

Privacy and Data Security Concerns with NFT Drops

Zach Lewis, Maria Nava, & Eliana Torres

Privacy + Security Forum

November 3, 2022

Frankfurt Kurnit Klein + Selz PC

This outline is a discussion in summary form and may not address all applicable issues or be relevant to all situations. It is not intended to be legal advice. Please consult your attorney for legal advice.

Primer on the Applicable Tech & Terminology

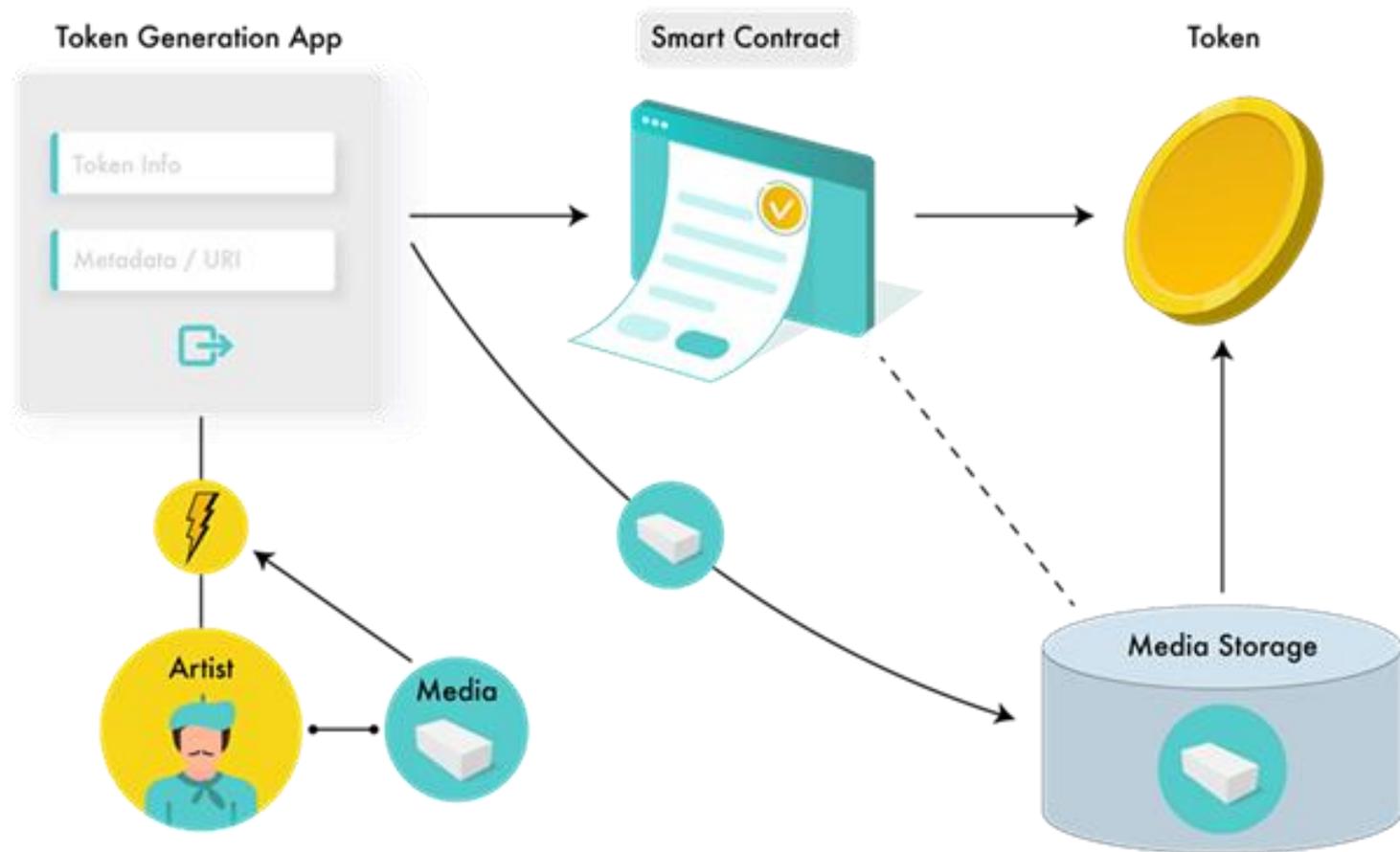
What is a Blockchain?

- **Block:** Database of transactions – bundles of transactions are grouped together into separate “blocks” that get added to the database
- **Chain:** Each block contains a “header” that includes: (i) a unique fingerprint or “hash” (i.e., a string of characters and numbers that uniquely represent a block’s transactions) of all transactions contained in that **block**, (ii) a timestamp, and (iii) a hash of the previous block, which creates a sequentially organized **chain**
- **Decentralized:** Maintained and replicated by “nodes”
- **Public:** All transactions recorded and publicly auditable
- **Protocol:** Each blockchain has a unique “protocol,” which is the underlying software that establishes the blockchain’s rules
- **Immutable:** Because each block incorporates a hash of the preceding block’s header, anyone trying to modify the content stored in a block will inevitably break the chain
- **Examples:** Bitcoin, Ethereum, Solana

What are NFTs?

