Revolution Populi

How to return digital power back to the people to whom it belongs

Table Of Contents

Objective

To return the money and power that belongs to people back to them.

Structure

Revolution Populi (RevPop) is taking a 3-legged stool approach to advance this mission digitally:

1) RevPop is a decentralized user-controlled database and permissioning layer-1 blockchain which allows any person to be accessed - but only if they choose to be; and, as a Decentralized Autonomous Organization (DAO), it would operate decentrally, apart from any central authority.

2) A distributed crypto exchange & clearing house mechanism built on top of the layer-1 can be an economic engine to fuel a Decentralized Application (DApp) ecosystem, which can begin with a social media utility, itself governed democratically.

3) Finally, a social net DApp also built on top of the blockchain can be a portal for people to establish their blockchain accounts, and act as an elegant engine to allow anyone, anywhere to control and capitalize on their digital property, and can provide a tech stack template and proof of concept for an open DApp development ecosystem.

Distributed Clearing

The DeFi Problem

Many platforms are now building Decentralized Finance (DeFi) products. These can be lucrative and empowering structures, however they come with sizable risk – in fact much more risk than is being contemplated by the blockchain and cryptocurrency industry.

DeFi is often a loose knit of disparate and fragmented lending markets, with disparate and fragmented lending tokens, trading across disparate and fragmented trading markets, with nothing truly settled until all the native underlying token transactions in the structure are finally and immutably recorded directly on their respective native blockchain ledgers. And many of these structures are tied together through deposits and trades and synthetics that all rely on one another. This is frightfully reminiscent of the CLO-CDS (Credit Default Swap) markets of the 2000's. No one really knew who truly owed what to whom. All it really took was one counterparty-fail to bring down the entire financial system, even though many participants were solvent. This is what caused the financial crisis of 2008.

Scarily, the same thing could easily happen in DeFi – and in fact, candidly, it will. It's only a matter of time.

And what happens then? What happens to an exchange that has guaranteed a large position whereby some ancillary attachment to that trade, that they didn't even know existed, fails at some OTC shop? There would be a cascading effect that could wipe out whole businesses – whole exchanges. This coupled with a PR disaster could devastate the industry, perhaps permanently.

Clearing solves this. Clearing solved this for CDS – and it will solve it for DeFi and crypto, in one fell swoop. Counterparty risk mitigation works to stabilize markets plain and simple. It has worked for as long as there's been clearing houses.

RevPop DeFi Clearing House

RevPop's decentralized DAO layer-1 blockchain would allow for atomic counterparty-risk novation — a digital risk-offloader for counterparties in crypto trades — ushering in a multilateral market where anyone could trade any crypto on a guaranteed basis (and not just ERC-20 tokens and a bunch of synthetics) without fear of the other side re-neg-ing; and

where anyone, anywhere can be a clearing broker for crypto trades & earn yield by doing it.

We propose a layer-2 deposit platform where users can earn yield as Decentralized Clearing Brokers (DCBs). Anyone would be able to make a deposit and an atomic risk manager would take care of all the risk management and clearing functions, and then pay that person as soon as the trade settles. And the system only clears what the system's atomic collateral framework allows it to clear.

Decentralized Clearing Finance

- The decentralized RevPop layer-1 is a natural neutral third-party base layer upon which a layer-2 could atomically clear crypto trades, with true counterparty risk novation through a clearing house structure.
- These mechanics can be underwritten by decentralized clearing brokers — where anyone could be one.
- Make a deposit, and a clearing risk system would take care of all of the risk management and collateral requirements, and then settle the trade; and you would earn yield on the deposit once settled.

Distributed Exchange Onboarding

- With the RevPop layer-1 you own your data. So you'd have a secure spot for all your information.
- Trading crypto often requires an onboarding process, where you need to provide personal information like passport, proof of address, etc.
- If you provide it once to your own personal blockchain, it would then belong to you and could be permissioned by you for any number of exchanges or Alternative Trading Systems (ATSs), including incumbents or new ones; and any of these could then seamlessly utilize the clearing house if they wanted to - and they might. It's a way for them to offload counterparty risk and free up capital they're setting aside to insure against counterparty fails.

- So now, if you want to search around for the best prices and deepest liquidity for a cryptocurrency like Bitcoin, you can permission your information as you go to whichever platform you choose.
- The clearing house layer-2 can also be a standalone for exchanges or ATSs to connect into directly for their existing customer base, and be able to find new customers who prefer to shop around decentrally for prices.

Consumer Facing DeFi

- With exchanges & clearing sitting atop RevPop's decentralized layer-1, the RevPop blockchain now becomes the perfect base layer for consumer-facing DeFi apps to build on.
- Now consumers can take advantage of new DeFi products. You don't have to be a sophisticated trader with complex algorithms. Apps can build those algos for the masses, with simple UXs for people to be shown yield/risk choices, and then seamlessly execute. RevPop's atomic clearing could take care of all the back office and trade settlements.
- Users can establish accounts on the blockchain through social nets or games or any kind of app that sits atop the RevPop layer-1. And with an intermediate clearing mechanism guaranteeing trades, consumers can have a trusted ecosystem to avail themselves of DeFi innovations and marketplaces.

