The issue of authentic ownership in the Web3 world

Fenbushi Capital | 分布式资本

Follow

--

Listen

Share

（Fenbushi Capital had an interview with Nest's founder Charles.)

1. There is a dispute around Web3. Someone thinks it will smash Web2 empire; Someone thinks it is always about gambling and Ponzi plans. What's your opinion about Web3?

Charles: Web3 is a parallel and potentially more expansive, trust-based digital ecosystem. We see it as the next stage of digital evolution. Web3, if or when enacted correctly, will supersede Web2. To paraphrase, Web3 is conceptually a user-led rewiring of what people commonly hold to be 'the internet' or 'online functions'.

Web3 encompasses the connections, services and data access across most all of digital space. Rewiring is made possible by certain types of technologies. Blockchain is the most familiar example. The choice, control and secured exchange capacity that has recently been permitted through distributed ledger technologies, blockchain is just one of them, holds the potential to upend currently centralized services, digital and traditional (physical), alike.

Due to the technologies and structures that were available then, Web2 proliferated gated access to services, data and features. These gatekeepers were Amazon, LinkedIn, Facebook and the like. Today, Web3 has the potential to genuinely democratize both the input as well as the access and control of engagement. This next stage is somewhat of a flattening out of digital access and ownership controls. Also, it is user-led. These users are obviously in the real-world, not in any one location. So, Web3 is naturally a decentralized repositioning.

Web3 is a burgeoning concept and potential. It is still in its infancy. New Web3 tools are being introduced in rapid succession. For those that think it's always about gambling or 'schemes' — in order to draw a practical comparison of a mainstream adoption timeline for Web3 — we could reference say the internet bubble of the 90's and the more recent ICO bubble in the blockchain space. Fringe practices and 'dodgy' offerings are typically the first headline grabbing focal points in certain emerging tech. Such teething issues generally do not speak to, nor indeed limit, the true underlying potential impact of the tech itself. The Web2 issues did not kill the internet, ICO's did not stop blockchain then and current Web3 issues won't kill the true capacity now. Web3 is quite a conceptual, user-first change in positioning. It speaks to a different form of 'online' access-control for most, which is only starting to see the light of day.

Through user-led personal choice capacity, of both their data control and secured exchanges, the options and indeed responsibilities in Web3 are somewhat repositioned to the individual rather than say Web2 empire fiefdoms. Web3 adoption is a user-led practice. Engagement will determine the shape as well as the speed of effects that the underlying technologies will carry.

1. What do you think about the acquisition of Gem by Opensea? Will it undercut the innovation of the industry? What kinds of innovation will come up (could be infrastructure, tools, and NFT applications)?

Charles: Initially, it strikes as somewhat contradictory to their intended mission statement of "Gem is on a mission to create a decentralized and open future for the internet, and even more so, the metaverse."

There are three top of mind considerations. Firstly, current mainstream pseudo-anonymous wallets and asset ownership structures are insufficient.

Access does not and cannot equate to ownership. In most cases of popular NFT sales and use, when using typical wallet solutions there is 'no one' who can actually claim to own either the wallet or content (as the wallet is by design pseudo-anonymous), and there is nothing 'to own' should the master-file of say an NFT artwork a) not have been sold under contract and b) remain publicly accessible. In short, the setup for typical NFT sales and ownership demands a massive overhaul — which NEST® is addressing but which forms the content of another answer.

Secondly, the lazy-mint structure of OpenSea does feel, to some, as generally misleading.

This 'lazy-mint' being the process by which digital assets' listed on the marketplace are not actually NFT's until after they have been purchased by a second party or 'buyer'. Meaning they are in many ways not secured, registered or 'on-chain' in the commonly perceived capacity until they have actually been sold to someone else. This methodology, and many variations of it, allow for the 'free mint' or 'low fees' offered by numerous services. The Gem website, we believe for inventory and listings, is primarily scraping the OpenSea databases through APIs. So, this leads to questions of what an 'aggregator' does and at what time or stage in the process this is performed.

Thirdly, OpenSea is a decentralized, layer-two application with integrated support for 3 networks — Ethereum, Polygon and Solana.

