

# Twitter Thread by Misha

Misha

@mishadavinci



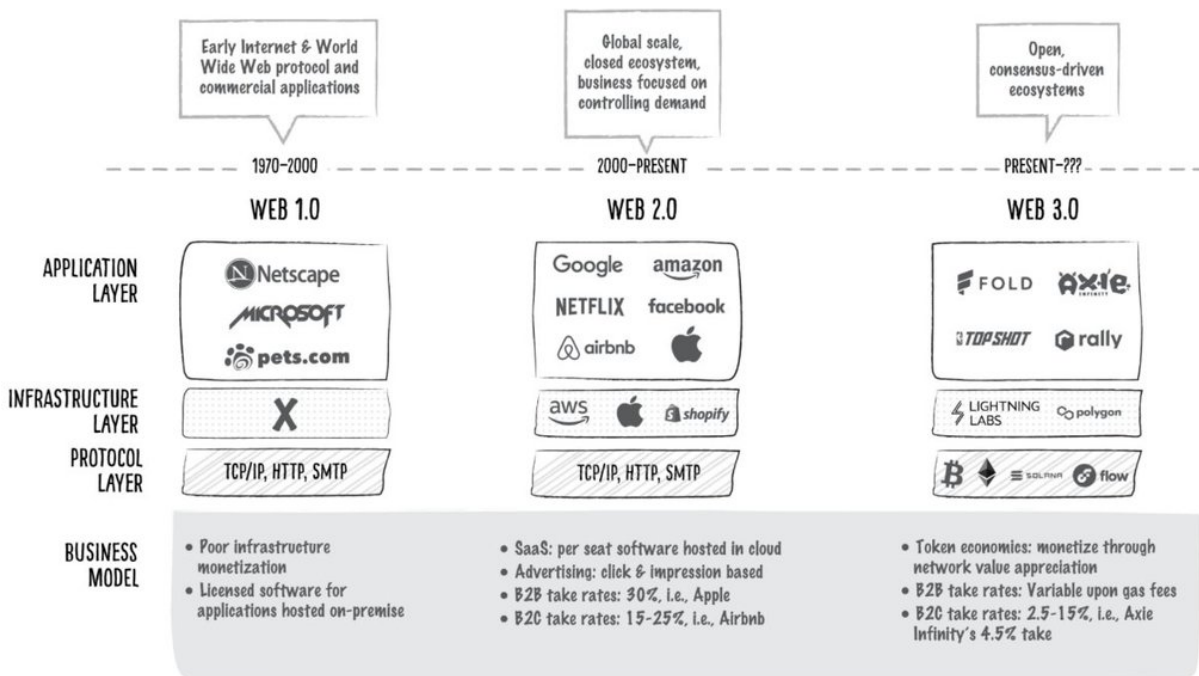
The future is already here.

The 1% who understand it will run the world.

Here's a thread of key concepts that will get you up to speed, quickly:

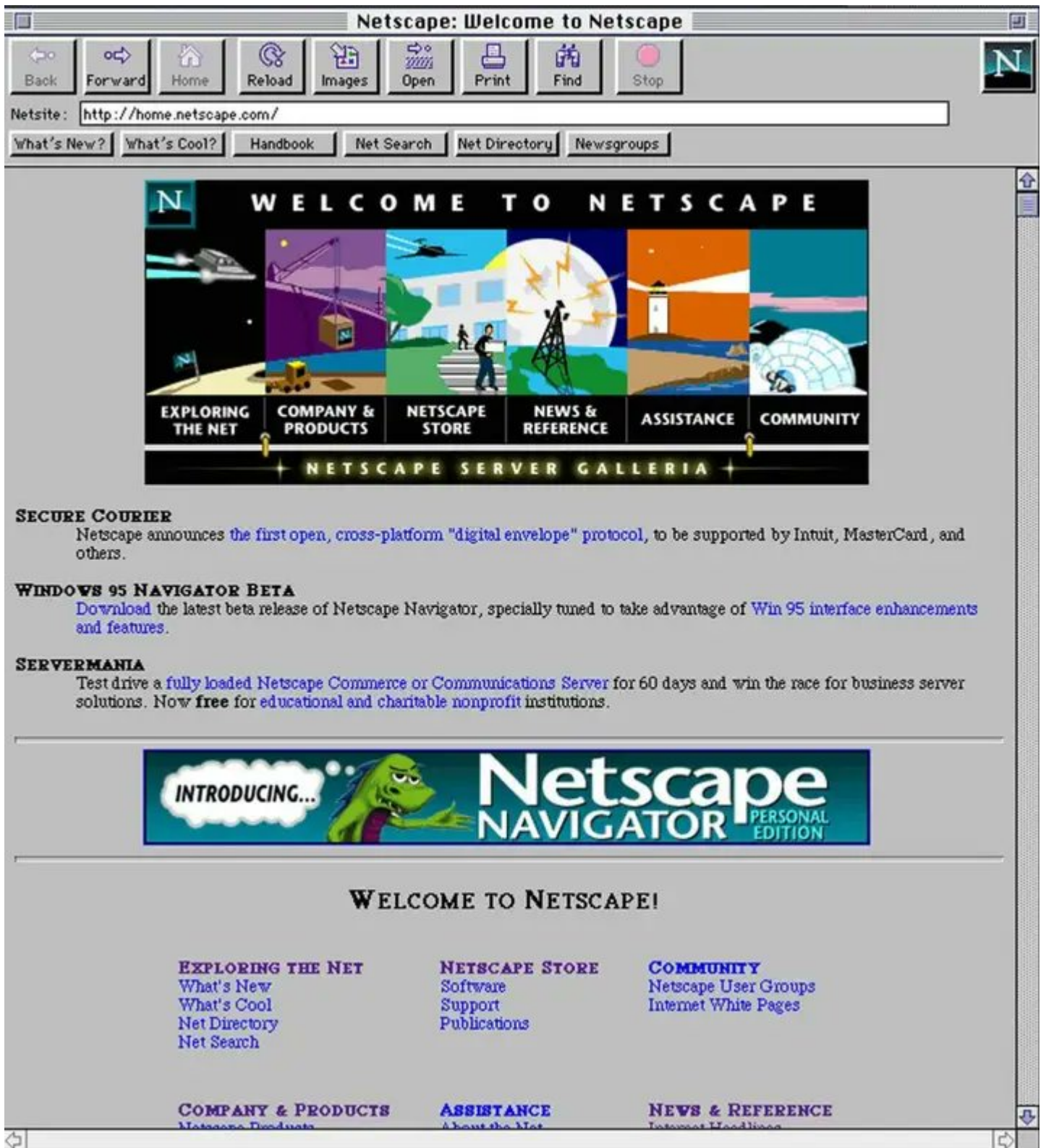
WEB3 is the new internet that is rapidly emerging on blockchain computer networks like Ethereum.

Web3 transforms the internet, making it a better place for humans.



In the early 1990s, web1 emerges on the free internet protocols.

Users can navigate between pages, but the content is static.



In the early 2000s, web2 brings the ability to interact.

Google, YouTube, Facebook, and Twitter mean we can now watch, search, and share.

But while we create the content, it is all controlled by these platforms.

More here ■ <https://t.co/9zQ7VUDmPN>

Every single day, the 5 tech giants use your online property to make massive profits.

Last year alone, they took in \$1,400,000,000,000.

Here's what you need to KNOW & DO:

— Misha (@mishadavinci) [July 31, 2022](#)

In the 2020s, web3 is bringing digital ownership to users.

The norm: no rights, security, privacy or ownership for users.

The shift: you can own digital assets, control your content and data, and have real security and privacy.

## Web 3.0 Simply Explained

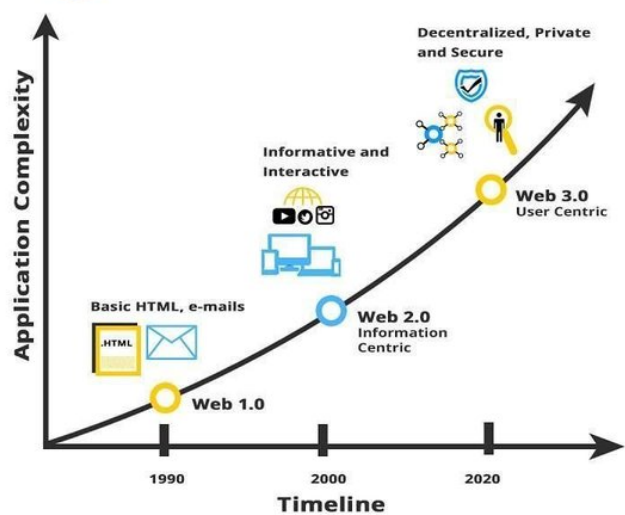
### 1 What is Web 3.0?

