

Nimi q

A simple, secure and censorship-resistant payment protocol, native to the web.

Executive Summary

What is Nimiq?

Nimiq is a decentralized, censorship-resistant payment protocol native to the web, with its own diverse ecosystem of apps. The native NIM token is transacted within Nimiq as a store and transfer of value: it acts as digital cash. The cutting-edge, browser-first blockchain approach means that users directly connect to the blockchain with nothing more than a browser. Therefore anyone with an up-to-date browser can join the payment network directly, pay and accept payments without having to install software or rely on unnecessary intermediaries. This gives Nimiq its 'it just works' characteristic, which is further strengthened by an ethos of simplicity and ease of use. NIM is designed to be a cryptocurrency used by the masses.

Nimiq's Mission & Vision

Revolutionizing money by realizing the full potential of cryptocurrency. While Nimiq itself as a tech-focused project is dedicated to ushering in a new era of independent and censorship-resistant digital cash, the Nimiq Ecosystem aims to bring universal access and the ease of use of NIM to both the tech-savvy and typical Internet users. All efforts are guided by an overarching philanthropic mindset such that as NIM is increasingly adopted, its charity's ability to support good causes will grow.

Project Status

The Nimiq Mainnet was launched on April 14, 2018 and the payment protocol is fully operational. Nimiq's browser-first blockchain has been deployed and streamlined for the web. All user interfaces are focused on simplicity, maximizing ease of use, including onboarding, easy address verification, and a simplified backup process. Nimiq is also home to a growing ecosystem of apps, and has dedicated significant efforts to advance blockchain and crypto adoption research. Nimiq has acquired a stake in German WEG Bank to secure a licensed ally in implementing the first version of the Open Asset Swap Interaction Scheme (Nimiq OASIS), while diversifying project assets. The project offers active support and advice to community developers, as well as limited seed funding for qualifying community projects.

Resources

- [JavaScript codebase \(https://github.com/nimiq-network/core\)](https://github.com/nimiq-network/core) for browser and backbone nodes
- [High performance Rust implementation \(https://github.com/nimiq/core-rs\)](https://github.com/nimiq/core-rs) of the backbone node
- [Nimiq Developer Center \(https://nimiq.com/developers/\)](https://nimiq.com/developers/)

Collaborations & Grants

- [WEG Bank \(https://www.weg-bank.de/\)](https://www.weg-bank.de/): Collaboration on peer-to-peer fiat-to-crypto bridge
- [Stanford University's Applied Cryptography Group \(https://crypto.stanford.edu/c2rg/\)](https://crypto.stanford.edu/c2rg/): Research grant for blockchain research
- Arthur Gervais at [Imperial College's Centre for Cryptocurrency Research and Engineering \(https://www.imperial.ac.uk/cryptocurrency/people/\)](https://www.imperial.ac.uk/cryptocurrency/people/) : PhD research grant

Research Publications

- [Albatross: An optimistic consensus algorithm \(https://arxiv.org/abs/1903.01589\)](https://arxiv.org/abs/1903.01589)
A technical research paper resulting from Nimiq's collaboration with Trinkler Software. It is a new PoS consensus algorithm that is able to achieve a performance close to the theoretical maximum for a single chain.
- [Nimiq OASIS \(https://medium.com/nimiq-network/nimiq-makes-fiat-currencies-blockchain-compatible-7503096a6252\)](https://medium.com/nimiq-network/nimiq-makes-fiat-currencies-blockchain-compatible-7503096a6252)
The Open Asset Swap Interaction Scheme is the blueprint for a potentially disruptive crypto-to-fiat bridge, making fiat currency behave as if it were tokens on the blockchain, providing a unique way of connecting the traditional banking network with non-custodial crypto exchanges.

2017

JUN 17

Nimiq Betanet
released

NOV 17

Luna Testnet
released

2018

APR 18

Mainnet
launch

NOV 18

Community
funding

2019

FEB 19

Nimiq OASIS
concept

MAR 19

Albatross
announced

Motivation

Cryptocurrency as a valid concept has been confirmed by the growth and persistence of [Bitcoin](https://bitcoin.org/bitcoin.pdf) since its launch in 2009. More than just a technical idea, it laid the foundation for a disruptive means of transacting value not seen before in the history of humankind, by allowing “[payments to be sent directly from one party to another without going through a financial institution](https://bitcoin.org/bitcoin.pdf)”*. This brilliant concept has fostered a grand ecosystem with a broad range of ideas and technical solutions.

Cryptocurrencies still represent only a small fraction of the global [money supply](https://coincenter.org/entry/how-do-cryptocurrencies-affect-monetary-policy). And much of their adoption so far has been driven by centralized services that hold your crypto assets for you (centralized crypto exchanges, payment providers, etc). We are therefore still far away from the goal of crypto mass adoption, even more so in its original peer-to-peer, non-centralized sense. The reasons centralized solutions appeal to users seem to be convenience and ease of use, as they employ the same interaction patterns we became familiar with by using online banking. This familiarity in turn leads to a feeling of safety. But this convenience and feeling of safety come with a serious trade-off: giving up the ownership of your keys to a third party, violating what is considered to be the most fundamental reason for the creation of cryptocurrencies in the first place.

In light of these facts, Nimiq recognizes an enormous opportunity. Namely to pursue and deliver the **most accessible and easy-to-use but also censorship-resistant and decentralized payment solution** for mass adoption. Nimiq seeks to achieve this by researching, implementing and combining cutting-edge technologies from:

- Cryptocurrencies,
- Cryptography,
- Blockchain technologies,
- Peer-to-peer networks,
- Distributed ledger technologies,
- Web development,
- Usability,

- User experience,
- Human psychology and behaviour.

Design Approach

Web apps have become the standard of the Internet and are disrupting business models of traditional software industries. From Encarta to Wikipedia, from Office to Google Docs, web apps are far more attractive because they improve the overall usability of software for the user:

- **No installation needed:** Users can open a website and start using the application with one click.
- **Cross-device compatibility:** By focusing on the browser instead of each specific OS and device, a more coherent codebase is achieved, which translates into stability and a consistent experience across devices for the user.
- **Built-in security and privacy:** Browsers are one of the most secure, tested and audited pieces of software. Providing untampered client-side software that runs in the user's browser allows for inherently secure and private applications.
- **Intuitive:** By tapping into the user's familiarity with their browser it is possible to create a smooth and easy-to-use user experience that 'just works'.
- **Future-proof:** Web apps are a clear long-lasting trend in software development, since the web has become ubiquitous even in developing countries.

Crypto for Everybody

Even though there are obvious advantages in using cryptocurrencies and holding your own funds, it is clear and understandable that non-tech-savvy users are drawn to **convenient and easy-to-use payment** methods.

Nimiq learned from commercial payment providers that, **frictionless payments** are the key for user adoption, especially as they directly influence the perceived safety and trustworthiness of a system. In other words, a payment system that is intuitive and frictionless makes users feel much more confident about trusting this system with their money.

Looking at the history and origins of cryptocurrencies, it is logical that the focus was on tech-savvy users. Over decades, the primary objective was solving tremendously challenging research and engineering problems in the realm of cryptography, distributed ledgers, and network communications. At such an early stage it was out of scope to consider streamlining blockchain technology towards user experience and daily payments on the web.

Powered by the knowledge we now hold and in deep gratitude for the hard work of crypto pioneers, we are now standing on the shoulders of giants. Nimiq is working on outperforming the convenience of conventional payment services with an enhanced user experience that is **intuitive through simplicity**, whilst providing the privacy and censorship-resistance of decentralized cryptocurrencies to create a novel payment experience. This is the Nimiq Payment Protocol, embedded in the Nimiq Ecosystem.

Open Source and Developer Accessibility

Nimiq is encompassed by a strong philanthropic mindset, it is open-source and aims to become entirely community-driven.

Team Nimiq is a tech-focused team with a deeply rooted open-source mentality. The project's source code is released to the public on the [official GitHub repository \(https://github.com/nimiq\)](https://github.com/nimiq) to encourage peer review and interaction with developers. The project's main focus is to enable the most accessible, censorship-resistant payment solutions. This intrinsically means that Team Nimiq works to provide the framework and tools for developers to further build applications that tap into the Nimiq Payment Ecosystem. To guide and support developers on this journey, Nimiq provides the [Nimiq Developer Center](#)

Browser-First Blockchain

It is already possible to pay online with crypto. Through intermediaries. But the heart and soul of crypto is to make ourselves as independent as possible from third parties and intermediaries.

