White Paper

CRYP2NOVA

Executive Summary

What is Cellframe?

Cellframe is a service oriented blockchain network. It is built very close to the hardware, to provide efficiency of use on any machine — from supercomputer to smart fridge. Post-quantum encryption is standard in Cellframe, providing the highest level of security. It is important to note that we did not invent a new, unproven technology; we are building the blockchain the way it must be done to be worthy of being called infrastructure.

How can Cellframe be used?

Cellframe's architecture is a structure designed with integrated dual-layer sharding. The first layer (heterogeneous layer) can launch customizable subchains and tokens. On the second layer (homogeneous layer), subchains are organized into Cells. These interoperability features allow us to build

Archived copy · cryp2nova.com

an ecosystem of services where every app (or dApp) is able to exchange information with another app in a P2P manner.

> Our mission is to create a safe, decentralized environment sustaining the freedom of the Internet while making people more relaxed and confident in their everyday use of it.

Cellframe is both a public and enterprise solution at the same time.

Performance and scalability of Cellframe meet not only demand from the public blockchain market, but also from enterprise, and can be used widely for enterprise solutions. Here are a couple examples of use:

1. Service-oriented architecture makes it easier to build 2nd-level protocols with dedicated services. Cellframe's built-in payment system and private shards (networks) give builders the ability to focus on developing the service itself. Conditional transactions, on which Cellframe's app architecture is based, can effectively replace 90% of typical smart contract operations, (less gas consumption, higher security, simpler development, lower development risks and less time spent);
2. Cellframe offers an enterprise blockchain-in-a-box solution. In addition, it is one of the most advanced solutions to secure existing public and private blockchains from terminal attacks;
3. Due to its architecture, Cellframe is the only system that can protect a blockchain from terminal attacks (including quantum) without user migration or implementation of third-party code..

Abstract

In this White Paper, Cellframe documents our vision of a blockchain platform with fundamentally broad functionality, capable of building and delivering a variety of high-demand, high-load, high-security services. Cellframe is the zero-level protocol for building the services underpinning emergent Web 3.0 business models, adding not only the performance and integration required, but also an integral foundation of post-quantum security. The key innovations are decentralized services, new fine sharding implementation (which offers performance and resilience) combined with a low-level architecture (performance and security) and a high level of modifiability (flexibility).

Challenges

History teaches that no one can predict the future. We are offered predictions by smart people in the press and in books, and know invariably that some will come true, and others will not. While it may be difficult to find a single reliable truthsayer, we can note that certain macro phenomena about guessing the future seem reliable: people tend to overestimate the rate of change in the near future and underestimate it in the distant future. Taking this into account, let us carefully separate the facts from opinions and build a suitable, in our opinion, narrative for the further development of our technology.

Archived copy · cryp2nova.com

1. **Fact #1:** The rate of generating new information is growing. What does this mean for creating the foundational technology for future industry? Maybe it's time to build in such a way as to track the dynamics of growth? In addition to the need to deliver on performance and efficiency, a basic infrastructure protocol also requires extensibility and flexibility. We know that there will be an insatiable appetite for performance, but we invariably cannot predict future needs and inventions, and must safely support all possible improvements and modifications that will undoubtedly appear.
2. **Fact #2:** The technological limit of the size of the transistor of modern CPUs is very close. According to various estimates, in the period from 2025-2030 we will not be able to reduce the size of the silicon chip, as it will be limited by the size of the atom. Therefore, an infrastructure protocol that wants to be future-proof will be efficient and scalable across a network. It is about maximizing usage of available computing resources and interconnecting these resources in effective networks. Understandably, we maximize performance by building code as close to hardware as feasible using plain C and low-level hardware optimization.
3. **Fact #3:** Quantum computing has been getting increasing worldwide attention. Certainly the premiere cryptographers are riveted on quantum computing progress. The Post-Quantum Cryptography sector is now engaged at NIST (National Institute of Standards and Technology), sifting through dozens of algorithms and protocols, in search of an industry standard. We expect this standard will take more than the coming year or two to resolve. While a functional quantum computer is still somewhat indefinite in its delivery date, we are making plans now. PQC is also developing its own specific needs and quirks. Any future-proof architecture must work equally well with both classical cryptography and post-quantum cryptography.

Vision (design goals)

Cellframe was born as a response to the challenges we have described, leveraging design elements we believe will squarely address our coming future. It offers:

1. Low-level architecture. In order to maximize the efficiency of the protocol, it must be built in such a language so that it can speak with the kernels of any operating system without using kernels itself. And it must be efficient in working with everything from mainframes to smart refrigerators. This is why Cellframe is built entirely on C with no third-party code.
2. Zero-level protocol. Over the past years, we have seen the emergence of dozens of different protocols, each of which wanted to improve or change something. This activity signals that people want to apply blockchain technology in various fields. However, until now they did not have a universal platform that would offer effective tools for solving their problems. From our point of view, it looks like an attempt to invent a steam engine before the invention of the wheel. This is how the Cellframe Tissue concept was born, which will be discussed later.

Archived copy · cryp2nova.com

3. The inability to predict all the tasks that will be solved using Cellframe. In other words, it must be possible to modify the protocol to solve a particular problem without compromising security and performance. This means it should already be flexible (or variable) by design.
4. Decentralized services will eventually replace current web infrastructure, removing multiple points of failure.

Web infrastructure is a complex of interconnected service structures or objects that provide the basis for the functioning of the system. Our protocol was originally conceived as an infrastructure (wiki), which means it was created for high loads and a high level of interactivity. We are creating a flexible and efficient system, each element of which could be used to solve different problems with different characteristics. If the load on a specific Cell increases to such a limit that it interferes with efficient functioning, the owner of the Cell can create any number of Cells in support of the first one. Different Cells in the same system can perform different functions using smart contracts. As a result, the system of different Cells forms Cellframe Tissue, the second most important “organ” of the system. The first is ZeroChain. The architecture of the resulting system allows us to reach a gigantic level of scalability and virtually infinite bandwidth while creating the maximum level of security.

The motivation behind the proposed system is to create a system which can be used for both independent, decentralized applications as well as enterprise solutions. Truly decentralized services and applications can exchange microtransactions without overloading the system. Cellframe’s built-in P2P payment system works more efficiently without the need for smart contracts, making it cheaper and more secure. In addition to unprecedented vertical and horizontal performance, variability, and a developer-friendly approach, this will be achieved by implementing tools that reduce the cost of mistakes, or arbitrary acts. From the start the system will be launched with a combination of Proof-of-Genesis (<1% of total blockchain consensus) and Proof-of-Stake (up to 99%) consensus mechanisms.

The network itself consists of dependent peer cells. The network can launch a chain with its own attributes, own token, and own type of consensus without severing the unbreakable bond with ZeroChain. This is why these Cells are called syngeneic — they are similar to stem cells (which easily can convert to any specific cell type in the human body). This metaphoric comparison means that each shard can be launched with any possible attributes and connected to any other shard. Administrative information about Cells, tokens and its initial ledger’s locations are stored on ZeroChain, which has a PoG mechanism. This decision has two other consequences:

1. Pseudo-centralization of the system is leveled down by the opportunity to create pseudo-dependent Cells, which can’t be affected by arbitrary acts or deleted by root nodes. This is because all of the inter-Cell communications are direct, i.e., peer-to-peer;
2. In the future, we plan to implement a type of consensus that will be able to fully govern the decentralized system.

Archived copy · cryp2nova.com

Using this mechanism, Cells become homogeneous and have a high level of inter-cell communications. Cellframe hierarchy also presumes a fractal-like model: each Cell has an initial Base Chain inside. This Base Chain is similar to the ZeroChain of the whole protocol, but for one specific Cell.
Summarizing all of the above: Cellframe is not a blockchain protocol. Rather, we can call it an infrastructure layer for building a blockchain ecosystem. All existing blockchain solutions can be transferred to Cellframe and get previously unattainable levels of performance and security.
There is another question that we would like to discuss in this chapter. A lot of bright minds have been working in the blockchain sphere in recent years. Why, then, do we think that there is a room for Cellframe on the market? Does this mean that no one in the whole sector is moving in a similar direction? What caused the current situation?
The development of any technology passes through stages or generations. When some generations show their inaptitude, we learn and create new, better ones. Blockchain technology today has several fundamental problems that we described above. The ways to solve them can be divided into two groups:

- Tactical problem solving is improvement of specific components of conventional systems. This is the way in which most projects from the blockchain sector are moving, since it is less labor-intensive. They work with a system that has already proven its effectiveness at a certain level, which they consider sufficient;
- Strategic problem solving is an attempt to create a new technological platform (system), which is fundamentally different from existing solutions. Fewer projects are moving in this direction, since it takes time, is labor-intensive, and requires a deep understanding of computer networking devices and cryptography. The labor-intensive aspect of this is reflected in the fact that the first private version of Cellframe’s dev net was launched in July 2018, about a year after the start of the project.

Highlights

Variability

Usually, blockchain developers try to save every byte of information onchain because a blockchain size is often not a priority because the price of disk space keeps decreasing. Because of Cellframe’s flexible structure, we’re not limited by this fact, so it is possible to add a few more bytefields in the wallet’s address, event headers, signature and public key structure, network protocols and other shared structures that need to be recognized by software for processing.
A few added bytefields give us the ability to create more transactions types, signatures, events, wallets, datums and other data structures on the fly without total code reconstruction, blockchain structure change, issuing new wallet types, etc. This variability allows us to produce backward compatibility between different versions and prevents version incompatibility.