- **Non-Fungible Tokens:**
 - Each individual token is unique, with distinctive **ID codes** and **metadata** that distinguish them from one another
 - The metadata contains a **Uniform Resource Identifier (URI)** that points to an **off-chain** location where users can see what the token represents
 - When someone creates an NFT, they are essentially **executing code** that is added to the blockchain where the NFT is being managed
- **Smart Contracts:** Manage minting, sale, and distribution of NFTs and collect and pay proceeds
- **Secondary Sales:** Marketplaces (like OpenSea) collect and pay royalties to NFT minter
- **Utility:** May be accompanied by other rights + benefits (IP, access, merch...)

What are NFTs?



What are Smart Contracts?

- **Code:** Computer program (e.g., Solidity)
- **On-Chain:** Deployed and executed on blockchains (e.g., Ethereum)
- **Automated:** Designed to execute transactions without human intervention
- **Escrow:** Can receive, hold, & pay funds according to programmed logic
- **NOT a “Traditional” Contract:** But code is law. Smart contracts cannot be deleted by default, and interactions with them are irreversible

```
1  pragma solidity 0.8.7;
2
3  contract VendingMachine {
4
5      // Declare state variables of the contract
6      address public owner;
7      mapping (address => uint) public cupcakeBalances;
8
9      // When 'VendingMachine' contract is deployed:
10     // 1. set the deploying address as the owner of the contract
11     // 2. set the deployed smart contract's cupcake balance to 100
12     constructor() {
13         owner = msg.sender;
14         cupcakeBalances[address(this)] = 100;
15     }
16
17     // Allow the owner to increase the smart contract's cupcake balance
18     function refill(uint amount) public {
19         require(msg.sender == owner, "Only the owner can refill.");
20         cupcakeBalances[address(this)] += amount;
21     }
22
23     // Allow anyone to purchase cupcakes
24     function purchase(uint amount) public payable {
25         require(msg.value >= amount * 1 ether, "You must pay at least 1
26         ETH per cupcake");
27         require(cupcakeBalances[address(this)] >= amount, "Not enough
28         cupcakes in stock to complete this purchase");
29         cupcakeBalances[address(this)] -= amount;
30         cupcakeBalances[msg.sender] += amount;
31     }
32 }
```

NFTs in the Smart Contract

- Each NFT in the smart contract has a unique ID to show which token it is and an owner, represented by a public wallet address

TOKEN ID	OWNER
1	0xf0950f5a951637e0307cdcb4c672f298b8bc6f29
2	0x9fb2a47fde5bbe18ddd08d17de8bda30ab869cd2
3	0x2a044fea858d6a7ab01fb45c2d104ebae2ea0933
4	0xd053efb1703703ae5bc3dcadd0d88ebccf6c90b
5	0x7f49f67a538b8ae4123ed2765dc8a028df0dc87e
6	0xef99cc1e4b41488c3a00017b7f45bbbabb21288d
7	0x19b4796f42c006685b69e1b59c4abd0cbd5e91c8
8	0xe8a9a74415cbae81dd9eced463a091ba1c354aec
9	0x16962d78465430915ac360761c22c088c44391e2
...	...

HT @bcgandalf

What is a Digital Wallet?



They securely maintain a “key pair” used to manage digital assets

- The **public key** is a hexadecimal string of digits associated with an address on a particular blockchain visible to anyone who has knowledge of the public key
 - Like a publicly-available account number
- The **private key** is also a hexadecimal string of digits mathematically-associated with a public key address on a particular blockchain
 - Like a password for the account that can be used to sign instructions to transfer digital assets held at the public key address or to sign other instructions



Oddly, digital wallets don’t store digital assets



There are a variety of wallets available

Cold
Hot
Custodial
non-custodial, etc.

