SAHARA

March 2022

Sahara Protocol

White Paper

The idea of true blockchain privacy

Privacy is blockchain's biggest Achilles' heel. So we decided to do something about it.

Sahara is the first dedicated privacy protocol ecosystem that allows on-platform trade between stable and volatile assets.

In short, Sahara will allow users to enjoy the benefits of blockchain trade in true privacy. No more transferring funds onto separate chains with separate protocols. No more having to choose between volatile assets and financial privacy.

We're on a mission to make privacy possible for the future of finance.

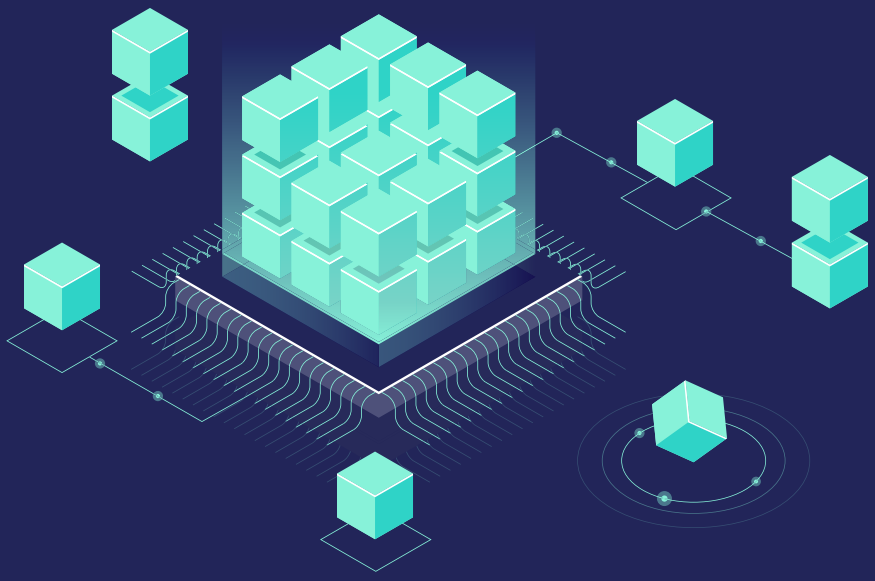
THE IDEA OF TRUE BLOCKCHAIN PRIVACY

Project background

Blockchain's come a long way since 2013. From thousands to billions. From cult niche to mainstream. But the one thing that's remained constant since Satoshi Nakamoto published his Bitcoin white paper almost a decade ago is transparency. The public ledger is a cornerstone of every blockchain. And while anonymous addresses were meant to ensure similar privacy to the one offered in traditional financial systems, that's just not the case as things stand now.

Find the transaction, you find both the recipient and sender address. Putting two and two together becomes a whole lot easier when everything is tracked in public, and today the following things directly threaten the privacy of the blockchain user:

- Enough location data (even when it's pseudonymous) can make individual identification possible
- By monitoring communications between different nodes on the blockchain, it's possible to link transactions to internet protocol addresses
- Wallet software can be forensically analyzed and so linked to the individual - without passphrases and keys



The main problem with blockchain today and the above-mentioned points of concern is that the maintenance of privacy lies in the hands of the user. Navigating the tech required to make sure the things you want to keep private stay private is challenging. Navigating crypto, DeFi, and synthetic assets trading is tricky, too. The combo is a minefield, especially for novices. Unless they're experienced, users won't know how to maintain their privacy with watertight accuracy. And so it's easily lost - at the expense of the transparency blockchain lives and breathes.

You can secure your privacy with protocols, sure. But they can only be activated once your funds have been converted into the protocol's native chain, and that chain's native token. Which tend to be highly volatile.

Additionally, in order to even start trading, more and more personal information is required from users. If you want to set up an account on Coinbase or another blockchain entrance platform to buy your first Ethereum or Bitcoin, you must leave your ID name, your address, and your banking details. More and more, it feels like banking - not disruptive, decentralised finance.

Blockchain is slowly merging into a hybrid version of disruptive and traditional. So how do you navigate all of this and create something that allows total privacy and maintains the pillars of blockchain's functionality - all the while making sure things stay above board?

THE IDEA OF TRUE BLOCKCHAIN PRIVACY

The future of blockchain privacy: by Sahara

Blockchain is the future of finance, there's no doubt in our minds. But if this disruptor is going to take the big step forward to join the ranks of big banks and stock exchanges, it needs to have all bases covered. Privacy is a massive part of that. As people around the world are becoming increasingly aware of how important it is to protect their personal data, this won't just be a flashy benefit for blockchain finance - it'll be a consumer demand.

And it needs to be easy. Mass adoption will never take place if we can't offer users the same luxuries they've gotten used to in traditional financial systems.

So what's Sahara going to do? Tick as many boxes as possible. Starting with ease of privacy.

