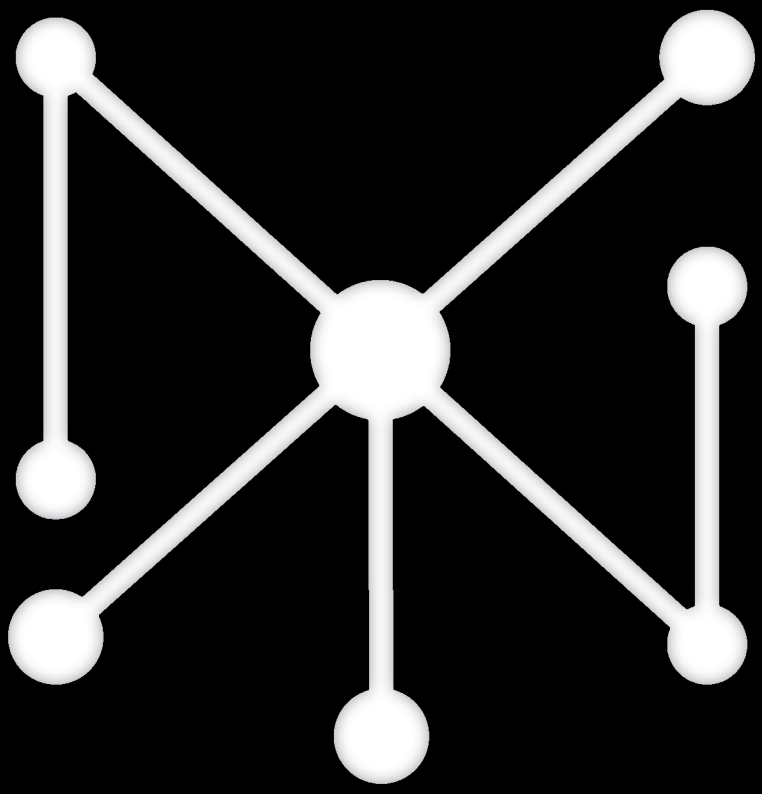
NYX white paper
draft rev. 0.9



Contents

General Provisions

This document is a comprehensive description of the NYX − a solution for decentralized recovery of access to a crypto assets, like tokens and cryptocurrency, implemented on the basis of the Blockchain and the logics of smart contracts.

Legal compliance

As for the legal component of the project and the situation with the use of the Blockchain and cryptocurrencies in the world community, our team declares that we respect the legislation of all countries.

Taking into consideration the situation in the world community and the legislation of some countries, we deem it right and honest to state that our tokens are not stocks or securities, in any form whatsoever.

We express gratitude to all who have found time to become acquainted with NYX.

Mission

NYX provides users with capability to uniquely identify themselves and each other on blockchain (or other decentralized technologies). We view the problem of identity validation as blocking decentralized technologies from reaching vast majority and prevents user acquisition.

As a practical example we're currently concentrated on access recovery as a confirmed and growing problem but a successful solution will open possibilities to other applications, like decentralized democracy, banking, assets inheritance and much more.

Problem

By forgetting the password or losing private keys, users lose access to their accounts. There is no way to withdraw money from an account to which access has been lost, besides centralized solutions that are insecure by definition. There are also companies which provide bruteforce passphrase guessing and they demand up to 20% of account contents.

The same problem exists for physical (cold) wallets like Ledger, Trezor and others, as there is always a possibility that the device will be damaged or stolen, besides forgetting the passphrase.

Storing data for restoration in cloud services is a risky way to ensure access recovery, both at the level of network interaction, and at the level of provision security of servers from hacker attacks. Moreover, almost all major cloud services contain a waiver of liability in the license agreement in the event of data loss or its transfer to third parties.

The biggest problem is that all of above methods do not identify the person. They provide access to Ethereum (or other cryptocurrencies) access.

Solution

"Everything should be made as simple as possible, but not simpler." Albert Einstein.