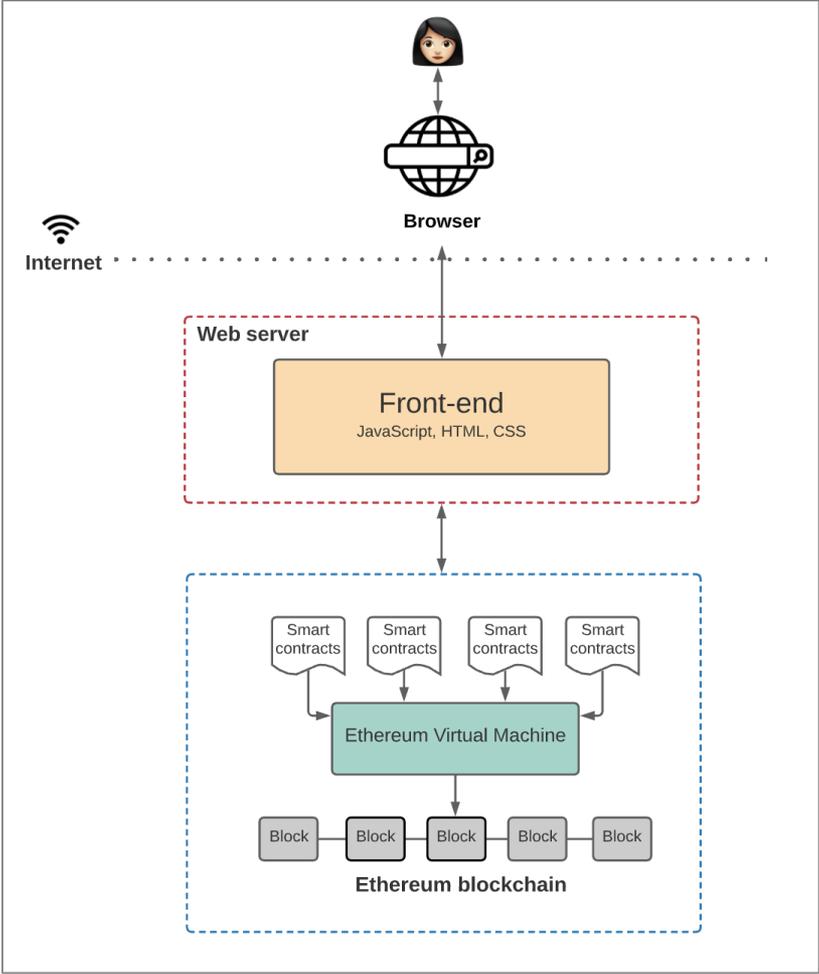
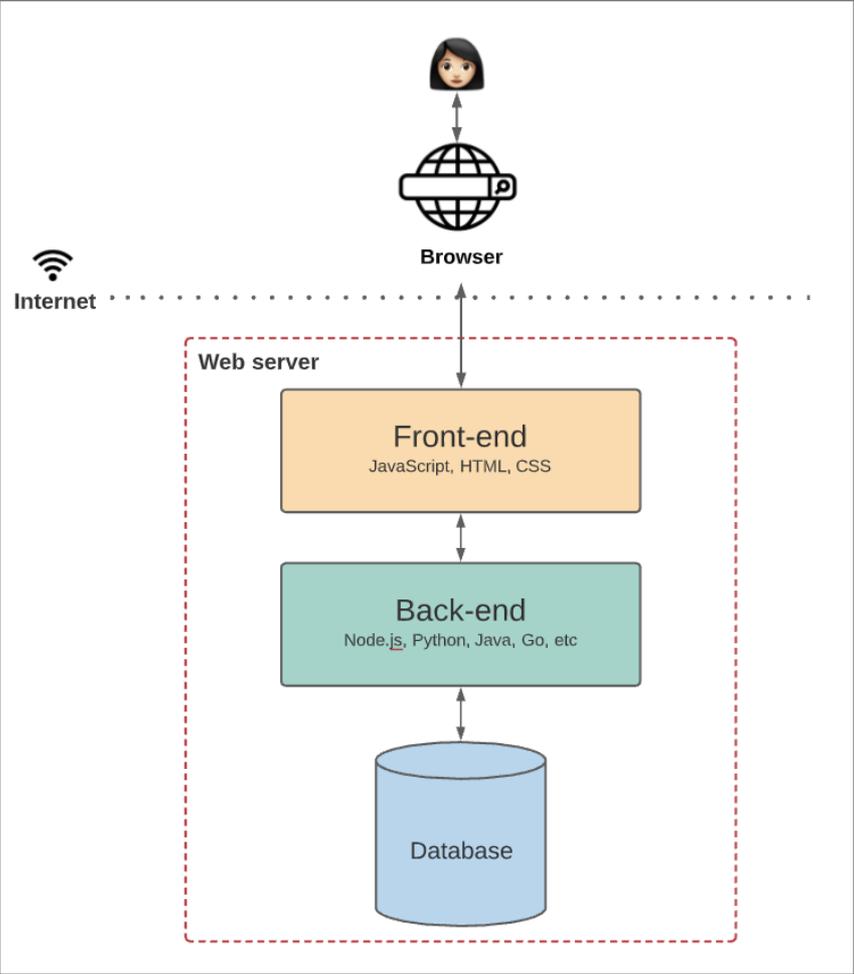


Why do you need digital wallet?

- To send and receive crypto
- To mint and transfer NFTs
- To interact with Web3 virtual worlds built using blockchain technology

What is Web3?

Web2 app vs. Web3 dApp



Primer on the Culture

Popular NFT Use Cases (2022)

- Art/Photography
- Music
- Collectibles
- Gaming
- Entertainment
- Fashion
- Expression & Identity (PFPs)
- Organization (DAOs) & Community
- Virtual Worlds & Experiences
- Access to People & Events



Art/Photography



“Fidenza #135”
Tyler Hobbs



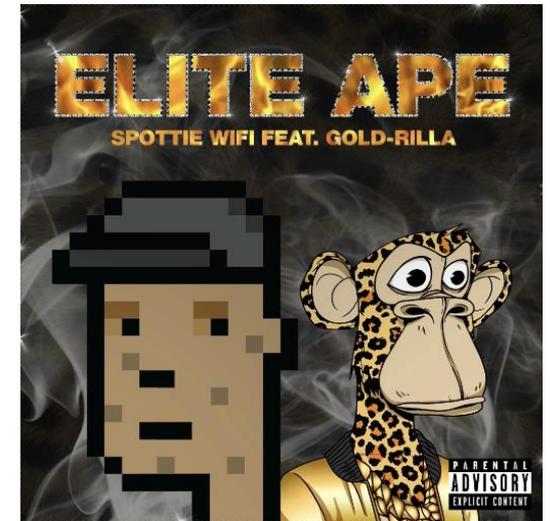
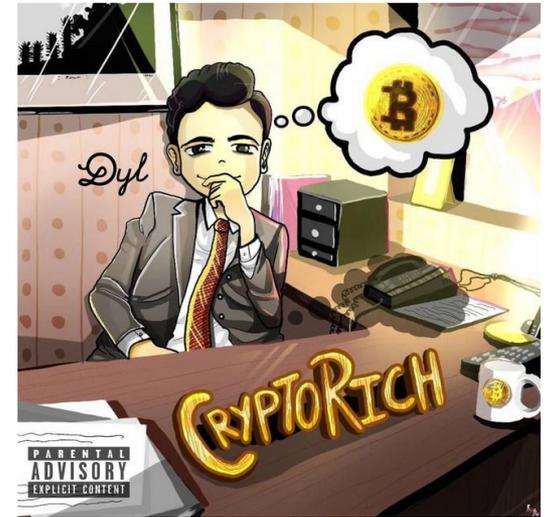
“The Day I Decided to Fly”
FEWOCiOUS