We'll give traders and users the power to choose between more than just big chains and keeping their financial affairs private. By creating a comprehensive protocol ecosystem, Sahara will make that dream of trading in privacy - without switching to separate privacy-dedicated chains - come true.

This ecosystem will expand, and cover more and more blockchains as our project develops. Ultimately, Sahara will become the universal privacy protocol for crypto and DeFi traders worldwide.

THE IDEA OF TRUE BLOCKCHAIN PRIVACY

Sahara's main features

True trading privacy

Privacy is a philosophical pillar of blockchain technology. But as the space has grown vaster and vaster, the responsibility of privacy has become an increasingly tough nut to crack. Now it's up to the individual users to ensure they keep their affairs private. Navigating this has proven a challenge, and continues to be a massive thorn in the side of blockchain users worldwide.

With Sahara, a relay and anonymity set functionality takes the worry of privacy off the hands of the end user. So they can trade like they're used to, without having to stay on top of keeping this private, too.

Multiple networks and on-platform trade

You can have privacy on the blockchain today. You just can't have it while staying on the big chains like Ethereum or Binance. That's because privacy protocols are reserved as separate functionality on separate chains. These chains carry their own tokens, which are often highly volatile - and not the token users may have wanted to trade in the first place.

Sahara is building on multiple blockchains, and will launch on Polygon and Ethereum, with Binance, Avalanche and Solana to follow. It means end users will be able to keep trading the assets they want to trade, in complete privacy.

Synthetic assets protocol functionality

Synthetic assets have become particularly popular amongst blockchain traders who want the benefits of crypto trading, with less volatility. These assets allow the users to trade in real-world assets that back the value of the blockchain token equivalent. But guess what?

Privacy is just as elusive in this space as in every other blockchain trading context.

Sahara is the first privacy protocol ecosystem that enables on-platform trade between volatile and stable assets. With full functionality for synthetic assets, Sahara thus opens up the world of blockchain and crypto to an even wider scale of user adoption.

Privacy-oriented NFTs

NFTs are taking the decentralized world by storm. Art, in particular, is becoming huge on the blockchain, with everything from hobby enthusiasts to renowned artists creating digital art and selling it in some seriously massive deals. Maintaining privacy when you want to buy or sell NFTs is no joke, whether you're an artist or art collector.

Sahara will make it possible for artists to create, sell, lease, and own their art with privacy-oriented NFTs that combine the power of non-fungible with the importance of keeping things private and protected.

Privacy-oriented metaverse

On-blockchain metaverses are launching everywhere and have marked a big step further on the way to Web 3.0. As users from across the globe participate in these interactive, decentralized experiences, they're also witnessing first-hand how important (and elusive) privacy is as your identity moves into the metaverse.

Sahara will launch its own privacy-oriented metaverse as part of the protocol's ecosystem. This will make it possible for users to enter the metaverse with a private identity and enable private land purchases within the platform.

Sahara is a privacy revolution, bringing one of the founding pillars of blockchain technology back to its modern expansion and functionality. It will empower users everywhere and help fuel large-scale mass adoption of decentralized financial services.

Where does blockchain privacy stand today?

As we've already established, blockchain is a double-edged sword where privacy is concerned. Users are currently struggling to maintain their financial privacy, and it's becoming harder and harder as the technology expands and develops. This is due to two primary problems:

1. Maintaining privacy is in the hands of the user, which most individuals aren't used to - and maintaining privacy is complicated. Traditionally, we've relied on banks or other financial institutions and their privacy protocols and procedures to do this job for us. Decentralized trading can also be a complicated affair, which makes privacy maintenance an even bigger challenge.

2. Blockchain is becoming a hybrid version of what it once was: It's neither cult nor mainstream. To start trading on an entry-level platform like Coinbase or similar, you're required to provide considerable amounts of identity-revealing information about yourself, which only strengthens the feeling that blockchain is becoming increasingly centralized. And adds more individualized data points about the user to the system.

WHERE DOES BLOCKCHAIN PRIVACY STAND TODAY?

Current solutions to the privacy problem

User-managed privacy

The only way for blockchain users to maintain their financial privacy is by familiarizing themselves with the steps they need to take in order to make sure no one links their individualized data to their transactions. This is a considerable undertaking. It would require the use of complicated and sophisticated privacy software, as well as diligence around things like avoiding the use of location services on their phones. And even then, transactions are public on the blockchain. If someone were to make the connection between transactions and person, it's impossible to erase the information because of the nature of blockchain's design.

Privacy protocols

A number of blockchain projects dedicated to privacy have launched in recent years. That's because users are experiencing and seeing first-hand how hard it is to maintain control over their financial information while trading on the blockchain. In order to make use of one of these privacy protocols, however, the user needs to migrate their assets and funds onto the protocol's native chain before the protocol can be activated. The tokens on these blockchains are typically highly volatile, and the transactions also mean cost and unnecessary transactions - which are, again, forever carved into the blockchain's public ledger.