Security

Archived copy · cryp2nova.com

Security in the Cellframe is achieved mainly due to the variability features. It does not rely on any particular signature algorithm nor – due to the multi-client use – on a single consensus. Safety standards become more complex over time. If you use one specific algorithm, then the stability of this algorithm will determine the stability of the entire system in the context of encryption hacking. Since we are working with the concepts of a quantum computer and quantum encryption, it is necessary to create a system that will not be dependent on this factor. In other words, you need an ability to safely change the type of encryption to increase security. The same applies to the type of consensus mechanism – our task is to create a system where you can quickly change the consensus algorithm either in the current cell or with the creation of a new one.
In case of any problems, we will be able to quickly locate them and prevent their distribution throughout the system by isolating a shard or using arbitrary acts as a security mechanism in the first several months after launching mainnet. An Arbitrary Act is a mechanism that can mark a transaction as invalid and roll it back. This feature is planned as a temporary measure for the first year until the system is stable enough. Also, there is the so-called Rat Announcement that could be issued by any Node, then verified with the Root Node and placed in a special Support Chain where Arbitrary Acts, Rat Announcement and System Warnings prevent both of possible attacks or reduce the damage from them. This is how the ZeroChain announces that it has found a malicious participant.
The entire architecture of the Cellframe system has almost no third-party code, which also increases the overall security level. This means that all the code has already been written by our engineers without the use of third-party modules. There are no known vulnerabilities or hacking methods. Supersingular curves and lattice permutations are used as the basis. Implementations of such algorithms for public key communications are already available on the network, as well as some variant signatures based on supersingular curves.

Scalability and Performance

Cellframe node structure and scalability is robust and limited only by hardware power. Since we use low-level optimization and organization from scratch, we are able to make a high-throughput system with exceptionally good parallelization. The curve of productivity growth vs. hardware power is almost linear. Node capability is planned to handle up to ten signatures without any lag, and can even handle up to 100-gigabit traffic if it is equipped with the appropriate number of CPU, RAM and well-established traffic distribution between them.
The event-driven architecture is what makes all these things possible. There is an I/O grouping method in which all the same operations are performed in a row in a non-blocking mode. This allows us to optimize them at the level of OS's and hardware, and to additionally optimize I/O by grouping it in one place. In turn, this allows using Zero Copy technologies (or similar) by sharply reducing the load on so-called “context switching”. It is impossible to work at high speeds without it.
The Cellframe network’s scalability largely corresponds to the scalability of any peer-to-peer system, but with an added nuance. Given the fact that the uplink node is identified by the principle of the shortest network path, our network should function faster and have a quicker response time to external requests. Data is transferred with the shortest possible latency. Latency in the multichain system

Archived copy · cryp2nova.com

leads to an increase in the number of chains and extension of rounds, plus its influence on the time needed to spread changes in the network. We cut the latencies and increase the speed.
Supersingular curves and lattice permutations are used as the basis for our cryptography. Implementations of such algorithms for public key communications are already available on the network, as well as some variant signatures based on supersingular curves. We plan to “invert” and modify it into algorithms for forming digital signatures, and some of these are already present on Github.

dApps: how to make them truly decentralized?

Information today transfers almost instantly. The number of possible social connections is limited only by access to the Internet and a computer. One of the crucial issues nowadays is trust. How can we trust and verify those we communicate or work with? During the last century, humanity has been focused on the complexity of verifications. Governments started using passports and identity databases to track almost every move of their citizens, in addition to visa systems with multiple levels of control. Compliance departments now are very significant divisions in almost all major banks.
At the end of 2008, the Bitcoin network white paper was released. It proposed a pseudo-anonymous peer-to-peer trustless network. It doesn’t require trust in ordinary meaning, as the network architecture itself provides an unconditional level of trust between its members. Since then, the blockchain industry has come a long way. We saw the hype caused by the first appearance of smart contracts, which was followed by the ICO bubble, the first serious governmental implementations of blockchain technology, along with ridiculous things like tokens for memes or garbage mining. Today, almost all Fortune 500 companies list established blockchain departments. Many world celebrities managed to either make a lot of money or receive a fine from regulators for the promotion of crypto scams.
The market of dApps has been developing rapidly in recent years. In just one year the dApps industry demonstrated greater traction than the entire blockchain industry in 2017–2018. In the Defi sector, represented mainly by Compound, MakerDAO, Synthetix, and Uniswap reached $1bln worth of frozen assets in their contracts, according to defipulse.com.
Yet, very few people outside the developer community understand how smart contracts really work and what their technical limitations are. The popular opinion is that “smart contract” = “secure, trustless system”. But this is not exactly true. And we are not only talking about Ethereum scalability issues here. When we speak about limitations, we mean functions that cannot be performed by existing contracts. We'll discuss this further, as well as some security issues of which many ordinary users are unaware.

Problems of current dApps architecture

Despite the decentralization of the Ethereum network, we can (rather conditionally) say that the smart contract is de facto “owned” by the private owner(s). This person(s) can become a tasty morsel for hackers if there are significant holdings of digital assets in the contract. Thus, there are one or more critical points of vulnerability in the system. A properly executed attack can lead to loss of users’

Archived copy · cryp2nova.com

funds.
If, instead,the funds could be distributed to an unlimited number of private key holders (as is the case of the Cellframe blockchain services), even if someone could steal a set of private keys, the money could be stolen only from this person. Other participants and users of the service would not be affected.
The second drawback of the existing contract architecture is the limitations on the types of business logic that can be implemented into a contract. Taking into account limitations of the EVM (in its current configuration), it's impossible to interact with the hardware resources of the computer, which cuts off the possibility of implementing a wide range of dApps.
The drawbacks described above limit builders' ability to create dApps to the level of a smart decentralized "calculator". Of course, a simple form of business logic such as "simultaneous transfer of assets upon condition" or "if the token is frozen in the ERC20 contract, then..." is relevant and sufficient to create a lot of useful decentralized services, which is proved by the success of the Defi sector. But, today the market for such dApps is still small if we are talking about real numbers, outside of a few crypto enthusiasts. At the same time, there are a vast number of services where decentralization would affect the lives of billions in a positive way. We can assume that anyone reading this article uses these services every day: DNS, cloud storage, VPN, CDN, and many others. Of course, there are a number of projects that are creating decentralized analogs of file storage (Filecoin, DADI) or VPN (Sentinel, Orchid, Lethean). However, none of those initiatives so far has turned into a project on a mass scale in terms of user base or any other metric. In essence, projects either have not reached the mainnet stage, or their audience is limited to a couple of dozen crypto enthusiasts.
We suppose that there are several reasons for this, including the imperfection of the current blockchain architecture. It is not anyone's fault – these blockchain platforms were not developed for this purpose. As a result, it is necessary to build a lot of things additionally. In this regard, each project is trying to solve the particular problem of building a blockchain service (and very often from scratch), which is completely ineffective. This approach resembles reinventing a web server, rather than taking the well-known Nginx. We think that the solution to this problem can become a special blockchain framework that can be customized for the specific task of creating a particular blockchain service. First of all, it will reduce the time of development and narrow the scope of work – as CMS did a decade ago for building a website.

Cellframe: service-oriented blockchain platform

We decided to close this gap with Cellframe SDK, to allow anyone to create decentralized Internet services quickly and easily.
As mentioned earlier, in current solutions (like Ethereum, Tezos, NEO, etc.) smart contracts can't interact with operating system resources. In contrast to other platforms, in developing Cellframe we aimed to create a framework that would allow building types of business logic centered around the usage of computer resources, such as computing power, Internet connectivity, and disk space. Also, we kept in mind the decentralization of the ownership and protection of end-users.
As we mentioned before, the classic smart contract has an address from which it was deployed to the

Archived copy · cryp2nova.com

network, while the Cellframe-based blockchain service lives inside the system and does not have an owner address. Yes, the Compound contract, which stores $5B worth of crypto, has a specific owner. What if it didn’t? We think that this can reduce the risk of fraudulent activities or illegal uses of private keys (note, that even if you have an institutional-grade private key management system, it ultimately has a chance to be stolen). We think that cash flows generated by the service have to be distributed in a reliable way among the service providers without having to pass through the owner of the smart contract. We propose to define such kinds of decentralized applications with the term “t-dApps” (true decentralized applications).