The third question then arises — what would be the reaction to say a comparison site like Expedia, TripAdvisor or Kayak being purchased by a single airline? This could be extended to say any comparison websites being purchased by a single operator in the relevant space.

All in all, for sure there will be practical and immediate benefits for cross exploration and discovery potential throughout existing networks. But whether Gem's acquisition by OpenSea, a somewhat centralized marketplace, is actually in support and of benefit towards a truly distributed ownership-control for users, in the 'free market' sense, is something that remains to be proven.

In regards to innovation, the content of an NFT and its secured use, control and exchange is where the most exciting developments will come. Not simply from streamlined collection listings of any one 'form' of NFTs. We believe a more accurate or apt description of the future NFT space is to describe NFTs as 'data-as-an-asset'. What this 'data-as-an-asset' is leading to is users' own secured, omni-network and dynamic digital capacity that permits far more broad functions, as most any type of data can be included in this.

For the user, this 'data-as-an-asset' package enables new forms of protected engagement and exchange across any function or service. This ability for newly secured and controlled data has impacts that encompass most all activities, from those online right across to real world contractual engagement or participation. The tools and associated infrastructure that will first shine will be determined according to the most demanded features and services. Right now, first in mind NFTs are artwork and photos. Item purchases. Next up we may see ticketing with event participation. With this comes broader implementation of real-world contractual terms of usage and exchange, such as Intellectual Property (IP) right allocations, creator usage restrictions or persistent royalties associated with set data. Shortly after, we see dynamic long-term engagements, such as membership or employment right across to more intelligent forms of user profiles all implementing different forms of NFTs. And these examples only scratch the surface.

1. Keeping the safety of digital assets is the prerequisite of Web3. What we witness is theft, fraud, and scams all over the place. How could we solve the safety issue of the industry?

Charles: Absolutely correct. Enabling authentic ownership-control of digital assets is a prerequisite of Web3. Until this is done, Web3 will not reach its potential. To actually secure a digital asset requires a combination of protocols which we have found are quite often not understood and rarely, if ever, wholistically implemented. When taking an overview of online engagement, be it Web2 or Web3, again everything exists because of the users. It is the users' choice to download applications, participate, exchange or engage. Web2 and the concurrent precursors to our most familiar networks, primarily ended up consisting of gatekeepers. These were the leading services, functions and features that were either popularly embraced, such as social media, or somewhat professionally required, like communication and productivity tools. To operate, gatekeepers must maintain a certain environment of trust and facility. The access to gatekeepers demands from the users' varied forms of term acceptance as well as users' disclosure of information, behavior and details. This is centralized authentication e.g., allowed use of a hosted profile. The consequence of such central collation becomes a divulging of personal data (identity, access, use, connections, assets and so on), as well as these gatekeepers' retention of power and control over the services and environments offered. The centralized gatekeepers as businesses, groups or organizations are typically real-world companies with registered headquarters, offices and the like. The centralized nature of gatekeepers then places the services and environments able to be offered under geographically regional jurisdictions. This setup then poses multiple and major limitations on both sides, for sure.

Then we come to popularization of blockchain and associated technologies. The underlying promise or potential of truly immutable distributed technologies and networks is the unmediated distribution of trust itself. Meaning, due to the secured nature or the form of documentation and exchange facilitated through DLT transactions, the code itself and its subsequent entries can be more trusted than any one centralized gatekeeper. This is one key principle behind cryptographically secured forms of currency and smart-contracts which, for any user, result in quite simply no more than mathematical proof that something happened. No external or third-party verification is needed. DLT entries are immutable and decentralized so — ideally — they are then outside the purview or control of any individual jurisdiction, organization, agency or entity.

To not repeat the gatekeeper methodology and structure, or to indeed properly utilize DLT, users' must now retain confidential control of both their identity as well as digital assets. This is throughout any blockchain network or service of choice. And more than this, they must have the capacity to securely and privately link their real-world ownership to digital assets and then be the sole controller of such link. To authentically secure the safety of a digital asset, there needs to be 1) a real-world person, who 2) owns and controls a distinctly identified asset;

1 _ Pseudo-anonymous wallet solutions cannot accommodate real-world ownership.

