UNIVERSITY of NICOSIA

Week 5, Session 9

Tokens in the Broader Ecosystem

BLOC 528: Token Economics

Today's Overview

- Objective #1: To understand the role that tokens play in the broader web3 ecosystem.
- Objective #2: To explore the applications for tokens for NFTs, self-sovereign identifiers, and DAOs.

What Differentiates Tokens?

Digital tokens do what few other items can do

- They can create rivalry (i.e., the more I have, the less you have)
- They can create exclusivity (i.e., I can prevent someone from gaining access to X product/service)

Those two features are the foundation of markets – without them, there will not be investment.

There are physical counterparts – vouchers, centralized certificates, and more – but they lack the element of decentralization on the blockchain and the same degree of security and authenticity.

Applications of Tokens – NFTs and Utility

What do NFTs really do?

- They create rivalry and exclusivity on the blockchain.
- They allow content creators to publicly signal their ownership on the blockchain.
- They also provide a way to trade assets with an immutable link of prior owners so that the original content creator can get credit (compensation) for what they created – that is, a stream of future revenues.
- That fundamentally changes the incentives for content creators – and the competitive landscape.

Great interview Chris Dixon had on The Verge

- “I am not arguing that NFTs are magical new things that change human behavior, but they are a way for creative people to go direct to their audience and bypass these algorithmic advertising-driven feeds. Thus far, the results are really promising, and I think we are going to see a lot of new ways in which creative people monetize. As you said, that is not distribution. Think of it like Substack right now; a lot of people will build their audience on Twitter, but then they will monetize on Substack. I think it has been great for creative people.”
- “It is very similar to that. I own cdixon.org, and I own it because I host it at Netlify. If Netlify becomes evil, I will just switch it over to another place because I control the DNS record. An NFT is architecturally very different from other things on the internet.”

https://www.theverge.com/23020727/decoder-chris-dixon-web3-crypto-a16z-vc-silicon-valley-investing-podcast-interview

Applications of Tokens – NFTs and Utility

Great interview Chris Dixon had on The Verge (continued…)

- "Well, I think there are two things with NFTs. One, I do think architecturally it is very different from other objects on the internet, in the sense that most objects are controlled by an application and NFTs are controlled by users. It switches the polarity, and I think that is important. As we see the rise of Web3 gaming, you will see a whole different class of things where people own characters and other kinds of objects that they can take across different experiences. Instead of it being contained in an app, it is contained at the user level. There is an architectural aspect, and there is a social aspect. Why do people value wearing fashion — like Supreme T-shirts — or cars? A lot of value in the world is about showing that you are early to something, that you are high-status, and that you have great taste."
- "To me, there are two aspects that make NFTs different. One, you truly own it architecturally like you would a domain name. If you do not like how somebody is treating your NFT, you can just move it away. That is not true on the web today; everything is contained in an application or a website. Two, it allows you to have different social signals that people can see when you own something. This applies to everything from taste and status, to the fact that you are an early adopter, to whatever the particular design of the community NFT might be."
- "I view the internet today as millions of subcommunities. I think NFTs are a way for subcommunities to have cultural artifacts and create little economies within them. It is a big world, so some of the popular existing ones will go awry, but my bet is that there will be many positive communities."

https://www.theverge.com/23020727/decoder-chris-dixon-web3-crypto-a16z-vc-silicon-valley-investing-podcast-interview

Applications of Tokens – Identity Verification

Definitions

- Credentials contain a set of claims about the subject of the credential, and these claims can say anything about the attributes, relationships, or entitlements of the subject.
- But a credential must be verifiable – that is, it must be possible to determine: who issued it, that it has not been tampered with since it was issued, and it has not expired or been revoked.
- We have traditionally had public key infrastructure approaches – where there are a few centralized entities that produce certificates – but we are now moving towards a new approach where credentials need to be: permanent (i.e., they do not change even if the entity moves), resolvable (i.e., able to reach the owner's agent), cryptographically verifiable (i.e., prove that they have it or control the private key associated with the identifier), and decentralized (i.e., avoid single points of failure).

Examples

- Suppose Alice and Bob meet at a conference – then they connect on LinkedIn (possibly even with a QR code that contacts information that populates) – that is still centralized.
- An alternative, using self-sovereign identities (SSI), opens up an entirely new way of peer to peer communication, which we explore in more detail next.

