instructing any other node as to what to do. That means that any app that uses a blockchain alongside other peer-to-peer tools can be distributed and decentralized.

Kalkulus blockchain technology can be used to create the so-called dApps, decentralized applications that runs without need of a central server or middlemen that control informations. Kalkulus dApps are tools created using the blockchain technology of Kalkulus and are strictly connected to the KLKS-dApi, an element characterizing the Kalkulus network and that will be further explained later.

When trying to understand what a decentralized app is, the first thing to focus on is the server talk. While for classic applications there is a central server on which they are stored, decentralized apps do not reside on a single central server. This feature is not only the first difference with the classic applications, but also the first advantage, since it frees the dApp from the dependence on a single server.

Another element that differentiates decentralized apps from the current standard is privacy. The dApps offer the user the ability to fully protect their personal information and their privacy, and in fact it is not necessary to register as with traditional applications. No registration is required to take advantage of the applications because each user is already identified by a unique string of encrypted numbers and does not need to identify himself further by providing sensitive personal data.

Like the traditional applications that we usually use, decentralized apps can also be used in a variety of industries. A first and immediate use is that in the field of online commerce and finance. However, the economic sector is not the only one in which decentralized applications can offer their benefits. They can be used, for example, to transfer files from one user to another and to authenticate and validate a wide range of operations, including but not limited to electoral voting. Privacy protection and independence from a single central server make decentralized applications much more efficient and safer than the applications we typically use.

Through the KLKS-dApps architecture, each developer can obtain his own KLKS-dAPI with secret key in order to create distributed, autonomous, permanent and decentralized databases using common programming languages (a simple REST API). Another important element is that, through KLKS-Storage, it is possible to combine the databases in continuous sync with the blockchain with IPFS Technology, a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system retained by the entire The Hub VPS network.

These technologies open the way to Kalkulus dApp Store, a virtual space that will gather all the applications based on Kalkulus, which can be accessed through a particular "passwordless" digital identification system that we call Kalkulus-Identity.

Kalkulus dApps are 'blockchain enabled' websites, where the KLKS-dAPI is what allow connection of those dApps to the blockchain. The easiest way to understand this concept is to understand how traditional websites operate.

The traditional web application uses HTML, CSS and Javascript to render a page. The application also grabs details from a database utilizing an API. When you go onto Facebook, the page will call an API to grab your personal data and display them on the page.

**Traditional websites:** Front End → API → Database

Kalkulus dApps are similar to a conventional web application. The front-end uses exactly the same technology to render the page. The main crucial difference is that instead of an API connecting to a database, you have a KLKS-dAPI connecting to Kalkulus Blockchain.

**dApp enabled website:** Front End → KLKS-dAPI → Kalkulus Blockchain

As opposed to traditional, centralized, applications, where the back-end code is running on centralized servers, dApps have their back-end code running on a decentralized P2P network, that reside in special nodes that we called DIN (from acronym Dapps Infrastructure Network) that can be deployed by individuals or organisations. We suggest developers to run their own DIN nodes in order to decentralize the network and improve security.

Decentralized applications consist of the whole package, from back-end to front-end. Klks dAPI is only one part of the dApp:

Front-end (what you can see), and Back-end (the logic in the background).

KLKS-dAPI, on the other hand, consists only of the back-end, and often only a small part of the whole KLKS dApp. That means that if you want to create a decentralized application based on KLKS-dAPI system, you can combine several KLKS-dAPI and rely on 3rd party systems for the front-end.

KLKS-dAPI are RESTful so you can expect the logic of a common REST API. Representational State Transfer (REST) is a software architectural style that defines a set of constraints to be used for creating web services. By providing a simple REST API to read, write and search for entries in the Kalkulus blockchain, the developer has everything needed to make his own dApp.

In particular, the write operation is entrusted to the OP\_Return, a script opcode used to mark a transaction. Each data is assigned a UUID, a REF ID and is divided into encrypted blocks, the Blockchain stores them autonomously through the HTTPS POST operations in random positions selected and known only by the Network.