“Where My Vans Go #83”
Drift

Music

- Audio files
- Music videos
- Commercial rights
- Royalty sharing
- Fan engagement
- Avatar Artists/Record Labels

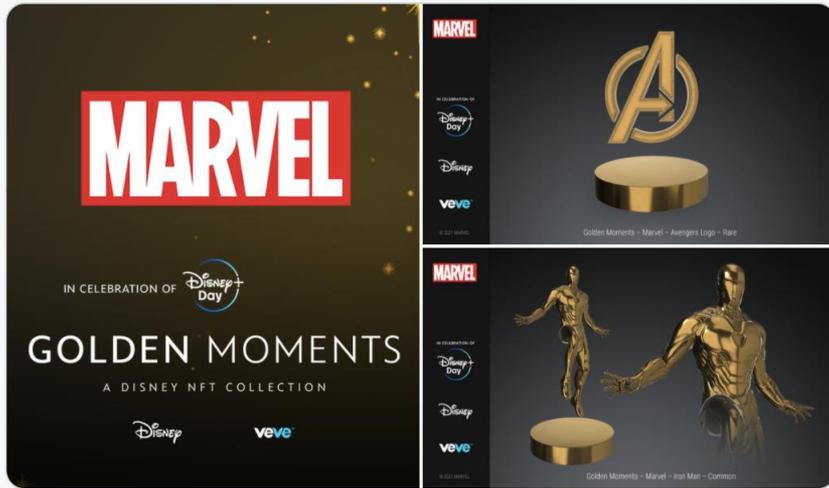


Collectibles

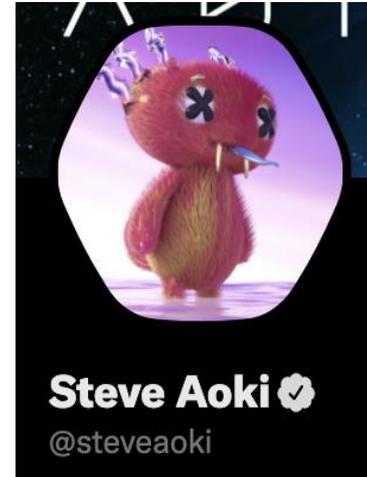


Start your #DisneyPlusDay celebration early with @veve_official's Golden Moments set featuring Iron Man and the Avengers logo!

These new digital collectibles drop at 12PM PT/3PM ET:
bit.ly/31Q323x

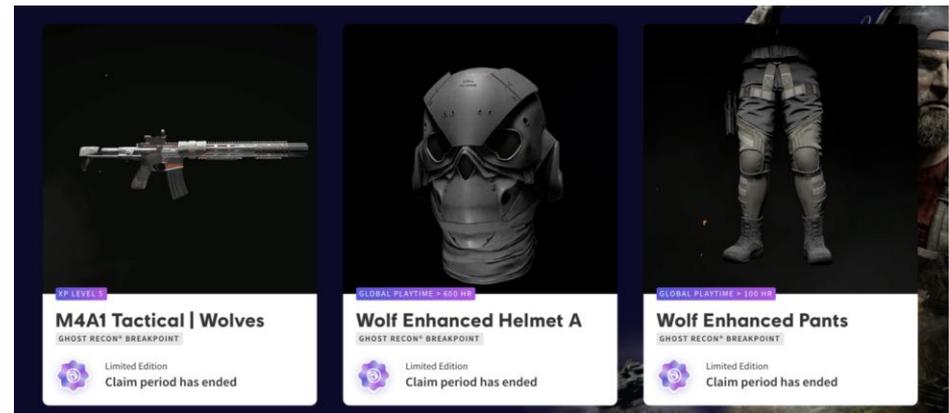


PFPs (Profile Pictures)