Simplicity means bringing crypto and blockchain technology to where the user already is: online, on the web. Instead of offering payment services for the web, Nimiq is a blockchain and payment protocol **native to the web** offering any form of payment, be it online, in a shop, or between friends, as long as the device is connected. Being a browser-first blockchain means paying becomes as simple as browsing a website: no apps, no plugins,

completely installation-free. It works on all devices that come with a browser, from desktops to mobile phones.

To achieve this vision, two major challenges needed to be overcome. First, the core blockchain components had to be translated to the web platform, including:

- Network for establishing P2P connections
- Storage for persisting keys and blockchain data
- Cryptography for hashing, signing and verifying

In addition, the protocol had to be adapted to the requirements and constraints of the web:

- Compression of blockchain data to sync within seconds instead of hours
- Blockchain parameters optimized for the browser

Blockchain Streamlined for the Web NEW

Nimiq is building a blockchain for the web to provide the liberating features of blockchain-based payments to the masses. The experience of a cryptocurrency native to the web must meet, and hopefully exceed the expectation of users who are used to the convenience of web applications which rely on centralized servers and legacy technology. While these systems usually don't suffer from connectivity constraints — since the user is dealing with a single authority of truth, i.e the bank — they come with a major disadvantage: a single entity holds custody of the assets and thus becomes a major threat to security and privacy.

In the case of Nimiq, each user connects to multiple peers and receives the information needed to check their balance. Variables like amount of data per connection, latency, bad actors and other attack vectors need to be considered. To overcome these additional challenges, Nimiq is built using state-of-the-art cryptography, blockchain and web technology to reach a result that levels the ground with popular centralized web payment processors, while being true to the cryptocurrency spirit of borderless decentralization, neutrality and censorship-resistance.

Proof-of-Stake NEW

With the switch to Nimiq 2.0 also comes the switch from Proof-of-Work to Proof-of-Stake. Our Proof-of-Stake algorithm is called [Albatross](#) and is able to provide a high throughput of transactions with eventual finality. One big advantage over Proof-of-Work algorithms is the vastly reduced energy consumption of Proof-of-Stake schemes. Instead of investing energy into the system, miners become validators that invest into the currency itself and set aside parts of their stake as security.

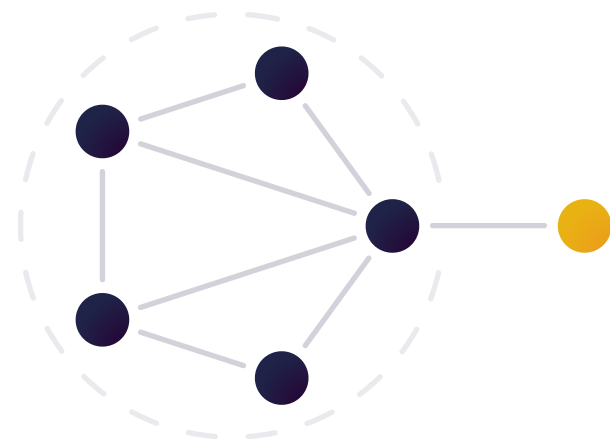
Client Types

There are two types of clients in the Nimiq 2.0 Network: **Backbone Clients and Browser Clients**. Both types leverage the same isomorphic Rust codebase. While Backbone Clients are doing most of the heavy lifting supporting and securing the network, the Browser Clients are the ones who are making Nimiq native to the web but also introduce all the constraints that need to be addressed to achieve a **blockchain streamlined for the web**.

Network

Other Blockchains

Your browser needs to connect to a node in order to access the blockchain network



Nimiq

Your browser is a node in the blockchain network



Backbone Clients run on servers and desktops. They communicate with each other via the WebSocket protocol, and act as entry points and signaling servers for Browser Nodes to establish browser-to-browser WebRTC connections. Additionally, validators may span a UDP-based network to speed up signature aggregation.

Browser Clients are built upon browser engines, supporting the latest version of Blink (Chrome, Brave, Opera, Edge), Gecko (Firefox) and WebKit (Safari) and connect to the network by initially establishing a WebSocket connection to at least one Backbone Node before initiating secure browser-to-browser connections using the Backbone Node as signaling server. Once the connection is established, Browser Nodes can also act as signaling servers for further browser-to-browser connections.

Storage

Browser Clients use the IndexedDB to store blockchain data and encrypted keys on the user's hard drive. By default, IndexedDB has a limited capacity. Depending on the browser engine, that might be a fixed amount of only 5MB on mobiles or a percentage of the disk space available. Given the space constraints as well as the overall limited memory on mobile devices, compression mechanisms are used to reduce the amount of information that

a browser needs to download and store in order to achieve consensus and become an operational node of the network. By contrast, **Backbone Clients** rely on **LMDB** (<http://www.lmdb.tech/doc/>) which has no size constraints.

Connectivity Constraints NEW

Nimiq 1.0 combined three techniques to reduce the amount of data a client needs to download, speeding up the time to consensus and reducing the bandwidth and storage being used: Accounts Trees, Non-Interactive Proofs of Proof-of-Work (NIPoPoW), and an optimistic approach.

Nimiq 2.0 builds on top of that and relies on a **Hybrid Model** between **UTXO**-based transactions and an **Accounts Tree**. In this novel hybrid model, the Accounts Tree provides easy access to all unspent transactions of an account while also allowing to use all the benefits of an accounts-based model (e.g., provable account statements) without its drawbacks. This way, the validity start height in transactions (as present in Nimiq 1.0) can be omitted – also improving the usability of the system.

On top of that it is planned to implement a blockchain compression system that can replace the Non-Interactive Proofs of Proof-of-Work currently being used in Nimiq 1.0. At the time of writing, the most promising candidate for this task is building upon **Recursively Composable Zero-Knowledge Proofs**. **Coda** (<https://codaprotocol.com/>) was the first cryptocurrency to explore this avenue, relying on zk-SNARKS and a trusted setup. Recently, Electric Coin Company proposed a new construction for a recursive proof composition called **Halo** (<https://electriccoin.co/wp-content/uploads/2019/09/Halo.pdf>), which does not require a trusted setup anymore. Using such a proof system, it is possible to verify the complete blockchain in just a single constant size statement.

This allows reaching consensus with just a few hundred kilobytes of data. More details in the **Compression** section below.

Privacy NEW

While the initial release of Nimiq 2.0 will not come with any advanced privacy features, this is an item on Nimiq's roadmap. Preliminary research efforts into this direction have shown that currently one of the most prohibitive drawbacks of a lot of privacy solutions is the need to scan the entire blockchain to find one's transactions. This is especially difficult on mobile devices – one of Nimiq's core features. Other solutions, such as **Zether** (<https://crypto.stanford.edu/~buenz/papers/zether.pdf>) are able to remove this constraint at the

expense of privacy guarantees. Team Nimiq plans to continue working on an acceptable solution after stabilizing the initial release of Nimiq 2.0.

Nimiq Blockchain NEW

Accounts and their unspent transaction outputs are stored in a Merkle-based accumulator. Pruning of Micro Blocks and condensing information into Macro Blocks improves synchronization time for full nodes. Recursively Composable Proofs (as used in Coda or presented in Halo) might be integrated in the future allowing for super lightweight nodes, where consensus can be established in seconds, even on mobile devices.

[Albatross](#) is Nimiq's Proof-of-Stake algorithm; [Ed 25519](https://ed25519.cr.yp.to/) (<https://ed25519.cr.yp.to/>) [Schnorr signatures](https://en.wikipedia.org/wiki/Schnorr_signature) (https://en.wikipedia.org/wiki/Schnorr_signature) secure transactions, and [Hierarchical Key Derivation](https://github.com/satoshilabs/slips/blob/master/slip-0010.md) (<https://github.com/satoshilabs/slips/blob/master/slip-0010.md>) allows a practically unlimited number of accounts to be generated from the same seed. The protocol is implemented in Rust and compiled to WebAssembly for use in the browser.

Nimiq Supply Distribution

The Nimiq Network has been designed for a total supply of 21 Billion NIM. The smallest unit of NIM is called Luna and 100'000 (1e5) Luna equal 1 NIM, which results in a total supply of 21e14 Luna, identical to Bitcoin's 21e14 Satoshi. The NIM are distributed as follows:

- 88% Validators Reward (mined over ~100 years)
- 5% Token Sale Contributors
- 2.5% Long-Term Project Endowment Foundation (10-year vesting)
- 2% Good Cause Partnerships and Sponsorships (10-year vesting)
- 1.5% Early Contributors (6-month vesting)
- 1% Creators (3-year vesting)

When launching the Mainnet on April 14, 2018, the first 721 blocks totalling 3'176'435.57 NIM (0.00015% of the total final supply) had been mined and [burned to NQ07 0000 0000 0000 0000 0000 0000 0000*](#). This was done to prevent several problems associated with a low difficulty in the network, such as multiple chain forks, orphaned blocks, and

possible malicious attacks. The NIM were burned so as not to adversely distort the NIM stakeholder distribution.

