crypto.com

Social Graph and Digital Identity in Web3

November 2022

Research and Insights

Research Analyst (Operations)
Olivia dela Rosa

Published on 6 Dec 2022

RESEARCH DISCLAIMER

The information in this report is provided as general commentary by Crypto.com and its affiliates, and does not constitute any financial, investment, legal, tax, or any other advice. This report is not intended to offer or recommend any access to products and/or services. The views expressed herein are based solely on information available publicly, internal data, or information from other reliable sources believed to be true.

While we endeavour to publish and maintain accurate information, we do not guarantee the accuracy, completeness, or usefulness of any information in this report nor do we adopt nor endorse, nor are we responsible for, the accuracy or reliability of any information submitted by other parties. This report includes projections, forecasts, and other predictive statements that represent Crypto.com's assumptions and expectations in light of currently available information. Such projections and forecasts are made based on industry trends, circumstances, and factors involving risks, variables, and uncertainties. Opinions expressed herein are our current opinions as of the date appearing in this report only.

No representations or warranties have been made to the recipients as to the accuracy or completeness of the information, statements, opinions, or matters (express or implied) arising out of, contained in, or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) that may arise from any person acting on any information and opinions contained in this report or any information made available in connection with any further enquiries, notwithstanding any negligence, default, or lack of care, is disclaimed.

This report is not meant for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of Crypto.com in any form is prohibited except with the written permission of Crypto.com. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction, where such distribution or use would be contrary to applicable law or that would subject Crypto.com and/or its affiliates to any registration or licensing requirement.

The brands and the logos appearing in this report are registered trademarks of their respective owners.

Contents

Executive Summary

- Of the five billion Internet users in the world today, **4.7 billion use social media**.
- **Privacy, security, and surveillance capitalism** are common issues with Web2 social media platforms because they compromise the foundation of social networks: relationships (represented as social graph) and identity.
- A social graph refers to the global mapping of all users, which reflects individuals, their connections, and their interactions and behaviours towards others.
    - Decentralised social networks present a **universally accessible**, **unified**, **and decentralised social graph**, acting as a standard that maintains users and all their social data across different platforms and networks.
    - **Lens Protocol is a decentralised, smart contract-based social graph** which aims to empower profile owners to decide how they want to build their social graph and monetise their own content.
    - **CyberConnect is a decentralised, smart contract-based social graph protocol** that enables ownership of users' social identities, content, and connections in a social network, and provides a composable social data layer for developers.
- Compared to traditional identifiers, **decentralised identifiers** are different in that they are owned, held, and controlled entirely by the individual.
    - The **global decentralised identity market value** is estimated to reach US$6.8 billion by 2027.
    - **Cronos ID is a decentralised identity and communication protocol**, offering NFT domains with a '.cro' extension, making it easy for users to transfer digital assets without having to worry about non-readable wallet addresses.

1. Introduction

The Internet has evolved from being a network of links and documents to being a network of people, as individuals continuously bring their social connections online. Social media marries people's collective social needs with the Web, and today it has become a way of life**. More importantly, social networks are proof that identity and relationships are the fundamental building blocks of this evolving hyperconnected digital world.**

However, one major issue users face today is the lack of control and ownership of their personal data on traditional social media platforms. In these traditional social networking services, or Web2 social, users typically have no choice but to blindly trust the service provider to not misuse their personal data. The opposite is true in most cases: private user data that is supposed to enrich the user experience is either being monetised, censored, or even weaponised by these companies.

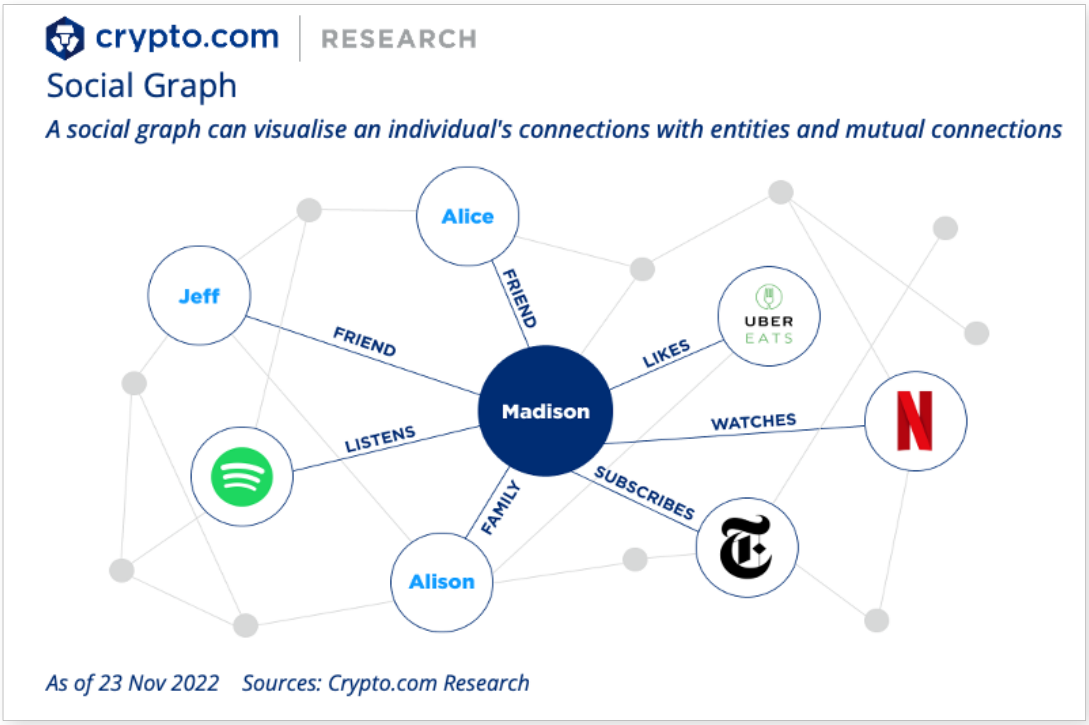
To ensure and establish a secure digital world, proving and managing one's identity has also become critical. While we have existing identity systems in place today, they have their own limitations too. A complete solution and infrastructure doesn't exist yet. We will explore how blockchain-based identity systems can help to solve these problems.

