Review – Newrl The trust network

https://www.newrlscan.io/block-explorer
Twitter: @newrl_layer1 (1200 follower)
Discord: https://discord.gg/yHcxjSeErz
122Mio $ in tokenized assets
10k+ users
800 tokens
400 Nodes

Making DeFI mainstream and inclusive. India based, nameable "backing" (unverified) by economic and tech experienced institutions. From the first site about the project one can see that the project is geared towards real world usability especially in financial areas, providing identification and accountability possibilities. Neural is unique because it uses a new Consensus model that utilizes a trust score of all participants that is derived from their on-chain history and community history.

Current state:
Currently in early adoption phase with the trust network in development as a social graph
DApp onboarding
Implementation of own wallet
NoCode DAOs in work
Bridges adoption as per user feedback

Planned for Q12023:
Dex
Staking
Nodes as a service
Private sale

After:
Neural architecture with infinite scalability
Distributed computing and storage
Sidechains for enterprises offering both privacy and accountability

Tokenomics:
5Bn tokens at Genesis of which 50% go to Validators and are the only free floating tokens not vested or locked. New tokens can only be issued as token rewards for block creation. Of these a 80% are burnt. Over 30 years the total new issuance would be 5Bn of tokens. Hard cap, reached after 30 years is 10Bn tokens therefore.

Each node has to fullfill a staking requirement that is used as a pool for damage done by malicious network activity.
The staking requirement is 500,000 NWRL tokens for each node.

Architecture:
Layer 1 architecture
Specific underlying public blockchain
State-based validation process i.e. for validating any transaction, having the latest state is sufficient and each valid transaction updates the state. The state can be changed by execution of transactions by each node locally
Atomic swaps
Identity management (personal and wallet by KYC custodian)
In PoT, any node can broadcast a transaction to its peers. Receiving peers ignore transactions that they already have (checked using transaction id). For valid transactions, each node stores them in the local memory pool and transmits it onwards through a gossip protocol using the transport layer. (Hedera Hashgraph uses a gossip protocol aswell). Newrl uses the libp2p protocol.
Each node has to deposit a fixed amount of native tokens or USD stablecoins to a dedicated staking smart contract.
The transaction fees from all included transactions in the block are transferred to the treasury smart contract. The treasury smart contract either burns NWRL tokens received, or stakes NWRL-NUSD tokens in the liquidity pool of NWRL-NUSD or buys NWRL from the pool with NUSD, based on the relative balance of NWRL and NUSD in its own wallet.

Nodes can vote "true" or abstain from voting with a "-2" vote giving the other network members the information and not holding up the validation process.
A blocks validity is estimated using receipts, references to former hashes and index.

1 node creates a block
1 committee member validates receipts.
Each recipient confirms the validity of the signature and includes in the memory pool as well broadcasts onwards if it is valid. This way, most of the participants in the network have valid receipts of votes by committee members on a given block.- This is in contrast to other protocols such as Azero where nodes only get shares of private and public keys and have a second layer for deducting or verification of them. Possible security weaknesses remain yet unverified by the reviewer.
The receipts shared by the whole network are later saved in the memory pool of nodes and an update of the trust score happens.

Node structure and process:
1. Each node on the network stores only part of the data required for the operation of the blockchain.
2. Each node participates in only part of the computation during the operations.
3. All transactions and all blocks are not equal. Some are more valuable than others. The network spends more resources on larger-value transactions and blocks than smaller-value transactions.

The brain like Neural network achieved scalability by:
„reducing or increasing the number of block creators as well as number of transaction validators based on the importance accorded to the transaction by its proposers – through the transaction fees."

Governance:

Native token holders vote on adaptions to the public code repositories, currently held as custodian by ASQI organization. Planned and over time implemented will be to fully decentralize even the custody function by implementation of directly enforced Governance smart contracts. The idea and concept behind Neural are truly gamechanging, creating a Form of decentralized DAO-KYC system.

Dapps:
Integrated by using REST (a certain kind of software architecture used for webservices) api calls by the clients or Newrl SDKs, no other programming language or deployment on Newrl is needed.
Certain apps need specific smart contracts though (unspecified) – templates for a variety of uses cases already exist though
Grants are provided for applications based on the use case and scalability by the foundation. Which can be passed onto users.- Centralization? Censorship?
At present, any new smart contract which need to be deployed on Newrl will need to be done via the foundation after review and approval. – Again Centralization and possible censorship questions have to be researched by interested individuals.