Parameters

- Block time: as fast as the network allows
- Block reward: to be determined
- Max block size: to be determined
- Total supply: 21B Coins divisible by 100'000

Team Nimiq is currently consulting with experts in economics to optimize reward distributions. Details to be announced *soon*.

Albatross NEW

Albatross is a new proof-of-stake consensus algorithm that improves on the current state-of-the-art by reaching a performance close to the theoretical maximum for a single chain. A [technical paper describing Albatross \(https://arxiv.org/abs/1903.01589\)](https://arxiv.org/abs/1903.01589) was published in March 2019 by members of Team Nimiq in collaboration with Trinkler Software. The Albatross consensus algorithm is inspired by speculative Byzantine-fault-tolerant (BFT) algorithms and then improves on classical BFT algorithms by adding what we call the “optimistic approach” which increases speed and efficiency without sacrificing security.

Classical BFT algorithms provide consensus in distributed systems while considering a limited number of malicious or Byzantine actors. One of the most prominent examples of such an algorithm is PBFT, which the Tendermint cryptocurrency is leveraging at its core for example.

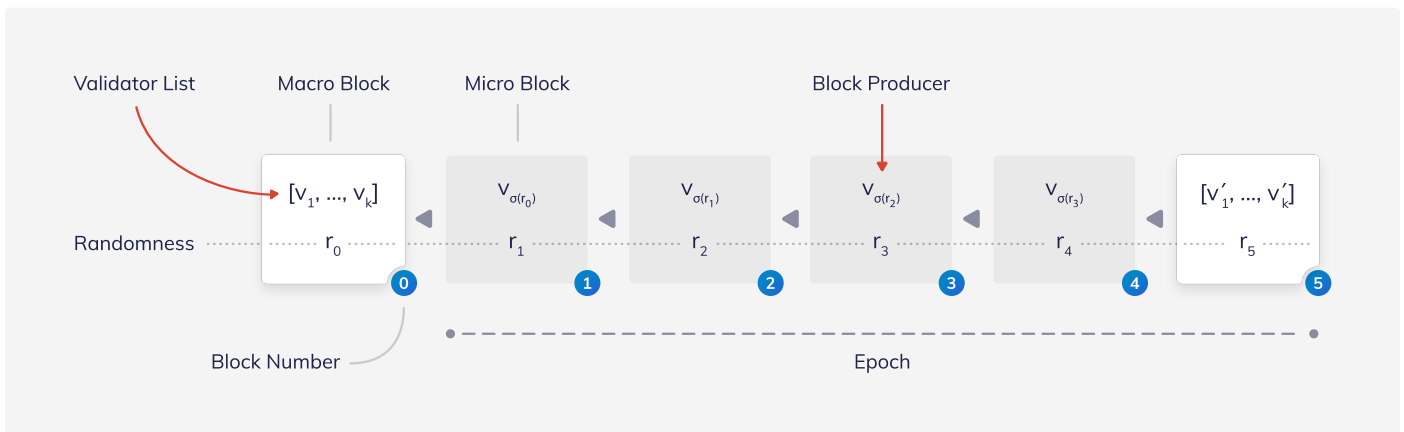
A new advancement over Classical BFT algorithms are Speculative BFT algorithms. They allow for drastic performance increases in the case of no malicious actors being present. This is the so-called **optimistic case**. In case Byzantine actors are present and try tampering with the protocol, other network participants will notice and switch the protocol into its slower and more conservative mode, offering the same security guarantees as standard BFT protocols. Otherwise, in the best case, the optimistic consensus algorithm is able to perform much better than classical ones, while still having a performance similar to standard ones in the attack case.

Team Nimiq is also working on optimizations for Albatross such as [Handel](https://github.com/consensys/handel) (<https://github.com/consensys/handel>), which is a fast multi-signature aggregation protocol. New research results and developments will be added to this whitepaper accordingly.

Block Production NEW

In proof-of-work blockchains, every new block is mined (created) by a node from the network, called a miner. In Albatross, the nodes that are responsible for producing new blocks are called validators. Anyone who has a stake in the system can volunteer as a validator by depositing their stake as a security that can be *slashed* as a punishment for misbehaving.

Block production in Albatross is divided into epochs. As the following figure shows, each epoch consists of a constant number of micro blocks — four micro blocks in the example below — followed by a macro block. Micro blocks contain the transactions and have a single block producer that is randomly chosen from the set of validators. While anyone can volunteer to be a validator, the actual set of validators in a given epoch — the active validators — is chosen by the macro block of the preceding epoch.



In the example above, block number 0 determines the active validators v_0, \dots, v_k for the epoch from block 1 to block 5. To be able to randomly choose the next block producer from the list of validators, each block contains a random beacon, depicted above by r_i . The block producer of a block uses a so-called Verifiable Random Function (VRF) to produce the next random value r_i from the previous value r_{i-1} . Every other participant can then verify the correctness of the next random value.

Given these random beacons in each block, every participant of Albatross is then able to determine the next block producer $v_{\sigma(r)}$ from the list of active validators. The production of

micro blocks is thus as simple as the selected block producer putting transactions into a block, signing the block cryptographically, and sending the block to the network.

The production of macro blocks is a bit more involved but happens much more rarely. Macro blocks are built using the classical PBFT protocol. To this end, the chosen block producer — or in this case rather a proposer — constructs the next random value and, from this value, determines the new list of active validators for the next epoch. The list of validators is chosen from all volunteers weighed by their stake and based on the random beacon. The block proposer then publishes its proposal, and all other active validators vote on it in two rounds. Macro blocks do not contain any transactions. There is no notion of targeted block time between blocks, and thus blocks can be produced almost as fast as the network allows.

Handling Malicious Actors NEW

The Albatross protocol remains secure under the assumption of at most $\frac{1}{3}$ of the validator list being Byzantine actors. These actors, however, can temporarily slow the chain and put block production into the more conservative mode. Byzantine actors can mainly trigger two mechanisms:

- Forks, which cause the next block producer to pick one of the conflicting blocks and allow validators to slash the malicious validator's stake, and
- Delays, which causes another validator to produce the block instead.

A more detailed explanation of these cases can be found in the [technical paper \(https://arxiv.org/abs/1903.01589\)](https://arxiv.org/abs/1903.01589).

Compression NEW

*As a **blockchain streamlined for the web**, Nimiq must minimize the amount of data necessary for web users to achieve consensus.*

The following methods are built into the Nimiq Blockchain to reduce the amount of data a browser client needs to download in order to achieve the key functionalities of a decentralized payment system: reach consensus, check balances, validate received transactions, and send transactions.

UTXO-Accounts Tree-Hybrid NEW

For keeping track of balances, a hybrid of UTXOs and an Accounts Tree is being used. The current set of UTXOs is managed in a hash tree structure that consolidates the UTXOs for each non-empty address. This allows to easily prove and determine the balance of an address. The root hash of the tree is stored in each block header.

Nimiq uses a [Patricia Merkle Tree](https://github.com/ethereum/wiki/wiki/Patricia-Tree) to store the UTXOs for all accounts that are not empty. For each new block, the tree is updated, and the new Merkle root is stored in the header of the block to ensure consistency and agreement between nodes.

Storing UTXOs instead of account balances in the tree allows for more efficient pruning techniques and improves usability: in contrast to transactions in Nimiq 1.0, transactions do not need to provide a validity start height anymore.

Micro Block Pruning NEW

The concept of Micro Blocks in Albatross allows to create blocks as fast as the network is able to. However, at times of low transaction rates, nearly all of these blocks can be empty, wasting unnecessary space. Thus, all nodes are allowed to prune Micro Blocks once an epoch is finalized by a Macro Block. To compensate, Macro Blocks also need to commit to an accumulator summarizing all transactions that happened during the epoch. New nodes to the network can then download and verify the chain of Macro Blocks.