In this report we will discuss the concept of **decentralised social networks (Web3 social)**, **or blockchain-based social networks built for data exchange**, **social interaction**, **and content creation**, and how they offer to solve the challenges faced by users today. We will take a deep dive into their inner workings through two key elements: social graph and identity.

2. Social Graph

Of the five billion Internet users in the world today, 4.7 billion use social media. Thanks to these social networks, large quantities of personal digital information are being created on a daily basis. To represent these data sets and their relationships, a social graph is formed. **A social graph refers to the global mapping of all users, which reflects the individuals, their connections, and their interactions and behaviours towards others.** Given the relationships between its nodes (users) and its edges (connection between users, e.g. bidirectional "friend" or single-directional "follow"), social data can be modelled as a graph.

Social networks utilise social graphs as a data structure to visualise social relationships efficiently. Aside from an individual's connections (friends), social graphs can also show their relationships with organisations, mutual connections with other individuals, and other personal information (e.g. posts that the person liked and commented on) shared on the platform.



As the amount of user data grows on each social network, these social graphs will begin to overlap. However, because there is no standard being used by these platforms, moving a user's social identity and connections from one platform to another is not always possible. Before we discuss what an ideal

solution looks like, let's take a closer look at other major pain points that Web2 social users experience.

2.1 Role of Social Graph in Building Web3 Social Networks

Data privacy, ownership, and control: Every successful social network has their own social graph, which has become their core asset. What's important to understand here is that **the value of these centralised social networks is created by their unpaid users who worked hard building their online presence, which includes both their social graph and also their persona** – not by the company itself nor its underlying technology. Private information, content, connection, and interactions created and shared by the user in the platform can be farmed and used in various different ways, mainly to the benefit of the companies. Typically, the privacy policy agreements in these social media platforms legally allow the sharing of their users' personally identifiable information with third parties – advertisers, developers, partners, and other companies – depending on how these users are using the platform. Therefore, with this centralised model, **monetisation potential stays with the entity who controls and owns the social data, which is the company instead of the user.**

Web3 social offers an ideal alternative, wherein at the end user level, social identities are user-owned and private by default. **Data ownership and control are returned to individuals, giving them the ability to authorise access to anyone and they can monetise their content however they want.** Every connection and content is typically secured with a signed key, and only the person with the private key could have authorised these links. By applying privacy solutions such as data encryption and zero-knowledge proof, trustless verification and privacy preservation of user data within social networks becomes possible. More importantly, this overall framework eliminates the possibility of an external party misusing users' personal data.

Data storage*:* The infrastructure within traditional social networks uses centralised databases for storing users' data. However, this monolithic approach to data storage is not ideal, as the platforms can become a single point of failure and can lead to huge amounts of data being compromised. Case in point: it was reported that social media leaks made up 41% of all data records breached in 2021, proving that social media can be a security weak point for online channels. Additionally, the breach of personal data also leads to other security issues, such as identity theft and fraud. This can affect both users and their network.

The infrastructure for Web3 social is different: **the storage layer predominantly relies on decentralised storage solutions and is therefore not affected by a single point of failure.** Decentralised social networks can fully store their social data on-chain (e.g. DeSo), where public data can be accessed by anyone and private data can only be accessed by properly authorised parties. Meanwhile, some protocols offer a combination of on-chain and decentralised storage solutions (e.g. CyberConnect), mainly to efficiently balance performance and scaling with permanence and on-chain costs.

Read our detailed report on dynamic storage solutions in Web3*: Dynamic Storage Solutions in Web3*

Portability*:* Users struggle with data portability for vertically integrated social media platforms. If users want to switch from one social network to another (e.g. moving from Facebook to Twitter), they have to check if their connections exist on the other platform, and follow people and add their friends all over again. Users' actions are basically limited by the platform, where all information is locked into its own ecosystem.

The pain points are not isolated to end users either: this walled garden approach presents a high barrier of entry for developers, hindering the expansion of social networks, and ultimately the growth of the ecosystem. If developers want to implement a new feature or a new social application on top of a centralised social platform, they will be facing much bigger problems when there is no single open-source social graph to build upon.