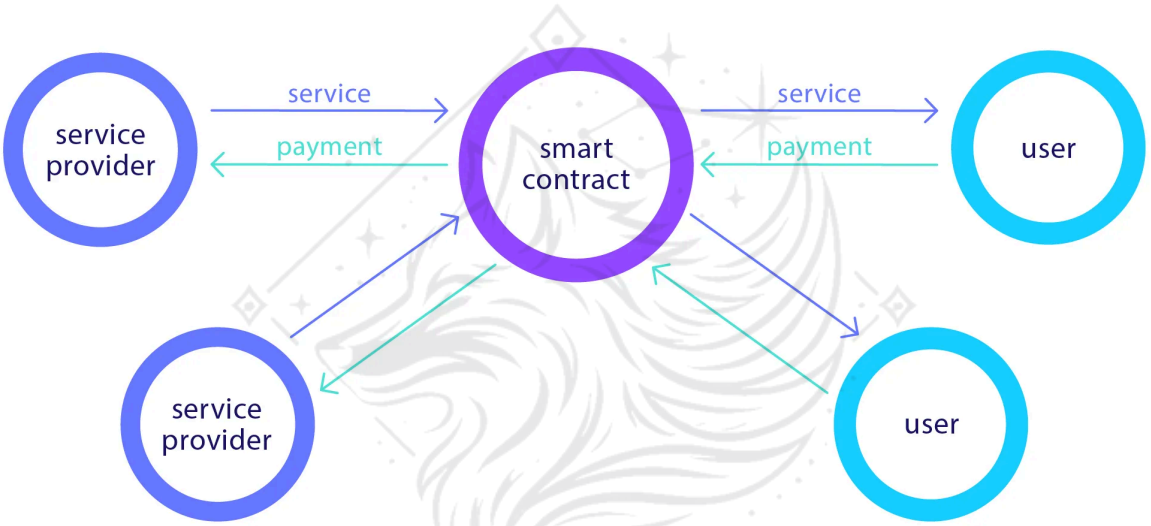


CRYP2NOVA

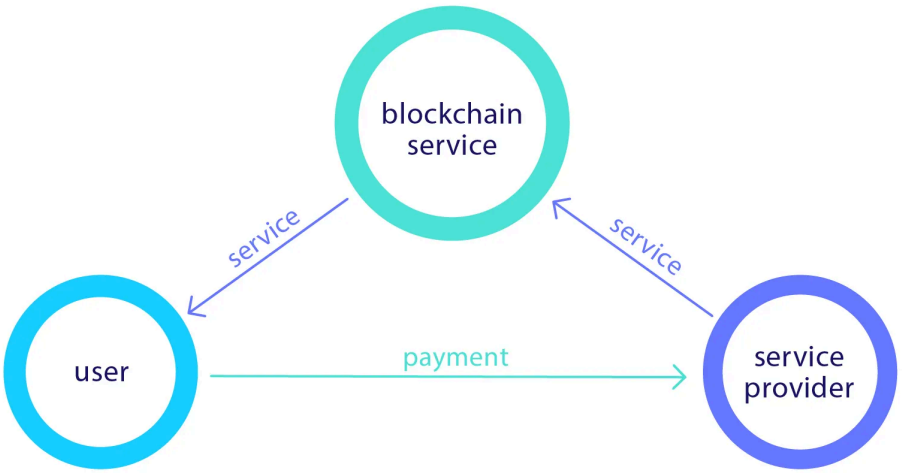
Archived copy · cryp2nova.com

Archived copy · cryp2nova.com





CRYP2NOVA



Archived copy · cryp2nova.com

At the same time, the process of developing blockchain services should be no different from creating web scripts or other system services. Such an approach will make development easier and cheaper, as teams won't need to hire specialized blockchain programmers, who are much more expensive than developers from the "traditional" areas.

Yet, these two principal approaches to building dApps have their own areas of efficient practical application. There are situations when a blockchain service cannot replace a smart contract for fundamental reasons. For example, the main case is follows: you need to create a dApp, the business logic of which doesn't rely on installation of a service node and maintaining them online. Also, we can highlight an opposite situation where a blockchain service will be preferable to a smart contract. Here we are talking about applications where running a certain number of physical nodes and maintaining them is a crucial point of the service model, and you can attract enough users who want to provide the service (by launching the node) as well.

Cellframe is a platform for creating blockchain services in which the problem of scalability is solved at the outset. To achieve high scalability, we use sharding, but not in an ordinary way. In Cellframe, we eliminated the bandwidth bottleneck – the intermediate hub, which is commonly used in some blockchain platforms (for example, Polkadot) for the exchange of information between chains. Cellframe shards can interact autonomously in P2P mode, which ultimately increases the performance of the entire system. Talking about security of the system, we took care of how Cellframe will work "tomorrow", in the era of quantum computers. It is the reason why we protected the system with variable quantum-resistant encryption.

Our vision is that decentralized Internet services (blockchain services) would become one of most important components of Web3.0 architecture, similarly to centralized services in the era of Web2.0. Of course, we have no doubt that decentralization of value transfer (bitcoin, stablecoins), as well as simple fintech applications (Defi), is a significant contribution to building the Internet of the future. However, as long as the base Internet layer is centralized, and can thus be completely censored, all this will have a lack of integrity. How valuable is the opportunity to send bitcoins or tokens if your connection can be censored? We strongly believe that to build effective Web3.0 it is necessary to solve the task of creating infrastructure modules that are safe and do not have a single point of failure.

As closing notes, we want to point out that substance, flexibility, and freedom are the values that Cellframe is based on. We (and millions of people with us) are convinced that the Internet needs change. There is no doubt that centralization creates a dangerous fragility. What is the Internet worth when a single decision made by politicians or a corporation can threaten access to information and communication opportunities for millions of people?

Cellframe Core

The Core code is based on entirely original C code with its object-oriented programming. All other elements of Cellframe code are also original: the HTTP protocol implementation, key exchange, streaming and multiplexing, as well as low-level services like VPN, CDN and edge computing. We stick to this approach to secure against ready-made hacking tools and to increase the network's event handling speed.

Archived copy · cryp2nova.com

Cellframe’s low-level optimization and event-driven internal structure allows it to handle previously unreachable levels of performance. We reduce the number of queries to system functions and their associated context switches. This is how we avoid data processing ceilings, which can appear when using large amounts of data at high speeds, causing these switches to grow exponentially.

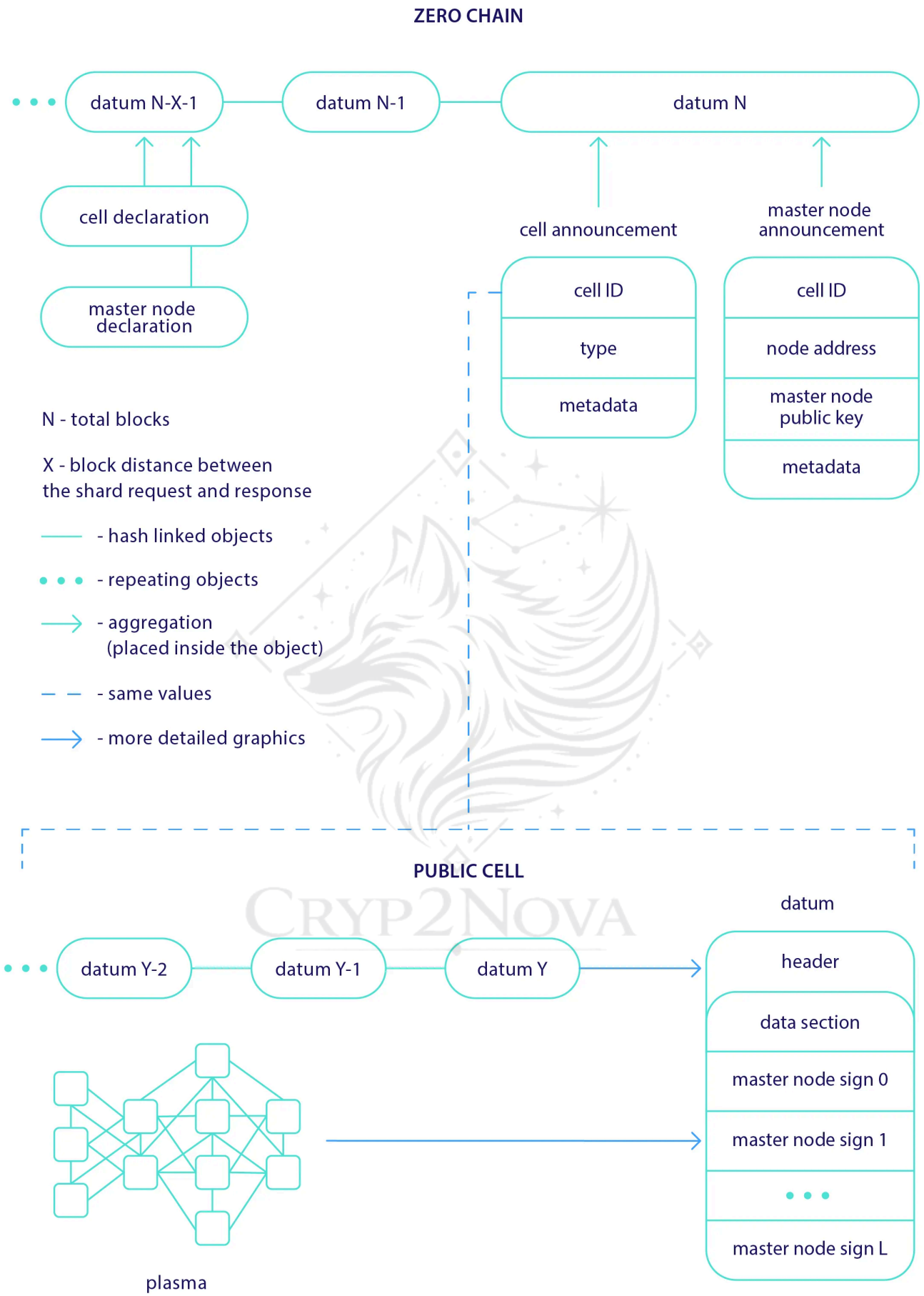
Blockchain Structure

The main idea of Cellframe’s architecture is support for multiple subchains, which contain Plasma (any blockchain element) inside of syngeneic Cells (shards). ZeroChain is a single line of plasmas that work across all the cells and carry inter-cell communications.