We are developing a smart-contract which is currently based on Ethereum blockchain which will allow users to identify themselves from any device with a camera. The basic concepts behind it are game theory, neural-network algorithms and a decentralized storage. It is is relatively simple and has quirks only in the implementation. Complex systems are sensitive to attacks, that is why it is also is being developed formally verified.

The complexity problem is what happened to ParityTech's multisignature account, freezing over $150 mln forever. Badly designed technical solutions tend to cross the threshold of its complexity very quickly, when there's a big chance for a programmer doing a local task not to understand global consequences of his decision.

Besides smart-contract itself and blockchain operations we're developing mobile and desktop open-source GUI applications which will allow conventional using of the technology. Some of the API will be public intentionally to allow integration with popular wallets.

NYX usage scenarios

- Access recovery
- Escrowing
- Voting
- Third party integrations
- Unique but safe global id
- Social networking
- Assets inheritance

Formal description

NYX identity validation requires a user (Requester) to record the video during account creation and other users (Authorizers, Identity Miners) to validate his identity during identification request with help of specific algorithms.

Conceptually it's as simple as that but to escape fraud and errors some more complex concepts are required underneath the UX.

On-chain operations

The on-chain operations contain:

- Account creation
- Storing footage data (currently on swarm)
- Identification request events
- Rating on identification requests (from Authorizers)
- Blocking fraudulent identification requests (from account owner)
- Transferring assets to another account

On-chain operations consensuality is proven by underlying blockchain.

Off-chain operations

The off-chain operations contain:

- GUI for creating accounts, making identification requests
- GUI for Authorizers to vote on identification request
- Neural-network based face-recognition supporting Authorizers
- Receiving notifications on identification requests
- Local biometry authorization

To insure that off-chain operations are unbiased and non-cooperative we utilize game theory.

Schelling point

Schelling (focal) point is a game theory concept developed to find a "symbolic value" which has meaning for a specific group of respondents. For example if you ask a group of New-Yorkers where would they meet if they hadn't means of communication, the general assumption would be the Empire State Building.

More importantly Schelling point allows you to get an unbiased opinion from participants of a poll. Basically you ask a group of people the same question and expect countable answer from binary 0–1

(yes-no) to 0-infinity. Then you find average of all answers and reward only those participants whose answer wasn't very different from this average.

The obvious problem of Schelling point is communication. If we imagine participants coordinating when asked a question then we must assume they might all fall into average threshold of a biased answer. And they obviously will have their motivation — the reward. Thus the best strategy for the group will be to cooperate so everybody has the guarantee of getting a reward which we're going to avoid down below. Cooperative games are generally more rewarding then non-cooperative so here we obviously need some kind of Nash Equilibrium.

To escape coordination we use Markov chain Monte Carlo randomization algorithm. This also lowers the chances of successful account flooding.

Neural network

NYX utilizes VisionLabs neural network for face detection and comparison. This algorithm is also capable of detecting possible generated imagery or even compare sources to find previously used footages. It's going to be used in open-sourced (or other license) application by account owners or more importantly Authorizers.

Based on Nash Equilibrium Authorizers is rationally motivated to use latest most advanced software to quickly compare faces because he\she knows that other participants most likely use it. This is a scientifically proven way of getting consensus even without a blockchain technology to formally to validate it.

Typical scenario

Requester's side:

1. A user makes a video of himself when creating the account. One can choose level of security, for example set flags to include depth map, or 3D-map of his face. Obviously the same level of detail will be required later;
2. To protect further from using footages or generated imagery Requester might be required to pronounce some random words. This will help create more unique descriptor of his facial features;
3. Moreover user might even add specific information which will give Authorizers some additional way to verify his identity, like "I got a birthmark on a cheek";
4. The footage is uploaded to the Swarm decentralized network — one of the kits of Web3 technology stack, on which Ethereum stands. Swarm used to save large data outside of the blockchain itself. Swarm link to the footage file. The footage is encrypted and not accessible to anyone including the account owner, he might only replace it with another one;
5. Later, if access is somehow lost, Requester publishes a restore access event to the blockchain. It must include address of the account to restore;

6. Account owner is notified on all active wallets that request has been made so he might mark it as a fraud outright (using the passphrase he presumably remembers at this variation);
7. This event is not free and requires payment (or some other form of reward, like tokens) which will be distributed between authorizers. This also makes brute-force expensive for an attacker; In addition to payment, the Requester supply the video, in which is recorded the owner of the lost account. This video must have the same level of security (depth map, IR) as in the initial one. Smart-contract will reject videos without specific features, but even without such check one will definitely fail the consensus decision.