Social Net DApp

A social net could be a powerful initial consumer app for this system. By using a social net, a user can establish a genesis block for their data (though they could also do this through all range of apps); and the platform's access to the blockchain database would be based on user permissions. This is a critical distinction with Facebook and other social media platforms where user data is shared and sold without obvious consent. And in fact, it's revolutionary because it decouples the platform from the database entirely. A permissioning system where the users

determine various degrees of access that outside applications can have to their data sets this layer-1 apart from the databases on standard social networks, or anywhere really.

This would allow for a trusted and credible system, decoupling the internet from the data that goes across it, and placing more and more control of data into the hands of the people to whom it belongs.

Social Net Advertising

Advertisers could target audiences by way of an ad platform, but with payments going directly to content producers. We propose a Cost Per Mille (CPM) structure, which is cost per 1000 impressions. Current digital ad platforms use Cost Per Click as a sort of head fake to advertisers. Behind the scenes, there is a calculation that occurs that determines what the "effective" CPM is for ads, and based on that, black-box ad placement algorithms prioritize those ads in order to generate the highest amount of revenue on a per impression (per placement) basis. We propose making it simple and fair: advertisements get placed based on price-time priority, meaning the highest bid wins, and if there's a tie, the earliest bid wins. Then an advertiser simply gets charged based upon the number of impressions (the number of "shows" on the platform).

Once ads are placed, revenue generated can go directly to users based on a "sandwich" method. Meaning: If an ad was placed between two posts in a feed, the content owners of the top and bottom posts would share that revenue. And while they may not share equally, that would have nothing to do with the users' respective "popularity" or their "presence"; it can be calculated based on how much transparency they themselves are willing to provide to advertisers, to allow advertisements to be delivered to them more relevantly. So, for example, if user A wants to earn as much money as she or he can from their content, then they'll willfully decide (this is important - users will opt-in) to open themselves up to advertisers, to turn the dial all the way open. If user B chooses less openness, then user A will get more money than user B, but user B will

still get some money. Think of it like a hero sandwich. If there are 5 slices of ham, but only 2 slices of turkey, it's mainly a ham sandwich. So, user A gets more money. More ham, more money. This is enormously important, because on any given ad, for example, Joe Peffl could make more of the share of the money from that ad than LeBron James. And while LeBron may make more money overall because he has more followers, there's fairness to the distribution of the money that's made from all users' content.

The power of such an end-to-end economy cannot be overstated, across business-to-business and business-to-consumer products and structures: from B2B (e.g. DApp → layer-1), to B2C (e.g. music streaming service → user), to C2B (e.g. user → advertiser), to C2C (e.g. consumer based marketplace apps).

MVP Consumer DApp

A minimally viable product (MVP) social network, with embedded music streaming to follow can be a powerful change agent to overturn the model of today's social networks, where user privacy is not exactly held in much esteem, and user data is being monetized by the platform itself instead of by the users.

Creating a social network with music streaming is a natural fit because music streaming is both a personal experience, and a bonding element between people, all at the same time; and because the money made from a user's content could be used seamlessly to pay for their music streaming, if a user so chooses. Users would be able to create their own playlists and stream them, and yet also share them as a part of their profile, and also share and promote individual songs that they like. And songs can be integrated elegantly into the social network home "feed", which can act as a playlist as well. Integrating music with a social media network can lead to significant engagement. Music streaming, and discovery, enhances a social network experience: nowadays, listening to music is something we all do while we're doing something else. So a one-stop-shop, where a person can engage in their social activities, all

the while listening to their favorite music and discovering new music, can certainly work.

Layer-1 Blockchain Topology

Summary

We propose a unique and elegant roundtrip structure for a blockchain architecture which is both groundbreaking and simple.

Social net (or any app) → server (e.g. EC2 or a decentralized server, it'll be up to the app) → API → RevPop layer-1 → pointer → storage → API → server → social net (or any DApp).

We've devised a method that can combine decentralization, security and speed. This layer-1 is a database enabling users to have control and ownership over their data, with other elements of the infrastructure residing off-chain to enable fast throughput. This, combined with an innovation on the Proof Of Stake consensus mechanism, would allow this layer-1 to service users at scale.

Access Controls

Users would be able to provide access to individual apps (any DApp) as they choose. The access provisions and other data and content can be recorded on the layer-1 blockchain. Each app accessing the blockchain database is responsible for choosing their own method of serving data. And data could be fetched only if the user allows access.