WHERE DOES BLOCKCHAIN PRIVACY STAND TODAY?

What solution do we actually need?

Neither existing solution is ideal. With user-managed privacy, you either need to be a highly technical person - or accept the fact that your details aren't as private on the blockchain as you'd like them to be. With privacy protocols currently on the market, traders are forced to convert their assets to often volatile tokens before they can activate the chain's privacy protocol. That poses a whole other group of problems in and of itself.

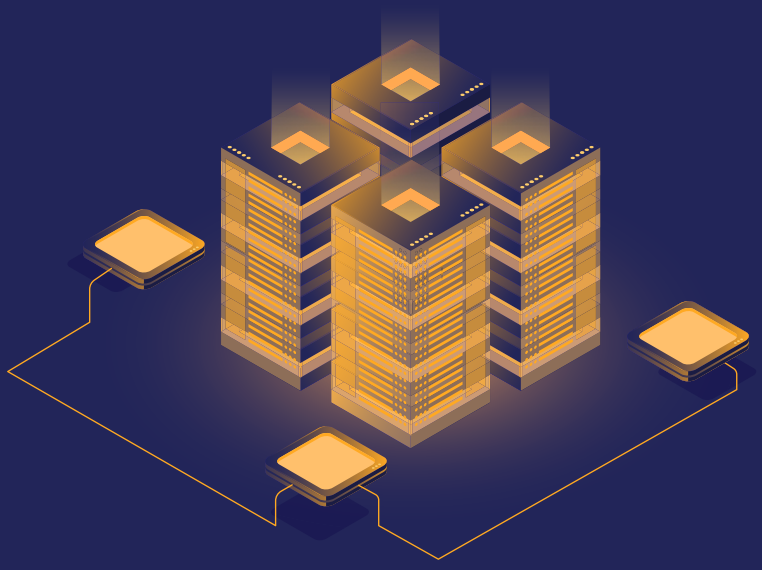
The solution we need is one that combines both, and solves the privacy problem without taking from the users' freedom to trade the assets and cryptocurrencies they'd like to trade. What this means is a privacy protocol that can be activated on multiple chains and that runs as an all-encompassing ecosystem for maintaining each individual's right to privacy. This way, you effectively solve the privacy problem, without forcing a trade of lower-value volatile assets.

Where is blockchain privacy headed?

Blockchain privacy and its issues: *A quick recap*

So, what went wrong with financial privacy on the blockchain? In the beginning, blockchain and Bitcoin seemed to be a joint utopian solution to both the issue of centralization and equal access to global financial systems. People would no longer be dependent upon banks or other financial institutions, they would maintain their privacy, the system would be decentralized and so inflation-proof, and it could all be managed with a smartphone.

The primary issues of maintaining financial privacy arose as a result of two main things: The growth of blockchain and crypto interest and market cap - and the continued expansion and development of technology. With more sophisticated location data trackers, more individualized data points are now collected from our phones. With several hundred billion circulating in crypto, the market has obviously become vulnerable to people with criminal intent. And with an enormous expansion of different types of digitized assets, blockchains, and projects, traders are faced with an increasingly complicated jungle in which to navigate with their privacy intact.



WHERE IS BLOCKCHAIN PRIVACY HEADED?

Growth of blockchain markets

We're past the days where people genuinely considered blockchain a fad. That's just not looking like it's going to happen. Even with its volatility, even with its ups and downs, this market just keeps growing, both in terms of reach and in terms of cap. Fewer and fewer whale holders dominate the market, and more and more individuals choose to tap into cryptocurrency, even if it's just to dip their toe in the water. At a governmental and legislation level, nations are opening up to blockchain as a possible solution in an array of different industries and sectors. Some have even launched their own national cryptocurrencies.

The speed of blockchain's market growth also puts enormous pressure on it. If decentralized solutions are going to step up as real contenders to centralized ones, they can no longer lean on cult status. They must present viable alternatives to existing services, and that means covering the same areas for the end user as centralized options do today. The next big step for blockchain to propel market growth even further is to establish itself as a globally accepted option. A key component of making this a reality will depend on solving the issue of privacy.

WHERE IS BLOCKCHAIN PRIVACY HEADED?

Privacy forecasts

Cryptocurrency

Cryptocurrency is the blockchain market segment that's gotten furthest in terms of user spread and worldwide adoption. In the form of Bitcoin it's been there since the very beginning, and is where most people usually start their decentralized journey. Cryptocurrency still presents a highly volatile market and this volatility is a main reason for adoption reluctance. So far, only about 4% of the world's population has chosen to invest in cryptocurrency, and established institutions are sceptical to say the least.

If cryptocurrency is going to function as a viable option to fiat currencies, it needs a framework around it that ensures the same level of privacy as these established currencies do. The end user will value financial privacy more than the benefits of decentralization.