Kalkulus team will provide guides in order to deploy easily your own DIN Nodes, even in a local machine, ensuring that your data never leave it. This means that only you can access your data, unless, of course, you decide to make them public.

A KLKS public address could be generate by your own wallet or through a Special Javascript Library, also offline. The initialization of the dAPI key and relative dAPI secret happens by importing the public address in a DIN Node in Watch-Only mode. In this way, the private key of the address is never exposed, ensuring a very high level of security and protection.

Moreover, it is possible to obtain a progressive data management in such a way that the KLKS dAPI returns only the updated data parameters, i.e. those referring to the most recent blocks, while maintaining a permanent history that can always be accessed to check the changes made.

A wide technical documentation of all the processes listed so far is provided, which makes it easy to create decentralized applications over Kalkulus Blockchain.

KLKS dApps can't be shut down because there is no server to take down. All data in a dApp are decentralized across all of its Data Infrastructure Network nodes. Each DIN node is independent; if one fails, the others DIN nodes are still able to run on the network. There are a number of decentralized database systems on which to build dApps that can support this feature, such as IPFS (Interplanetary File System).

The limit to face is that for every single piece of data to be included in the blockchain, the available size is limited to 1 MB, not allowing the storage of file with bigger size. KLKS dApp architecture implements IPFS technology with the purpose of pass this barrier of 1MB file size: IPFS in fact allows storing and sharing hypermedia in a distributed file system retained by the entire The Hub VPS network.

IPFS layer offers very interesting properties such as:

- App or websites that are completely distributed, that have no origin server, that can run entirely on client side browsers.
- Distributed high volume of data with high efficiency.
- Historic versioning for mirroring data.
- Deduplication, high performance and clustered persistence.
- Secure P2P content delivery.
- Fast performance and decentralized archiving.
- Resilient access to data independent of low latency or connectivity to the backbone.

There is a symbiotic relationship between IPFS Technology and the Kalkulus Blockchain. Blockchain technology is not suitable for storing large amounts of data, IPFS instead can be used by blockchain applications that need a publicly accessible database. Meanwhile, the immutability provided by the stakers and the transparency of the blockchain make it the perfect place for the timestamp of the contents and public verification.

### Kalkulus dAppStore & KLKS-ID

Kalkulus dAppStore will be the official platform which lists all popular dApps build over Kalkulus blockchain. User can access to dAppStore thanks to a decentralized system of digital identity that have the name of KLKS-ID.

KLKS-ID is an official Kalkulus dApp that enable users to create an account through a registration process on the KLKS Blockchain providing an email address and username (pseudonym).

KLKS-ID application will encrypt your email address and assigns to you a specific KLKS address with relative private key, and a unique public dAPI Key with relative Secret Key. The only data that remains public and visible in clear will remain the chosen username.

This system can be used in several application fields, but mainly will allow the users to use most of the applications on the Kalkulus dAppStore making possible various operations with some of them, such as: sending payments by entering a user name (instead of the public address) and participating in specific initiatives that require voting (Governance).

KLKS-PoE (Proof-of-Existence) is a notary decentralized application that give the chance to immutably record any document into the public distributed ledger of Kalkulus blockchain, removing all needs to trust any central authority that certify existence and ownership iof files and documents.

Simply using a process of registering and timestamping, KLKS-PoE enables anyone to anonymously and securely store a document through IPFS (via KLKS-Storage architecture) with a online distributed proof-of-existence for any kind of document (text, audio files,video, images, pdf and more).

Some of the common uses for KLKS-PoE are:

- Demonstrating data ownership.
- Digital Sign Agreement.
- Document time stamping.
- Checking for document integrity.

Privacy is guaranteed thanks to the encryption of files (when requested), but the key advantage is getting a decentralized proof which can't be erased or modified by anyone. Your documents, with the irrefutable proof of his existence, are permanently validated and written over the Kalkulus blockchain.