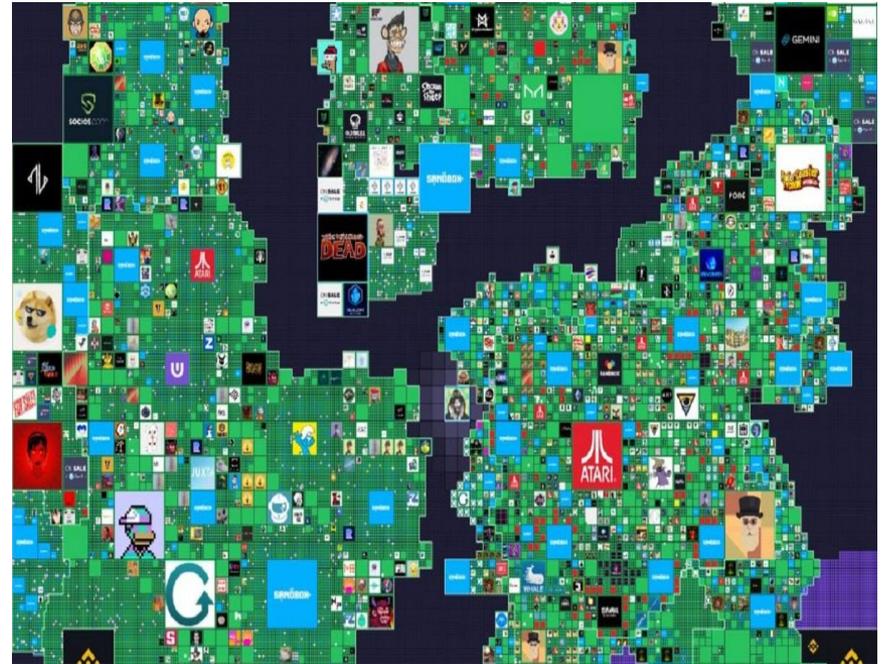
Gaming

- Access to games
- Play-to-earn games
- Games of chance



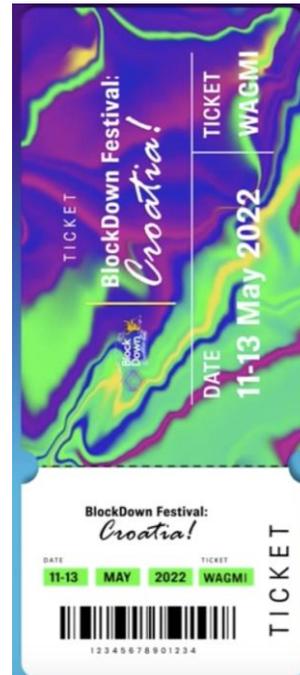
Virtual Worlds / Experiences

- Sandbox/Decentraland
- NFT Worlds
- Others
- Personal Galleries



Entertainment

- Tickets/Proof of Attendance
- Access to content
- Community driven content



BUZZER BEATER • BUZZER BEATER • BUZZER BEATER

7,110 Mavs NFTs

DALLAS

MAVERICKS -VS- CELTICS

FINAL MAVS 107
CELTICS 104

SATURDAY, NOVEMBER 6, 2021
@ 9:47 PM • DALLAS, TX
AMERICAN AIRLINES CENTER

MAVS WIN! MAVS WIN! MAVS WIN!

BUZZER BEATER • BUZZER BEATER • BUZZER BEATER

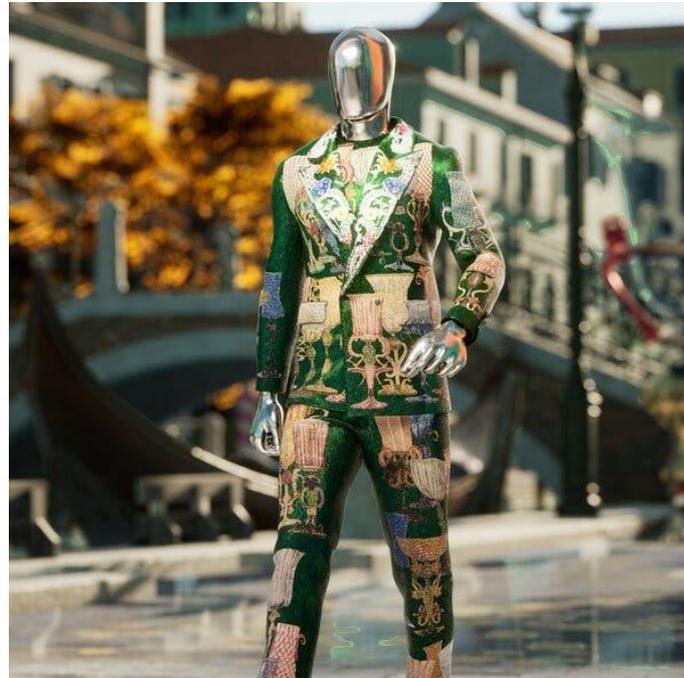
🔗 **Mavs vs Celtics Buzzer Beater**

This NFT ticket was only distributed to fans in attendance on November 6, 2021 at American Airlines Center, when the Dallas Mavericks beat the Boston Celtics with a three point game winning shot.

❤️ 80 **\$500 - \$9,000**

Fashion

- Redeemable physical clothing
- Virtual clothing
- Augmented Reality Clothing



Access to People & Events

- Virtual access
- In person access



Organization & Community

DAO LANDSCAPE

Curated by @Cooopahtroopa • Pixels by Carlos/

DAO Operating Systems

- ARAGON
- DaoStack
- DaoHaus
- COLONY
- Syndicate
- Orca
- CW

Investment DAOs

- MetaCartel
- theLAO
- Flamingo
- Komorebi
- UdacityFund
- BitDAO
- Free Company
- Duck DAO

Grants DAO

- MetaCartel Ventures
- MolochDAO
- Audius Grants
- Uniswap Grants
- Mint Fund
- Sevens Foundation
- Compound Grants
- Aave Grants

Collector DAOs

- PleasrDAO
- Flamingo
- SquiggleDAO
- FingerprintsDAO
- BRRDAO
- Whale
- MUSEO
- herstoryDAO
- BeetsDAO
- JennyDAO
- MeebitsDAO
- Gremlins