Consensus Mechanism

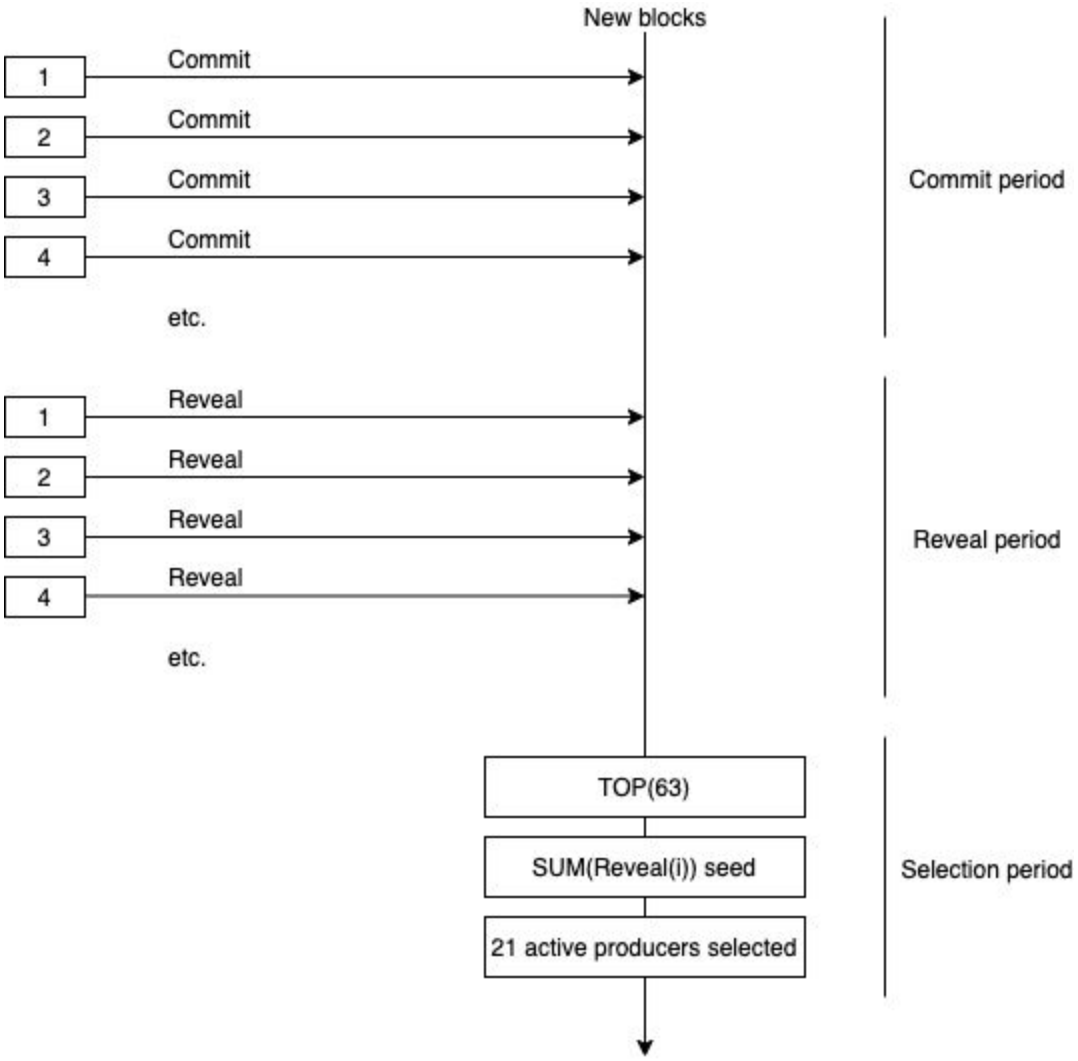
A protocol based on dPOS "delegated Proof Of Stake" can achieve a robust transactions per second (TPS) rate - using either dPOS itself, or something accretively innovative such as our plan for rdPOS "random delegated Proof Of Stake". A consensus mechanism with 63 pre-elected

nodes, but with 21 randomly selected pre-determined nodes serving at any given time, can mean fast transaction speeds along with security, scalability and elected accountability. Due to the maturation of consensus algorithms, along with ongoing innovation and technological improvements, a modern social network, or any modern application for that matter, should have no problem operating on a blockchain technology foundation that functions as a database.

rdPOS behaves like its predecessor. At the final stage, during the vote counting phase, 21 active witnesses are chosen randomly from the list of TOP 63 candidates. This attracts more nodes to the production of blocks while keeping the number of active producers small, speeding up the blockchain.

Pseudo-random number generation in the blockchain is not an easy task. We've implemented a commit-reveal scheme for obtaining a random seed each time 21 new active witnesses are selected - and it works! Now, by randomizing the selected block producers, coupled with regular, robust and public elections, the mix of producers is different for every block, and each producer remains accountable. This functionally removes the threat of "centralization" that had been at the heart of the critique of dPOS consensus in the past. It's important to note that the number of top elected candidates can be calibrated, e.g. if the system proves to be so lightening fast, and updating from 63 TOP to 126 TOP has de minimis (or acceptable) impact on speed, then such a change can always be implemented if the community deems it worthwhile - or the community can even seek to randomize the total number of TOP witnesses per cycle. The system, by the nature of its structure can be self-improving and ever-striving to functionally obviate the "Tri-lema", to allow speed, security and decentralization to all co-exist in harmony.