Web 3.0 is the 3rd generation of the internet where the devices are connected in a decentralized network rather depending on server-based databases.

The new internet is a user-centric, more secured, private and better connected.



### 2 The History of the Web



### 3 Web 3.0 Benefits



Anti-monopoly and Pro-privacy



Secure Network



Data Ownership



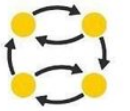
Interoperability



No interruption in service



Permissionless blockchains

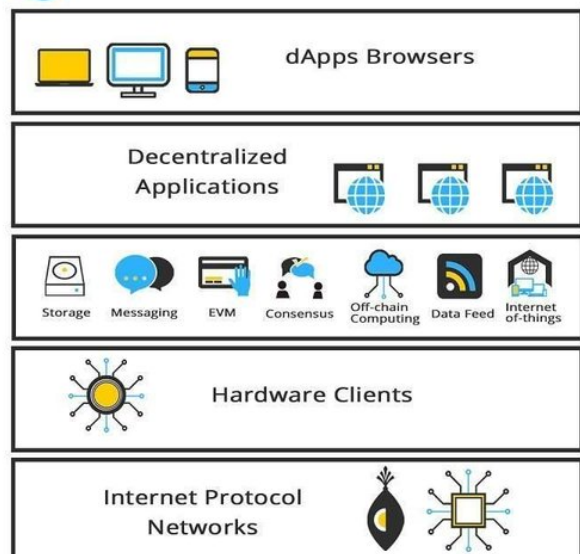


Semantic Web



Ubiquity

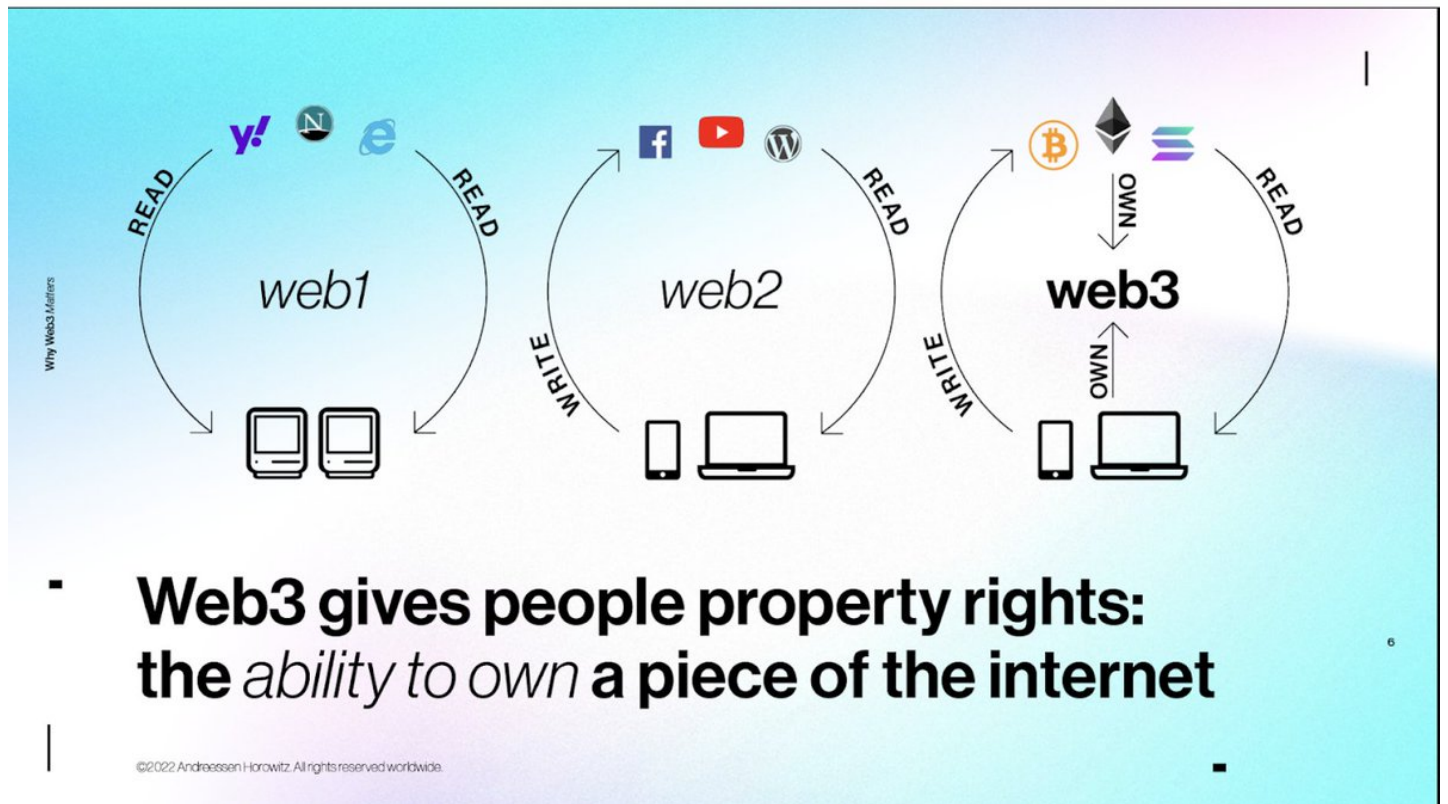
### 4 Web 3.0 Stack



DIGITAL OWNERSHIP means you can create or purchase a digital asset and have full control of it.

You have digital property rights and can perform transactions or move your assets.

[img a16zcrypto]



Now you:

- own your online identity and social media content
- own your online personal, medical data and browsing history
- can participate in and benefit from the internet economy.

NFTs make digital ownership possible.

More on this from [@cdixon](#) ■ <https://t.co/kdVI7BdNhP>

NFTs add a new layer of value \u2014 digital ownership \u2014 that didn\u2019t exist in a credible way before NFTs.