Protocol DAOs

- MAKER
- Compound
- UNISWAP
- Aave
- Yearn
- Sushi
- SYNTHETIX
- Curve
- Index Coop
- PieDAO
- tornado
- GITCOIN
- LIDO
- pool
- KeeperDAO
- Badger
- RaribleDAO
- Olympus
- hDAO
- Rari Capital
- Balancer
- Cream Finance
- AUDIUS
- Universe
- inverse finance
- Aavegotchi
- INSTADAPP
- OceanDAO

Service DAOs

- RAMP
- DXdao
- PartyDAO
- MetaFactory
- Fire Eyes
- DeepDAO
- Reverie
- NeptuneDAO
- Llama
- Llama
- MetaverseDAO
- LexDAO
- d0rg
- DaoHaus
- VitaDAO
- ShinyDAO
- OPOLIS
- DoinGud
- DEEP WORK
- YGG
- HoneyDAO
- Myco
- UniWhales
- Yam DAO
- AladdinDAO

Social DAOs

- FWB
- Seed Club
- Radicle
- FiatLuxDAO
- Metafam
- KrausHaus
- ProsperDAO
- Bright Moments
- Meta Gamma Delta
- SongCamp
- CabinDAO
- PROOF OF HUMANITY
- BAYC
- TheWIPmeetup

Media DAOs

- FOREFRONT
- BanklessDAO
- GCR
- DarkstarDAO
- rekt

NFT Marketplaces



- Most NFTs are often bought and sold through third-party marketplaces (many of which are built on the Ethereum network) that have consumer facing apps or websites that facilitate the minting (i.e., uniquely publishing your token to the blockchain), selling and purchasing of NFTs in a consumer-friendly way.
- The most common NFT marketplaces today are:
 - Marketplaces like OpenSea, which are like NFT-eBays, and typically do not conduct any independent verification of whether a party has the right to sell an NFT associated with a particular asset.
 - Curated art auctions, like SuperRare, which allegedly conduct some verification of creators and their work before an NFT may be sold on their marketplace.
 - Marketplaces created and built to offer NFTs for a single company, creating a less decentralized environment (think NBA Top Shot).

Ethos of “Web 3” & the NFT Space

- Empowering creators
- User Owned (vs. Generated) Content
- Diversity and inclusion
- Privacy and (pseudo-)anonymity
- Culture, memes, and inside jokes
- Decentralization
- Authenticity
- Commitment / longevity

Growing Pains in the NFT Space

- Scammers, fraudsters, thieves
- “Rug pulls”
- “Pump and dumps”
- Unauthorized derivatives
- Environmental concerns
- Intervention vs. Decentralization
- Notice & assent to terms
- Lack of education

What is Privacy?

- Privacy
 - Respecting consumer expectation and choice regarding use of their personal information
- Security
 - Measures taken to secure the confidentiality, integrity, and availability of personal information



Why Does Privacy Matter for NFTs?

“While NFTs offer the promise of Web 3.0, most of the ecosystem—including the websites where NFTs are bought and sold and the platforms where NFT communities engage—still exists on “Web 2.0.” As a result, NFT drops rely on a “Web 2.5” ecosystem (as we like to call it) where data collection and monetization rule and a plethora of privacy laws, rules, and regulations apply.”

<https://advertisinglaw.fkks.com/post/102hq7y/nft-compliance-key-privacy-issues-to-consider-before-your-drop>

Why Does Privacy Matter for Your Business?

- Violation of law
- Breach of contractual obligations
- Reputational risk

Step 1: Generating Hype

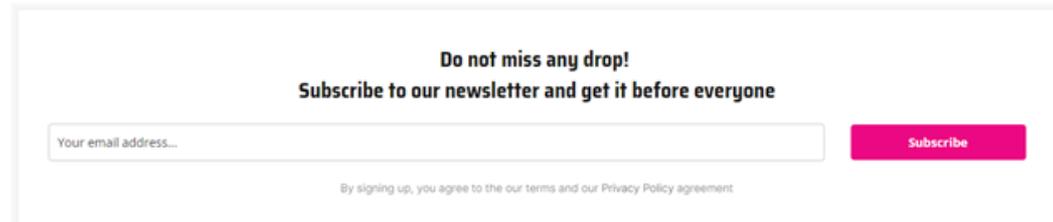
Before dropping an NFT collection, most brands try to build excitement around the drop. A brand typically starts by setting up a website and/or Discord server dedicated to the NFT drop. The brand then announces the NFT drop using Twitter, and often embeds a URL in its brand profile or tweets that links to the brand's Discord server and/or website.



Privacy Considerations

“As a rule of thumb, a brand is responsible for personal information it collects and processes, whether through its website, Twitter page, or Discord server (and beyond)

- Website data collection
 - Tracking technologies / targeted advertising
 - Email sign-up
- Social media data collection



Do not miss any drop!
Subscribe to our newsletter and get it before everyone

Your email address...