In short, this elegant innovation of randomizing block producers, we feel, is a powerful enhancement.



1. A new list of 21 active witnesses is generated.
2. There are two periods during this time: commit and reveal.
3. During the commit period, each witness candidate generates a random number RN and sends its one-way hash H(RN) to the blockchain.
4. During the reveal period, they send their random numbers (RNs). Each random number is checked in the blockchain using the H(RN) sent during the commit period.
5. When selection time comes, the revealed random numbers of the candidates are used to generate a unique seed (SUM(Reveal(i)), and then the random number generator randomly selects 21 new active producers.

6. Candidates who don’t send a RN during the reveal period cannot be selected.

We have developed a docker-compose configuration that demonstrates this scenario. When a node runs, 63 witnesses are activated on top of it. Active witnesses are changing every 1 minute in the example. Commit and reveal periods succeed each other on each stage. Each witness automatically provides its own commit of a hash followed by a reveal number.

A sample file provides details:

1. Votes for 5 witnesses upon initiation.
2. Continuously prints an account of each witness who produced a block.
3. Prints a number of selected active witnesses after each maintenance overturn (selection).

Layer-1 Prototype

Repositories can be found here:
https://github.com/Revolution-Populi

Implementation

Because this layer-1 is really just a decentralized data facility, transaction speeds can be lightning fast by comparison. Simply put, the mainnet doesn’t get clogged up by a bunch of unnecessary traffic. With this new layer-1, there is just a distributed, decentralized database for different apps to connect into and to share data decentrally, and yet commonly, without betraying or compromising the user’s data.

Each blockchain account can be controlled using a small secret key stored on the user's device - in what we can call a wallet. Keys are used to sign and send transactions to the blockchain. They can also be used to obtain access to content.

Components

Core Blockchain

The structure includes the Core Blockchain based and a cloud storage "starter kit". The starter kit is for "ease of demo" purposes, and uses a standard mainstream commercial storage just for these purposes. The end system can employ a secure and decentralized storage system (or even multiple systems) such as the InterPlanetary File System (IPFS) or some other similar module or modules. More generally, any app will be able to employ different storages.

RevPopJS

This is the client library for the Core Blockchain, which enables other applications to use the layer-1 blockchain. This idea is commonly referred to as the "DApps" construct in the blockchain space. It'll be open for any app to use, with open options for tech stacks, pipelines and services.

RevPop Samples

We've also included sample files demonstrating different RevPop blockchain scenarios.

How To Run

In short, you need to build and run the Core Blockchain, then install and run sample scripts.

Build and run the Core Blockchain

The easiest way to do this is by using a Docker image. Instructions on how to build the blockchain on your own are available in the repositories.

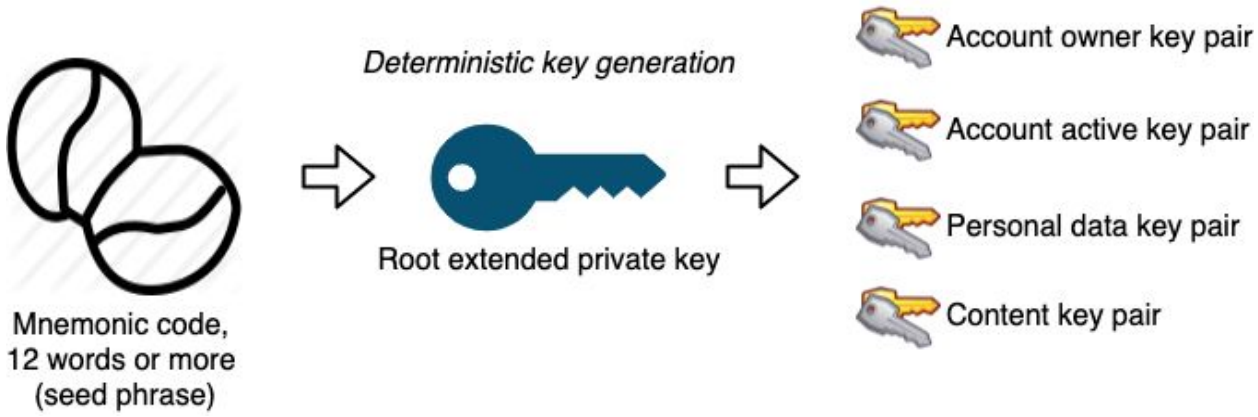
Build and run the Prototype

You can use a pre-configured Docker Compose environment to run all components (in minutes).