DeFi

DeFi was launched as a direct opposition to traditional, centralized financial systems. They were intended as a means to give the individual user more power to operate in finance - without banks or middlemen setting the framework rules. DeFi applications run on the basis of smart contracts, and offer everything from exchanges, lending platforms, stablecoins and prediction markets to the more recent concepts of yield farming and liquidity mining to mention a couple.

In finance, privacy is everything to the end user. In other words: For DeFi to continue to grow and contribute to mass adoption of decentralized products and services on a global scale, it must provide this essential functionality to its users.

Metaverse

The metaverse is an old idea that goes back to immersive video games, but on the blockchain it's turned into something different and substantially bigger. With juggernauts like Facebook changing their entire business development trajectory to tap into the possibilities of the metaverse, these virtual realities are likely to expand massively in the next couple of decades. The only problem? Privacy.

The tracking possibilities in the metaverse are incredible - and terrifying to the end user, especially those who are already familiar with the amount of identity tracking we are exposed to on a daily basis. When entering the metaverse via the blockchain, it'll be essential for people to protect their privacy and be in full control of what information is shared, and what information isn't.

NFT

Non-fungible tokens have taken the blockchain by storm, and in 2021, the NFT market surpassed $40 billion. Nowhere are these data packets more applicable than in the digital art world. They allow artists to create the same unique pieces of work traditional art creation and trade has previously held monopoly over - and the interest is immense. When you buy an NFT, you effectively buy the digital version of a bespoke piece of art, and the prices are staggering. Beeple by Mike Winkelmann was sold for a record $69 million USD.

Now, as the NFT market grows and expands, privacy becomes an issue here, too. The exact same issues other blockchain-based solutions pose. And just like art dealers and traders of traditional, physical art reserve the right to maintain anonymity, privacy will become an increasingly afterthought property of NFT projects as well.

WHERE IS BLOCKCHAIN PRIVACY HEADED?

User demand and mass adoption

Now, the question on everyone's lips - certainly anyone involved and invested in a blockchain project of any kind - is as follows: What will need to happen in order for global mass adoption of blockchain-based solutions to take place? Ultimately, that's what will ensure continued market growth and continued technological expansion, as well as the normalization of decentralized products and services.

The growth of any market is dependent on user demand, and user demand is driven by self-interest. Which problems will blockchain solve for users across the globe? And what does the offering actually look like? Consumers are rarely willing to opt for something completely different if that something is just the same as - or an inferior version of - what they already know.

The right to privacy will be one of the main hurdles to overcome if blockchain is to succeed on the path to mass adoption. Whether it's in banking, art, or social interactions, the individual user will only ever be likely to accept the unknown if it comes with a superior offer. Decentralized with embedded and complete privacy is that something superior.

Sahara's solution

What is Sahara?

Sahara is a multi-chain privacy protocol running on Ethereum-based blockchains. It's the world's first ecosystem that enables on-platform trade between volatile and stable assets. Sahara gives blockchain users power back over their financial privacy while operating on the blockchain - without forcing them onto separate chains with separate privacy protocols and tokens.

As it expands and launches on more and more blockchains, Sahara will become the universal privacy protocol for crypto and blockchain traders worldwide. With a user-friendly interface, comprehensive functionality that supports both DeFi and synthetic assets, and plans to expand into NFT and the metaverse, Sahara is part of the solution for blockchain mass adoption.

How does it work?

The Sahara platform's main functionality is based on the collection of smart contracts, which are embedded with technology that ensures user privacy and eliminates traceability. Firstly, Sahara uses non-interactive zero-knowledge proofs for all deposit transactions. If used carefully, this breaks linkability between a deposit and a new withdrawal address.