Subscribe

By signing up, you agree to the our terms and our Privacy Policy agreement

Comprehensive State Laws

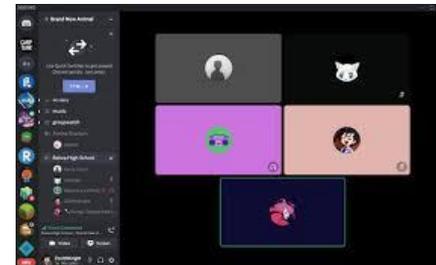
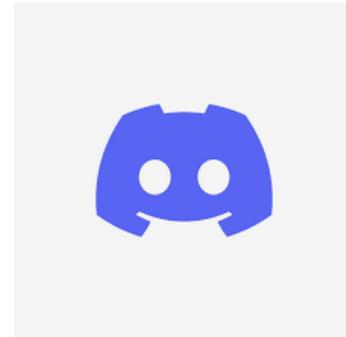
- California – CCPA (current); CPRA (Jan 2023)
- Virginia – VCDPA (Jan 2023)
- Colorado – CPA (July 2023)
- Connecticut – (July 2023)
- Utah – UCPA (Dec 2023)
- But No Federal (yet)!

Consumer Rights

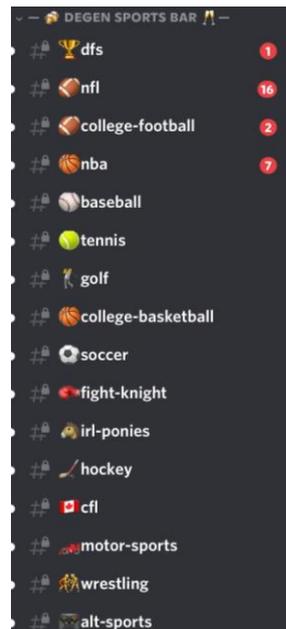
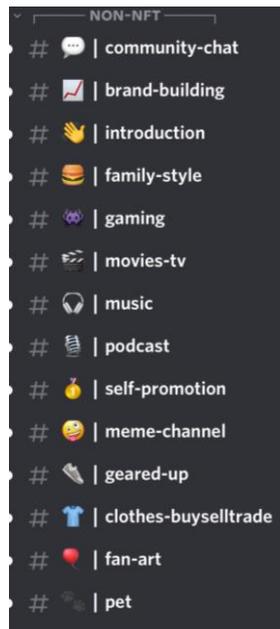
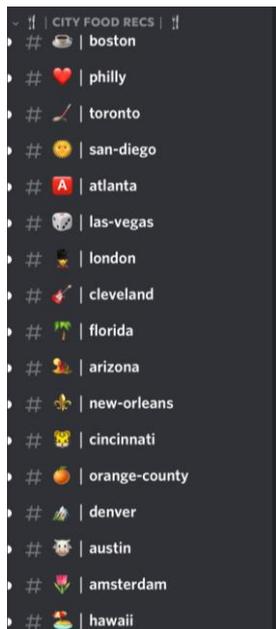
	CCPA/RA	CDPA	CPA	UCPA	Conn
Right to access/portability	x	x	x	x	x
Right to correct	x	x	x		x
Right to delete	x	x	x	x	x
Right to opt-out of sales	x	x*	x	x*	x
Right to opt out of shares	x				
Processing for targeted advertising		Opt out	Opt out	Opt out	Opt out
Processing for profiling	Regs	x	x		x
Processing of sensitive data	Opt out	Opt in	Opt in	Opt out	Opt in
Financial incentive	Opt in				
*Monetary consideration only					

Step 2: Developing a (Discord) Community

- Discord is a social media platform founded in 2015, but increasingly popularized with explosion of metaverse popularity
- Allows users to create invite-only topic-based spaces, called servers, which are made up of text channels and voice channels, and have cool features, like the ability to create custom emoji
- Text channels function much like on Slack, where users can organize conversations into separate topical discussion threads and even send and receive files
- Its voice channels allow users to speak to one another, video chat, share screens, livestream (including to a particular audience), and use a Spotify plugin to listen to music together
- Where people are talking to each other and activities are discussed and promoted



Discord Community



🔴 Sticker and Emoji Contest 🔴
NFH Discord Needs
New Stickers & Emojis to add to our collection!

How to submit:

- ✓ Complete this form!
- ✓ 100 \$LORE to each one added
- ✓ Up to 5 submissions

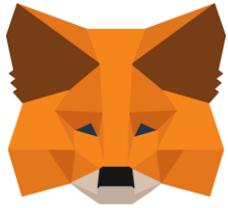
Full rules on the Google Form:
<https://t.co/L7zrWld7e7>

A cartoon illustration of a purple monkey character wearing a purple hoodie and holding a baseball bat. The letters 'LFG' are written in yellow on a black bat-shaped background behind the monkey's head.

Privacy Considerations

- Collecting personal information on Discord
- Linking to Privacy Policy
- Financial incentive opt-in & disclosure
- Biometric (voice) data
- Whitelists, Guest Lists, Allow Lists
- Applicable third-party policies

