The R-Squared Ecosystem

SUMMARY

This ecosystem is meant to function as a practical data sovereignty core, where any developer can provide a means for their customers and users to own and control access to their data and content by integrating the software. For some industries, this could very well present a significant opportunity for enterprise efficiencies and advancements – from health records, to verification information that you give to banks to open accounts, to even gateways / toll booths that can be put in front of AI bots that gobble up petabytes of data that doesn't belong to them.

In short, the software is designed as a flat, scalable, integrate-able, interoperable and stable data sovereignty ecosystem that can be used by anybody, where the power and control over data and content can immutably reside with its owner.

Systems Architecture

The problem that the system seeks to solve is lack of data sovereignty. People don't own or control their own data. Blockchain, as a software standard, may seem like an elegant way to solve it; however, blockchains by their nature can't store large files – trying to do so makes them impractical. So a construct has been put forward where anyone can have an account on a blockchain, and if any app integrates the software, all of their users can own and control their data.

The way it works is: if a user uploads a file – whether it's a photo, a txt file, a pdf, or any binary file regardless of file format – the software hashes and encrypts the file and stores it in a cloud storage of the app's choosing (adapters have been built for AWS and Google Drive), and simultaneously the link to the file and the permission-ing protocol is stored on the blockchain, connected to the user's account. So now the owner is the only person with the keys, and the power, to lock and unlock the file to share with other people – whether it's in app or across to other apps. And all of the heavy services that apps need to use that could weigh down a blockchain remain off chain – storage, servers, CDNs, etc.; these are all managed just as they are today. So the protocol is, in essence, a blockchain tool – almost like an add on or extension – for any app or company to use to provide their users with data sovereignty.

Problem solved, right? Well, not so fast. The first thing any app entrepreneur needs to decide is their stack. What are the components that I'm going to choose to use to build and support my business? This is a critical decision, because every new day the app's developers are going to be contributing layers of functions on top of the existing infrastructure, which makes that infrastructure sticky and expensive to carve out or replace. Developers need to build on something that's reliable and sustainable.

Blockchain technology is reliable. That's now a safe, if not obvious, statement. However, the marketplaces for cryptocurrency can be fiercely unreliable – from suspending withdrawals to going out of business. And while, as in this project's case, access to the native token as an

operating mechanic is essential for those who integrate the software, centralized crypto exchanges, which list hundreds of tokens, are unlikely to be overly concerned about the pressing need for the availability of one particular token when it comes to their businesses.

By way of example: let's say an app uses standard cloud services today (e.g., storage, servers, etc.). As long as that company has a credit card, they can pay the monthly fees and keep the lights on. However, what happens if there's a key new service the app uses that requires them to pay blockchain transaction fees in a native token? And what if the bulk of the available tokens are concentrated within a crypto exchange that goes out of business, or suspends withdrawals for even just a week? Then the app itself can go out of business.

This is why a decentralized token access facility (or TAF) built directly into the layer-1 blockchain itself is important for a data sovereignty model to sustain and grow. There needs to be a stable and sustainable place to go to acquire the native tokens, even if tokens are in fact available on centralized exchanges. And since the TAF is built into the layer-1, so long as the blockchain is running, the TAF will be running. Open source bridge software is also available to connect the Ethereum chain to the native chain which allows anyone to enter the TAF system by using real ETH to get wrapped ETH generated by the layer-1. From there they can then use that wrapped ETH to acquire native tokens in the TAF. And the same holds true in reverse for exit: you get real ETH for your wrapped ETH, and now you're out of the system.

BLOCKCHAIN OPERATIONS

Voting

Witnesses & Staking

The chain operates on a "delegated" proof of stake algorithm – meaning people vote with their tokens to elect witnesses to run block producing nodes. Witnesses are, in essence, the block producers. These witnesses earn native tokens for their efforts, and can be anyone. They themselves do not have to *stake*. It's up to a democratic vote of token holders to elect these witnesses – the token holders who elect witnesses are the ones who "stake" – they stake their faith in those who they elect with their votes. There is no locking of staked tokens in return for yield in this consensus mechanism.