System Architecture

Key Generation

Keys are generated from a memorable seed phrase. A user can get access to their account from another device simply by re-entering the seed phrase (while users mainly use their individual mobile devices for their activity, which is personal and secure, and typically in a person's possession, we've also made accommodations for users who wish to use the system on different devices that belong to them, e.g. a tablet).

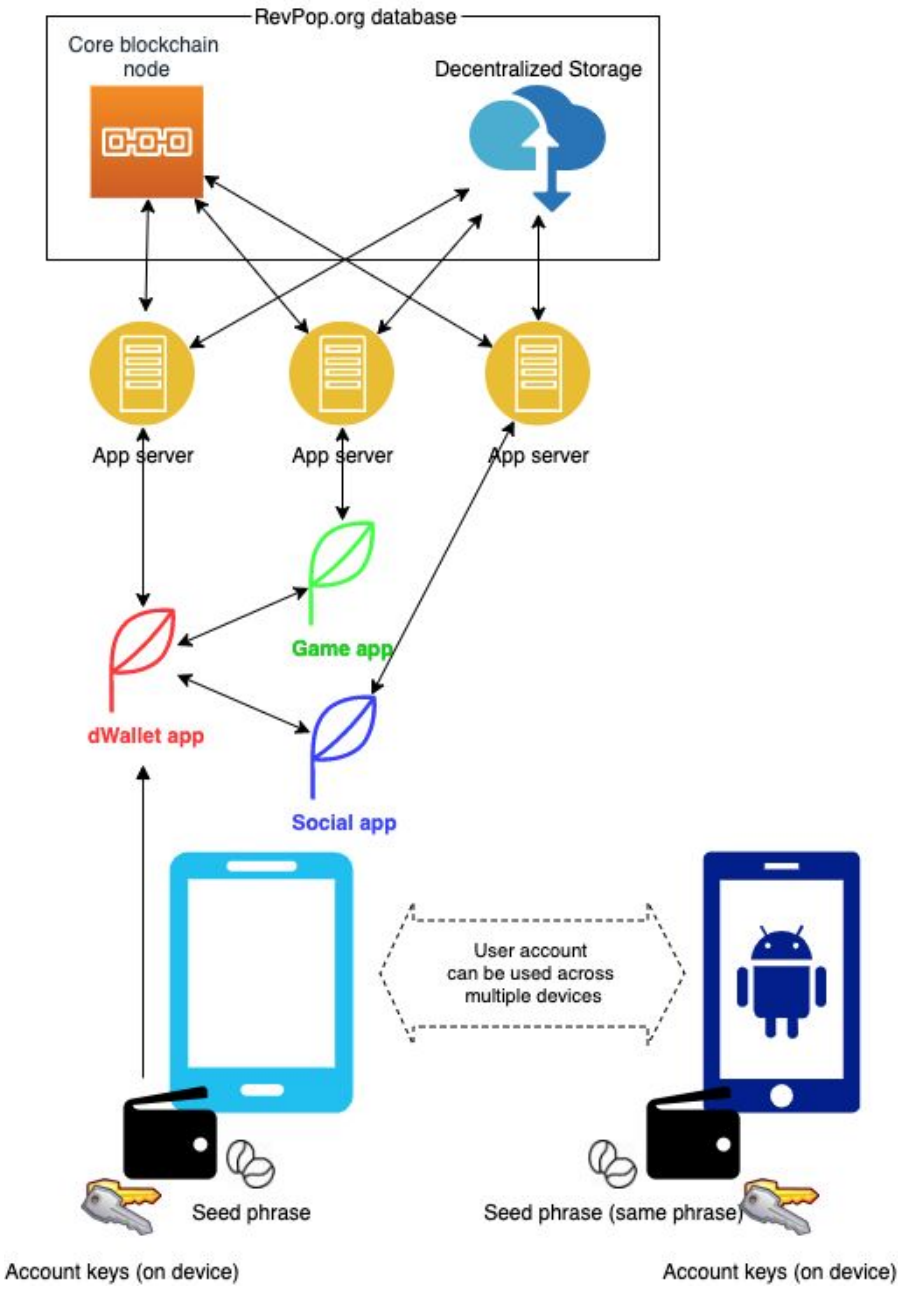


To protect the private key of a user, we've devised an option, but not a requirement, whereby a decentralized, distributed and secure "hot storage" application, based on Shamir secrets between nodes or some other advanced cryptographic mechanism, can be developed and implemented to store keys for other apps to reference. Let's call this a "dWallet" app or just the "dWallet". Other applications can then sign transactions on behalf of a user through such an app, which would have to be done with the consent of a user. These private keys may otherwise just be stored on a user's device directly, and DApps (e.g. social networks, games, etc.) can just access the keys directly.

Ecosystem

Applications would be installed on a user's device. The dWallet app creates a blockchain wallet for the user. All app data, except the wallet keys, can then be synchronized between devices using cloud.