CRYP2NOVA

Archived copy · cryp2nova.com

Archived copy · cryp2nova.com



Archived copy · cryp2nova.com

Node

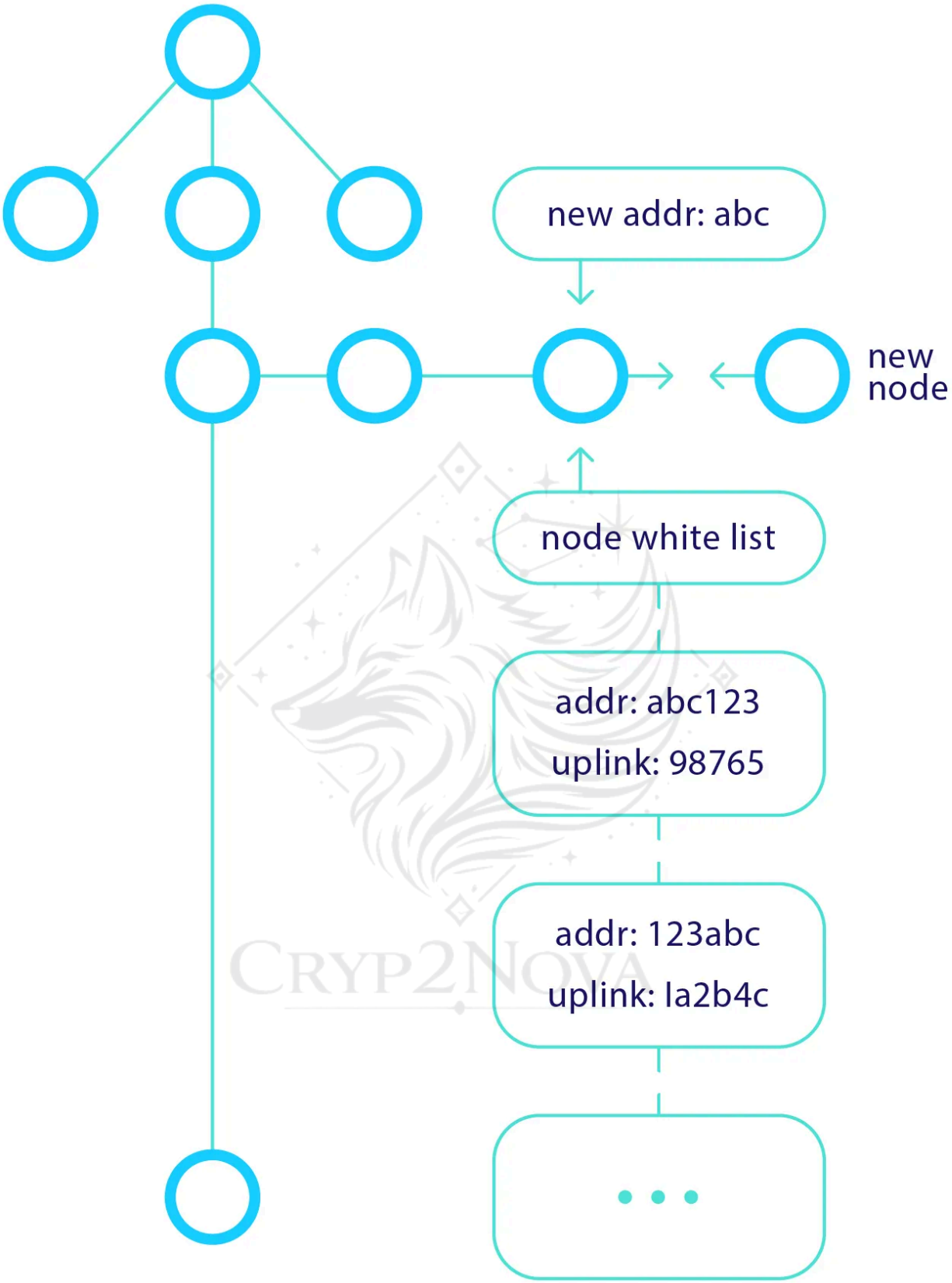
Node is the atomic element of the decentralized network. Most of the nodes have equal privileges in the system, so it is a “one-rank network”. We should mention that we need several particular types of nodes: light, full, archive, master, or root, as well as any number of private node types (seed, gate, swap, etc.).
Nodes can share Services via the Network. Services can use their own identifiers and share blockchain data, whitelisted data, stream channels, and other Cellframe Network feature abilities. Since everything is developed in a relatively low-level language, we can share toolkits for creating services such as VPN and Audio-Video streaming. This is made possible by Cellframe’s efficient usage of CPU and memory. Because of the need to support Post Quantum algorithms, which have very large file sizes, and to optimize their use with high-throughput (1M+ TPS) services, Cellframe makes use of Assembler optimization.

Nodes Organization

The node organization is performed with the help of a whitelist — a list of nodes with an uplink for each of them, which is copied from node to node. An uplink itself is a node that requests the entire whitelist at the first connection, and the non-blockchain data obtained from it is considered to be preferred. This means that if the downstream node sends a whitelist conflicting with the parent node, preference will be given to it. At the same time, a list comparison with all other nodes of the network will be required. If an IPV6 white address is available, there is always the possibility of a P2P connection to any other node. The uplink during the new node connection is readily determined — the whitelist is downloaded from the so-called “seed nodes” (center nodes), where data is requested by default and then traced to each location. These connections optimize for which Internet route is the shortest with the minimum response time. Thus, the nodes will be built into a hierarchical schema that will roughly follow the hierarchy of the real Internet.

Archived copy · cryp2nova.com

Archived copy · cryp2nova.com



Merging into the network

Nodes are merged into the network by the following algorithm:

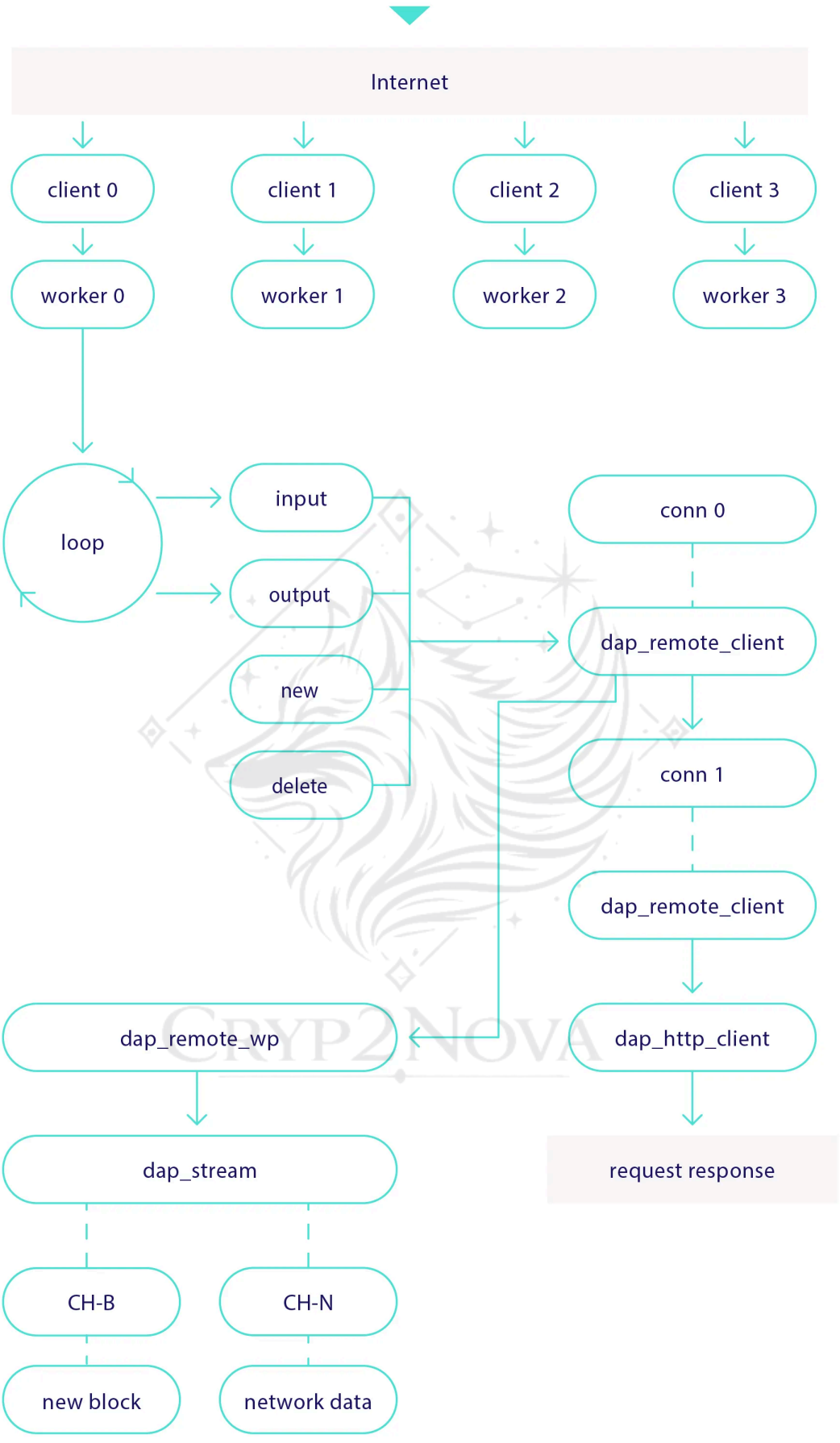
Archived copy · cryp2nova.com

1. Try to connect with root nodes;
2. When connected, asks them for node whitelists and their IP addresses;
3. Track nearest nodes according to their white IP addresses, selecting the closest;
4. Ping them and try to handshake with them to find the lowest latency and highest speeds;
5. Connect to the 2-5 of the best nodes;
6. The 1st node gives you your new id based on a key generated for it.;
7. Synchronize blockchain with uplink nodes;
8. Request address, broadcast you node’s public key and services price-lists into the zero-level blockchain;
9. After the key is accepted in the blockchain,the node can share service.