Recursively Composable Zero-Knowledge Proofs

Team Nimiq is currently conducting research in the applicability of Recursively Composable Zero-Knowledge Proofs to facilitate ultra-light clients. Such an approach is already being used by Coda, compressing their blockchain into a few kilobytes of data. While their approach relies on recursive composition of zk-SNARKs and thus requires a trusted setup, Electric Coin Company recently proposed a construction called [Halo](https://electriccoin.co/wp-content/uploads/2019/09/Halo.pdf) that eliminates the need for a trusted setup. Both approaches seem suitable to also compress Nimiq's Proof-of-Stake chain into a **constant size** proof.

Consensus

One of the advantages of the Nimiq's Browser Clients is that they are able to achieve **consensus*** on their own, without trusting in the information provided by any third party. This brings to the table a level of censorship-resistance on a par with cryptocurrencies such as Bitcoin, that, although having **SPVs*** (https://en.bitcoinwiki.org/wiki/Simplified_Payment_Verification)

available, always require a predefined third party node to broadcast transactions. The Browser Clients in turn will contact any Full Node on the network and are able to verify the data received, for example its own balance and if transactions have been included into the chain.

To allow Browser and Backbone Clients to reach consensus in various constraint environments, several browser APIs and compression techniques are being used as described in [Blockchain Streamlined to the Web](#). To suit each environment, multiple consensus levels are available and each consensus level defines a **Node Type**.

Node Types

History Nodes NEW

History Nodes download the full blockchain including all Micro Blocks thus requiring more storage. This node type should be used solely with Backbone Clients.

Full Nodes

Full Nodes download the entire Macro Block chain thus also requiring more storage. This node type should be used solely with Backbone Clients although, theoretically, it could run in a browser as well.

Light Nodes

Light nodes could potentially use [recursively composed proofs](#) to determine the current blockchain head state and then download parts of the [Accounts Tree](#) only. However, after initialization, it behaves like a Full Node. See [Compression](#) for details.

At the present time, Team Nimiq is working on an improved light node that only downloads the parts of the Accounts Tree required to process current transactions and blocks.

Nano Nodes

Nano Nodes are the preferred node type for Browser Clients, since they require less data to be downloaded in order to establish consensus.

Similar to light nodes, they could potentially determine the current state of the blockchain using [recursively composed proofs](#), but then only download block headers and the minimal

amount of information related to their own accounts. Once the correct state has been worked out, i.e. consensus established, account balances can be cryptographically proven to this type of node.

Pico Nodes

Similar to the Nano Node, it uses the Accounts Tree and account proofs. But instead of syncing block headers using [recursively composed proofs](#), it will first test if all its peers are on the same head hash (or a neighboring hash) and, if that is the case, it will accept that head as the correct one. This is also referred to as an optimistic approach. Only if it receives incompatible head hashes will it fall back to a nano consensus.

Leveraging available connectivity, this means consensus can be achieved almost instantly. The pico consensus is the latest development and expected to replace the nano consensus as new default as soon as it is fully established.

Seed Nodes

Seed Nodes are a common component of peer-to-peer networks. In the Nimiq Network, the Seed Nodes are Backbone Nodes set up specifically with one task in mind: serving as the entry point to the network (see [Network](#)). Team Nimiq provides a list of dedicated signaling Backbone Nodes called Seed Nodes to ensure users have a reliable entry point to the network. To maintain a decentralized architecture, Community Seed Nodes are also available and maintained by community developers.

Nimiq's **official Seed Nodes** implement the following security and high availability measures:

- Load balancing
- Architecture is scaled according to load
- Seed Nodes are distributed around the globe
- Load balancer and node servers are in close proximity to reduce latency

A list of Nimiq **Community Seed Nodes** is publicly available in a [community-maintained repository](https://github.com/nimiq/community/blob/master/seeds.txt) (<https://github.com/nimiq/community/blob/master/seeds.txt>). Community members are supported and encouraged to host Seed Nodes.

Scripts

Simplicity is the best formula when building a secure payment system, and simplicity means **no scripting language**. Nimiq's core feature is fast and secure payments. Nimiq intentionally does not have a scripting language, because projects such as Ethereum already focus on the smart contract problem. Nimiq is not trying to compete in this field. Instead, the goal is to be compatible with other blockchains so that Nimiq users who want to use advanced smart contract features are able to do so.

For enabling [Atomic Swaps](https://en.bitcoin.it/wiki/Atomic_swap) as well as potential off-chain transactions capabilities such as the [Lightning Network](https://en.bitcoin.it/wiki/Lightning_Network), Nimiq supports [Hash Time Locked Contracts](https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts) (HTLC) as part of the protocol.

To allow NIM to be locked in and released at a **certain time***, Nimiq supports Vested Contracts as part of the protocol as well. To prove Nimiq's long-term commitment, funds for team members, creators, early contributors, the Nimiq Foundation, and the Nimiq [Charity Foundation](#) are vested as described in [Nimiq Supply Distribution](#).

The protocol design allows further contracts to be added on demand in the future.

Nimiq Payment Ecosystem

All apps in the Nimiq Payment Ecosystem are built with ease of use in mind. Having a close bond with the community, Team Nimiq's vision is to enable the community to create amazing apps using the Nimiq Blockchain and supports developers in doing so with the [Nimiq Community Funding Board](#).

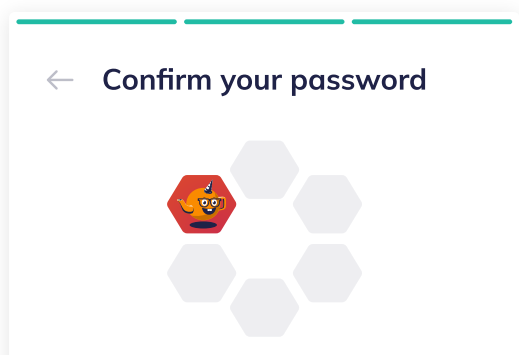
User Experience

A good and professional user experience is rare amongst blockchain projects. Technical knowledge and crypto-specific language are often required, rendering many solutions inaccessible to most potential users. As a result, it limits those solutions to the crypto sphere. Recognizing this significant barrier to entry for the average person, Nimiq is not only aiming to improve usability in the crypto sector but also to provide a user experience that exceeds fintech industry standards by utilizing the advantages of being browser-first. The intuitive user experience is an essential part of Nimiq and vital to translating the technical capabilities of the protocol into real-world value.

The aspiration to create the most accessible and easy-to-use blockchain payment system influences every decision. The most remarkable design choices steered by a usability-focused approach are:

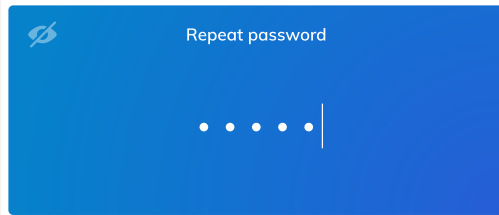
Fast and Easy Onboarding

The entry point for new users is designed for speed and simplicity and does not require downloads or personal data. By leveraging the browser-first nature of Nimiq, **new users can create an account with only three clicks.**



Successfully onboarded users are presented with a round trip through the ecosystem, focusing on the essential aspects of Nimiq: A small amount of NIM is dispatched to the newly created Account, which can then be spent at a webshop

This is your account with your first address in it.