Musicians, digital art producers and other professions that provide for intellectual property, can prove that they created their work and are the legal owners of the property and relative rights. For example: before sharing ideas with third parties, artists and entrepreneurs can upload and timestamp the information that is about to be shared, and also timestamp the fact that the information is being shared, avoiding any unwanted use of those informations or helping parts resolve possible disputes.

There is an immense and unexplored potential for further applications, and many of these could be developed to be implemented with the revolutionary "Internet of Things".



KLKS-DFS (Distributed File Storage) is a decentralized file storage system that allow to users and online business actors to use an innovative cloud storage service for a very low cost.

In just a few years cloud computing became so useful and popular that the majority of all data became stored in just a few of the major cloud data-providers. This infrastructure is still largely invisible to the end-user, even though most websites today are hosted by these 3rd party providers.

One of the biggest actual problems on this sector has been the centralized structure, developed, owned and run largely by for-profit corporations. This architecture makes the web brittle, undermines privacy, allows the price of storage to remain artificially high, and creates bottlenecks that prevent innovative new uses of data.

Instead of relying on expensive businesses to store and transmit humanity's trove of knowledge, KLKS-DFS architecture distribute encrypted data across a vast network of peers who are paid to store each other's data.

KLKS-DFS works by sharing a file across the Kalkulus blockchain peer-to-peer network. Let's summarize the steps:

- The uploader encrypts the file, and retains the private key to unlock the encryption. Then the file is splitted into many smaller encrypted pieces, and each of these gets duplicated through all nodes to ensure redundancy. Finally, each file shard get sent to various individual nodes on the peer-to-peer network.
- Those nodes hosting the files only have a small shard of the file's contents, and it's encrypted. This means hosts can't gain information from the file. It also means that launching an attack against an hosting node would be pointless and will not result in any consequence for the availability of file.
- To recall a file, the original uploader uses his private key and ask the network to reconstruct the file. Once the nodes send back the various shards, the file gets rebuilt. Then the uploader uses the original encryption key to decrypt the file for use.

Distributing user data to a large array of storage computers who are not owned by a company can increase the exposure of the data. However, if valuable data are stored encrypted end-to-end, then attackers with access to the encrypted texts cannot learn what is stored inside of them. Only users that have access to the keys can recall content of encrypted files, and the failure of a single cloud provider cannot harm the resilience of the data.

KLKS-DFS combines the futures of IPFS and Blockchain Technology with an incentive mechanism to maximize storage efficiency, and it has improvements in other aspects:

- Slice storage based on progressive data management, while maintaining a permanent history that can always be accessed to check the changes made.
- Ensures high availability and storage efficiency: reduce duplicated files and can help users thanks to much faster data transmission.

## KLKS-KYC

With data driving the world today, digital identity is critical to most business and social transactions. Traditional identity systems continue to be highly vulnerable, with single points of failure, attracting continuous attempts to gain access to the complete repository of high value data.

KLKS-KYC dApp ensure:

- Powerful algorithms to validate an identity and its claims.
- Identities to have a permanent shelf life.
- Interoperability.
- Sharing of data only with the consent of the user.
- Organizations should be able to access only what is needed and not the complete information.
- Protection of user rights.

With the combination of the decentralized applications and a comprehensive system for verifying identity, is possible that a digital ID can be created for each online user to serve as digital watermark affixed to all transactions carried out by the user. There might be a possibility of ascertaining the truth of individual identity.

The identity system offered by Kalkulus will work in combine with other applications, taking advantage from the power of biometrics and blockchain to provide a global identity solution.

In conclusion, KLKS-KYC (Know Your Customer) may be the way forward for developing an identity management system that gives full control to users. KLKS-KYC will also allow us as users to determine the data we desire to share across different mediums while also protecting our identity from theft.

## KLKS-MSG

KLKS-MSG (Messenger) is a private instant communication dApp that work in combination with KLKS-ID and KLKS-STORAGE System. KLKS-MSG offers IPFS technology coupled with a peer-to-peer messaging service. It's capable of sending multimedia messages with the benefit of live encryption of all files.

Most messengers App, store your data in a centralized database. KLKS-MSG eliminates these risks by completely removing centralized servers.