Node Data Processing

Archived copy · cryp2nova.com

Archived copy · cryp2nova.com



Archived copy · cryp2nova.com

Connections from the internet come to node from clients — C-0, C-1, C-2 and so on. After that, the connections are assigned to a certain worker, w-0, w-1, w-2, and so on.
The number of workers is strictly constant and is usually equal to the physical number of processors in the system. Accordingly, a worker is a separate thread strictly owned by the processor, i.e., executed solely on it. This allows the system driver to determine that the process is busy with network operations and generate an interrupt from the network card strictly on this processor, which significantly speeds up processing at speeds higher than 1–4 Gbps. Furthermore, inside each worker, there is a loop – an infinite cycle of calling the input and output fee. These f-groups are grouped into a dap_events_socket object, and each such object (more precisely, a pseudo-object) has a particular connection: C-0, C-1 .... it also has an implementation – on the schema from different dap_events_socket to drag the arrow to dap_http_client, which carries out the operations-type request/responses that do not require a permanent connection, or other arrows – dap_events_socket which have a dap_stream implementation. dap_stream ensures the permanently existing session between nodes and drives data that requires speed, for example, the network traffic of VPN services,new blockchain elements of participants, audio-video streams, or any other data type. Each type of such data goes through its own channel, such asCH–B for blockchain elements, CH–N for VPN's network data, and so on.
All these channel packets are grouped within the stream packet, which goes through the UDP transport picked up by the dap_events_socket which is spinning inside the loop and reads the I/O from the remote connection that is inside the worker thread belonging to the individual processor.

The need for Cellframe’s implementation

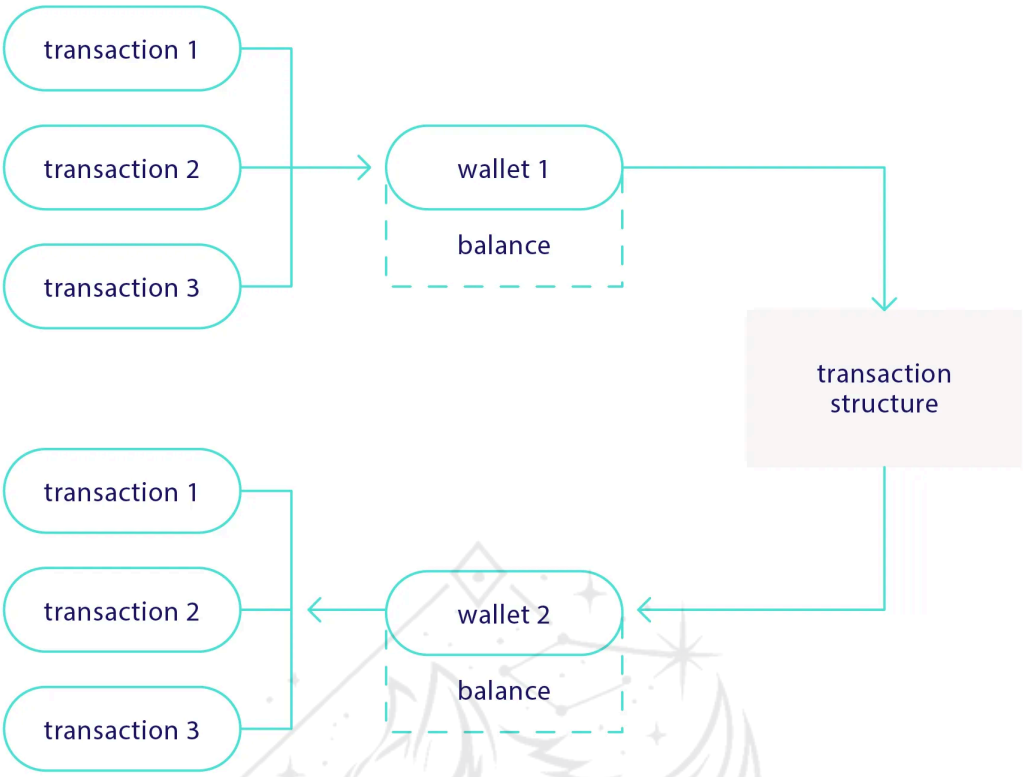
The fact is that in current multitasking systems the loss of computing power exponentially grows at high loads, which takes place due to the switching of processors between tasks and also directly via the input-output operations themselves. In Cellframe’s schema (as in the picture), I/O is grouped in one place, processors group the I/O operations, and subsequent processors remain on the same processor at all times. That excludes the switching back and forth, which is essential at high loads. Actually, without this technology, pumping even a GB of data is difficult, and more than 4 GBit is totally unrealistic.

Transaction Structure

This is a scheme of processes going inside of every transaction.

Archived copy · cryp2nova.com

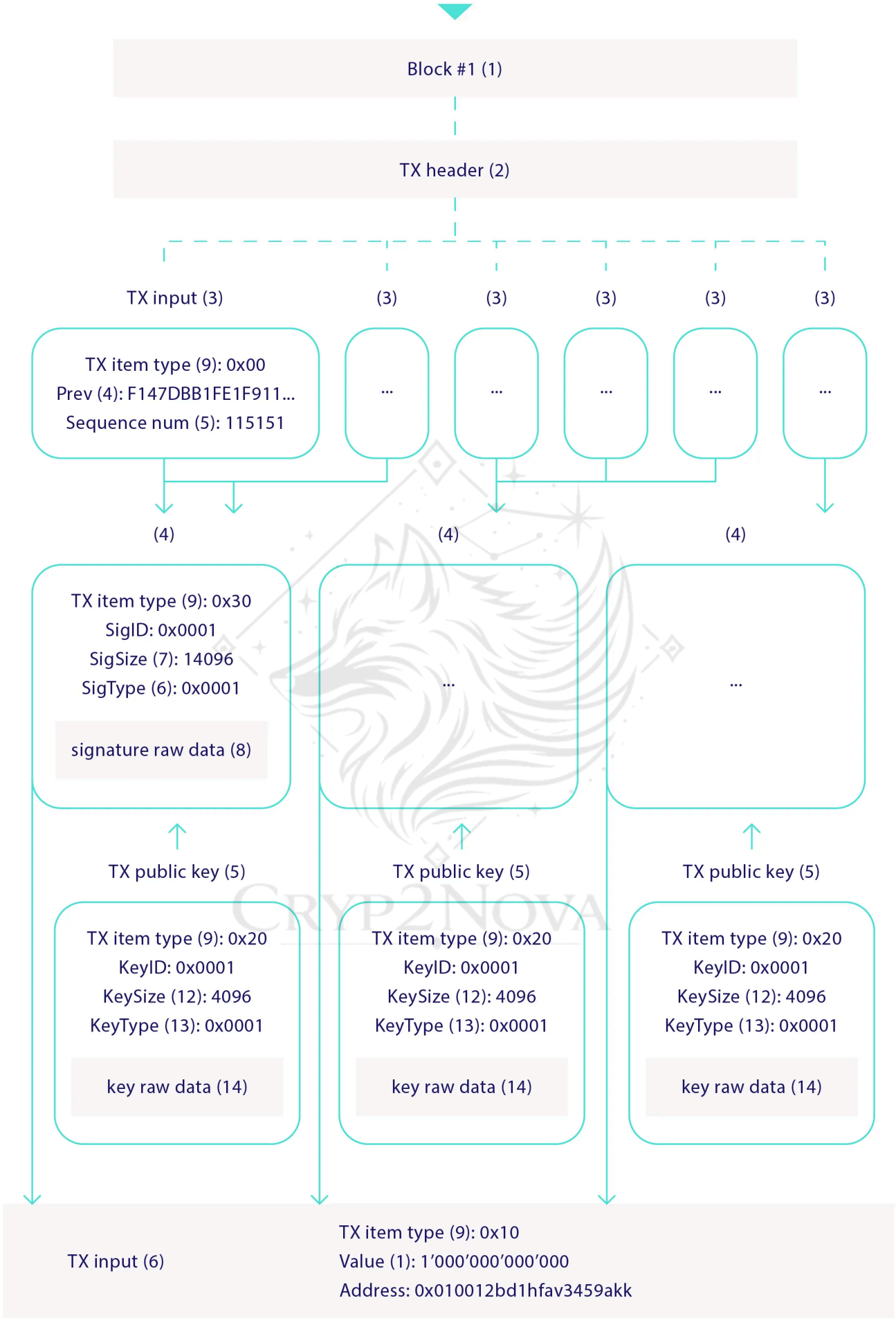
Archived copy · cryp2nova.com



The beginning is a statement of a balance from the other Cell, verified by at least three randomly picked Master Nodes or a verified token copy from ZeroChain. So if a transaction goes to another Cell, the outgoing transaction is verified by the Master Node of the sender's Cell when the income transaction of the receiver is verified by the receiver’s Master Node. This is just the same as when one bank’s client sends funds to the client of another bank. Each transaction should have at least three outputs – one for the receiver, one for commission (could be zero) and one for change. Outputs also could be open not only for the address but also for one-time keys, signed with a closing ring signature — Zero Knowledge transactions.