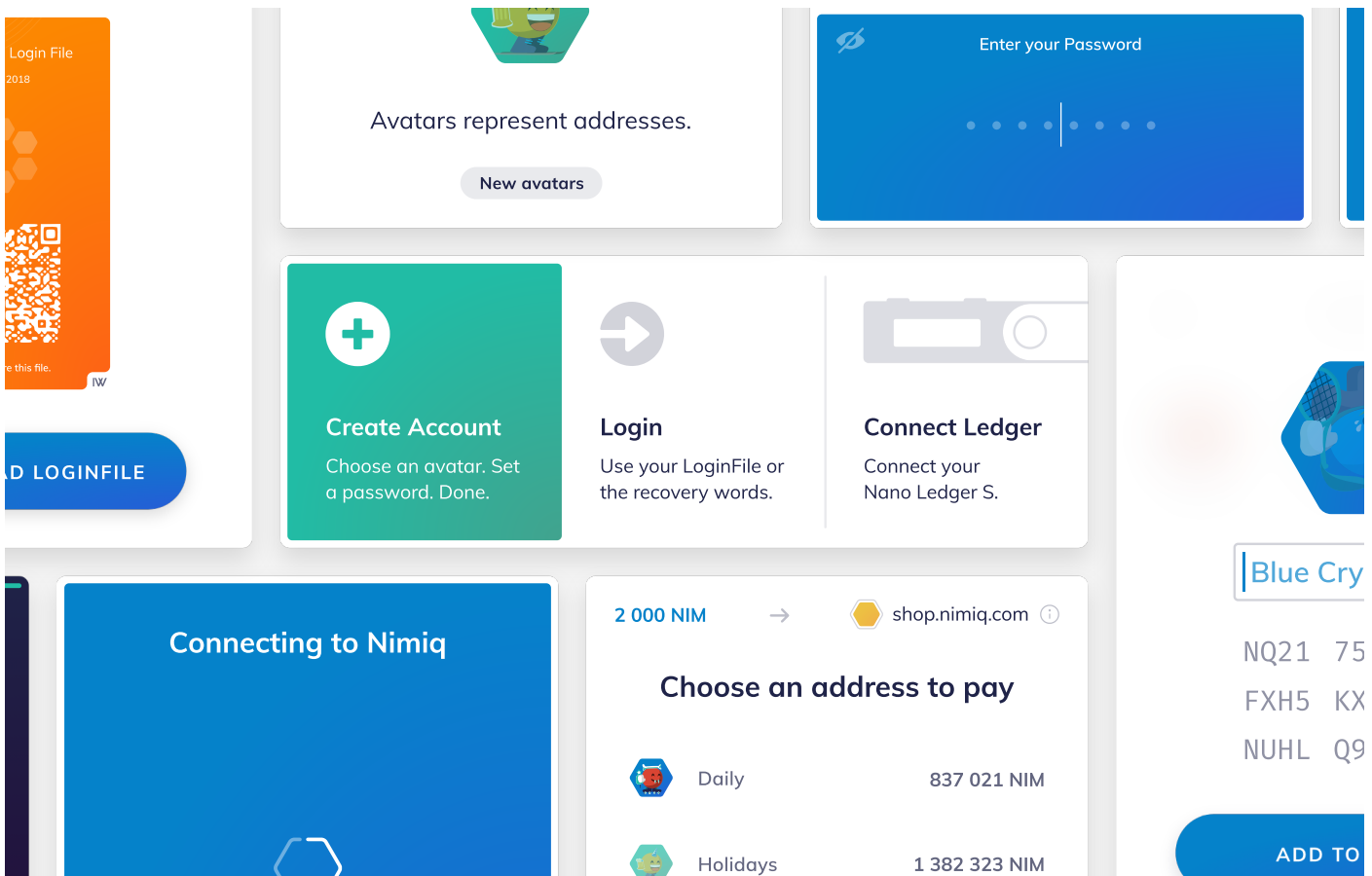
(<https://wallet.nimiq.com/?onboarding=signup>)

showcasing the Nimiq checkout experience.

Usability and Safety

More demanding user tasks, such as backing up the account, are not forced on users when they get in touch with Nimiq for the first time. Instead, this task is context-bound and only required later, when the Account actually holds value and the user is intrinsically motivated to do so, thus increasing usability without compromising safety. The backup can be performed by downloading a password-protected [Login File](#), providing an alternative form of backup to the cold storage (writing down) of the Recovery Words (24-word mnemonic seed).

Visual Identity



Focusing on simplicity and ease of use, Nimiq is built on a serene foundation: traditional colors, a minimal, geometric sans-serif font, and common layout patterns. We strive not only to push the boundaries of technology, but also the way we design our experiences and touchpoints, adding that bit of sophistication and edge that we believe makes the difference between convenience and fascination.

Nimiq is an open-source project that encourages developers to take part in the journey. Instead of dictating the way how the Nimiq ecosystem looks or feels, the intention is rather to provide the essence of our vision, stripped down to the very core, so that there's enough room for others to fill it out with their own ideas. To create a resilient visual foundation for Nimiq itself and for the community, we have gathered input from community members and conducted interviews with key stakeholders and the team from which we derived a common understanding of Nimiq as a brand: The [Nimiq Style Guide](https://nimiq.com/styleguide) (<https://nimiq.com/styleguide>).

Usable Denomination

A common hassle for users of cryptocurrencies is denomination. Time has shown that even if the mathematical value remains the same, 1.9 mBTC is easier to handle than 0.0019 BTC. This slight change in denomination creates a positive visual effect that we deem important for mass adoption of a cryptocurrency.

Considering this and inspired by Bitcoin, the total supply of NIM is 21 billion—21e9 NIM, shifted by a factor of 1'000 compared to Bitcoin—reducing the gap between minimum and maximum unit. The minimum unit of NIM is called a Luna and 100'000 Luna equal 1 NIM. This makes the total supply of NIM equivalent to 21e14 Luna, matching the total supply of Satoshis in Bitcoin.

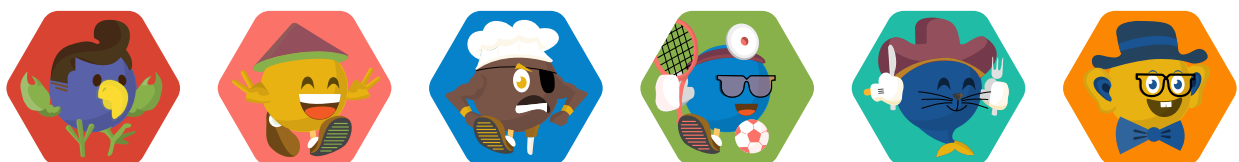
Addresses and Identicons

Addresses for Nimiq Accounts follow the International Bank Account Number format (IBAN). While this allows for frictionless integration with established payment providers in the future, it most importantly improves usability, as each IBAN has a built-in integrity check to prevent typos and is easier to read thanks to the standardized formatting. Each Nimiq Address starts with the code “NQ” followed by two characters defining the checksum for the remaining 32 characters, which are the actual address.

In addition to typos, clipboard hijacking has become a more common issue. In both cases the user will lose their funds if they are not able to verify the address. Nimiq has improved the concept of [identicons](https://en.wikipedia.org/wiki/Identicon) to create Nimiq Identicons, or “Nimiqons” for short. These are an easy-to-describe visual representation of a Nimiq address that allows users to visually verify that the address they intended to use is the one being used. This increases both the safety of the system as well as its usability. Furthermore, the Nimiqons turn a formerly dry and 'lifeless' address into a social and fashionable item that creates a wider sense of belonging.

Each Nimiq Identicon has a background color and four different body areas: bottoms, faces, sides, and tops, each with a distinct color. In total, Nimiqons are made up of a combination of 21 elements for each body part, 9 body colors, 10 background colors and 8 colors for parts.

That means $10 \times 9 \times 8 \times 21^4 = 140'026'320$ different Nimiqons can be generated. A slight change like a typo, or a replacement by malware will radically change the look of the associated Nimiqon. The highly differentiated and instantly recognizable Nimiqons look like this:



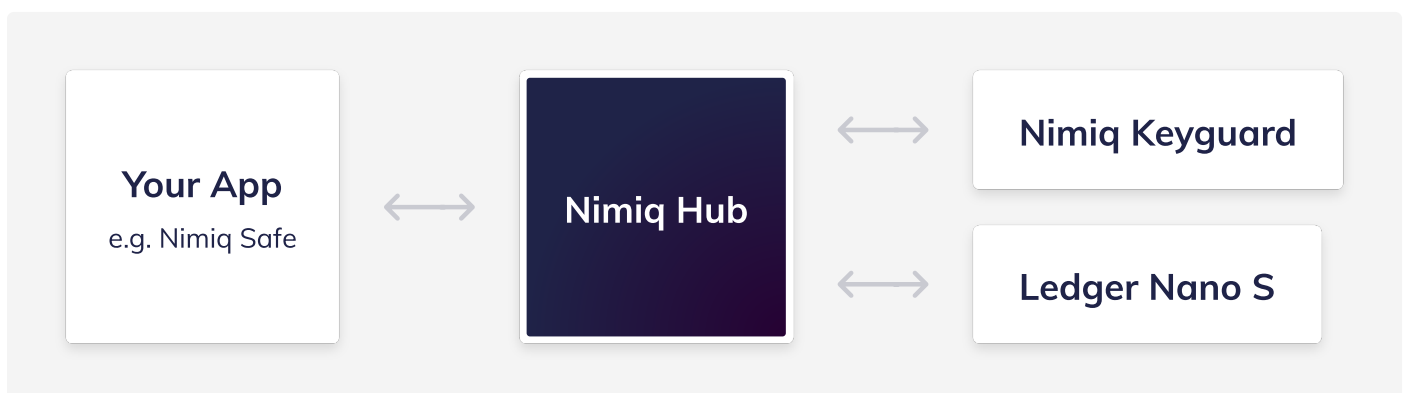
Every Nimiqon comes with a suggested label making it easy to describe.