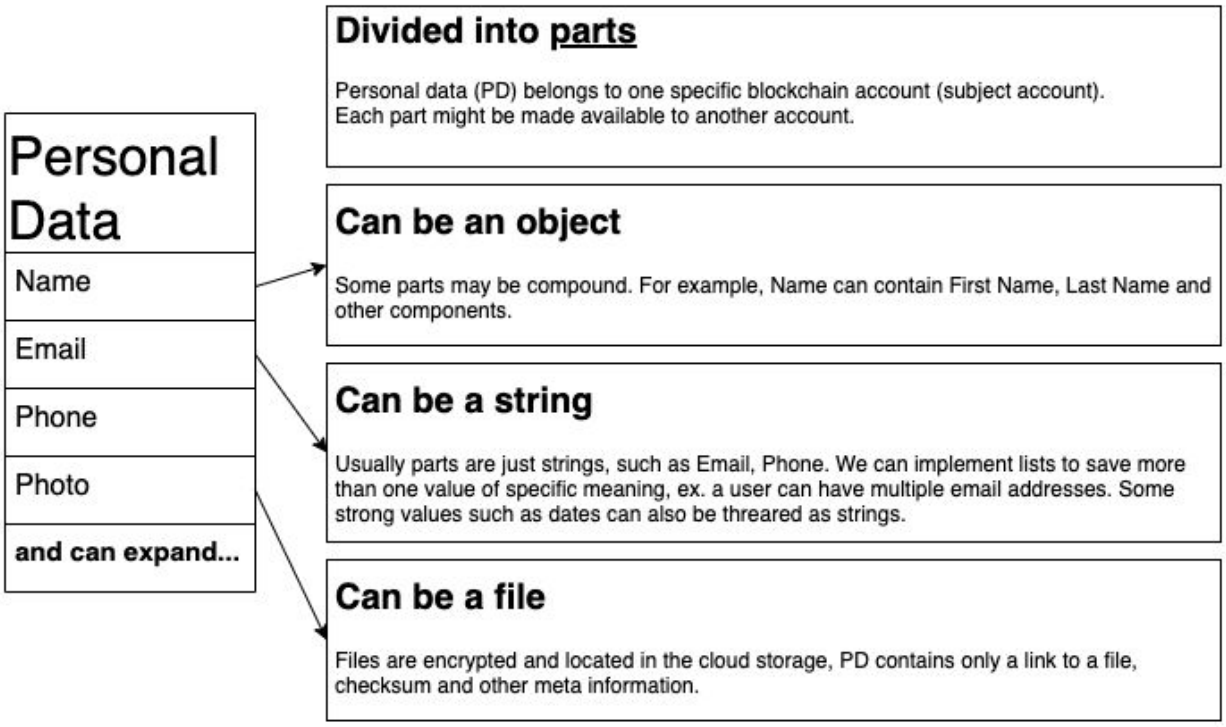
Applications can communicate with the blockchain directly or through an app server. They can read data from the blockchain as well as from the cloud storage (or decentralized storage, as the case may be). Restricted information can only be unlocked from the user's device, or the application server (but only if explicit permission is granted).

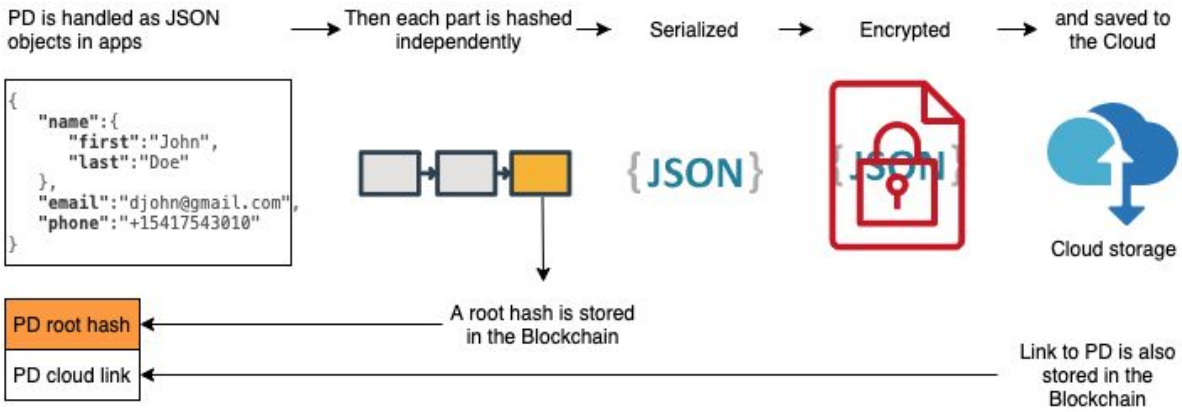


Users

Registering for the First Time

This demonstrates how a user registers in the RevPop ecosystem for the first time using a RevPop-powered app. Here's how the Personal Data (PD) is structured:



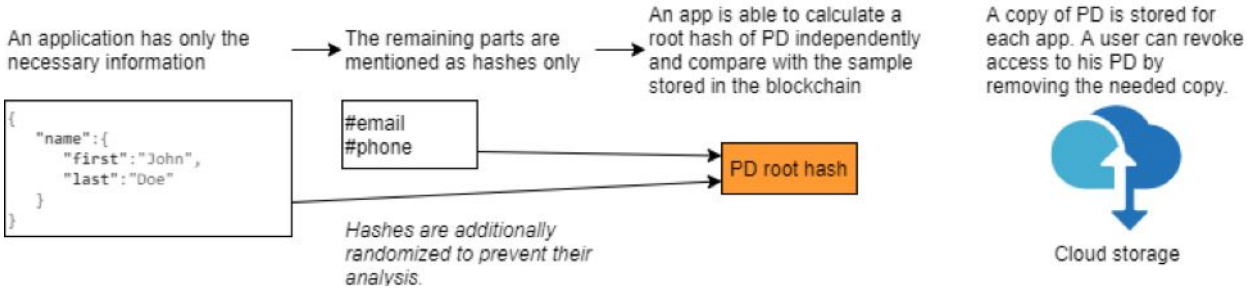


Sample files (available at https://github.com/Revolution-Populi):

1. case1-onboarding.js - an example of how to create a new blockchain account for a user. Then a user saves his personal data in the blockchain and allows access to the application. Some preparation steps are required before running this sample file. They can be performed by running case0-bootstrap.js.
2. sample-1-account.js - implements the following scenario:
    a. Generate private/public keys
    b. Get balance object and claim balance by registrar account
    c. Upgrade registrar account
    d. Create a new user account with keys generated
3. sample-2-personal-data.js - implements the following scenario:
    a. Save personal data photo to the cloud storage
    b. Create full personal data and sign with the root hash
    c. Save full personal data to the cloud storage
    d. Save full personal data record to the blockchain
    e. Load full personal data + record + photo from the blockchain and the cloud storage
    f. Verify full personal data with the root hash
    g. Create partial personal data and sign with the root hash
    h. Save partial personal data to the cloud storage
    i. Save partial personal data record to the blockchain
    j. Load partial personal data + record + photo from the blockchain and the cloud storage
    k. Verify partial personal data with the root hash

Using Other DApps

The following demonstrates how a user shares PD with another layer-1-powered DApp:



Various parts of existing personal data can be used for signing in to another app; and more information can be added through other apps as well. New apps can verify personal data using a root hash published in the blockchain.

Sample files:

1. case2-registering.js - an example of how to register in another layer-1-powered application using the personal data already stored in the blockchain. Some preparation steps are required before running this sample file. They can be performed by running case0-bootstrap.js and case1-onboarding.js
2. sample-2-personal-data.js - see the previous section for the details

Permitting Other Apps to Publish Content

“Content” is represented in the blockchain by a Content Card.

A Content Card contains:

- Owner account
- Url in the cloud storage
- Publication time
- Type (image, document, etc.)
- Checksum (for verification)
- Encrypted key (private, available to Owner only), used for content decryption
- Description, optional, can be used for indexing

To allow another account to access the content, we create the record in the blockchain.

Content permission information:

- Owner account (who granted a permission)
- Operator account (to whom permission is granted)
- Content card identifier
- Encrypted key (private, available to Operator only), used for content decryption
- Timestamp when a permission is granted

Each content card and permission can be added/updated/removed via a blockchain transaction.

The sample file sample-3-content.js implements the following scenario:

1. Save the encrypted content to the cloud storage
2. Remove the content card
3. Create the content card
4. Remove the permission
5. Create the permission
6. Read the permission
7. Read the content card
8. Load the encrypted content from the cloud storage
9. Update+read the content card

Liking Content

1. Any account can vote for (“like”) any content. Adding a vote means sending a transaction to the public blockchain.
2. Information about who voted for what is private by default.
3. A user can share all his votes with any other account. This account can see all user’s past and future votes.
4. Any user can see the total number of votes for specific content.

These properties of the system are achieved by a special design where each vote is processed by a randomly selected master node. A master node accumulates different votes, mixes them and publishes a generalized update. This is a powerful and confirmable structure to determine the total number of votes. The next sample checks that these votes (“likes”) go to the right place.

