ALBUS SECURITY

The Three C's of Web3

The web3 era is typified by three guiding principles:

- Control
- Composability
- de(centralization)

1. Control: Control refers to giving users more ownership and control over their digital assets, data, and online identity. In the traditional web (Web2), users often rely on centralized platforms and services that have control over their data and can manipulate or monetize it without their consent. In Web3, the aim is to shift control back to users by leveraging blockchain technology and cryptographic techniques. With Web3, individuals can have ownership of their digital assets, manage their data privacy, and have more autonomy over their online activities.
2. Composability: Composability is about the ability to combine and interact with different components or protocols seamlessly. In Web3, there is a focus on creating modular and interoperable systems, where various decentralized applications (dApps), protocols, and smart contracts can be easily combined and integrated to create new functionalities. This composability allows developers to build on top of existing protocols and leverage the collective innovation of the ecosystem, fostering a collaborative and open environment.
3. De(centralization): De(centralization) represents the move away from centralized authorities and towards decentralized networks. In Web3, the aim is to distribute power and decision-making across a network of peers rather than relying on a single central entity. This can involve various aspects, such as decentralized governance models, decentralized storage and hosting, decentralized finance (DeFi) systems, and more. Decentralization promotes transparency, resilience, censorship resistance, and fosters a trustless environment where users can interact directly without intermediaries.

There is not just one blockchain, however. There are a variety of blockchains, each with different benefits and communities. In this course, we will learn more about the Ethereum blockchain, which is built using Solidity programming.

Other blockchains you may have heard of are Bitcoin, Solana, or Flow. You can learn how to code on Solana, Flow, and more in our other courses! 🤪

SCARCITY

Imagine you have a ticket to a sporting event. The people organizing the event decide how many tickets to sell, right? They might choose to sell 5000 General Admission tickets, or maybe they want to make it more special by selling tickets with assigned seats. In some cases, they might even create a very rare and unique ticket to make it a special collectible.

Now, let's compare this to NFTs (Non-Fungible Tokens). NFTs are like digital tickets or assets that can be owned and traded on the internet. Just like the organizers of the event, the person who creates an NFT gets to decide how many copies or versions of that NFT exist.

Sometimes, the creator wants each NFT to be completely unique. It's like having only one ticket with a unique bar code. This uniqueness adds to the scarcity and value of the NFT. Other times, the creator might want to make multiple copies of the NFT that are slightly different from each other, just like having different tickets with assigned seats. Each copy still has its own unique identifier (like a bar code), but they are not exactly the same.

The important thing to remember is that the creator has control over the scarcity of the NFT. They can choose to make many replicas or create just a single NFT as a rare and special collectible. This information about how many copies or versions exist is publicly available for everyone to see.

Ethereum and NFTs

Ethereum makes it possible for NFTs to work for a number of reasons:

- Transaction history and token metadata is publicly verifiable – it's simple to prove ownership history.
- Once a transaction is confirmed, it's nearly impossible to manipulate that data to "steal" ownership.
- Trading NFTs can happen peer-to-peer without needing platforms that can take large cuts as compensation.
- All Ethereum products share the same "backend". Put another way, all Ethereum products can easily understand each other – this makes NFTs portable across products. You can buy an NFT on one product and sell it on another easily. As a creator you can list your NFTs on multiple products at the same time – every product will have the most up-to-date ownership information.
- Ethereum never goes down, meaning your tokens will always be available to sell.

The environmental impact of NFTs

Creating and transferring NFTs are just Ethereum transactions - minting, buying, swapping or interacting with NFTs does not directly consume energy. Since The Merge, Ethereum is a low-energy blockchain, meaning the environmental impact of using NFTs is negligible.

Don't blame it on the NFTs

The whole NFT ecosystem works because Ethereum is decentralized and secure.

Decentralized meaning you and everyone else can verify you own something. All without trusting or granting custody to a third party who can impose their own rules at will. It also means your NFT is portable across many different products and markets.

Secure meaning no one can copy/paste your NFT or steal it.

These qualities of Ethereum makes digitally owning unique items and getting a fair price for your content possible. Ethereum protects the assets using a decentralized consensus mechanism which involves 'proof-of-stake'. This is a low carbon method to determine who can add a block of transactions to the chain, and is considered more secure than the energy-intensive alternative, 'proof-of-work'. NFTs have been associated with high energy expenditure because Ethereum used to be secured using proof-of-work. This is no longer true.

Minting NFTs

When you mint an NFT, a few things have to happen:

- It needs to be confirmed as an asset on the blockchain.
- The owner's account balance must be updated to include that asset. This makes it possible for it to then be traded or verifiably "owned".
- The transactions that confirm the above need to be added to a block and "immortalized" on the chain.
- The block needs to be confirmed by everyone in the network as "correct". This consensus removes the need for intermediaries because the network agrees that your NFT exists and belongs to you. And it's on chain so anyone can check it. This is one of the ways Ethereum helps NFT creators to maximize their earnings.

All these tasks are done by block producers and validators. Block proposers add your NFT transaction to a block and broadcast it to the rest of the network. Validators check that the transaction is valid and then add it to their databases. There are lots of crypto-economic incentives in place to make sure validators are acting honestly. Otherwise, anyone could just claim that they own the NFT you just minted and fraudulently transfer ownership.

NFT security

Ethereum's security comes from proof-of-stake. The system is designed to economically disincentivize malicious actions, making Ethereum tamper-proof. This is what makes NFTs possible. Once the block containing your NFT transaction becomes finalized it would cost an attacker millions of ETH to change it. Anyone running Ethereum software would immediately be able to detect dishonest tampering with an NFT, and the bad actor would be economically penalized and ejected.

Security issues relating to NFTs are most often related to phishing scams, smart contract vulnerabilities or user errors (such as inadvertently exposing private keys), making good wallet security critical for NFT owners.

More on security