Smart contracts on Newrl are templatised and are part of the codebase. The idea is that there's going to be only a subset of generalised smart contracts – Adaptability and usability for all usecases? Future enhancements/updates easily possible?

Dapps use API calls for communication with solely public nodes but after prototyping phase it is recommended to use own nodes for TXs and queries. – Easiness in adoption of Dapps with the need to have a node? Unclear whether it is a security recommendation or just to enhance Dapp functionality.

SDKs currently in development so communication currently only by using REST Api calls.

Wallet:
Need to be created and activated by a custody (no closer info on the process) and written into the chain
Sollet.io like webwallet forked from serum project
An identity document connected to an created wallet can be stored locally or institutionaly but there is a digital copy of it on-chain.
In this trust network existing wallets can vouch for the identity of newly opened wallets by signing the adding transaction to the full database of all wallets.
One ID per person but multiple wallets possible. Each connection between persons has a trust score.

Smart contracts:
Use template codes for a better security and performance – Customization possible to a needed degree?
Private-atate for smart contracts possible to store the crucial infos on chain

Github:
3-4 Contributors
Python language used
Repositories already exist for these project parts –
Blockchain Python Client
SDK for Blockchain developers
Wallet
Transaction listener for REST API
Explorer

Proof of trust consensus model:
-Advantages over PoS when Sybil attacked claimed (unverified).
A BFT Byzantine Fault tolerant consensus building upon the trust scores of participants.
Nodes participate in validating transactions and adding blocks - earning platform tokens and a higher probability of future selection for block addition for honest contributions.
Malicious nodes are less likely to add future blocks and lose a part of their deposits in tokens.
Two step block confirmation first by a randomly selected committee and then by the rest of the network.
Validation is not just a majority vote but a trust score weighted assessment.

The network as such has no algorithms to convert the available full history of all TXs into a historical score but network members can use the data to do so.
Automatic updates happen with each TX but can be manually reset by the source person, regarding the destination person.

The protocol leans on the well known Tendermint Protocol but replaces the financial stake envisaged by using the Trust score mechanism.
In a first step a committee of nodes is selected out of which one is chosen as the block minting node.
A Tx consists of the Standard Tx, the block reward Tx and the Network Trust Tx, the latter two being considered as signed along with the signed Standard Tx.
The minting node also calls the network trust score manager smart contract.
The transaction data is not sent in the Standard Tx data (only Transaction ID) and is derived by other nodes locally received the blocks.
There is a committee internal time-out window and a network wide time-out window after which an empty block will be created to inhibit the network becoming stuck.
Rehabilitation of untrusted nodes is possible and started by highly trusted persons with a collective deposit that resets the trust score and the ability to use/vote on using the submitted deposit for compensation from any malicious act's losses in future.
Even without application of Trust scores the probability of dishonest nodes forming a majority is at 0,002%.
A malicious actor would need to build up trust over time, using real KYC documents or controlling other actors including their KYC documents and would still be quickly discovered since TXs, blocks and receipts are validated even if one actor mints a false block.

Audit Nodes:
"On Newrl, anyone can report suspicious activity by a specific person on the network. Upon such a request, specifically designated auditor nodes can verify the accuracy or lack thereof of such reports. If a person is verified to be engaged in malicious activity, his/her/its personId is included in the grey list table in the state of the network, available to all participants to view".

Sentinel Nodes:
These specially chosen very high trust score nodes have the function to „unstuck" the network by broadcasting an empty Block. Malicious nodes could stop the network by randomly sending empty blocks.
It may yet happen that the committee and minting node were dishonest, and they send an invalid block. In such cases, majority of the honest nodes will not update their local state and keep waiting. The sentinel nodes can send an empty block to get the network restarted.

Rehabilitation of Trust score for Nodes and enforcement of claims:
„a rehabilitation smart contract can be called by at least C persons with trust scores in the top decile of the network and with a collective deposit of at least K*C times that of the standard node deposit (K set at 100 to start with). This transaction if picked up by a minting node will reset the trust score of the rehabilitating node at 1. The community can decide to use the deposit submitted here to compensate any loss from malicious behaviour of the rehabilitated node in future."

The probability of malicious nodes having a majority in block creation committees is – even without implementation of the Trust Scores – a 0.002%.