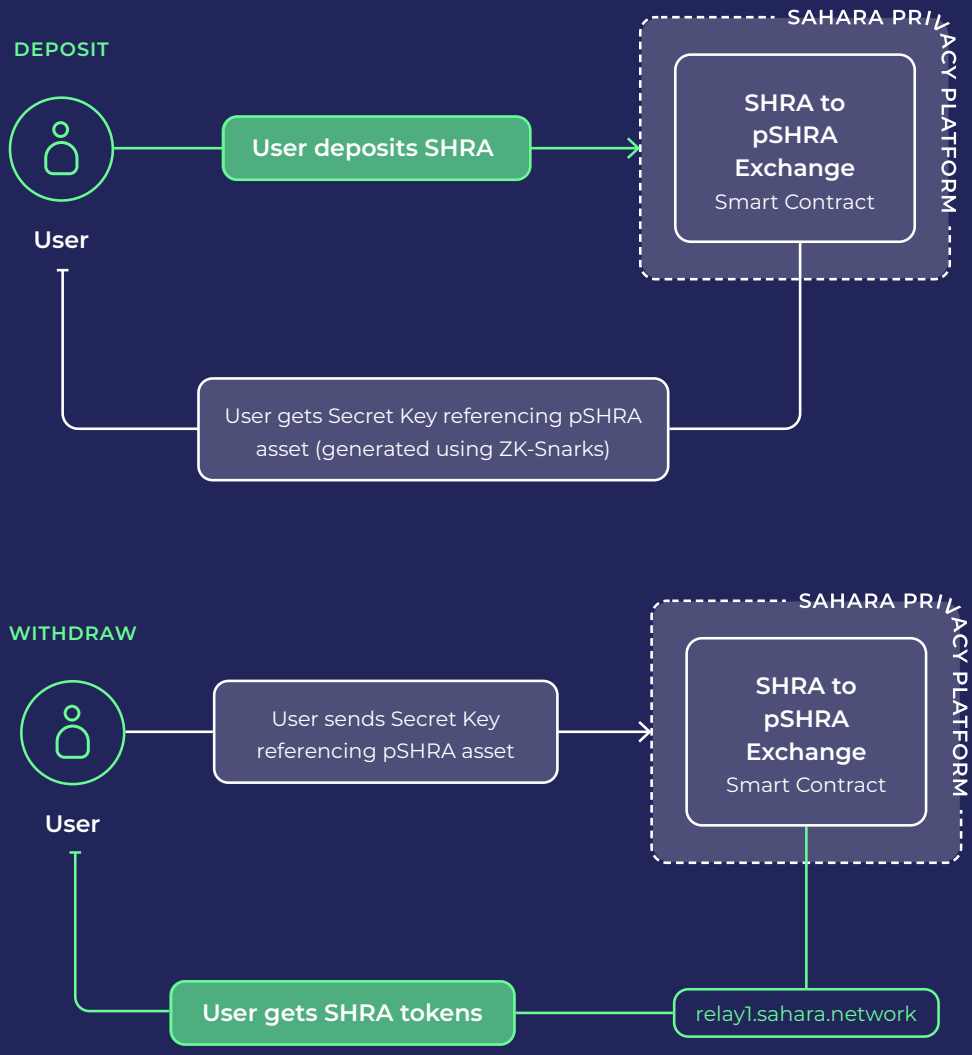
At the transactional level, Sahara implements two main technologies to be able to provide on-platform trade in complete privacy:

Anonymity sets: These are sets of users that the most recent transaction could have been made by. The higher the number of users, the greater the anonymity - and so privacy - for the given transaction. This anonymity set suggests that, given a withdrawal transaction, the corresponding depositor can be hidden among the specified amount of addresses. If 0.1 ETH is traded, it's harder to analyze a set of 1000 addresses than a set of 10, for example. The anonymity set is recalculated after every transaction that takes place in the Sahara ecosystem.

Relayer functionality: In addition to the embedded anonymity sets, Sahara is also designed with relayer functionality, which is optional, but highly recommended for withdrawal transactions. Relayers break the link between sender and recipient addresses by pushing the transaction through multiple stops, without changing the withdrawal data or recipient address.