Meanwhile, Web3 social runs on independent blockchain-based services, enabling social network portability across platforms and chains. **Decentralised social graphs serve as an interoperable solution that allows 1) users to easily take their data with them across different networks, and 2) for developers to build social dApps upon**.

Federated vs. decentralised networks: In the pursuit of a fully decentralised and user-centric world, another type of social network structure also came about — federated networks. Federated networks are not dependent on a single set of servers run by one company, allowing individuals to access the entire network made up of many different servers. In federated networks anyone can run a server, which removes the client-server model which Web1 social operates on; however, it is still a step away from decentralised networks in that it still needs servers to connect users.

2.2 Social Graph Infrastructure for Web3

The concept of a fully decentralised social network presents a universally accessible, unified, and decentralised social graph. It acts as a standard that enables users, along with all their social data, to move seamlessly between platforms and networks. They will not need to repeat the entire identity verification process for every platform and rebuild their connection network.

Because user data is readily available and accessible, **decentralised social graphs make it easier for developers to build new applications and features on top of social network platforms**. Given their interoperability enabled by the blockchain, these on-chain social graphs can connect other social networks with ease, and can also extend to other decentralised applications such as blockchain games and the metaverse.

Decentralised social networks are not perfect and they do have their own set of limitations. However, they bring individuals closer to a self-sovereign identity and user-owned social graphs.

Comparison of Different Types of Social Network

crypto.com | RESEARCH

	Centralised Social Network (Web1)	Federated Social Network (Web2)	Decentralised Social Network (Web3)
Description	Relies on a central server to mediate communications between all other nodes	Trust is established and standards are accepted between multiple independently-run servers	Identity is self-issued and data ownership truly belongs to individuals
Examples	*Facebook, Twitter, Instagram*	*Mastodon, Pleroma, PeerTube*	*Lens Protocol, CyberConnect, Mem Protocol*
Data storage	Centralised storage	Distributed storage (controlled by a single entity, for example, cloud)	Decentralised storage (peer-to-peer)
Data privacy	Low privacy, data is managed by service provider	Limited privacy capabilities	High privacy
Data control and ownership	Social media platforms own user data	Provides some sense of user data ownership and control	Users own and control their personal data
Portability	Data is locked in the platform	Data export is mostly available, but not full portability	Portability is possible between platforms, data can become platform-agnostic
Transparency	Low transparency	Data is publicly accessible via database servers	Data is publicly available and verifiable on-chain
Interoperability	Mainly isolated within the platform and applications built on it	Interoperable with other federated sites	Allows for cross-protocol and even cross-chain interoperability
Data sharing	Platforms decide what can be shared and who it can be shared with	Tend to be ad-free, crowdfunded, and community-owned	Can be parameterised on how much data can be shared

As of 23 Nov 2022 *Sources: Crypto.com Research*

2.3 Social Graph Solutions

Lens Protocol

Built on the Polygon proof-of-stake (PoS) blockchain and brought to life by the same team who developed Aave, **Lens Protocol is a decentralised, smart contracts-based social graph**. It enables the formation of a fully composable, user-owned social graph by allowing users to own their connections between themselves and their network. The protocol is designed to be permissionless and controlled by a community multisig to authorise certain actions.

It features three standalone key modules, or whitelisted smart contracts, that allow profile owners to add custom functionalities and further value to their social connections and content:

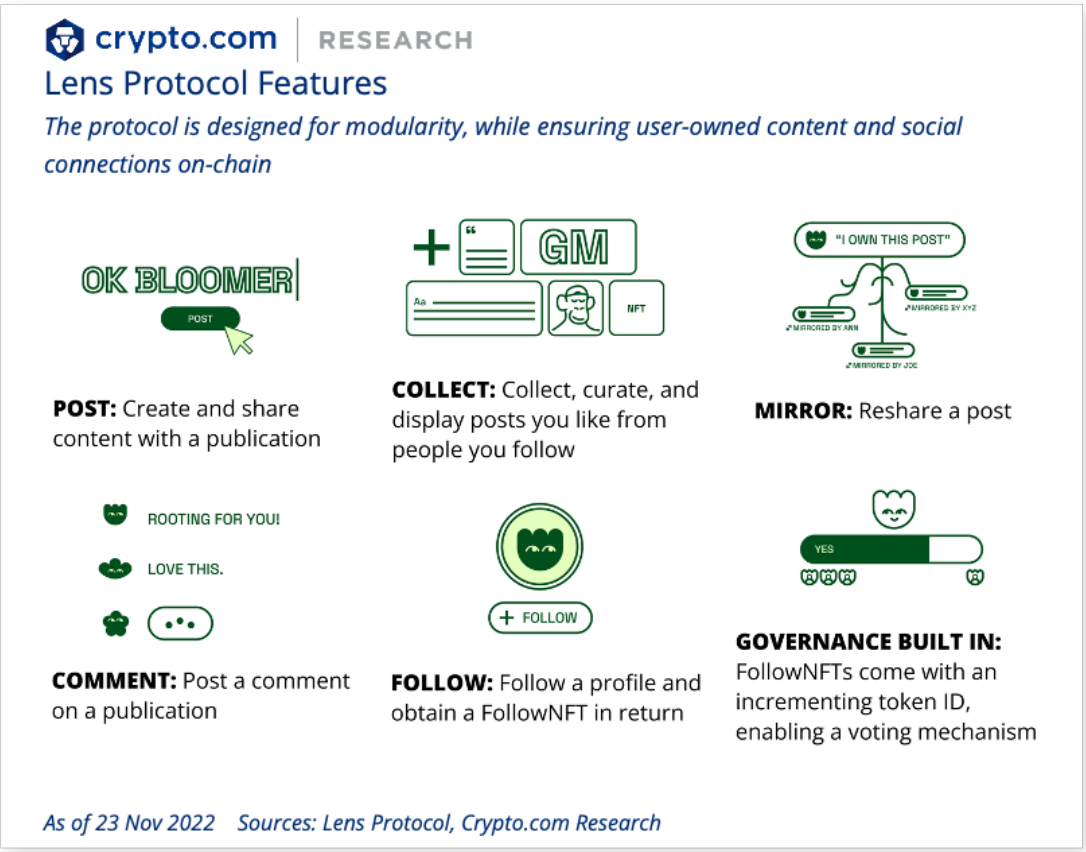
- **Follow**: executed when a given profile is followed;
- **Collect**: executed when a publication is collected, excluding mirrors;
- **Reference:** executed when a profile mirrors or comments on a publication, and publications can opt to have no reference module