Nimiq Wallet & Nimiq Hub

Payments should be frictionless, regardless of the device being used. Nimiq Wallet and Nimiq Hub provide an interface comparable to your online banking but with a decisive difference: It does not run on a server controlled by a third party. Instead, all data is stored locally, never leaving your device. Furthermore, usability and user experience are optimized for a smooth flow and do not depend on the platform or operating system being used. While Nimiq Wallet is the place where you can view your transaction history and balances, Nimiq Hub handles and stores a list of accounts, i.e. an address with a label, but never the keys. The keys are stored in a dedicated, highly secure location, such as a hardware and/or software wallet (i.e. Ledger, Nimiq Keyguard, etc). The Hub is positioned in front of the various key storage solutions, providing a unified interface for users to manage all their accounts that might be associated with multiple keys from multiple locations. Thus, the user will always see the same, familiar user interface wherever they make a payment.

To get started, a user can import existing accounts and create new ones. When requesting to send a transaction or a payment, Nimiq Hub is the interface where users are able to select the source account from which to move NIM funds, add a note for the recipient, or cancel the request altogether.

The concept of simplicity reaches all the way to the developer. Nimiq is making it easy to integrate payments by making it as simple as adding a JavaScript library. All major platforms and recent browsers are supported. Our Hub API supports both, async/await function calls and traditional top-level redirects with callback. At the same time, an ecosystem of wrappers and full integrations via plugins and modules is continuously growing.



The implementation of both Safe and Hub are, of course, open source and can be run self-hosted. They are intended to be an example for best practices and we encourage others to build their own solutions, enriching the Nimiq Ecosystem.

Supported Wallets

Following the principle of simplicity, the [Nimiq Keyguard](#) is a software wallet solution to get new users started instantly. It is optimal for day-to-day transactions, and while maximum care is taken with respect to security, the Keyguard is not intended to replace a hardware wallet when it comes to holding larger funds.

The first hardware wallet supporting NIM is the popular Ledger Nano S. Ledger's security maximizing approach is ideal for larger amounts and may also function as a cold wallet.

The first multi-coin wallet supporting NIM is Binance's [Trust Wallet](https://trustwallet.com/) mobile app. The integration was contributed by Nimiq Community developers.

Keyguard

Making things easy for the user to get started is crucial for onboarding new users and promoting wider adoption. For many users who are new to crypto, writing down 24 words and ensuring that they are in the correct order is a serious effort and a task that can prove too technical for many regular internet users just starting with cryptocurrencies. In particular, the initial step of asking users to get a pen and paper can feel archaic or intimidating, and can prevent users from trying out Nimiq spontaneously. To consider asking a first-time crypto user to set up a Hardware Wallet is out of the question.

Instead, the Nimiq Keyguard is a software wallet living entirely in your browser and is set up during the onboarding process. The Keyguard exclusively handles your private keys locally on your device. The entire process is streamlined to be smooth, short and simple. You create your account, set a password and are ready to go.

It is not necessary to write down your mnemonic phrase; all that can be done later. As soon as a user has gained a natural interest in Nimiq and, by holding NIM, also an intrinsic motivation to secure their funds, they will be glad to do the backup. In addition, the Nimiq Ecosystem apps will kindly remind the user.

The convenience is underpinned with strong security measures. Your private keys are stored locally, fully encrypted in the private storage of your browser, hosted on its own, secure

origin, isolated from other websites. Besides the mandatory [Security Considerations](#), to ensure the maximum security of your keys, the Keyguard is engineered with special security measures in place:

- It is entirely free of external dependencies, making sure that a changing or even malicious dependency cannot corrupt the behaviour of the Keyguard. This includes the build process of the app from its source code - it is a simple reviewable script.
- Each update to the source code is independently reviewed by at least two other developers in the team.
- Each potential new version is first deployed to the testnet for user testing by developers in the team and members of the community.

Login File

Avid users of cryptocurrencies are familiar with the complexity and potentially intimidating process of handling private keys and the need to write down and safely store mnemonic phrases on a non-volatile analog format, i.e. a piece of paper or steel in an airtight, fire-resistant container. Every time a private key is used in a raw format, there is a risk of it being stolen by a malicious party. To increase usability and safety, NimiQ provides the option of using a Login File that contains a password-encrypted version of the private key of an Account. This is formatted as a QR code and presented as an image file for the user to download and backup. This method allows users to easily store their private keys while still being able to use the 24-word representation as a secondary recovery method.



In collaboration with Trinkler Software, this concept has been standardized as ImageWallet, so that the same format can be used for other cryptocurrencies and as a general means of authentication.

Security Considerations

One of the main advantages of cryptocurrencies over fiat* (https://en.wikipedia.org/wiki/Fiat_money) is that the user has complete control over their funds. This means that security of the software through which users control their funds is crucial. Several members of Team Nimiq are exceptionally knowledgeable about cybersecurity due to their background and scientific research experience at the Center for Information Security (CISPA) in Germany. Before a new software release is published to the Nimiq Mainnet, it follows a strict audit process described in this section.

In general, code is written in feature branches and reviewed as pull requests. For it to be merged into the master branch, independent approval from at least one additional team member is required (in some cases, such as for the Keyguard, two approvals are required). Before the major release of particularly security-relevant parts, such as the Keyguard and Account Manager, code audits will be performed by developers outside the team that wrote the code. In a last step, the code enters the scope of the Bug Bounty Program for continuous public hardening.

Core-Specific Build Procedure

When a new release is ready, it is built within special-purpose, virtual machines where binary packages for Linux (Debian, Red Hat, and derivatives) and Windows are created. Afterwards, the packages are tested by installing them from scratch on clean systems as well as by upgrading to the new version in systems that already have the previous version installed. Finally, the packages are signed and committed to their respective deployment repositories, tagged with a signed tag, and signed by one of the team members.

Front-end-Specific Build Procedure

Before a new release is deployed, it is built and tested locally for correctness. It is then signed, committed and pushed to the deployment server. Finally, when a release is ready, it is approved for deployment by being marked with a signed tag. The Keyguard requires a tag signed by two members.

Deployment Procedure

The deployment server checks the prerequisites and replaces the old version with the new version. There is no server side build process or run time code execution; the server only serves static files.

The deployment procedure is first carried out on testnet servers to test the new version on a live system. If deployment is successful and the release is approved, the procedure is rerun on the mainnet servers.

Besides deploying apps and publishing binary packages on Nimiq's servers, libraries are built from the master branch and published as packages to the npm registry by a team member.

As an additional layer of security, [Nimiq has been working with HackerOne from early 2018 until 2020 and set up a US\\$200'000 Bug Bounty Program](https://medium.com/nimiq-network/public-bug-bounty-program-now-live-1eb09eee47ea) to incentivize security researchers and professional white hat hackers to look for vulnerabilities in the code and infrastructure of our network. The bug bounty program has since moved inhouse: [Nimiq Bug Bounty Program](#).

As part of this program, people who find and report a successfully exploitable bug in Nimiq's most security-critical code can earn as much as US\$20'000 for discovering critical vulnerabilities.

Before adding code to the scope of the Bug Bounty Program, it is first reviewed by several team members who were not involved in writing it. Each member will provide a short report and solutions will be discussed in meetings to resolve any issues. Only after the source code has passed internal testing does it become part of the Bug Bounty Program.

Peer-to-Peer Fiat-Crypto Bridge

Nimiq believes that in order to achieve mass adoption, the emerging crypto ecosystems will benefit from collaborating with the traditional financial system in complementary ways, providing freedom of choice. Cryptocurrencies provide a degree of censorship-resistance never seen before in the history of humankind. However, traditional centralized financial institutions are currently used and trusted by most people in the world.

Nimiq has made a solid step in this direction by setting out to develop the **Nimiq Open Asset Swap Interaction Scheme (OASIS)**, a middle layer that allows fiat currency to understand and interact with blockchain logic. In its first version, this innovative approach focuses on making Euro (USD, etc) bank accounts the programmable counterparty to non-custodial cross-chain transactions. In simple terms it means that in a non-custodial (Atomic Swap) transaction to buy or sell crypto, the counterparty can now be a fiat account holder.

With Nimiq OASIS already in development, the plan is that the first real-world transactions powered by it will be facilitated by WEG Bank AG on the banking side and a [DEX*](#) or market

making entity on the non-custodial crypto exchange side. In the spirit of decentralization, following an introductory period, OASIS will be open for other Banks and DEX to tie in.