Archived copy · cryp2nova.com

Archived copy · cryp2nova.com

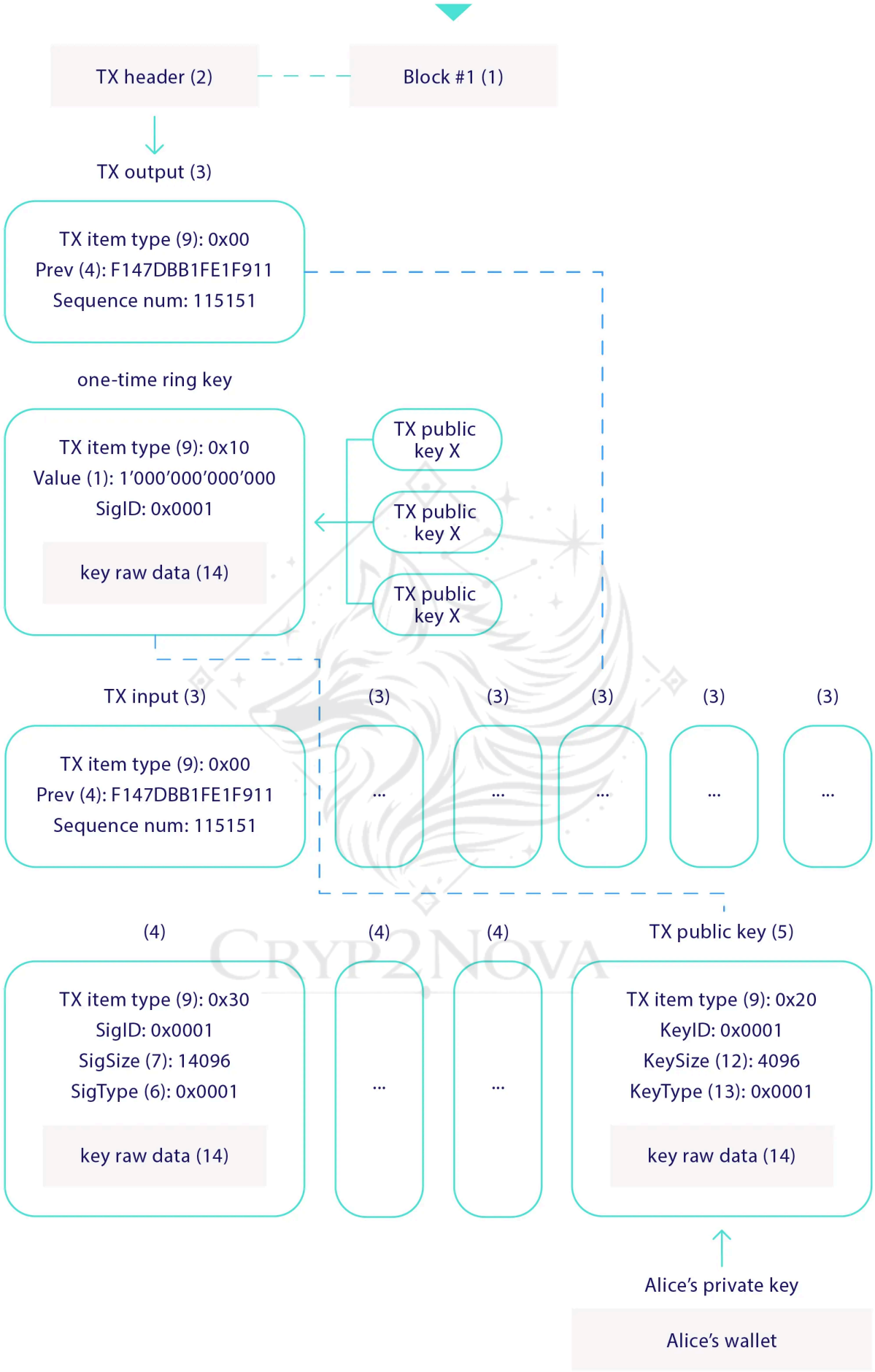


Archived copy · cryp2nova.com

ZK Ring Signature

Archived copy · cryp2nova.com

Archived copy · cryp2nova.com

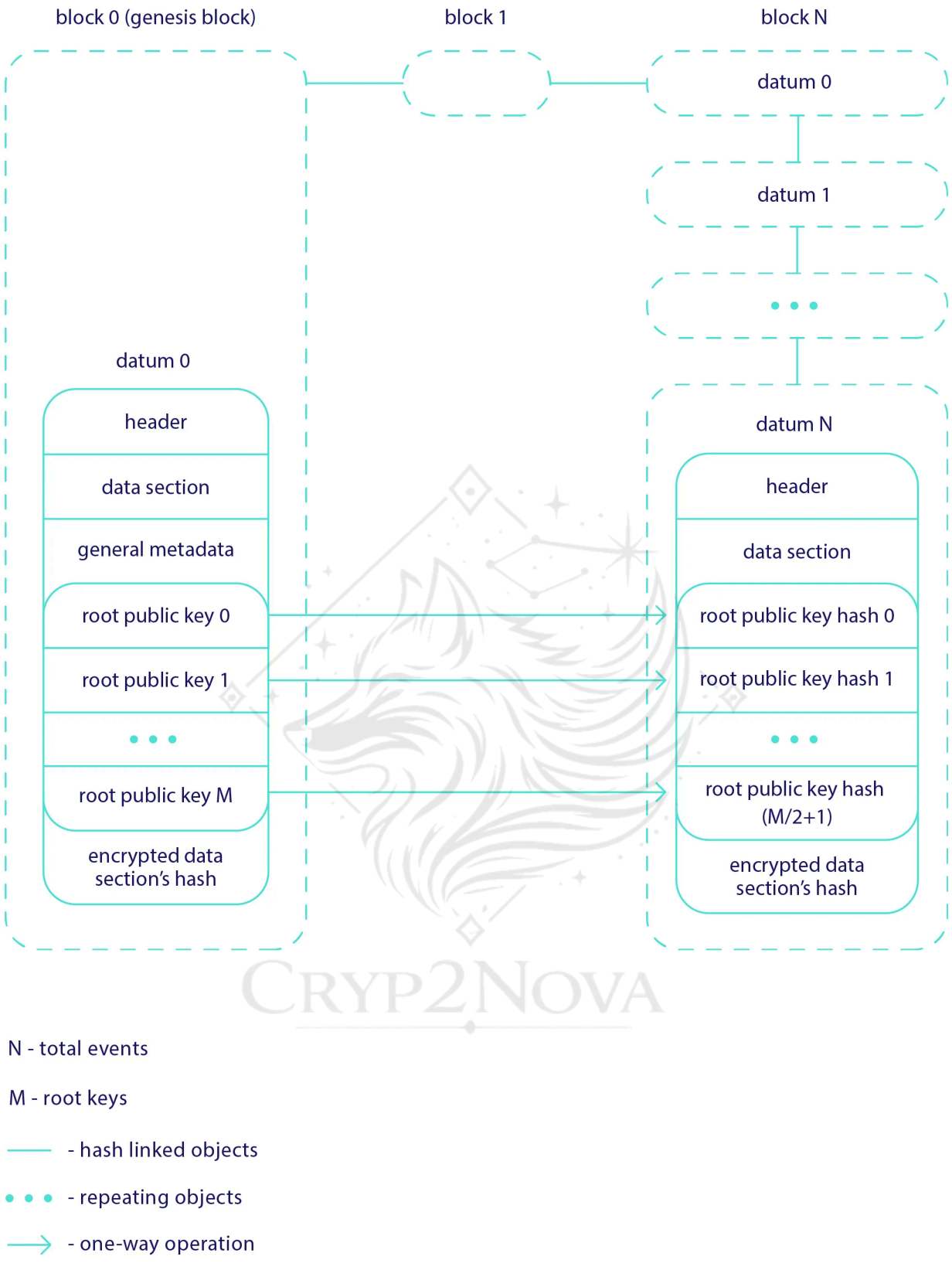


Archived copy · cryp2nova.com

Zero-level (Zero Chain) consensus

Archived copy · cryp2nova.com

Archived copy · cryp2nova.com



On the ZeroChain level, we use only one consensus: Proof-of-Genesis.

It works as a modified PoA: the first block holds only the one datum with general metadata and set of the root public keys. Every datum following the genesis block must be signed with the root key (genesis block keys).

Archived copy · cryp2nova.com

Every subsequent block must be signed with half plus one of the root keys number, e.g., if we have eight root keys in genesis block, we must sign every subsequent block with any five randomly selected keys.

Sharding

Cellframe’s proposed sharding technology involves breaking the whole blockchain into specific “shard chains” or Cells. These shard chains are composed in such a way, that all the same account information is present within one shard chain. The shard could be limited in size, for example, to 1GB. Sharding will be tied to the topology, and the topology, in turn, is tied to the real network infrastructure. Accordingly, the hit in the desired particular shard is determined by default by its network proximity. If desired, you can define shards yourself or request to make a new one by default. However, overcrowded shards may refuse new members to register. All requests for shards occur through messages inside the zero-level blockchain.
All shard events happen in two stages: Declaration and Announcement, with at least X blocks between the two. For Cellframe this means a minimum time of 10,000 seconds (could be more if the network is not loaded).
The declaration can be sent by Master Node or by Root Node. So if somebody wants to become a Master Node, they must send the request to any Master Node mempool to be presented to the root nodes.
Root nodes check if the Master Node Candidate holds enough coins staked with the specific output – Hold Output. They can be unlocked only with Zero Chain consensus. If the Candidate is good, then after X blocks a Master Node Announcement with its public key declaration (related to the cell ID) should appear.
Cell Declaration works the same way, but such requests can be sent only by a Master Node that is already presented in the list. It must point to the cause of sharding – overloaded shard for previously launched Cellframe shard or coins held, plus some metadata as usual. After all of the checks, root nodes announce the new Cell ID, and after that, the new Master Node Declarations would be accepted.
Inside each Cell there are two parts — the Cell’s Base Chain and Plasma DAG. Cells' Base Chain is similar to zero chain: it stores verified balance states from other chains, where the next transactions could be placed only in Plasma.