Lens Protocol aims to empower profile owners to decide how they want to build their social graph and share their own content in various ways. For instance, because creators own their content, they can monetise them via 'Collects', while 'Follow' modules allow profiles to set fee-on-follow or other subscription mechanisms. Users and developers alike are free to build more advanced monetisation and content-gating rules, thanks to these modules available.

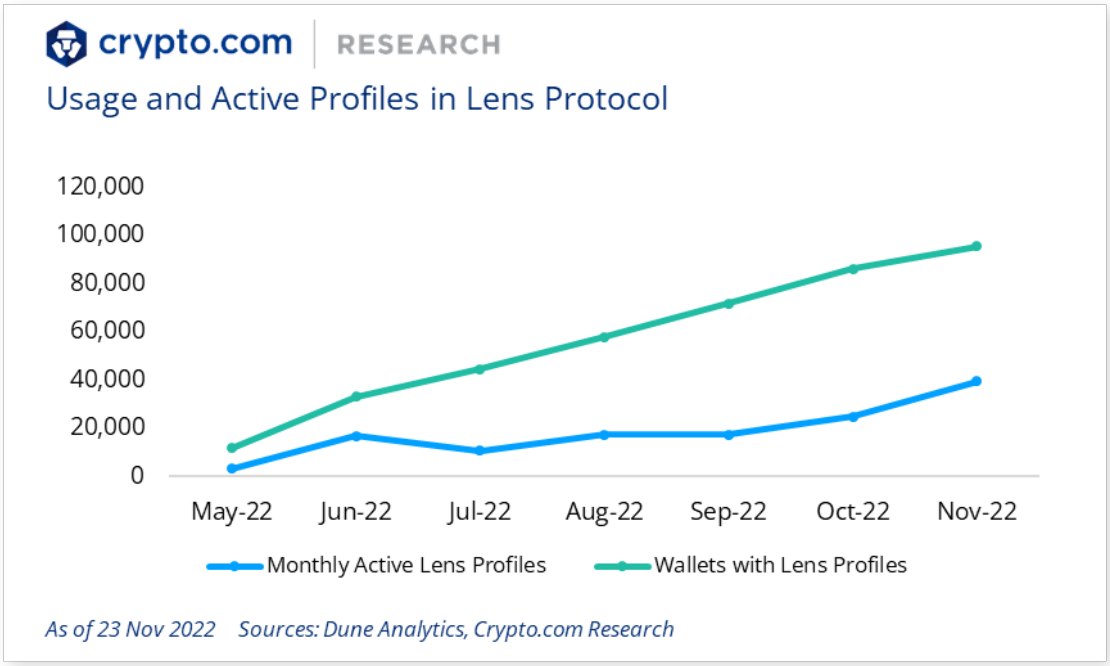
The following key features act as primitives that define the layout and relationships between profiles, such as who follows who or who owns a publication. Each feature serves as core building blocks of the Lens Protocol social graph. They are similar functions that can be found in Web2 social platforms, with the main difference being that they are enforced through the use of smart contracts.

- **Profile:** A user can create multiple profiles in Lens, and a profile NFT is issued for each profile created. This profile NFT acts as an on-chain identity that proves ownership and control of all content generated by the user. Users without a profile NFT cannot create posts but can still follow other profiles.