Authorizers side:

8. Authorizer opens some UI application (presumably open source) to scan the blockchain to find an unsatisfied recovery access requests.
9. Upon finding, participant is presented with both account creation footage and recovery request footage, user provided additional info, security layers (depth map, IR), possible reward for the correct answer, probably even audio.
10. According to his impression Authorizer sets his score indicating whether in his opinion the person on the source matches to the person on the recovery footage. Currently it's just three options "Fraud", "Not sure", "Match"
11. The average of all votes is counted in smart-contract and processed as follows: "Not sure" indicates that additional footage is required or will require more Authorizers to join the process. "Fraud" will result in Requester losing the fee and wallet owner is notified; "Match" will transfer assets to the supplied account;
12. The Authorizer receives the reward and his rating is automatically increased.

Attack vectors

The obvious problem of such concept is sybil attack: an attacker might flood the network with auto generated accounts and thus receive access recovery events with higher chance.
This is dealt with in three ways:

- Rating system, based on two variables: amount of successful recoveries, and amount of edges to a user which is essentially how many other users trust him to be their Authorizer
- Guaranteed unbiased participant - the neural network on-chain;
- Viral growing — accounts are generated only through invites from validated ones.

The rating system per se still might be attacked with flooding just with extra steps, one can emulate the successful recoveries and even edges with a little more complicated algorithm. To fight this we use neural network and demand fee in NYX tokens for Authorizers. Moreover we have a little more protection by that fact that some currency is burned to execute the contract itself.

Stage Alpha

Currently we have developed a simple proof-of-concept application to validate the idea. It doesn't have problem of account flooding and might be even considered safer.

Instead of having random people trying to identify a person in this variant user creates specific whitelist of those who can restore access for the account — friends, family, escrows.

One still has to capture video creating the account and also upon access restore request only opinion of users from whitelist will matter. This variant includes several options like selecting minimum amount of confirmations (all, >50%, at least one highly trusted person). This also allows recovery for inheritance purposes or fixing face disfigurement, because relatives or escrows are able to acknowledge this in real life.

Trust graph

Stage alpha is not only easier to implement but is also required to get a critical mass of validated persons.

We call the User ∈ Whitelists set a Trust Graph. The more edges of the Trust Graph are connected to a single user the more is possibility of him participating in identification of users which are not directly connected to him through whitelist.

NYX tokenomics

Based on etherscan.io data for 2017 Q3-Q4, number of unique accounts in Ethereum will increase at last 6 times to 90 000 000 in 2018. Statistically 17% accounts are lost as a result of corresponding data loss (i.e. keys, passwords). 17% - 15.3 mln accounts (at least) will be lost in 2018. Let's assume, that NYX, as the only possible solution for now, will handle the task to take the market share in amount of 7.5% of all new ethereum accounts in 2018. This results in total number of NYX accounts of 7.5% of 90 mln = 6 700 000 accounts. 17% of users will lose access to their Managing accounts, thus requiring NYX tokens to restore access to their funds. This is about 1 mln accounts. To recover access to 1mln accounts there will be demand of about 80 mln tokens, while the maximum available to the public sale is 12 mln. At price of 80 NYX (20-30 confirmations) for a single access recovery request there's 6 times lack of NYX tokens on the market which will increase the demand. It will be flexible though, likewise the miner's fee you can spend smaller amount of tokens but wait longer.

This is the factor for growing NYX price when using NYX as utility token but it's also a unit of capitalization of NYX company as well. In this aspect its price will grow along with NYX's popularity and usability.

We hope these preliminary calculations will help you make right decision. Keep in mind that our primary goal is to create a small economy which will help people deal with a very serious problem rather than just accumulating token’s price growth.