Communication and Network Protocols

All communications are performed with the usage of the DAP SDK framework, an event-driven system that gives an ability to process a lot of I/O operations in one thread. It starts by default with a thread number equal to the CPU count, and assigns them exclusively to processing cores. The same technique is used by the popular web server Nginx that gives it a huge number of same-time connections processed and served. We expect to have the same profit.

Archived copy · cryp2nova.com

Key Exchange Connections

Cellframe starts every network activity from the public key exchange connection. First, a client connects to the server and receives the public key, signed with the particular key included in Cellframe whitelists. The client validates the key, and then sends a short message encrypted with a server's public key. Then the server decrypts it with its private key, encrypts the answer with a client's public key and sends the result back.
After entering the exchange, the client can easily initiate any Request-Response session or bring up the stream connection. The server produces the private symmetric SALSA2012 key for the stream connection to reduce the processor's load. Moreover, once every 30 mins, the key is changed.

Encryption with PQ–algorithms

To sustain the variability principle, a 2-byte ID is added at the beginning of every spot for encryption. We expect that humanity will not invent more than 65'536 digital signature algorithms. For the beginning, we've selected the most promising PQ algorithms: NewHope, NTRU, Frodo, SIDH* and others. One of the most interesting algorithms that we use is Picnic — a Zero Knowledge Post Quantum signature. By default we use the CRYSTALS-Dilithium digital signature.
Also, a combination of more than one algorithm is available; e.g., a user could protect all the deposits in his wallet with more than one key (Multi-Algorithm Signature). A safe is more secure when it's locked with more than one key.

Tokens

The ZeroChain does not require token implementation for successful operation, as it is based on proof-of-Genesis consensus and there is no mining in a traditional sense. All decisions regarding block formation are made by initially authorized nodes, and this chain stores only necessary technical information and does not store address balances, so it does not affect the security of launched Cells. All significant interactions in the network occur inside the Cells. In the case of inter-cell communication such as asset transfers, the operations are conducted via the P2P approach only and therefore do not require adding additional records on ZeroChain. Each cell is a pseudo-independent chain that is included in the overall ecosystem by inter-cell interactions. Thus, each network has its own consensus based on flexible POS (or DPOS/POA if required) that can be configured by a chain initiator. But Cells within a single network have a single type of consensus. Cells provide two main token functions: first is staking, for participation in consensus (for POS consensus), and second is the value transfer unit/unit of account inside the ecosystem (including inter-cell interactions).
The token emission process is as follows:

1. Root nodes receive a token creation request;
2. Nodes check if the author request has enough rights for token emission, and in the positive case, they publish the token declaration;
3. The token declaration contains the signatures of emission holders, which then allows them to add events to the emission of a token through the memory, and then publish a basic transaction

Archived copy · cryp2nova.com

with this emission to a convenient Cell. Important: the emission in the ZeroChain is tied to the address, not the key and not the Cell;

4. At the moment of the emission, neither the key of the emission holder nor his shard is known until he wishes to use the funds and form the basic transaction in any Cell. There is a similar process when you transfer tokens from Cell to Cell — the basic transaction in the new Cell points to a transactional token indicating the plasma chain ID, Cell ID, and hash of transaction, the output of which points to the address signing the basic transaction;
5. Thus, the transaction between Cells has an atomic swap structure “under the hood” and it is slower than transactions inside the Cell.

Tokenomics

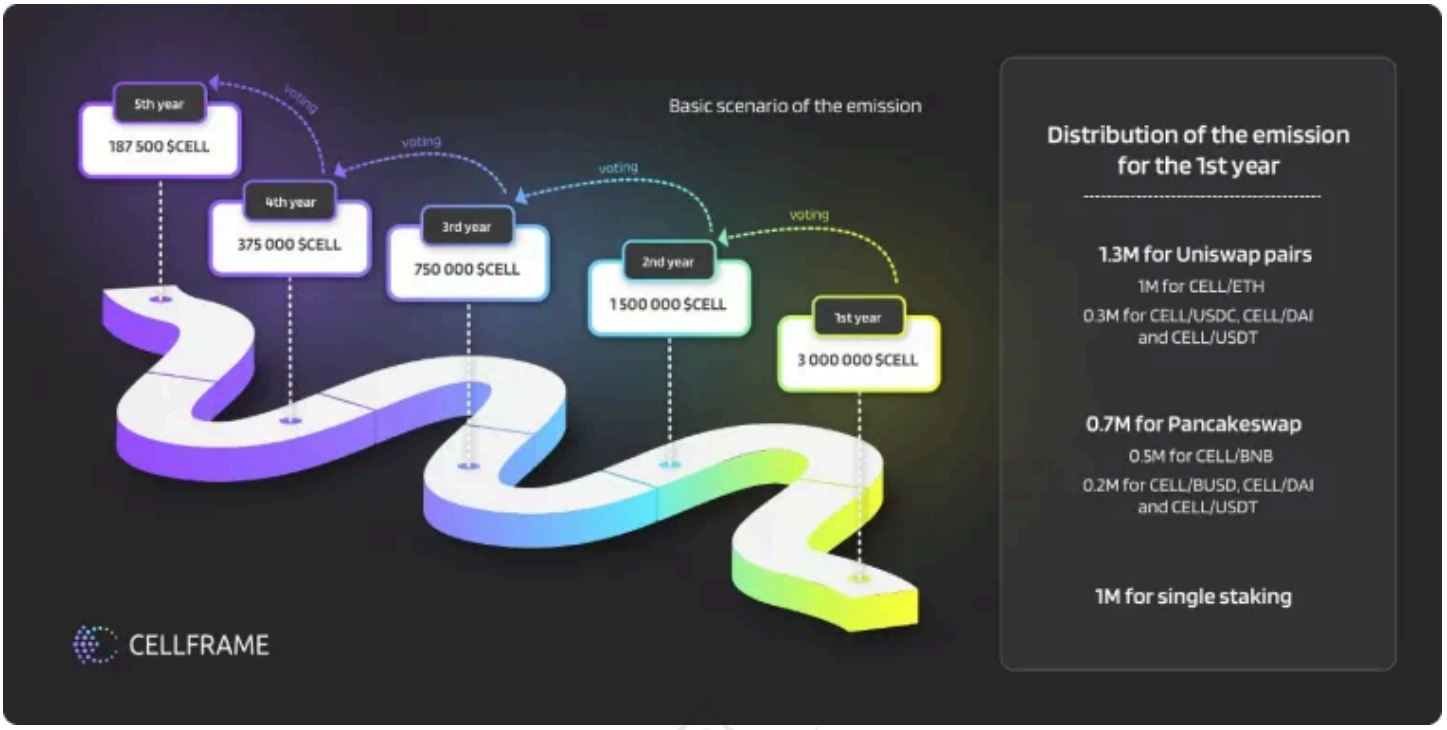
The updated tokenomics assumes revenue not only from the provision of services but also from liquidity. Additional rewards are also available from long-term LP-holding.

Emissions



CRYP2NOVA

Archived copy · cryp2nova.com



For structuring a reward system for stakers, the plan is to emit 3M tokens next year. Then there will be a vote on the issuance for 2024 and beyond. The basic scenario is to halve the emission to 1.5M for 2023, with a further halving each year. It can be revised depending on the success of the ecosystem development and the sentiment of the holders.
The distribution of the issue will be as follows:

1.3M for Uniswap pairs:

- 1M for CELL/ETH pair
- 0.3M for CELL/USDC, CELL/DAI, and CELL/USDT

0.7M for Pancakeswap pairs:

- 0.5 M — CELL/BNB pair
- 0.2 M — CELL/BUSD, CELL/DAI, CELL/USDT

1M for single-sided staking.