- **Post:** Once a user creates a profile, it can post content on any application built on top of Lens Protocol. Post is a type of publication that is posted directly to a user's profile NFT.
- **Mirror and Comment:** Mirrors and comments are two other types of publications, offering functionalities to posts which then help expand the Lens Protocol social graph. Mirrors are a function similar to reposting or amplifying existing content typically published by another profile. Meanwhile, profiles can comment on a post, and this comment is then saved to the user's profile NFT.
- **Collect:** Users can collect, curate, and display posts they like from other users they follow. Users can also set a 'Collect' module to their own posts, enabling mechanisms such as allowing users to purchase their content, setting a specific number of 'collects', or even sharing time-limited posts.
- **Follow:** At a basic level, following a profile in Lens will issue a user a "Follow" NFT to record the connection, which comes with a unique token ID. The Follow Module enables users to set requirements for other users who want to follow their profiles (e.g. pay x tokens to receive one "Follow" NFT).
- **Built-in Governance:** These "Follow" NFTs are also crucial to the Lens ecosystem as they include traits that enable voting and governance mechanisms, depending on the governing body and voting strategies set. For example, profiles (which can represent a social DAO or an organisation) can involve their followers and connections in the decision-making and governance process, employing "Follow" NFTs as voting requirements.



Given these capabilities, the Lens Protocol social graph today features a growing list of partners and enables an ecosystem of interoperable social applications.



CyberConnect

CyberConnect is a decentralised social graph protocol that enables ownership of users' social identities, content, and connections in a social network, and provides a composable social data layer for developers.

Like Lens Protocol, **CyberConnect also uses smart contracts called middlewares to support the functions of social networks**. Essentially, middlewares provide users control of their connections and content, and enable developers to build dApps on top of the protocol.

There are three main types of middleware in the CyberConnect infrastructure:

- **ProfileMiddleware**: executed upon profile creation;
- **CollectMiddleware:** executed when publications are collected;
- **SubscribeMiddleware:** executed when a user subscribes to a profile

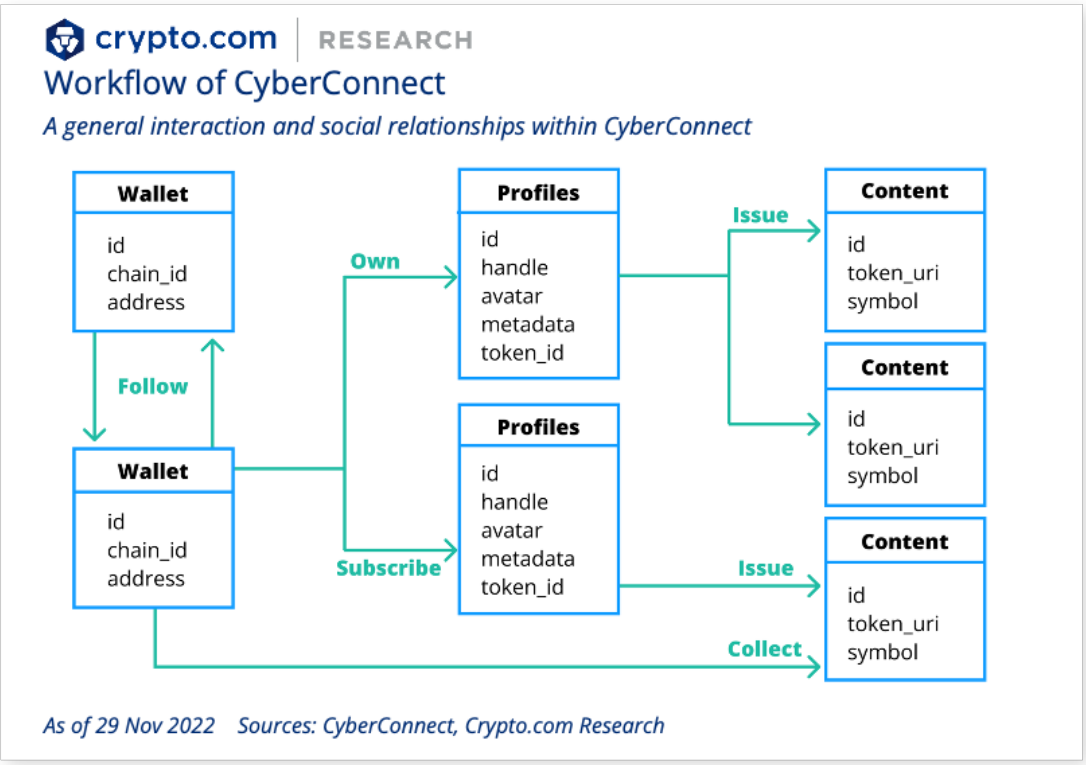
A general workflow in CyberConnect looks like this:

- **Profile creation**: A user (represented as a wallet) can create one or multiple profiles. Social connection occurs when a user follows another user, or when a user subscribes to a profile. Each user profile is represented as an NFT and serves as the main entrypoint for every

on-chain action. A user can create multiple profiles, and each profile owns its paid subscribers and content – all of which are stored in the profile NFT.