Messages automatically could be erased, from both the sender and receiver's phones after 24 hours. Also, you can choose to have their messages deleted upon reading confirmation.

It includes an internal built-in payment system with QR code technology.

## The Hub Overview

**The Hub** is a proprietary set of web-tools dedicated to favour and increase the adoption of Kalkulus and other digital assets. It is an innovative product, useful, stable and reliable and that allows a great browsing experience.

Thanks to a technically advanced system of integrated functions, The Hub require minimum or almost null technical skills offering a wide range of solutions to stakers, masternodes holders or simple investors.

The Hub platform was launched in July 2018 and represented a turnaround for the project, because prominently provided to KLKS a true, real and tangible use case for the proprietary digital asset, also because was one of first platforms dedicated to automatic masternodes deployment.

The Hub embodies different functions, including a KLKS online wallet accessible also from mobile, but the main purpose is to offer an easy way to deploy masternodes of 30 and more digital assets with a simple and fast process, that doesn't require programming skills or advanced technical knowledge.

Through The Hub, all customers can rent dedicated VPS servers, deploy masternodes and benefit of other services subscriptions, and pay for all those services using KLKS. Recently we add other payment methods, starting to accept BTC plus other digital assets like Solaris, Bulwark, Deviant and Alqo. At date, Kalkulus the most used from all customers, giving to the coin a real use case, but for sure other digital assets will be added to the platform, including BNB, the proprietary token from Binance.

Alongside the well-known and most adopted function of masternodes deployment, The Hub have his most innovative and unique to date feature on the **Staking V-Box** (Staking Virtual-Box): a full node that allows users to lock their holdings in the process of staking without needs of any other physical device or client open on the computer 24/7, as required for taking part to staking.

Another innovative feature that we recently developed and implemented (but is still in beta for few users and available only for Kalkulus), is a new product: **COMA Nodes** (Clientless Onsite Masternode). This feature will be explained better in next paragraph.

The Hub also provide a series of additional advanced services like monitoring tool with statistics, charts, earnings history and forecast, graphically represented through an UI that will be continuously updated with new indicators and graphics. Thanks to the referral program, the platform provides also a unique way for all customers to earn a lifetime 10% of all daily fee paid by another signed up person through your referral link. All bonuses are automatically paid in Kalkulus equivalent.

Thanks to The Hub, Kalkulus project grows by strengthening its position in its market segment and acquiring greater visibility and notoriety.

## Staking V-Box

For his own nature, in order to mint new coins, the process of creation of new digital coins in a Proof-of-Stake blockchain require that the client is open, unlocked and connected to the network. According to this condition the amount of new coins minted depends not only from the available holdings that the validator put in stake, but mainly from the time that the client is open. For this reason, to optimize the staking process, and maximise gains and passive incomes from staking, the client should be open 24/7.

First in his genre, the service of Staking V-Box was created with the main purpose of bypass and eliminate these technical requirements. Not everybody can have a dedicated computer for running a process of staking 24 hours per day 7 days a week. If we think to a laptop running 24/7, when powered for long times, the device could also experience physical damages, hard drives or power failure and other obstacles that could break the process. The Staking V-Box was developed to solve all those issues.

What makes the Staking V-Box different from other online staking services is the primary focus on customer's funds security. Differently from staking pools, where users have to send their holdings to the wallet of owners of the staking pool, losing access to their funds, Staking V-Box is a dedicated client with all main functions of desktop client. Users can manage autonomously a client developed with an enhanced level of security and innovative features such personal passphrase encryption, private key export and wallet dump option protected with 2FA, fully managed through The Hub GUI.

When the customer launch a new Staking V-Box creation instance, the system deploy a new VPS running a Kalkulus client, that is unlocked for staking and connected to the blockchain 24/7. As soon as the process of deployment is completed, users are immediately asked to encrypt the client with a password that only they know.

This password, exactly as is in the desktop client, is required to perform any sensible operation on clients (send funds, withdraw, import/export private key, and other tasks).