Step 3: Setting Up and Maintaining a Digital Wallet

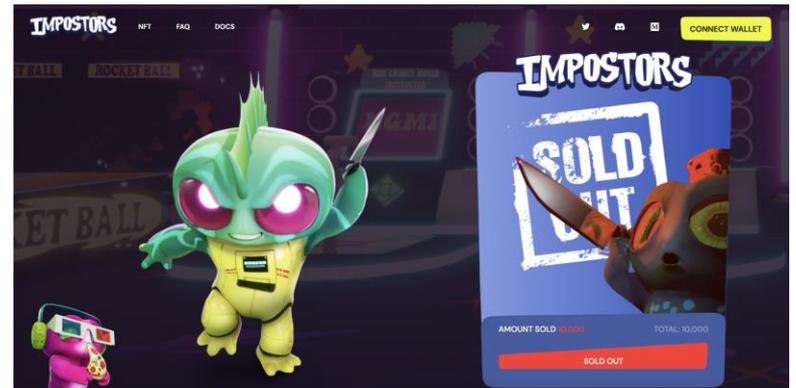
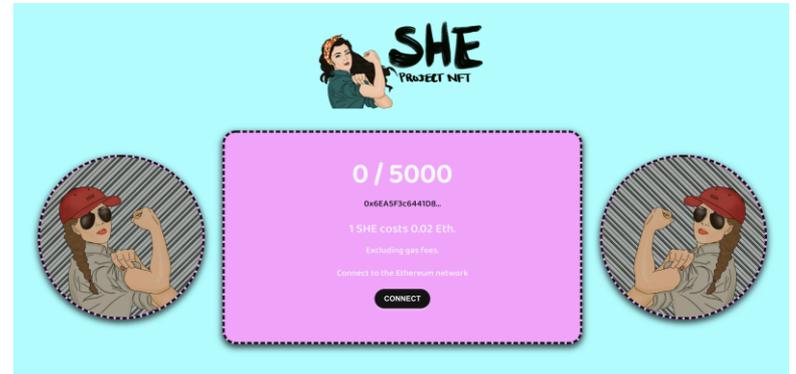
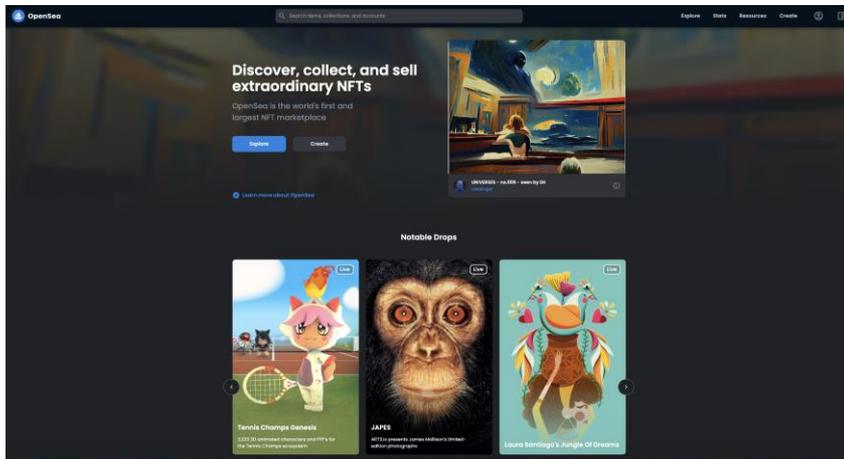


Security Considerations

- Custodial or non-custodial?
 - Employee rights?
- Securing the secret (AKA seed or recovery) phrase
- Bad actors, social engineering, and malicious links
- Incident response



Step 4: Dropping the NFT Collection



Is a digital wallet anonymous?

Through a quick search, a brand (and third parties) can view all of the transactions and assets associated with a digital wallet (or smart contract address) and find out:

- when the wallet was opened
- what assets the wallet holds and has held;
- when assets were purchased and sold;
- from whom assets were purchased and to whom assets were sold; and
- whether any blockchain-based domain names (i.e., customized wallet addresses) are associated with the wallet (e.g., janedoe.eth)

Block Explorers

The Ethereum Blockchain Explorer

All Filters

Featured: Curious on Ethereum's hottest 🔥 trading pairs? View top pairs and details with [DEX Trading Pairs!](#)

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x256cc232a95f8b77dc9...	Transfer	13332173	1 hr 31 mins ago	0x480bbc368197d44c6...	OUT Tether: USDT Stablecoin	0 Ether	0.0030444733
0x80a3cc0f344651b3de...	Transfer	13332078	1 hr 53 mins ago	0x752c8191e6b1db38b4...	IN 0x480bbc368197d44c6...	0.025 Ether	0.001559212674

Overview Access List State Comments

Transaction Hash:	0x80a3cc0f344651b3de745b2f1efbe8d35d4f348e95b345c8a840ebf955414fa5
Status:	Success
Block:	13332078 210 Block Confirmations
Timestamp:	46 mins ago (Oct-01-2021 07:25:45 AM +UTC) Confirmed within 30 secs
From:	0x752c8191e6b1db38b41a8c8921f7a703f2969d18
To:	0x480bbc368197d44c6f54a738e59c33eff004b6a
Value:	0.025 Ether (\$77.60)
Transaction Fee:	0.001559212674537 Ether (\$4.84)
Gas Price:	0.00000074248222597 Ether (74.248222597 Gwei)
Txn Type:	2 (EIP-1559)

[Click to see More](#) ↓

Privacy Considerations

- Is a digital wallet address personal information?
- Is the data within a wallet personal information?
- What if you associate data with the digital wallet address?
 - IP address (such as with a purchase)
 - Email address (such as with account sign-up)
 - KYC
- What if you associate data with data from the wallet?
 - Inferences generated based on publicly available information

Step 5: Post-Drop Utility

- Accessing/shipping physical goods
- In-person or virtual meetups
- Popular NFT use cases



Privacy Considerations

- Will vary depending on the utility and engagement
- Important to stay up-to-date
- Remain nimble to address obligations

Questions?