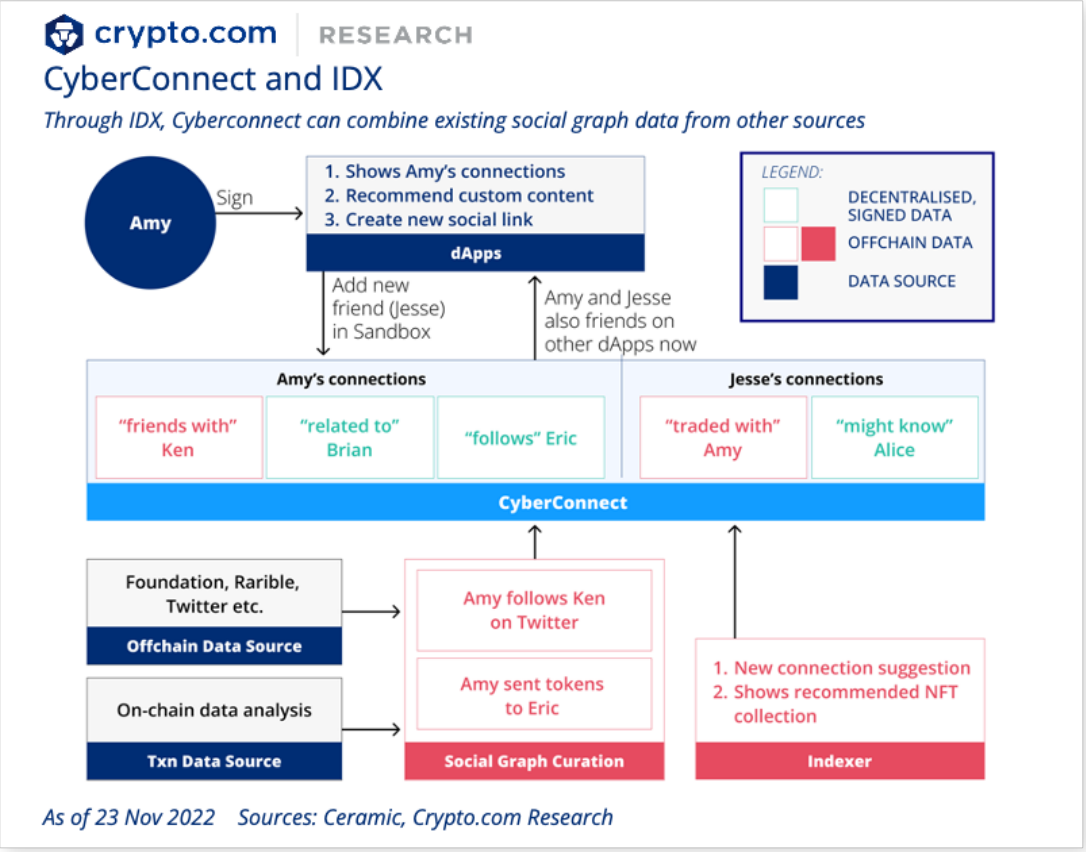
- **Content publication**: Every piece of content is tied to a specific profile, and this content is represented as an ERC721 token called EssenceNFT. It supports standard content like published long-form posts, as well as dynamic content such as badges or verifiable identities. These pieces of content can all be stored on decentralised storage platforms such as IPFS or Arweave. Through the Collect Middleware contract, other users can also collect these pieces of content and profiles can set functionalities for their content (e.g. pay X tokens or hold a specific NFT to collect).

  Since they have ownership of their profile and content, users have the ability to enable monetisation on their profile through paid subscriptions: They can set up subscription rules which specify the requirements (e.g. pay X tokens or hold a specific NFT/badge to subscribe) needed to subscribe to their profile. In return, subscribers will be given a SubscriberNFT as on-chain proof. The diagram below illustrates these interactions and relationships:



CyberConnect uses IDX, Ceramic's cross-chain identity protocol which enables the creation of an identity index and keeps track of a user's social information and activity. Through IDX, applications built within CyberConnect can access a

shared, universally available identity layer, making it easy for them to integrate with other social applications. **By leveraging the indexing capabilities of IDX, CyberConnect can combine existing social graph data from different sources**.



In terms of data storage, CyberConnect offers a hybrid solution to handle updates to connections between users through "operation logs" wherein a new hash-linked list is created on the first transaction.

Let's say User X follows User Y for the first time. This starts an operation log. As states change between these two users (e.g. X unfollows Y), a new node is created and appended to the tail of the log. Each new state is stored locally on a central server, while the tail of each log is uploaded to a decentralised storage system (IPFS via Ceramic) through a batch upload logic.

CyberConnect focuses on being developer-friendly by providing them with a rich set of tools to build social applications. Two components are currently available for developers to build with: Social Data Network and Interest Graph Engine.

3. Decentralised Identity

Another key element to social networks is identity. In a broad sense, digital identity can be defined as a set of information that is used to represent, evaluate, and authenticate a person or an entity in the digital world.

Privacy and security concerns are common with Web2 social networks. General users are vulnerable to fraud and identity theft on social media.

Surveillance capitalism is another major issue within traditional social networks: Most centralised networks operate on business models centred around selling anonymised user data to other entities. Furthermore, because identity verification on these networks relies heavily on external parties, the platforms are susceptible to inauthentic accounts, the majority of whom tend to share unwanted content.

Decentralised social networks aim to take identity ownership and control away from centralised systems and return them to users. Because the user identity and all its on-chain history are free to move, it breaks down the barrier between platforms and makes it easier for users to move from one platform to another without having to rebuild their connections.

Through a programmable on-chain identity, **users have full control of their digital identity by allowing them to set parameters for anyone to gain access to their profile and content.** This also offers various opportunities for users to further monetise their content.