WEG Bank AG is a fully licensed German private bank catering to corporate accounts and has recently started widening its scope in a way that selectively approaches the crypto space. After a successful collaboration process, Nimiq partnered with WEG bank and acquired a minority stake in the bank. As a result of this partnership and acquisition, Nimiq has new means of **interacting with the traditional financial system**. An example is Nimiq OASIS being able to leverage the SEPA instant banking network through WEG Bank. Combining Nimiq OASIS, WEG Bank and a DEX like Trade Telegraph would enable customers at any of the 2'000+ banks in **20 EU countries*** that are part of the SEPA instant network to exchange value between crypto and fiat systems. DEX Crypto-to-fiat swaps for NIM / BTC / ETH powered by Nimiq OASIS are targeted to become available by the end of 2019 / early 2020.

Making the Vision a Reality

Team Nimiq

In true blockchain spirit, Nimiq has a decentralized, horizontal team structure. Valuing quality over quantity, Nimiq consists of highly qualified, freelancing team members, cutting out the need for complex hierarchies and bureaucratic overhead. Areas of responsibilities belong to one or multiple team members who collaboratively work on them:

- Core
- Front-end
- UI/UX
- Communication & Marketing
- Infrastructure
- Documentation
- Operations

Areas of additional external services include:

- SEO
- Press
- Legal & Administration
- Local Community Managers

A detailed description of team members is available on the [team page](https://nimiq.com/en/#team) (<https://nimiq.com/en/#team>).

Nimiq Foundation

The not-for-profit Nimiq Foundation was set up to support the ongoing development and progress of the Nimiq Blockchain and Ecosystem.

The Nimiq Foundation was donated 2.5% of the final NIM token supply, the equivalent of 525'000'000 NIM. The Nimiq Foundation receives those tokens via a ten-year vesting contract (NQ09 VF5Y 1PKV MRM4 5LE1 55KV P6R2 GXYJ XYQF), securing the longer-term use of those funds. It also oversees the allocation of project funding contributions from the Token Event of Nimiq Network Ltd. The US-based Nimiq Foundation is governed by a board of seven members who are re-elected every two years. The board president is elected annually by the board. While to date the board has consisted of team members involved with the project since its inception, the longer-term vision is to broaden the governance and include community members as Nimiq's reach and the Nimiq Ecosystem mature to reflect the decentralized and global spirit as much as possible.

Roadmap: Milestones Achieved

Please find a high level roadmap below. For more details and the goals ahead, please visit [the official Nimiq Roadmap](#).

2017

- [First preliminary white paper \(https://medium.com/nimiq-network/nimiq-a-peer-to-peer-payment-protocol-native-to-the-web-ffd324bb084\)](https://medium.com/nimiq-network/nimiq-a-peer-to-peer-payment-protocol-native-to-the-web-ffd324bb084) published
- [Nimiq Betanet release \(https://medium.com/nimiq-network/introducing-the-browser-based-blockchain-63d408add368\)](https://medium.com/nimiq-network/introducing-the-browser-based-blockchain-63d408add368)
- [Fundraising \(https://medium.com/nimiq-network/nimiq-network-token-sale-terms-9af2e7fd6228\)](https://medium.com/nimiq-network/nimiq-network-token-sale-terms-9af2e7fd6228): reached cap of 60k ETH **in ten days** (<https://medium.com/nimiq-network/token-sale-finalized-closing-analysis-ee5b92d0cd9c>)
- [Luna Testnet released \(https://medium.com/nimiq-network/luna-has-landed-1da78170a88f\)](https://medium.com/nimiq-network/luna-has-landed-1da78170a88f)
- [Nimiq Identicons concept \(https://medium.com/nimiq-network/nimiq-identicons-8789b68e1668\)](https://medium.com/nimiq-network/nimiq-identicons-8789b68e1668) published

2018

- [HackerOne Bug Bounty Program](https://medium.com/nimiq-network/public-bug-bounty-program-now-live-1eb09eee47ea) (https://medium.com/nimiq-network/public-bug-bounty-program-now-live-1eb09eee47ea) started (since moved to [Nimiq Bug Bounty Program](#))
- [Activation tool for NIM from NET](https://medium.com/nimiq-network/attention-net-holders-a735d67d0e8a) (https://medium.com/nimiq-network/attention-net-holders-a735d67d0e8a) launched
- [Nimiq Mainnet launch](https://medium.com/nimiq-network/first-week-of-the-nimiq-blockchain-f34f9d3a6b32) (https://medium.com/nimiq-network/first-week-of-the-nimiq-blockchain-f34f9d3a6b32)
- [Pool mining server](https://medium.com/nimiq-network/nimiq-update-965e7148c3e1) (https://medium.com/nimiq-network/nimiq-update-965e7148c3e1) implementation released
- [First exchange listing](https://medium.com/nimiq-network/nimiq-past-present-future-9eca2496ff76) (https://medium.com/nimiq-network/nimiq-past-present-future-9eca2496ff76)
- Support for [Ledger Nano S](https://twitter.com/Ledger/status/1006174507751694337) (https://twitter.com/Ledger/status/1006174507751694337)
- Opened [Swag Shop](https://medium.com/nimiq-network/nimiq-swap-shop-b33eabb2e3ec) (https://medium.com/nimiq-network/nimiq-swap-shop-b33eabb2e3ec), showcasing Nimiq payment plugin for Wordpress: shop.nimiq.com (https://shop.nimiq.com)
- [First Transparency Report](https://medium.com/nimiq-network/transparency-report-74d4d89933fe) (https://medium.com/nimiq-network/transparency-report-74d4d89933fe)
- [First Community meetup in Amsterdam](https://medium.com/nimiq-network/nimiq-community-meetup-c8128400c582) (https://medium.com/nimiq-network/nimiq-community-meetup-c8128400c582)
- [Nimiq Community Funding](https://medium.com/nimiq-network/community-project-funding-9a0ebdbeb819) (https://medium.com/nimiq-network/community-project-funding-9a0ebdbeb819) launched
- Beginning of [crypto adoption research with TotalCrypto](https://medium.com/nimiq-network/nimiq-totalcrypto-io-cdfef4e22804) (https://medium.com/nimiq-network/nimiq-totalcrypto-io-cdfef4e22804): cryptoadoption.io (https://cryptoadoption.io)
- [End-of-life for NET token](https://medium.com/nimiq-network/and-then-there-was-only-nim-962f43a53aad) (https://medium.com/nimiq-network/and-then-there-was-only-nim-962f43a53aad) reached

2019

- Published [Nimiq OASIS](https://medium.com/nimiq-network/nimiq-makes-fiat-currencies-blockchain-compatible-7503096a6252) (https://medium.com/nimiq-network/nimiq-makes-fiat-currencies-blockchain-compatible-7503096a6252) concept
- [Announced Albatross](https://medium.com/nimiq-network/research-collaboration-albatross-63599386a7c9) (https://medium.com/nimiq-network/research-collaboration-albatross-63599386a7c9), a new, optimistic consensus algorithm
- [Nimiq integrated into Trust Wallet](https://medium.com/nimiq-network/trust-wallet-collaboration-b6b90c0bb1d5) (https://medium.com/nimiq-network/trust-wallet-collaboration-b6b90c0bb1d5)

- [Nimiq acquires stake in WEG Bank AG](https://medium.com/nimiq-network/nimiq-acquires-stake-in-weg-bank-ag-f2637b7b2e7a) (<https://medium.com/nimiq-network/nimiq-acquires-stake-in-weg-bank-ag-f2637b7b2e7a>)
- [New Nimiq Keyguard and Nimiq Hub](https://medium.com/nimiq-network/the-biggest-release-since-mainnet-launch-f8096e33dab9) (<https://medium.com/nimiq-network/the-biggest-release-since-mainnet-launch-f8096e33dab9>)
- Beta release of [full node implementation in Rust](https://github.com/nimiq/core-rs) (<https://github.com/nimiq/core-rs>)
- [Web shop plugin for payments with NIM](https://wordpress.org/plugins/woo-nimiq-gateway) (<https://wordpress.org/plugins/woo-nimiq-gateway>) has been released for WooCommerce on WordPress
- [Nimiq 1.0 Whitepaper](#) published
- [Cashlink integration](#) in Nimiq Wallet
- [Nimiq 2.0](#) white paper (this one here!)
- Testing of [Nimiq OASIS](#)
- Gift cards with cashlinks and QR code at nimiq.com/cards (<https://nimiq.com/cards>)