Additionally, there's a feature to the algorithm (which is an open source option for other blockchain projects to consider) that adds a randomization element to witness selection, creating a "random" delegated Proof Of Stake process or *r*dPOS. The way it works is as follows:

1) Votes are counted for all valid witnesses
2) The top 63 vote getters are assessed
3) Of the top 21 vote getters, 17 are chosen at random
4) Then, an additional 4 witnesses are chosen randomly from the remaining 46 of the top 63
5) The formation remains in place for an hour while blocks are produced
6) The process starts all over again

While it's initially set up to ensure that 17 of the top 21 vote getters are witnesses, the Committee (see below) can dynamically change the parameter by a majority vote – meaning if the Committee wanted to change it from 17 of top 21 to, for example 15 of the top 21, or 19 of the top 21, such parameters can be easily changed, and then re-made, etc.

Committee

There will be 11 elected Committee members and decisions will be made with a majority vote. As mentioned above, there are certain network parameters that the Committee can approve by majority vote; and the Committee can also approve worker proposals (and payments) for system changes or improvements. A Committee member's incentive to do the job as a volunteer is to ensure the system is maintained and improved for their benefit (as token holders) and for the benefit of the ideal of data sovereignty. And as volunteers, the Committee is unlikely to be especially motivated to do things just to show that they're doing something; i.e., the "if it ain't broke, don't fix it" maxim can be better upheld. And then, perhaps, truly warranted changes can better prevail.

Worker Proposals

The blockchain itself has tokens in reserve for ongoing maintenance, sustainability and improvements; and, of course, this reserve will continue to accrete tokens by way of transaction fees for operations. Under the worker proposal schema, the Committee will decide, by way of majority vote, how, if and when to deploy these resources; whether it's a grant for an app, or upgrades to the blockchain mechanics, etc., a worker proposal will be able to be submitted for review by the Committee. The proposal will include a budget, and it's incumbent upon whomever is making the proposal to make their case to the Committee by way of community channels, social media channels, or whatever means they choose. If the Committee approves the proposal, whomever made the proposal will receive native tokens based on the budget parameters to complete the work. It's the responsibility of the elected Committee to ensure responsible stewardship and propriety in approvals.

Note: the worker proposal component is currently under construction pending updates.

Membership & Sponsorship

The blockchain has a sponsorship based model. Those who pay a one-time fee to the blockchain reserve pool to become a "Lifetime Member" get discounted blockchain transaction fees (the fees charged by the blockchain itself) and also can register new users; and for every new user they sponsor for registration (and then pay the blockchain transaction fee for that registration), they will receive 80% of the blockchain transaction fees from that user's activity, with the remaining 20% of the blockchain transaction fees going to the blockchain reserve pool – which is in effect a treasury reserve of native tokens to be used at the discretion of a Committee. Anyone can become a Lifetime Member – they just have to pay the one-time fee to do so.

The powers and privileges of Lifetime Members (LTMs) are:

1) To create (and become) a witness node (and have an opportunity to get paid to produce blocks)
2) To be able to be voted in as a Committee member
3) To create and submit a worker proposal
4) To establish new users on the blockchain (and have an opportunity to receive native tokens from the ongoing activity of the new users they register)
5) To get discounted blockchain transaction fees for their own transactions

Regular members (non LTMs) have full voting rights and pay transaction fees to the blockchain reserve pool for any of their activity – however, LTMs will pay the blockchain transaction fees for new users they sponsor for registration who join the blockchain, taking the risk of covering those costs.

Clearing Services

Clearing House Participants (CHPs)

A CHP operates bridge software and can be of benefit when it comes to TAF stability. They can also act as sort of an added insurance policy to protect against cascading failure of the system by maintaining their own reserve fund of native tokens to cover off systemic risk events – governed by their self-interest in seeing that the system is stable and vibrant. CHPs are charged with providing entry and exit mechanics for external tokens that they wish to bring into the ecosystem (starting with ETH) and for making a wrapped version available intra-ecosystem; so they must be trusted (day 1 of bridge operations there will be a starter CHP). In return for assuming the costs and risks involved in providing and operating such a service, there's a CHP transaction fee associated with transfers of any of the wrapped look-alikes that the CHP is responsible for creating – for instance, day 1 it will be for the transfer between the native token & wrapped ETH.

The Entrance and Exit Service software (EES / bridge), is available open source (as is the portal software which is a web UI for user-friendly interaction). The bridge mechanics rely on atomic swap protocols for the transfers, using a HTLC (Hashed Timelock Contract) method to communicate between the native chain and the Ethereum chain. And as the framework matures to include more and more CHPs, the open source EES software is there for any CHP to make use of.