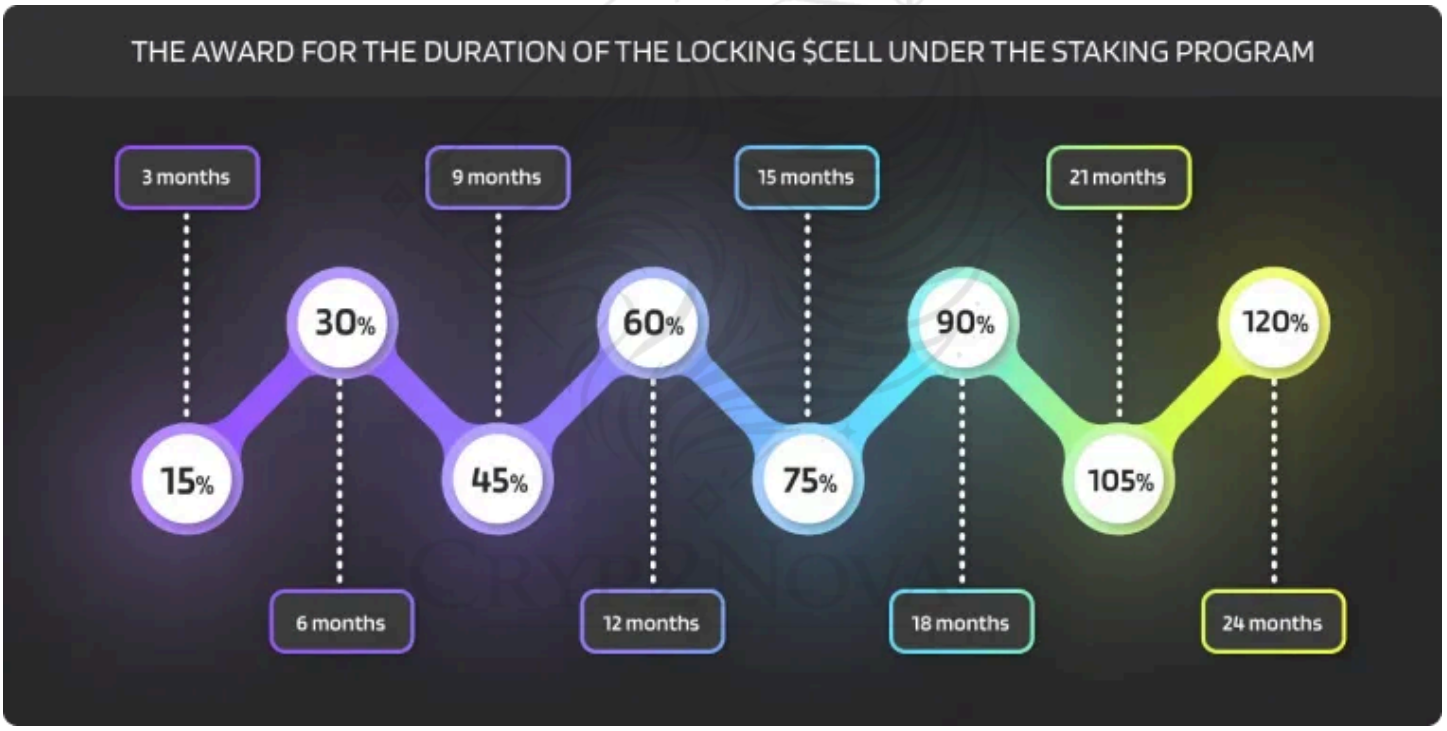
Reserves

To build a viable ecosystem in the long term, there will be an emission of reserves, 2 million $CELL. One million will be emitted in mid–2023, and one million will be emitted in mid–2024. These funds will be used to develop the project.

Additional rewards and bonuses



Archived copy · cryp2nova.com



Staking Rewards Program

Cellframe Staking rewards are calculated using a points system. Your points depend on the size of your stake and the duration of the lock-up period. To calculate the number of points awarded for a given stake, we multiply the locked-up amount by a coefficient that depends on the duration of the lock-up period. When you provide liquidity in the Cellframe staking program, the rewards coefficient increases by 15 percentage points for every 3 months of lock-up. The maximum lock-up period is 2 years. If the funds are locked up for this period, the coefficient will be 220%, which means that the number of points awarded will be 2.2 times the total number of tokens you locked up. When creating a stake, you can decide to reinvest some or all of your accrued rewards to your stake balance to prof-

Archived copy · cryp2nova.com

itability. Any portion of the rewards you choose not to reinvest will become available for withdrawal prior to the end of the lock-up period.
Bonuses for providing liquidity prior to the launch of the staking program.
Holding LP tokens in the Uniswap or Pancake pools before the Cellframe staking program launches will earn you additional points. Even before locking up LP tokens in a stake or auction, the coefficient will increase by 0.16 percentage points for each day. If the LP was created 30 days before the start of the staking program, this will increase the coefficient when calculating points by 4.8 percentage points. If the LP duration was 313 days, the multiplier would be increased by 50 percentage points. 50 percentage points is the maximum bonus for early provision of liquidity.

APY Calculation Examples

Let's look at some numbers to show how the points system works. For convenience, we will assume that all stakes are fixed, although in fact they are recalculated every minute. Depending on the refinancing share you choose, the size of your deposit will grow, the points will also increase. This is true both for the user and inside the system. When a staking period ends, the total number of points in the system decreases.

Single-token

1 000 CELL locked for 1 year gives.
1 000 × 160% = 1 600 points.
Let’s say the total points of other participants in single token staking equals 2M points, so this staker will have a reward of 1 000 000 / (2 000 000/1 600) = 1000000 / 1 250 = 800 CELL per year.
With an initial investment of 1 000 CELL, it gives 80% APY.

Pair

CELL/ETH pair for a similar amount that was staked for 3 month before staking program and then locked for 9 month:
1 000 × (100 + 15 × 3 + 3 × 5)% = 1 000 × 160% = 1 600 points.
Let’s say the total points of other participants in CELL/ETH equals 1.5M points, so this staker will have the following rewards:
1 000 000 / (1 500 000/1 600) = 1 000 000/ 937.5 = 1 066.66667 CELL per year.
With an initial investment of 1 000 CELL, it gives 106.666667% APY.

Archived copy · cryp2nova.com

How to bring up a master node for staking participation?

The participants of the staking program and auctions will get additional rewards in the form of an air-drop of special mCELL tokens. The mCELL tokens will not be transferable, nor will they be tradeable, exchangeable, or withdrawable. Their only purpose is as a stake for master nodes. This means that there will be no need to choose between the staking program or the auctioning of the opportunity to raise a Master Node. Everyone who participates in the staking program will also be rewarded as a percentage of the value of the services provided and transactions processed by the Master Node. This award is an extra bonus and is not a substitute for the CELL awards but rather a supplement.

UPD:

At the end of 2024, we held three votes within the community. The first vote determined the reward pool size for staking in 2025 — 2 million tokens. In the second vote, the team proposed redirecting rewards for LP-staking pairs with stablecoins towards project development, but this proposal was rejected by the community. The third vote concerned the distribution of the reward pool between stakers and validators. The community decided to allocate 2 million tokens in an 80/20 ratio. 80% of the pool will go to rewards for validators, while 20% will be allocated to staking rewards. This distribution reflects the current ecosystem priorities aimed at sustainable development and supporting network activity.
The current token distribution data across the network is as follows:

A total of 2 million tokens:
● 1.6 million — for validator rewards
● 0.4 million — for staking rewards

Distribution among stakers:
0.144 million — for solo staking

0.16 million — for pairs on Uniswap:
● 0.12 million for the CELL/ETH pair
● 0.04 million for the CELL/USDC, CELL/DAI, and CELL/USDT pairs (0.013333 for each pool);

0.096 million — for pairs on Pancakeswap:
● 0.068 million for the CELL/BNB pair
● 0.028 million for the CELL/BUSD, CELL/DAI, and CELL/USDT pairs.

At the beginning of 2025, we stopped accepting new LP-stakes in external networks. This decision was made due to the rapid development of quantum technologies and the increasing risks associated with storing funds in non-native networks. All active stakes remain valid, and rewards for them will be paid in full, but no new stakes will be accepted. Instead, we are beginning the development of a mechanism to create LP tokens on the Cellframe platform. Once launched, rewards intended for LP-staking will be transferred to holders of Cellframe LP tokens.

CRYP2NOVA

Archived copy · cryp2nova.com

Future decisions regarding reward distribution in the Cellframe mainnet will be determined by subsequent votes.

Conclusion

In this paper, we demonstrated Cellframe’s principal technical features and execution paths. The protocol structure is proposed to be a zero-level layer for blockchains and distributed systems because it can solve several existing challenges in the space: scalability, security and flexibility. Cellframe is capable of providing modifications to solve any future blockchain problems without harming the scalability or performance.
This paper will be extended with time with a more detailed description of interchain interactions, use case architecture, test results, etc.

Contents

- Executive Summary
- Abstract
- Challenges
- Vision (design goals)
- Highlights
  - Variability
  - Security
  - Scalability and Performance
- dApps: how to make them truly decentralized?
  - Problems of current dApps architecture
  - Cellframe: service-oriented blockchain platform
- Blockchain Structure
  - Node
  - Nodes Organization
  - Transaction Structure
    - Zero-level (Zero Chain) consensus
    - Sharding
  - Communication and Network Protocols
    - Key Exchange Connections
    - Encryption with PQ–algorithms
- Tokens
- Tokenomics
  - Emissions
  - The distribution of the issue will be as follows:
  - Reserves
- Additional rewards and bonuses
  - Staking Rewards Program

CRYP2NOVA

Archived copy · cryp2nova.com

    - Bonuses for providing liquidity prior to the launch of the staking program
- APY Calculation Examples
    - Single-token
    - Pair
- How to bring up a master node for staking participation?
- Conclusion

Get started

- Download
- Cellframe Bridge
- White Paper
- VPN Service
- Cellframe Shop
- Cellframe Vote

Learn

- Roadmap
- Team
- Blog
- Changelog
- Partners
- FAQ
- Logo Usage

For developers

- Documentation
- Telegram devs channel

CRYP2NOVA

Contact us

- pr@cellframe.net
- tech_support@cellframe.net
- telegram support icon cellframetechsupport
- Feedback form

- x socials link image
- telegram socials link image
- instagram socials link image
- medium socials link image
- gitlab socials link image
- youtube socials link image

Archived copy · cryp2nova.com

- book socials link image
- book socials link image

© 2026 Demlabs Inc

Terms of service Privacy Policy Cookie Policy

Our website uses cookies

We use cookies to ensure secure and personalized website operation. Learn more in our Cookie policy.

Accept Reject Settings

Archived copy · cryp2nova.com