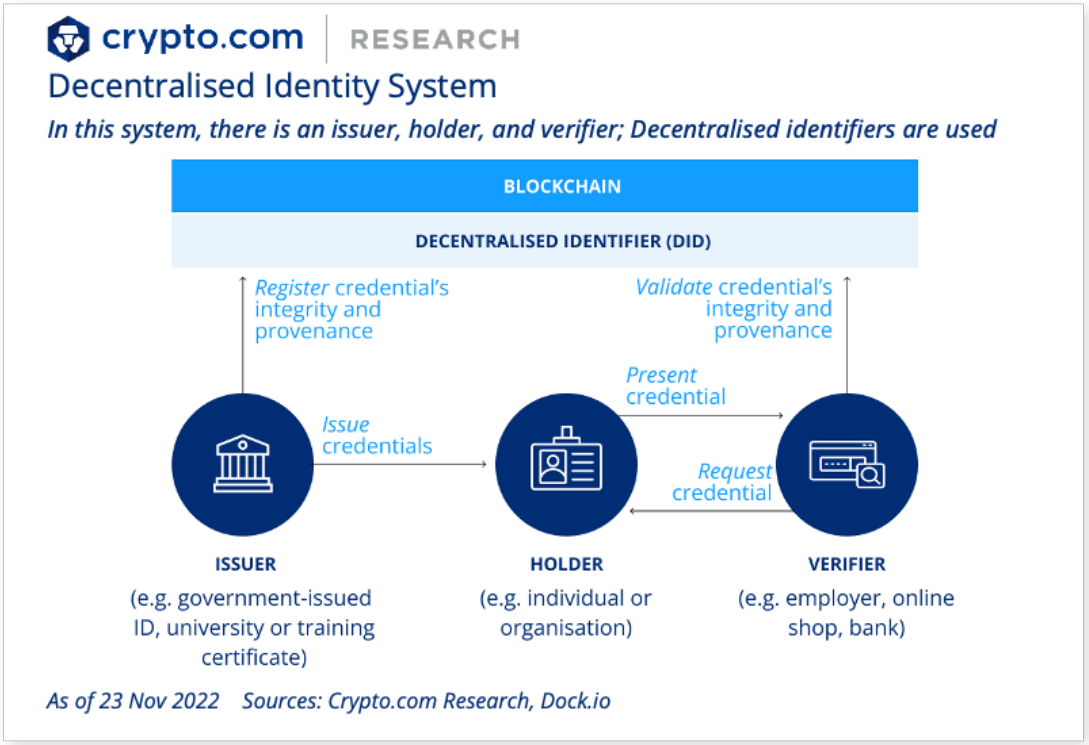
These issues highlight some of the limitations of privately-owned social networks and serve as a catalyst for blockchain adoption. Ultimately, the rise of decentralised social networks can be foreseen in the future.

KBV Research reports that **the global decentralised identity market value is estimated to reach $6.8 billion by 2027**, with a 78.5% compound annual growth rate. There is massive potential for decentralised identity to disrupt the social network space and other industries where digitisation is a main factor, and the commercial opportunities are also worth paying attention to.

3.1 Decentralised Identifiers

Identifiers, in the traditional sense, are pieces of information that act as pointers to a particular identity or identities — much like how a birth certificate acts as legitimate evidence that your identity exists or how a passport proves you are a citizen of a certain country.

An alternative solution can be found in decentralised identifiers (DIDs) to address the challenges mentioned above. In a decentralised identity system, the issuer can issue signed credentials to an individual. This credential can be stored on-chain as a decentralised identifier, which is a non-transferable NFT. The verifying entities can then validate this credential from the blockchain.



Today this is mainly materialised through **Soulbound Tokens (SBTs)**, or non-transferable and non-tradeable NFTs containing verifiable information that's unique to its owner.

Most SBTs focus on linking users' real-life or off-chain credentials with their on-chain identity (e.g. wallet address). We can see their practical applications in the market today: For example, Binance offering Binance Account Bound (BAB) Tokens which serve as proof that its users have passed KYC, Otterspace empowering DAOs with the issuance of non-transferable badges, and Masa launching the first SBT single sign-on for Web3 applications.

Read more about SBTs in our report: *Soulbound Tokens & Decentralised Society*

3.2 Digital Identity Solutions

NFTs also have the potential to be an anchor for decentralised identity. Instead of mere usernames, users can utilise their NFTs to identify and build

their presence online. Projects within the Cronos ecosystem best demonstrate this utility, and we can point to Cronos ID as a prime example.