2020

- Intensive work on Nimiq 2.0 through out the entire year
- [Albatross demonstrator](https://www.nimiq.com/albatross/) (<https://www.nimiq.com/albatross/>) released
- Releasing [Cryptopayment.link](https://cryptopayment.link/) (<https://cryptopayment.link/>) and [Donation widget](https://www.nimiq.com/accept-donations/) (<https://www.nimiq.com/accept-donations/>)
- Nimiq OASIS closed beta
- First beta release of the [new Nimiq Wallet](https://wallet.nimiq.com) (<https://wallet.nimiq.com>)
- Vote on Nimiq 2.0 supply curve: [Results](https://www.nimiq.com/blog/supply-curve-for-nimiq-20-finalized/) (<https://www.nimiq.com/blog/supply-curve-for-nimiq-20-finalized/>)
- Albatross Alpha Testnet
- [Staking calculator](https://www.nimiq.com/staking-calculator/) (<https://www.nimiq.com/staking-calculator/>) for the upcoming Nimiq 2.0 with PoS
- BTC Support, crypto-to-crypto swaps, and multi-language support in the [Nimiq Wallet](https://wallet.nimiq.com) (<https://wallet.nimiq.com>)

- FastSpot API public release

For more details and the **roadmap ahead** see [the official Nimiq Roadmap](#).

Social Awareness

Crypto Adoption Research

Nimiq is passionate about exploring and evaluating potential pathways for mass adoption of cryptocurrency. Efforts include helping communities that are challenged by their financial infrastructure or monetary system in meaningful and responsible ways. Ideally it should open up the possibility of creating entirely new human and economic development models powered by crypto. These efforts led to Nimiq sponsoring [TotalCrypto.io](https://totalcrypto.io/) to create a crypto adoption proposal.

The first result of this sponsored research effort was an extensive Crypto Adoption Proposal, which can be viewed on [CryptoAdoption.io](https://cryptoadoption.io/). This initial research is entirely open content and anyone is encouraged to leverage this work to help develop their own crypto adoption methodologies as well as to improve the proposal. As such, the Crypto Adoption Proposal is a living document. In a next step Nimiq plans to evaluate potential case study candidates.

Adoption Research Overview

The Crypto Adoption Proposal put forward by TotalCrypto.io focuses not only on crypto adoption but also fostering wealth creation in the targeted area supporting its sustainability. The proposal advises drawing on the expertise and collaborating with academics, charities, and entrepreneurs to help refine, execute and enhance the academic value of the potential case study.

The current proposal comprises three components:

- A local exchange: To enable locals to swap crypto to fiat and vice versa. Additionally, this can also act as a cryptocurrency information center.
- Geo-targeted crypto airdrop: This would act as a one-off stimulus package for the area.
- Incubator: Focuses on promoting local economic growth by supporting locals with the know-how, tools, and resources to build online business and participate in the digital

economy in a more meaningful way.

The ultimate goal of Nimiq's crypto adoption research is to create a scalable blueprint for crypto-powered human development and adoption, which is backed by the execution of a tangible case study, the academic community, and other key groups. Most importantly, any research or data from Nimiq's crypto adoption efforts would be open source, as a wider contribution to the crypto, charitable and academic communities.

Nimiq is looking to commission crypto adoption case studies to evaluate potential locations and communities that could serve as initial roll-out internally, before making an assessment on whether and how to proceed.

Charity

Charity was built into the spirit and life-blood of Nimiq from day one. The team decided to set aside 2% of the final NIM token supply (420'000'000 NIM) for projects of high social and/or ecological impact. Nimiq wants to make sure that there is a counter-piece to the natural resource burden that securing blockchain initially with PoW entails, as well as manifesting a payment protocol that, through simply using it, will at least indirectly support good causes. As with the Nimiq Foundation, the ImpactX Foundation was set up to receive those donated funds via a 10-year vesting contract (NQ19 YG54 46TX EHGQ D2R2 V8XA JX84 UFG0 S0MC), securing the longer-term use of those funds and patience to build up its value over time. The US-based ImpactX Foundation is a not-for-profit, registered charity, governed by a seven-member board, currently matching the board of the Nimiq Foundation. This correlation is not necessarily expected to persist as the work of the charity and the qualification to steer it will likely differ in the future. The plan is to open its oversight to members of the community as Nimiq's reach and the Nimiq Ecosystem mature. The board will determine when the value of NIM held by ImpactX reaches a point where making a donation can make a difference without excessively draining its potential for additional grants. ImpactX plans to help fund projects that drive the vision of more sustainable societies, i.e. giving a chance to outstanding individuals, groups, and organizations in this virtuous pursuit.

Community Project Funding Board

Nimiq is passionate about being inclusive and empowering people to make a difference. To that end, Nimiq has created and sponsored the Nimiq Community Funding Board. Community members can submit project proposals to the Board requesting for assistance or limited seed funding in the following categories:

- Security audits, technical advice, and UI/UX design by Team Nimiq
- Application Hosting
- Miscellaneous costs required to create an MVP* or, in the case of a not-for-profit project, costs to maintain the project

The rules for the Community Board are simple:

- The Community Funding Board is made up of six members: Three community representatives and three from Team Nimiq
- Project funding proposals will be granted if more than 50% of the board accepts the funding proposal
- The Board meets at least every two months and discusses received proposals
- All decisions made by the Board are made public in a post on Nimiq's blog
- The Board members are replaced every six months

Up-to-date information about projects and proposals can be found in the [Nimiq Forum](https://forum.nimiq.community/t/how-to-request-for-project-funding/60) (<https://forum.nimiq.community/t/how-to-request-for-project-funding/60>).

Conclusion

Solving real-world scaling problems is one of the most important issues that various projects in the space are working on solving. Without a scaling solution, it is almost impossible for the current crypto payment technology to be widely adopted. But while a lot of effort has gone into improving scaling and speed of blockchain technology with very promising results (including the Albatross consensus algorithm), we are convinced that the limited adoption of cryptocurrencies is not only related to technical shortcomings.

Team Nimiq sees two driving forces behind adoption:

- Delivering **usability** and value incentives for average consumers in economically developed countries to switch from their familiar ways of payment
- **Accessibility** in countries with failing fiat currencies and financial infrastructure or a high number of unbanked people.

Additionally, crypto payment systems are struggling to bridge the gap between traditional banking and cryptocurrency ecosystems. Currently, the two ecosystems can be viewed as separate islands where it is not possible to directly and trustlessly transact value between the two. The research blueprint for Nimiq OASIS could provide the foundation for convenient and low-cost value exchange.

This whitepaper provided insight on how Nimiq is addressing these four angles: scalability, accessibility, usability, and **interoperability**. Nimiq aims to outperform traditional payment providers in terms of both convenience and costs, without falling back to centralized, closed platforms and services. Saying this, we see the greatest potential in identifying and addressing payment problems faced by consumers and businesses in both economically developed and less developed countries. Armed with this knowledge we would encourage migration to the Nimiq payment system with near zero-fee cross-border transactions combined with the convenience of a simple user experience and user-flow to enable barrier-free value exchange that is open to everyone. Nimiq is unique in furthering the essential features and ideals of cryptocurrency and blockchain technology by allowing users without prior technical knowledge to run a node in their browser with just the click of a button. Not using the network, but becoming part of it. Packaged in a beautiful, easy-to-use and well-documented ecosystem of applications, Nimiq stands for sovereignty of the individual,

censorship-resistance, self-determination, and freedom of choice: the true spirit of cryptocurrency.

[Create your account](https://wallet.nimiq.com/?onboarding=signup) (<https://wallet.nimiq.com/?onboarding=signup>). [Join the community](https://t.me/Nimiq) (<https://t.me/Nimiq>). Find out more on nimiq.com (<https://nimiq.com>).

Disclaimer

None of the statements must be viewed as an endorsement or recommendation for Nimiq, any cryptocurrency, or investment product. Neither the information, nor any opinion contained herein constitutes a solicitation or offer by the creators or participants to buy or sell any securities or other financial instruments or provide any investment advice or service. All statements contained in statements made in Nimiq's web pages, blogs, social media, press releases, or in any place accessible by the public, and oral statements that may be made by Nimiq or project associates that are not statements of historical fact, constitute "forward-looking statements". These forward-looking statements involve known and unknown risks, uncertainties, and other factors that may cause the actual future results, performance, or achievements to be materially different from any future results, performance, or achievements expected, expressed, or implied by such forward-looking statements.