Business entities may also be able to act as third-party services for apps that want to integrate the decentralized data sovereignty software but don't want to bother with acquiring the native tokens and paying the blockchain fees. In other words, services can arise that can take care of an app's integration and any of the token acquisition and payments that have to occur on behalf of apps.

It's also important to keep in mind that the TAF and the clearing mechanics are there to provide some comfort to apps that want to use the data sovereignty tool that there's a stable place to go to get the tokens, with a community of native token holders incentivized to ensure its maintenance and sustainability. At the end of the day, the technical implementation is public and decentralized, and so tokens can also be acquired and exchanged peer to peer or in any other

manner that may spring up such as OTC platforms or even through centralized exchanges if any of them choose to list the token.

Any which way however, in order for this all to work, putting the concept into practive with a live main net and web beta, and demonstrating real world structural stability, is going to be necessary.

Layer-1 Token Access Facility (TAF)

A true layer-1 token access facility – along with clearing operations – is a means to provide a stable and secure transactional machine for a data sovereignty ecosystem. There are mechanics that permit people to enter and exit, but once entered, it's really all software mechanics within the blockchain ecosystem. So the TAF is a living mechanic to best allow the blockchain to function and persist.

This, of course, does not mean that the TAF can't *become* a destination, a decentralized layer-1 destination, with CHPs bridging to different chains (public or private) and their associated tokens, to further undergird the blockchain mechanics and provide a more robust stability cohort for the ecosystem, and in doing so allow for an open fertile field for crypto, and even for incumbent fiat money rails that may want to connect to an inter-connectible blockchain universe (public or private) – for *any* of it – to settle digitally and stably, etc., etc.

Data Sovereignty Gateway

A data sovereignty design that allows for maximum flexibility, along with speed and security, is where the rubber meets the road. Once a user has an account on the blockchain, they alone have the keys. From there, a user can provide permission to any application to retrieve their data or content from any compatible storage. Through any app, a user can have a link to their encrypted files stored on the blockchain, along with the ability for them to permit access to the files. And this can be the case for quite literally any binary file – the blockchain doesn't care about file format. This keeps the blockchain clean and light. And now the user can give permission to access the files (and the user can de-permission at any time too). There are adapters for Google Drive, AWS and IPFS – however the system is designed to be open and universal, which means (among other things) that new adapters to new storages can be made, including adapters that can connect hardware storages like a laptop or a phone securely. These adapters can be fashioned by apps themselves or by other open source developers; or the Committee can approve worker proposals as and if such things are warranted. What this means is that if a user uses an app that has integrated the software, the data and content that they put through the app can reside directly with them. And if there's another app that has integrated the software, not only can the user share their information with this other app, but any information the user puts through this new app can also reside with them, to be shared with other apps in the ecosystem as they see fit and so on. And in fact, the system could potentially also be of benefit to web and mobile app publishers who wish to have a paywall in front of pieces of their sites or apps that they believe contain valuable information: again, the blockchain doesn't care about what kinds of files get encrypted; and so these could be JavaScript or HTML files as well.

What this means is that there's an ecosystem that's flexible and growable but revolves around user-control and owner-power. The blockchain itself can operate speedily because large files and user data isn't stored on the chain itself. The user / owner would get a request for access, and if they approve, the data or content will be made available. The structure is also backward compatible – meaning that if the Committee decides to, for example, add more fields to the personal data structure template, all of the old information will remain.

This design also includes a memory menu for apps to save costs. Apps that don't want to run witness nodes and just want to use the data sovereignty tool can choose a separate plug in that will allow them to do that.

In short, it's a system that permits: 1) ease of development for regular applications who use common technology stacks and services, 2) a scalable and reliable ecosystem for those who want to integrate the software, and 3) an open and free market where users can control their data and content, where value is properly aligned with ownership, and where an enterprise ecosystem can be realized.

Disclaimer: This paper is meant to encourage technical or operational (or philosophical) discussions and/or debate and to provide some measure of informal outline and intent of certain public software. Nothing in this paper should be interpreted as a confirmation of any ongoing or further efforts by anyone, or of what any of the software WILL end up doing, or of what WILL happen, nor should anything herein be taken exactly or literally. This paper is not intended in any way to promote, encourage or recommend the purchase, trade or acquisition of any digital token, digital asset, cryptocurrency or the like. By no means is this paper intended to confer or infer any equity ownership in any enterprise by way of purchasing or acquiring any digital token, digital asset or cryptocurrency or by any other means. This paper is in draft form and is subject to change over time.