Cronos ID

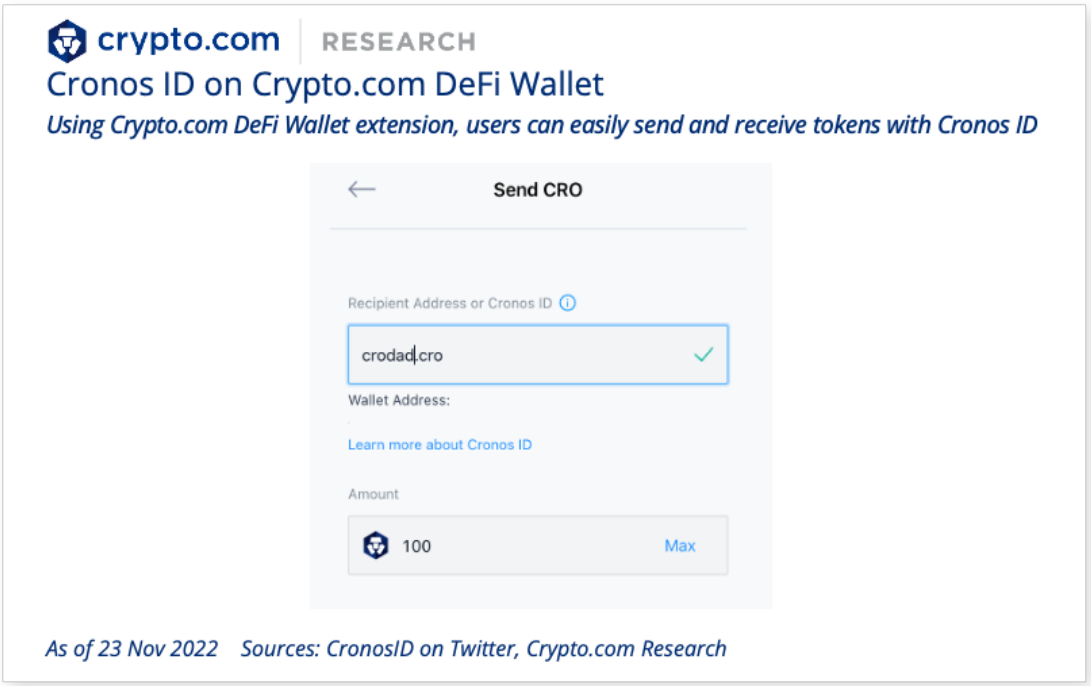
Cronos ID is a decentralised identity and communication protocol built on Cronos, an EVM-compatible chain. Cronos ID offers NFT domains which gives users the ability to send and receive information on-chain through human-readable identifiers.

These human-readable identifiers come in the form of easily recognisable domains with a '.cro' extension that users can associate with their EVM wallet address. Cronos ID domains are short and easy to remember so users can seamlessly send and receive digital assets while allowing them to find other people with ease. Each user has full ownership of their own unique username, which can also be bought and sold in Minted. Users can attach one or several identities to their Cronos ID domain, which will also serve as the key point of access to the Cronos ecosystem.

Cronos ID is designed to be a key infrastructure layer, and the Domain Service is only the first step in building the infrastructure groundwork for Web3: it will also release **Cronos ID Notification Service**, a subprotocol which will allow users' wallet addresses to receive on-chain event notifications, and **Cronos ID Messaging Service** which will enable communication between users via their wallet addresses or domain names.

Alongside Cronos ID, there are other popular solutions available today including Ethereum Name Service (ENS) domains, Unstoppable Domains, BrightID, and Space ID.

Read more about Web3 identity solutions in our report: *Digital Identity in the Web3 World*



Cronos ID also enhances an individual's trading experience: For instance, with the Crypto.com DeFi Wallet and Wallet Extension, users can seamlessly transfer tokens by copying and pasting their Cronos ID.

5. Conclusion

In this evolving and hyperconnected world, the need to decouple users from centralised platforms and break up monopolies will drive people to seek alternative ways to connect digitally.

The decentralised nature of blockchain technology makes it possible to build social networks that efficiently provide and manage users' social graphs and digital identities — all within a private, secure, and self-governed environment.

Decentralised social networks have still yet to tackle some barriers to mass adoption relating to its complexity, ease of use (it's not as user-friendly compared to traditional social platforms), security vulnerabilities (e.g. the network is open to anyone), and the burden of responsibility (e.g. key management, moderation) borne by users, among others.

Leading up to Elon Musk's takeover of Twitter, we have seen an influx of new users to Mastodon — an open source, decentralised microblogging platform emerging as an alternative to Twitter. Scenarios like this show a demand for decentralised social networks, and efforts are underway to likely accelerate their adoption. Despite the challenges identified, the current iteration of decentralised social networks looks promising, and we can expect to see its evolution in the future.

References

Omar Dib and Khalifa Toumi. “Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions” *SSRN*, 20 December 2020. Accessed 14 November 2022

“Decentralized Social Networking Protocol (DSNP)” *Project Liberty*, October 2020. https://unfinished.com/wp-content/uploads/dsnp_whitepaper.pdf, Accessed 14 November 2022

Robert Riemann. “Federated Social Media Platforms” *EDPS*, 2022 https://edps.europa.eu/system/files/2022-07/22-07-26_techdispatch-1-2022-federated-social-media-platforms_en.pdf, Accessed 14 November 2022

“Decentralized identity” *Ethereum.org* https://ethereum.org/en/decentralized-identity/#content, Accessed 14 November 2022

0x148D. “Why do we need a decentralized social graph?” *Mirror.xyz*, 19 November 2021 https://mirror.xyz/cyberlab.eth/Rqr8tiXed6helt5LfSotEdLFxB6Kv_fA1Poz3K_6g0c, Accessed 14 November 2022

“Getting Started with CyberConnect”. *CyberConnect,* 20 October 2022. https://cyberconnect.hashnode.dev/getting-started-with-cyberconnect

e. contact@crypto.com

Published on 6 Dec 2022