The sample file sample-4-votes.js implements the following scenario:

1. Create content cards
2. Find witness to choose the master node
3. Vote for the content
4. Read and check the vote counter of the content
5. Share voting information with another account
6. Read voting information of another account

Key features of the RevPop Blockchain

1. RevPop's blockchain topology introduces a simple method for storing, securing and serving immutable data, owned and controlled by each user.
2. The system is designed to allow the speed of existing centralized social networks, security through decentralization, full control of user data to the user; and a structure whereby apps can build as they see fit, using tech stacks and services that make sense for them (as an example Chainlink’s decentralized network for data transmission).
3. The blockchain protocol is set up for off-chain integrations both for developer flexibility, but also to limit unneeded throughput to the blockchain. Confirmation speeds can be upheld, less costly systems can run confirmation processes, and the network would still maintain a first rate level of security.
4. DApps would be able to access the layer-1 blockchain through preconfigured APIs that include user validations for data access. Users of these DApps can then have options for different levels of access on a per app basis. Once the user grants access, the data is

then integrated with the layer-1 database, with each person's data remaining theirs and theirs alone.
5. RevPop's system can offer a new paradigm for the money generated from data. Power over content and data would be vested in the hands of the data generator, where it rightfully belongs; and therefore the ability to monetize the data would too.

Starter Kit Software

Summary

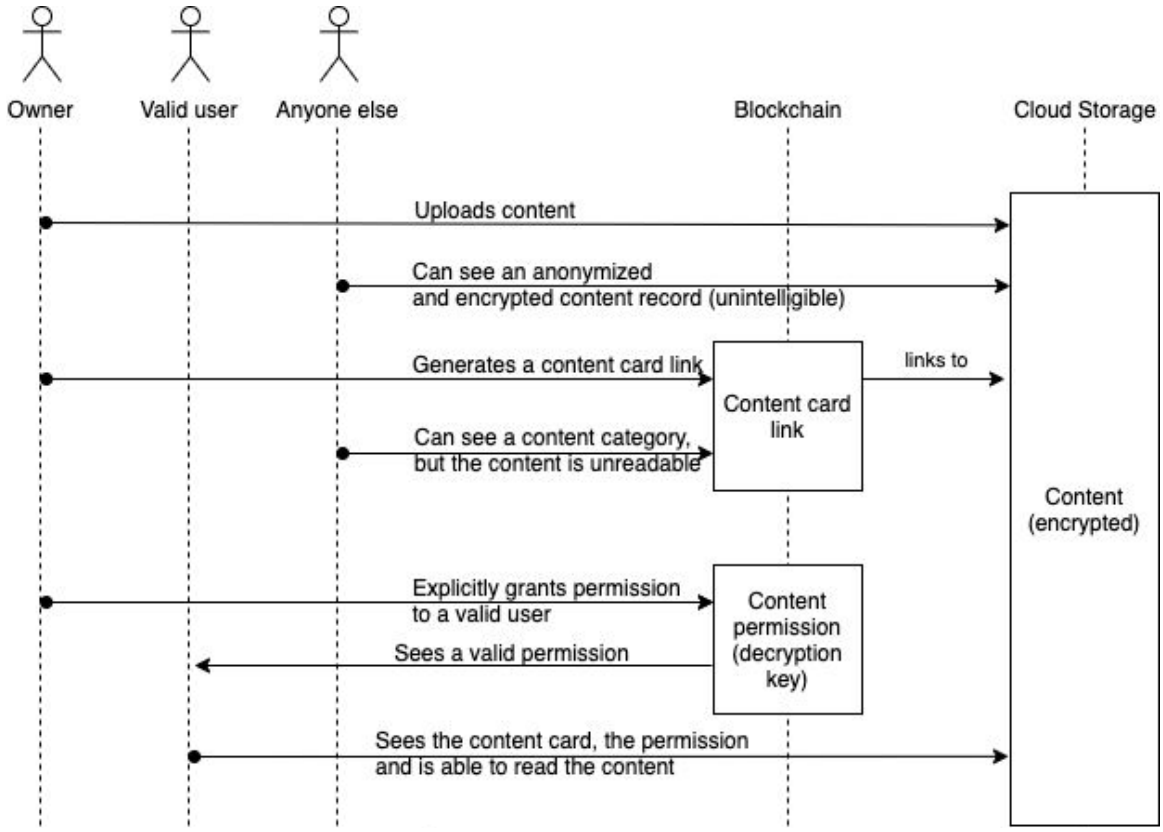
The published prototype is a starter kit, with more to come, beginning with the following:

1. Personal data of a user.
2. Content files.
3. Memorializing and counting user votes.

All this information is stored in the layer-1 database. Heavy content resides in cloud storage, while the link to it and other lightweight content lives directly in the blockchain.

Information stored in the layer-1 database is not available to everyone, since it is encrypted. Only selected individuals and apps can retrieve it by the owner's permission. An owner can do this by sending a special permission object containing a decryption key to the blockchain.

The following diagram shows the process of uploading content and granting access to it:



Conclusion

Many different services can be implemented on top of this new layer-1 in a way that is secure, well-functioning, and that foremostly honors data sovereignty.

Disclaimer: This paper is meant to advance discussions and provide some technical guidance, and is not meant to promote any token sales or equity investment by or in Revolution Populi Limited or any of its affiliates or subsidiaries. This paper is in draft form and may change over time.