„An attempt to vote maliciously against a valid block, with the objective of simply creating hurdles in the regular operations of the network (and prompting addition of an empty block) also gets caught fast enough as empty blocks prompt the network to review the discarded block and update trust scores - punishing majority if the block were valid and minority if it were indeed invalid."

Even if funds were stolen a criminal could not use any of the stolen tokens without revealing his ID by sending them to his wallets connected to his ID.

Current Blockchains store data relevant to a token or token issuance in its smart contracts, making them vulnerable.
Neural solves that by having no token issuance subsumed under smart contracts. Also all used tokens including the native one have the same hierarchical status on the network.

Assets can be easily tokenized in natively issued form or for special assets in custody form. Even cash-flow bearing smart contracts can be tokenized.
The whole concept is very smart and simple either having issued tokens representing the asset itself or having real life custodians of the assets issueing tokens to the (beneficial) owner that represents that real assets held by the custodian.

Even smart contracts like loans can tokenized and thereby transferred to others, if the underlying smart contract allows it, creating an easy to use, fully legally compliant field of new financial services becoming available for the mainstream. So far I have not seen any project addressing the real life solutions and markets and legal regulation problems in any similar way, not even close. This team shows again that it is a very serious and professionaly handled project, adressing all possible obstacles to becoming a truly mainstream DeFi service and financial platform.

Scalability is achieved by only storing parameters of smart contracts and DAOs on chain and leaving the codebase on local nodes from which the templates are drawn.

It is much like ETH is the chain open to all .apk filed for an app, including even third party apps that you can code yourself. Even storing and executing them on chain makes it a slow and risky solution for most mainstream participants needing to pay and develop custom risk prone contracts (and update them!).
Neural comes in with a simple but genius solution then being the „appstore" of smart contracts on chain. It is much harder to exploit preverified and tested templates of smart contracs, giving mainstream users without much expertise much more security in their actions. Scalability is also much higher by only loading up the chainbase with essential parameters.

Assets can be easily issued, transfered, split, aggregated, tranched or mutualized and securitized with secure community developed contract templates where 90% of usecases is covered by 1% of smart contracts (loans etc).
Setting up a DAO or DO or on-chain firm like a DEX becomes very since the contract templates already incorporate multisig and organization specific solutions.

Further scalability enhancement is achieved by:
„The block reward and network trust score transactions are not separately signed but are deemed signed by the minting node through its signature on the overall block. This removes the need for validating these transactions by other nodes since these are not transmitted ahead of time anyway. The selected node also updates its local state. The transaction fees from all included transactions in the block are transferred to the treasury address of Newrl. The treasury uses its balance as a liquidity pool of the tokens allowed for the transaction fees."

Groundbreaking vision:
„The immediate relevance of mutualization of IOUs is to enable groups of people to create money for suitable end-uses without having to rely exclusively on the banking system. In the current financial system, only banks can create new money based on their lending and as allowed by regulations like capital adequacy. This system is inherently inegalitarian and is often quite discriminatory. By enabling individuals to tap into their collective creditworthiness, mutualized IOUs put the power to improve their economic wellbeing in their own hands."

Some general points:
KYC compliant at chain level

Work on digital identity

Trust network social capital

Bridges to all major chains established

Ready to use tollbox as no code DAO to start tokenization of assets, contracts and providing liquidity

Aims to use social credit for proof of identity and creditworthiness in financial applications. Solving the anonymity and accountability problems of other chains. – Reader has to weigh the pros and contras of such an approach. The project clearly implemented and faced regulatory questions of future developments in contrast to most other projects where that question poses a serious risk.

An own identity layer within Dapps is used and leads to chrosschain usability of the identity service. – Maybe this is the reason why smart contracts aren't custom built since a faulty Dapp contract – speculatively seen – might cause a data leak or even identity theft?

All contracts on Newrl are legally enforceable.

Generalizing trust score use beyond credit - network itself, decentralized collaborations, jobs, tenant contracts etc. – A general question of future developments in this field stays unanswered, who controls our scores and what if a negative score is assigned falsely? The legal enforceability making Newrl unique is exactly what is needed to counter these risks but a uncertainty still remains how and how long it would take to enforce a correct score? Who will be the one to proof his right or carries the claim-proof need ie. has to lead a positive process of proving his claims in contrast to an "unguilty indication" until the opposite has been proven right?

Data storage and security have a higher importance in this project because a huge amount of data and metadata is stored among all nodes of the network (receipts, etc).