SAHARA'S SOLUTION

Sahara's tech

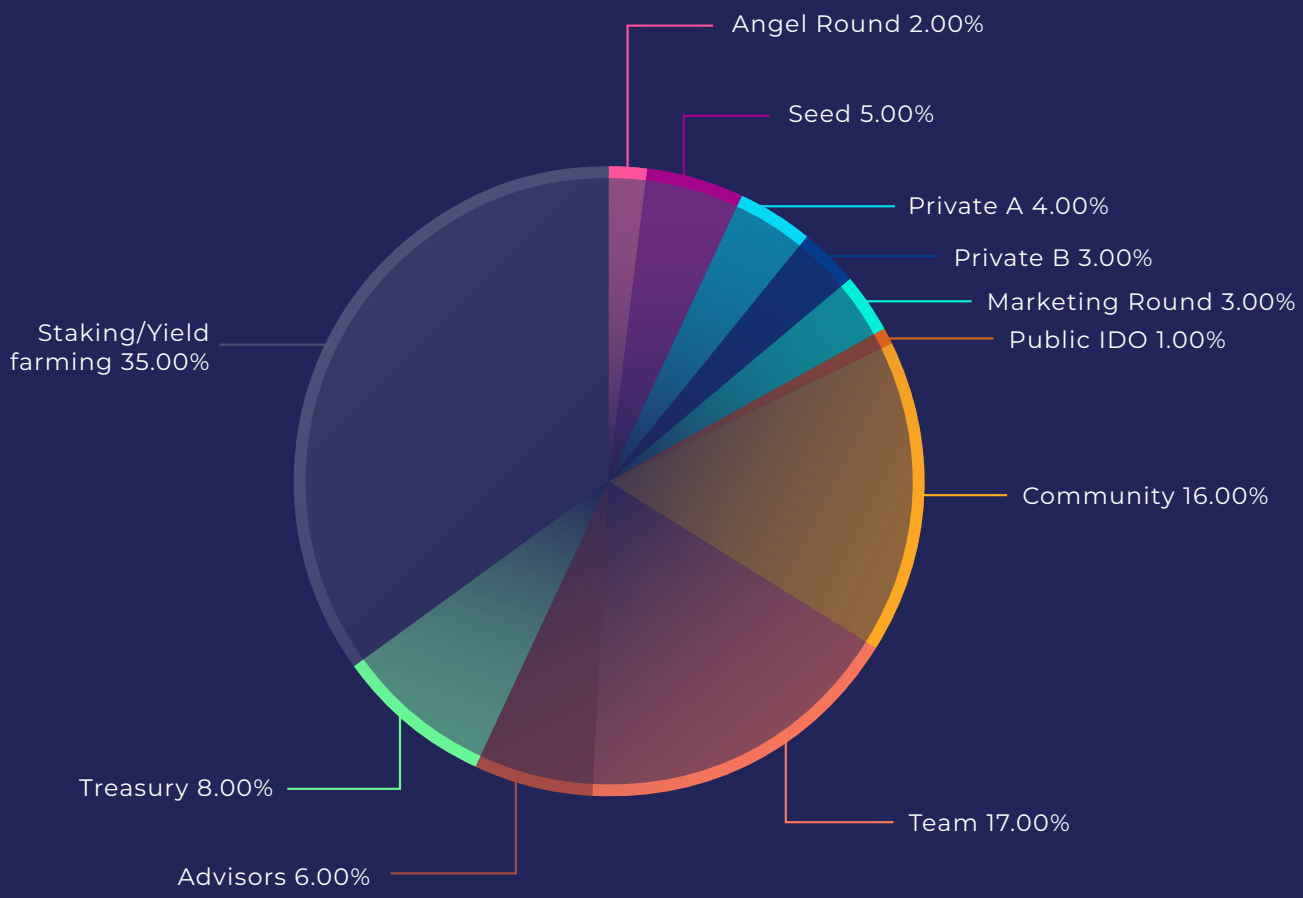


Wireframe on how users will deposit and withdraw SHRA-tokens by Secret Key generated using ZK-snarks to a chosen wallet.

The technological infrastructure supporting Sahara has been developed by SUPER HOW, a 24-developers strong company with considerable experience building blockchain companies from the ground up.

SAHARA'S SOLUTION

Sahara's tokens



Token value and functionality in the Sahara ecosystem

Token Name	Sahara
Ticker Symbol	SHRA
Token Decimals	18
Token Background	ERC-20. Launching on Polygon and Ethereum
Token Type	Utility
Token Sale Date	–
KYC/KYB Required	–
Restricted Countries	–
Project Status	MVP ready and beta version launched on testnet

Sahara's on-platform transactional economy is powered by the SHRA token, which is a utility token with an initial market cap of $195k. It is designed to serve stakeholders and their activities throughout the platform, as outlined below.

Deposit and withdrawal

By depositing SHRA tokens into the Sahara protocol, investors can use the platform services privately: Private swap, private staking, buy/sell NFTs privately, farming, voting, and so on. Platform users can claim their rewards - staked or deposited SHRA tokens - by using withdrawal with previously received non-interactive zero-knowledge proof of transaction. To increase anonymity users can also use relayers to receive funds to new empty wallets.

Staking

Sahara platform users will be able to stake SHRA tokens in order to make their assets work for them by generating rewards privately. The privacy will be ensured by linking the proof of transaction with staking within the Sahara ecosystem - not to a user's wallet, as is usually the case.

Private swap

By using SHRA tokens, investors can enter the platform's exchange service where they can swap any synthetic token in complete privacy, which will be achieved by using mixer contracts for each token supported by the Sahara platform.

The future of Sahara

Sahara is launching in Q1 2022 - but that's just the beginning.

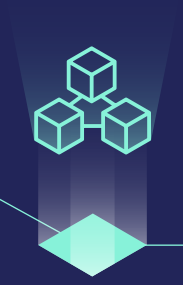
We believe in decentralized mass adoption. We also know that the only way that's ever going to happen - that blockchain is going to become a true competitor to traditional, centralized institutions - is by giving end users a better offer than the one they're currently using.

Sahara is thinking big and building bigger, far beyond a simple privacy protocol for trading crypto.

Multiple chains

Sahara launches on Polygon and Ethereum, with Avalanche, Solana, and Binance Smart Chain to follow. But we don't really see a reason to stop there. The privacy protocol is built compatible to be launched on any EVM-based platform out there. The goal is to make Sahara the obvious and preferred choice for any user looking to protect their privacy while moving around on the blockchain.

Sahara goes directly against previous privacy solutions in that it embeds itself on existing platforms - rather than forcing users to move away from the big chains and having to exchange their assets to a volatile token in the process. Privacy shouldn't be a choice between the assets you'd like to trade or decentralized solutions you'd like to explore. So we're making sure it isn't.