Wallet encryption ensure an additional level of security guaranteeing that nobody (not even the team that manage the platform) can require private keys and manage, move or touch users staking funds, because all sensible operations cannot be completed without the encryption password that only users know.

Regarding private keys, users have the option to import existing private keys or dump their private keys for each address generated inside the Staking V-Box where they are running the staking process or simply deposited their holdings. This measure increase the level of security for users because, also in case of server crash or hack, they can anytime recovery their funds simply importing in desktop client the previously backedup private keys.

To require private keys they are firstly asked with wallet password and 2FA: only after inserting the correct encryption password and own 2FA, the system reveal their private keys.

Thanks to wallet password protection, not even us can have access to funds or private keys of users, making impossible for anyone to touch funds inside Staking V-Box (for this reason we require to users to CAREFULLY save client password: in case of loss, there's absolutely no way to recover funds from an encrypted wallet, even for the development team).

Staking V-Box also provide the option to automatically backup the most important file "wallet.dat" where all addresses, private keys and users funds are digitally stored.

That way users can anytime import their "wallet.dat" easily on desktop client regaining accessing to their funds when needed, or simply checking their balance from desktop client while the Staking V-Box is operating on the server (this require that the client run with options "staking=0" in the klks.conf file.

Users can access on The Hub and manage Staking V-Box also from mobile phone and tablets and can easily use the QR code payment system in order to take advantage from a multiple full node mobile wallet.

The next versions of Staking V-Box will allow to customers to increase the number of supported blockchains from actual one to three different coins that stake at same time, ensuring a full, complete and optimized staking experience, that maximise their passive income in total security without any needs of physical devices running 24/7.

## Easy Masternode Deployment

A simple and intuitive user-friendly web tool that make the masternode deployment process easy and accessible for everyone, without any tech skill and in total security. The whole process of masternodes deployment is fully automated and hosted in secure servers.

Users are only asked to provide some basic data, needed to deploy the masternode: genkey, transaction-id and tx-out.

When all fields are compiled, the user is asked if he want to deploy the masternode in a new server or together with others already deployed masternodes.

This innovative environment, called “multi-support”, is available for the majority of coins listed on The Hub and allow to users to rent a dedicated VPS and host up to 3 different nodes from different blockchains on the same server.

During the deployment process, required collateral will never be sent outside of user's desktop clients, and the rewards are addressed directly to the same user's desktop client that act as masternode controller.

## COMA Nodes

COMA Node (Clientless Onsite Masternodes) is a cloud full node hosting system, hybrid with Staking V-Box, that allow to users to go through the process of masternode deployment in a clientless way, directly from inside The Hub.

Thanks to this innovative feature, users can fully manage their rented servers, experiencing the full power of masternodes and staking at same time, maximizing all benefits of passive income.

With this deployment system we was able to break a technical barrier: the needs of desktop wallet that not only hold your masternode collateral, but provide all data required during the process of masternode deployment (genkey, transaction-id and tx-out).

Through COMA Nodes, will be possible to setup a working full masternode in a clientless way, via browser, also directly through mobile phone and tablet, in less than 5 minutes, providing users ownership of private keys related to masternode collateral.

This service, like others on the platform, doesn't require any related technical skills, however users are required to know and properly handle the process of creation of a masternode, in order to fully understand how the whole process work.

This because the masternode collateral reside in the server (instead than the traditional system that hold the collateral on desktop client).

Security of collateral, as already happen in Staking V-Box, is protected by features such personal passphrase encryption, private key export and wallet dump option, that guarantee to users access to collateral at any time, for an high level of security. A last level of protection is provided by 2FA.

Explaining better how COMA Nodes works, is important to clarify that this system share some features with Staking V-Box (where the coins reside), but is empowered with masternodes capabilities.

Users that have previously deposited enough coins inside a Staking V-Box, will have the option to use a part of those coins as locked collateral for a masternode (required amount is 20000 KLKS), leaving the rest of coins as staking amount.