Team:
Founder has a rich background in finance and one can clearly see that in the professional approach and orientation towards financial services by the project.
Besides CTO there are 2 Blockchain developers and a full stack developer, and other business oriented managers, each with good experience in their fields, India being one of – if not THE – leading countries in Blockchain development and technology and software development in general.

Different types of tokenization processes/requirements can lead from a decentralized investor ownership to a custodian ownership, with some assets being possible as native tokens on chain while assets like listed shares, bonds, real estate, ETFs, copyrights or patents are not possible as native tokens. – Yet unclear as to why – whether it has regulatory reasons or to do with the inflexibility of smart contracts being coded into the chain as templates.

Benefits of low TXs fees payable not only in native tokens but also in stablecoins and CBDC.

Bridges and sidechains are claimed to be easily implemented in contrast to competition.

Smart contract languages are Python, Solidity and others and no need for deployment on chain is there. On the other hand a given set of template smart contracts serves to cover the planned usecases. No coding language needed for usage.

Easiness of DAO setup and nocode for usage.

Conclusions:
It is not a coincidence that the Microbanking movement and revolution was introduced in India and proved that mutual trust and small amounts of inner- and community loans can not only change a persons life but the whole financial markets and economy in a great way.
It is now Newrl taking the long needed next step in making financial services feasible and even possible to the mainstream users and small businesses.
And they have the perfect Team and background exactly for this task and major backing. A perfect mix of business knowledge and experience made the project formulate the core burdens of current projects for a mainstream recognition. Anonymity and missing Accountability. An effective and efficient Architecture concept and working solutions have been conceptualized right from the beginning. By just implementing on chain compliance and KYC processes the team has already solved what other even big projects assessments failed to do – mid and longterm legal compliance. This was possible because the team has the perfect mix of tech – financial and regulatory know how and experience for solving exactly what they have stated to plan.
This project gives DeFi its name righteously for the first time since there will never be mainstream solutions to real world financial problems and needs without the structure that Newrl already has implemented.
Even the biggest tasks for big competitors are solved by concept as the Blockchain Trilemma is solved by only adapting the KYC processes needed – as a feature – not as a bug. Scalability is solved not only by the new Neural architecture concept but due to the fact that a whole set of new solutions have opened up for this project in contrast to others.
A series of genius concepts solves all major issues that current Chains fight with – ranging from
Neural Architecture
Trust as an asset not a risk
Smart Contracts revolution in feasibility, easiness of use and security at the same time by using code templates and making life hard for any attacker.
Easyness of further scalability and interoperability by having sidechains or chain-agnostic DApps implementation on-chain – only needing minor usage of provided contract solutions or SDKs to create Fast, cheap, secure and innovative solutions for us all.
This is the so far best strategically thought through, conceptualized and implemented project that I have reviewed. There is a reason why most Blockchain and in general Software solutions come from India, and many projects – including my own have been or tried to outsource parts of their development to the IT superpower Nr. 1. If banking was invented in Italy then this project – standing for India's Microbanking tradition will reinvent it.
The project did not – like most of other projects – raise money and try to find (!) and develop solutions and even strategic concepts on the way as they promote their big plans. No. Newrl

started with the hard work actually, and already has more to show and offer than any other project before even launching the Token.
As a former banker, risk and debt restructurer and legal counsel I could not find one single question open that was not in concept thought through, conceptualized and decided upon.
The project has a bright future and will become my only other main project that I invest in longterm.

The only thing that an Investor has to decide upon and keep in mind are the general questions if they rather prefer a anonymity focused – not legally compliant- project or a an actually working concept.

If they support the generally breaking through concept of Social Trust or Trust Scores, especially in financial services or not.

And even if the new Consensus model of PoT still has to show that it solves the Blockchain Trilemma already at concept, the major risks are – again already by concept – neutralized by the Staking „security"-pool
Accountability and KYC by all participants and
Enforceability of the applied contracts/solutions.

Lightpaper:
https://newrl.net/docs/Newrl%20Introduction-Oct2022.pdf

Whitepaper:
https://newrl.net/docs/Newrl%20White%20Paper-Nov2022.pdf

Consensus Protocol Whitepaper:
https://newrl.net/docs/Whitepaper%20-%20Proof%20of%20Trust%20Protocol-v2-%20Oct2022.pdf

Website:
https://newrl.net
Well documented and easy to read for interested people. Very (!) professional in general!