Our vision: The metaverse and NFTs

The metaverse and NFT expansion is real. In the coming years, it's likely we'll see more and more of this technology launching in different decentralized forms. NFTs represent digital ownership - comparable to physical assets today - and considering the immense amount of money being poured into non-fungible tokens, privacy will become increasingly important to end users. Owning extremely rare artworks or even property can put you at risk if the ownership is for the entire world to see. In the metaverse, privacy is already becoming the single-most important topic of interest, as the tracking possibilities for service providers are immense.

Sahara will expand to a privacy-oriented metaverse and NFT protocol. This will provide collectors, users, and owners with the much-needed control over their own data as the transactions they complete and activity they undertake is recorded on the blockchains they frequent.

Our vision: The ethics gatekeeper

Privacy is a right. We should all get to decide what happens to our own data. The flipside of privacy in a decentralized setting is that it can also enable criminal or unethical activity. Sahara's vision is to - as the first blockchain-based service ever - step up and take an important responsibility in the fight against illegal actions on the blockchain. Our aim is to embed ethics into our privacy protocol, right from the design stage.

Currently in the research stage, our future ethics gatekeeper is intended to be programmed with a universal code of ethics. This will run atop the Sahara protocol, and will ensure any unlawful or unethical activity cannot be completed by making use of the privacy we provide.

THE FUTURE OF SAHARA

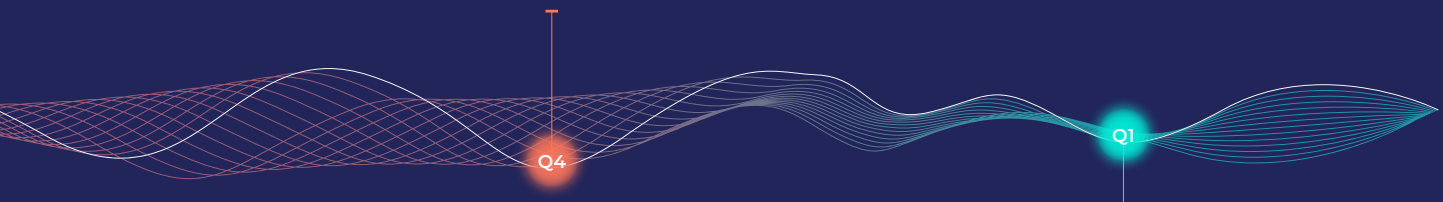
Our roadmap

Q2 2022
Vesting contract deployment
Multi-chain launch (Polygon + Ethereum)
Staking of synthetic assets in private (research)
Public sale
Exchange listing (DEX)

Q1 2022
Mobile version launch
Implementation of decentralized relayers
SHRA Token generation event
White paper publication
Pitch deck updates

Q3 2022
Staking mechanism within Sahara platform (implementation)
Synthetic assets private swap (research)
Multi-chain development (Solana, Avalanche)

Q4 2022
Synthetic assets private swap (implementation)
Multi-chain launch (Solana, Avalanche)
Governance platform token (voting)
NFT platform and marketplace (research)



Q1 2023
NFT platform and marketplace (development)
Metaverse (research)
Lending w/ collateral (research)

THE FUTURE OF SAHARA

Our team

Executive Team

Babak Rabiee is our CEO and is responsible for all aspects of the Sahara Project. With 8+ years of crypto experience and ICO's and DeFi investments dating back to 2017, Babak is spearheading our privacy revolution.

Babak Rabiee
CEO & CO-FOUNDER

Sam Farao is the CMO of Sahara, in charge of marketing and partnerships for the project. As a serial entrepreneur, blockchain enthusiast and seed investor with a decade's worth of experience, Sam is driving Sahara's global growth from the ground up.

Sam Farao
CMO & CO-FOUNDER

Andrius is our CTO, and is responsible for the magic that is Sahara's backend and technical infrastructure. With his extensive experience from blockchain technology development, cutting-edge NFT projects, and investments, Andrius is Sahara's tech leader.

Andrius Bartminas
CTO

Linas is our tech lead, in charge of driving Sahara's technological development forward. With his extensive academic experience teaching mathematics and informatics, and in-depth understanding of and work on blockchain projects, Linas constantly keeps Sahara's tech ahead of the game.

Linas Butenas
BLOCKCHAIN ARCHITECT

Synne Lindén is our CCO, responsible for all aspects of Sahara's comms. With her decade-long experience in writing, strategic messaging, and brand identity development, Synne is leading Sahara's content creation and expansion.