When users start the process of deployment of a COMA Node, a totally automated routine start, taking care of all single actions required for creating a masternode from scratch: the system automatically send the required amount for collateral to a new generated masternode address, then automatically create masternode genkey and grab all transaction-id and tx-out needed data to perform operations for masternode deployment.

The system also write all the configurations files with all requested data that are needed for the correct start of the masternode.

When deployment process is completed and the server is synced to the network, the masternode start to act as validator exactly like all others masternodes on the network, and when rewards starts to flow into The Hub masternode address of the user, they show on his address balance.

At the same time, the COMA Node is also already configured with Staking V-Box capabilities, in order that all masternode rewards are automatically collected and sent to the staking address without any action required by users, maximizing results of passive income, without any needs of additional software, in total security, and also from mobile.

Through the COMA Nodes exciting feature, not only we solve the problem of needing a desktop wallet from where to control masternodes, but we will give to our customers the amazing possibility to deploy masternodes through their mobile phones from any place in the world. They just need the requested amount of coins, that in future can be bought directly from inside The Hub.

COMA Nodes feature will be available upon request also for other assets already listed on The Hub.



## The Hub 2.0

Future developments on The Hub are focused to combine the IPFS based KLKS–Storage with the large amount of VPS deployed by users inside the platform. We are at work and research in order to share the revenue of Kalkulus file storage service with all the users that want to participate with this program.

This kind of approach permit to build a large infrastructure for future dApps with big hard disk space for IPFS and hypermedia.

Other developments planned:

- Payment method options expansion.
- Telegram and Discord The Hub Bot.
- KLKS–ID dApp integration.
- Internal buy future with exchange–bot technology and Block DX Atomic Swap by Blocknet.

## Cryptocurrencies Payment Gateway

**KLKS-PAY** is a payment gateway that provides secure cryptocurrency wallet and payment solutions for businesses and private deals, designed to be used in everyday life, providing convenient QR Code, NFC or URL payment options.

The payment gateway can have several applications fields:

### **On websites**

Accept cryptocurrencies payments and donations from your online customers. KLKS-PAY provides payments buttons, a hosted checkout, and embeddable invoices for your website. KLKS-PAY also works with plugins and integration tools for e-commerce or donations from patron.

### **By email**

Send invoices to vendors as quickly and easily as sending an email. You can be up and running in no time with KLKS-PAY email billing tool. No direct integration required.

### **In person**

Accept blockchain payments on your smartphone or tablet at your retail store or restaurant with the KLKS-PAY progressive app, without needing dedicated point-of-sale hardware devices.

## Appendix

Please be aware that this Whitepaper attempt to explain our plans and goals. We reserve the right to change anything in order to have the flexibility to adjust with changing market conditions. Surely we will add new ideas in the future that help us to grow faster. Our commitment is to work with diligence and integrity, inspiring others in the scene to do the same, in order to exceed the expectations of our community.

Thank you for your support!

## References

**Bitcoin Whitepaper:** <https://bitcoin.org/bitcoin.pdf>

**Dash Whitepaper:** <https://github.com/dashpay/dash/wiki/Whitepaper>

**Quark vs. Bitcoin:** <http://www.quarkcoins.com/bitcoin-vs-quarkcoin.html>

**PIVX Whitepaper:** <https://pivx.org/what-is-pivx/white-papers>

**Ethereum Proof of Stake FAQ:**

<https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ>

**InstantSend, Kiraly, B.:**

<https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend>

## List of Sources

**Kalkulus Website:** <https://kalkul.us>

**Kalkulus Block Explorer:** <https://chainz.cryptoid.info/klks/>

**Kalkulus Official Github:** <https://github.com/kalkulusteam>

**The Hub:** <https://hub.kalkul.us>

**KLKS-dAPI:** <https://dapi.kalkul.us>

**KLKS-PoE:** <https://proof.kalkul.us>

**Kalkulus Discord Channel:** <https://discord.io/kalkulus>

**Kalkulus Twitter Channel:** [https://twitter.com/kalkulus\\_team](https://twitter.com/kalkulus_team)