Centralized wallet solutions are by definition not authentically confidential nor truly private. So, at NEST® we start with confidential, individually encrypted, device-side control of personal information and data. Unlike most — NEST® never retains or stores private keys thereby removing even our capacity for user data access and ensuring full privacy for the user. This device-side, individually encrypted environment permits the users to generate, own, edit and control their Self-Sovereign Decentralized ID (SSDID). This results in a hyper-encrypted digital tool and signature capacity for the user which enables many things such as hard-coded provenance authentication, signatory to notary authority and access control. Use and any transaction appearance on any network is publicly retrievable, on-chain, yet only privately decryptable by the owner;

2 _ Access does not equate to ownership.

Legal rights to any asset cannot be sold, transferred, bought or exchanged if that asset is undefined and/or uncontrolled. Digital files are reproduceable, anyone with access may basically perfectly replicate that file. Additionally, in the digital space, multiple networks across varied jurisdictions are all without a single database for verification. One argument often made here, for the veracity of current NFTs, is that timestamped events on-chain are immutable. This position being the 'first claim' to registration wins. True. Access to one first appearance registration can hold an impact. Yet it does not answer in what situation or to whom or how can this claim genuinely holds impact. Asset hosting, as most frequently performed today, is often open and unsecured leaving genuine asset definition and ownership unaddressed. To solve this, at NEST® we ensure that the master-files for digital assets are not available to download for anyone else apart from the verified owner. Data is instead individually encrypted and kept differentiated from corresponding publicly accessible, purposefully open registrations. Taking art NFTs as an example, only a 'photocopy' or light-weight version of the artwork is kept on IPFS or similar open databases. The actual asset or primary master-file is individually encrypted to the owner him or herself. Transference and re-encryption are accommodated and this works for every stage from minting, imports, edits, swaps to contractual exchanges and the like. All SSDID and data (assets), are stored by users in failsafe blockchain networks, using splintered, quantum proof security. Only the authenticated owner has the capacity to access, decrypt, sell or exchange the distinct and secured digital asset(s). This permits the authenticated and secured expansion or use of NFTs from artwork to music, movies, contracts right over to personal data and so on.

Without the above two features — theft, fraud, and scams can be rampant. Without the above, there is generally and legally speaking 'no one' who 'owns' any asset in question. And without these two steps in place, there is a knock-on effect imposing significant limitations on digital assets by removing the potential user participation in legal contracts (copyright transfer, sale, exchange, etc.), value-added services (loans, mortgages, lending, etc.), real-world practicalities (authenticated verifications for items, membership participation), and the like.

NEST® can provide the tools that facilitate users secure choice selection. Enacting the control for the safety and security of digital assets is fundamentally in the hands of the users themselves.

1. Could you introduce NEST? What's your initiative in creating the company?

Charles: NEST® stands for Naturally Encrypted, Secure Technologies. We focus on bespoke development of easily accessible infrastructures and software that facilitate confidentially secured user access, ownership, and control of Web3. NEST® is truly interoperable and has its own layer-zero-to-one blockchain. We have built both desktop and mobile applications which together provide over 50 different, first of their kind features.In creating the company, we saw it more as a necessity than an option. Critical barriers for distributed genuine privacy, exchange participation, ownership, monetization, and user control exist that no one else seemed to be addressing. Solving these critical barriers and enabling user-led control was not really about starting a business; it feels more like personal responsibility.

We started with the question — how can you make choice personal? This is not an initially simple proposition to explain. To truly 'make choice personal' requires that the individual retains agency in action, that they have sufficient privacy to formulate their own judgments and decisions which are as free as possible from external influence or bias as well as they hold an active capacity to securely and safely execute those choices. For many years we have been building, in stealth mode, a multichain ecosystem able to accommodate this complete lifecycle. Our answer to how we can 'make choice personal' is what we provide to users through our infrastructure. Confidential, interoperable and authentically user-owned tools that privately bridge their digital to real-world divide.