Synne Linden
CCO

Development Team

Vytautas Kašėta

HEAD OF BLOCKCHAIN

Gintarė Košubienė

PROJECT MANAGER

Neringa Dereškevičiūtė

UI/UX DESIGNER

Diana Lypska

BUSINESS ANALYST

Marta Savastijonok

DEVELOPER

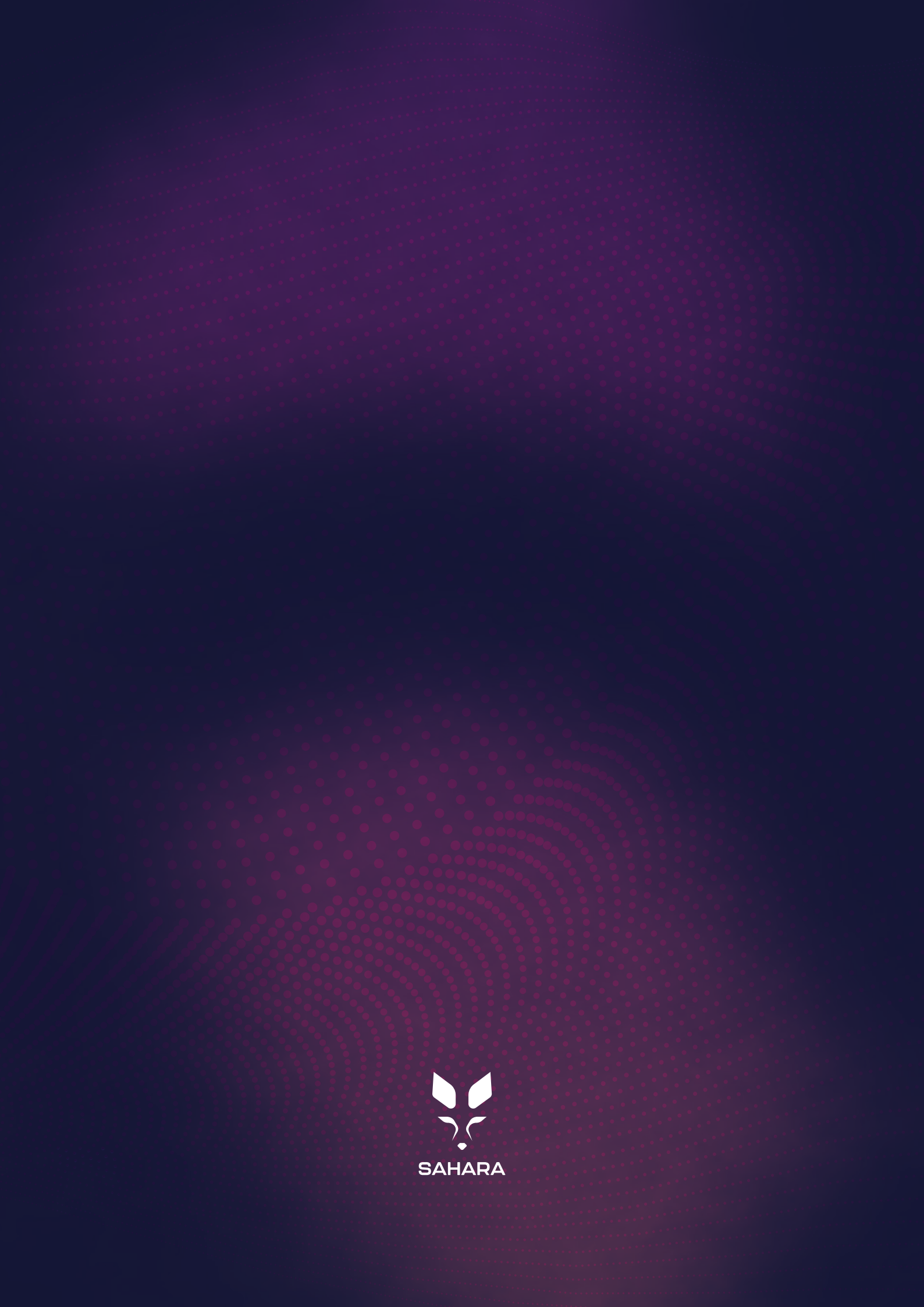
The future of blockchain privacy

The possibilities are endless. Once blockchain services - financial and otherwise - cross the threshold to mass adoption, they will do so with privacy embedded into their blueprints. Really, it's about coming full circle and bringing blockchain back to its core again: Decentralization, anonymity, and privacy all working together to offer users across the globe true, unrestricted functionality.

With Sahara's core mission of developing to become as diversely applicable as possible, we're spearheading the privacy revolution. We'll launch on an ever-expanding number of chains, effectively offering users more and more privacy. Pushing blockchain further and further towards that mass adoption breaking point - the one that will position the technology as a real and optimal alternative to traditional, centralized solutions.

Privacy is relevant to every single service blockchain has to offer. If an end user is considering it, they will want their data protected. It really is that simple.

Sahara offers the key to the Achilles' heel of a mass-adopted decentralized financial future. And we have to say, we can't wait to cross the threshold.


SAHARA