Investments distribution

Product development 45%

Of course, the product itself. This will include:

- Developing mobile and desktop NYX clients
- NYX smart contract developing
- Integration of NYX with popular wallets
- Developing decentralized dApp for owner identification
- Closed and open testing for vulnerabilities and bugs in the codebase, formal verification
- Technical partnership with best companies involved in the field of face recognition game theory practices

NYX user acquisition and marketing 35%

World's markets are overcrowded. Even those, which relatively young like in the blockchain area. That's why we plan to spend up to 35% of the investments to reach maximum amount of end users possible. We plan to make NYX a standard infrastructural thing. This will make the price of NYX tokens rise, because Ethereum user base is already growing explosively

Risks 10%

10% of funds will be reserved to deal with problems, which are not expected at the moment. These could be labor market problems, legal issues, claims from third parties and other issues of this kind.

Feedback and community 2-5 %

5% will be used to make NYX users and investors support as transparent as possible. For this purpose separate team will be formed. This will include publicly available roadmaps and agile boards, social network channels, real-time online events and so on - to provide each and every question with the answer.

Research & Development 5%

And last but not least, last 5% will be used to investigate opportunities and challenges in blockchain. This process will be transparent as well and will ensure NYX to be one step ahead of all it's competitors.

Project team members

Arseny Lebedev, co-founder, visionary

- Delivered several government projects with military level security
- Neural networks expert. Solidity and Ethereum involved professional
- Strong product development background (tens commercial B2B projects)
- Functional programming and formal verification enthusiast

Andrey Nagovitsyn, co-founder, CTO

- Software engineer with more than 15 years of experience in programming.
- Several successful mobile startups
- Product vision
- Shifted from mobile development to blockchain technologies last years. Blockchain expert
- Married with a kid

Sergey Pankratov, smart-contract developer

- smart-contract developer
- 7 years of software development
- Effective trader

Ivan Kukharchuk, DevOps, security expert

- 10 years of administering private data
- Practical cryptography expert

AI identification team

VisionLabs

- http://visionlabs.ai/
- 30+ engineers
- Neuronet solutions used in top Russian banks and government security

Project implementation roadmap

2017 Q3-Q4
NYX concept developing. Smart-contract implementation and testing. Developing NYX for Android alpha.
We have already implemented the smart-contract and have alpha Android app on Google Play Market. We support standard wallet functionality with some peer-to-peer capabilities.

2017 Q1
ICO Launch
Token distribution and crowdfunding
Whitelist authorizers wallet implementation

2018 Q1
Decentralized identity validation dAPP, Integration with JAXX, Ledger, etc
Release open-sourced applications to allow users to participate in decentralized identification.
Develop integrations with existing wallets to allow people not to change to a new one.

2018 Q2
Neural-network based anti-fraud system, Formal verification
Neural-network as participant of Schelling point identification with self-improving anti-fraud capabilities. Formal verification of the codebase to insure stability of the dAPP.

2018 Q3—Q4
Altcoins implementation, Full decentralization
Implement the solution in top altcoins which support smart-contracts. Seek opportunities to go fully decentralized so the system doesn't require manual tuning.

Glossary

Hash

In NYX the keccak256 hash algorithm is used. This algorithm allows you to effectively hide sensitive data, such as the address of the Rescue account, the passphrase and the hash of the photo.

Manager account

The account, from ″name″ (address) of which the NYX contract is managed.

Neuronet

A software model that implements the concept of machine learning, which allows us to implement algorithms with unclear input data and probabilistic evaluation of the result.

Rescue account

An account created simultaneously with the NYX account and used to withdraw funds when you lose access to the Manager account.

Emergency account

An account to which the funds are transferred if you lose access to the Manager and Rescue Accounts. In order to use the Emergency account, it is necessary to use the decentralized authentication mechanism.

NYX account

The smart contract of the Ethereum platform, implementing the logics of decentralization, access and protection of funds from third parties.

Blockchain

If you read up to this point, then you know enough about blockchain to contribute to NYX :)