Applications of Tokens – Identity Verification

- Alice produces a QR code that allows for a connection invitation that contains information about how Bob can connect with her on an encrypted channel – in doing so, Alice produces a “nonce” (random number) used for security so that it’s unique to Bob
- Bob scans the QR code and it instructs the wallet to generate a unique public/private key pair, and a peer decentralized identifier (DID) based on the public/private key pair that is a private and pseudonymous identifier used to identify Bob’s unique connection to Alice in a privacy-preserving way (only they know)
- Now, Bob’s edge agent composes a connection request message with the metadata that goes with the DID and it is prepared exclusively for Alice: the new peer DID, the public key, and the private network address
- Alice’s edge agent now asks to confirm the connection, and it does the same thing for Bob – now Alice’s agent can encrypt the message using the public key from Bob’s DID document so only Bob can read. Furthermore, now Alice’s edge agent can use the message to update the service endpoint and remove any vulnerability that might have been present from the initial invitation
- Since the connection was done in person, no verifiable credentials were exchanged, no interactions were needed with a public ledger or blockchain, and the connection is private and known only to them – that can all change when people communicate digitally and it’s all done on a public blockchain

Applications of Tokens – Identity Verification

Many benefits

- Higher revenues / lower costs (fraud detection, KYC compliance, and more).
- Improved efficiency (auto-authentication, auto-authorization, delegation, workflow automation, payment).
- Better relationship management (secure/private communication, authenticated public records).
- Regulatory compliance (preserving privacy without sacrificing value, data protection, data portability, KYC).

Example

- In 2017, during the CoinDash ICO, a hacker compromised their website that was on Wordpress.
- The hacker substituted their own wallet address for the legitimate CoinDash address, so customers sent their money to him rather than to CoinDash!
- If there had been verifiable SSI authentications, that would not have happened.

Applications of Tokens – DAOs

- DAOs are self-governing organizations typically formed by groups of similarly-minded individuals with specific goals. They can be as small or big as the users' desire.
- While a DAO is, on its own, simply software — that is, smart contracts that specify what happens when something else happens, i.e. a process that unites everyone together through executable code — it ultimately consists of the people and values that draw the users together. DAOs operate by working with "Contractors" who submit proposals (e.g., launching a product) and get approved and supervised.
- Contractors require a group of signatories ("the Curator") who validate the proposal and provide the transfer of funds from the pool of participants. That creates skin in the game — if a Contractor fails, then it would reflect poorly on the signatories. There is a "dynamic game" between the principals and the agents.
- That means the DAO needs to begin with an initial state – that is, an "agreement to develop a governance system that enables trustless execution of commands based on an initial set of assumptions."
- That also means deciding how to distribute the initial share of tokens.

https://mirror.xyz/0x367B4bDf414Df673Df0129838ebfB9913147427F/R-ZpVf8WUpgZh30FpoUtVsxG4ysRqgMe4JOliDfL5fk

Applications of Tokens – DAOs

Reputation-based Voting

- Controlled by the DAO
- Non-transferable (buying and selling can be strongly disincentivized)
- Resilient to malicious vote-buying at all participation rates (because vote buying is difficult)
- Performs well in making both objective and non-objective decisions (e.g. will A or B lead to a better outcome?)

Token-based Voting

- Controlled by the individual
- Transferable (buying and selling are features)
- Resilient to malicious vote-buying only with high voter participation (low decision frequency)
- Performs well in making objective decisions only (e.g. what is the temperature?)

Source: *Daostack Comparison of Voting Methods*

Applications of Tokens – DAOs

- "Based on the initial plan for token allocation, participants can gauge the degree of influence their voting participation can have on the DAO's governance both at genesis and as the DAO develops."
- Example with delegation of voting: ENS launched with an airdrop that required token holders to vote on the clauses of the initial constitution and to opt-in or out of making a delegation of their voting power to persons who applied to be delegates. Delegates creates the possibility that even with a fragmented distribution of tokens, outcomes may be determined by a subset of core contributors and create unwanted incumbency even after they leave.

Distribution and Vesting

Category	Total Supply	Available at Launch	Cliff Period
Private Sale	5%	0%	3 months
Launch Partner Rewards	5%	5%	N/A
BitDAO Treasury	30%	10%	3 months
Bybit Flexible	15%	15%	N/A
Bybit Locked	45%	0%	12 months

Hybrid Approaches

Create tokens with in-person utility

- Utility is a lot more than membership in an online forum – or even a metaverse sort of group.
- Tokens are the mechanism that allow you to make interoperability between decentralized, non-pecuniary compensation and sources of value, so they provide a vehicle for linking the digital and physical worlds.
- The Island DAO is the first – and in part an experiment – physical gathering of individuals in a community for living (at least for several months in the year) that would use tokens to enter.

UNIVERSITY of NICOSIA

Questions?

Contact:

Christos A. Makridis | Professor | Makridis.c@unic.ac.cy
Marios Touloupos | Teaching and Research Associate | touloupos.m@unic.ac.cy
Evgenia Kapassa | Teaching and Research Associate | kapassa.e@unic.ac.cy