— cdixon.eth (@cdixon) [January 1, 2022](#)

The norm: we take physical ownership for granted, but think digital ownership is not possible. And we give away our digital property.

The shift: digital ownership is not only possible but more accessible than physical ownership, and even expands ownership of real-world assets.

## New Digital Assets

Music	Games	Politics
Movies	Money	Government
Letters	Reputation	Voting
Advertizing	Dating	Journalism
Identity	Credit	Photos
Friendships	Banking	Revolutions
Conversations	Knowledge	Justice
Therapy	Languages	Parking Spaces
Medical	Maps	Hotel Rooms
Education	Work	Legacy

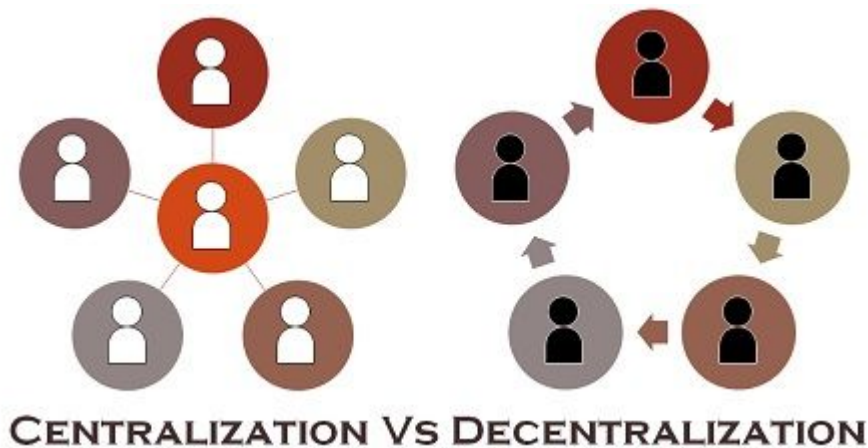
Here's a deeper look into the ownership possibilities that tokens bring to the internet and your digital life:

<https://t.co/dM41tNey7k>

DECENTRALIZATION is a core concept in web3.

It refers to replacing systems under a single entity's control with systems that distribute control among participants.

It's a current paradigm shift that will redistribute power and improve how societies function.



Blockchain technology makes decentralization possible.

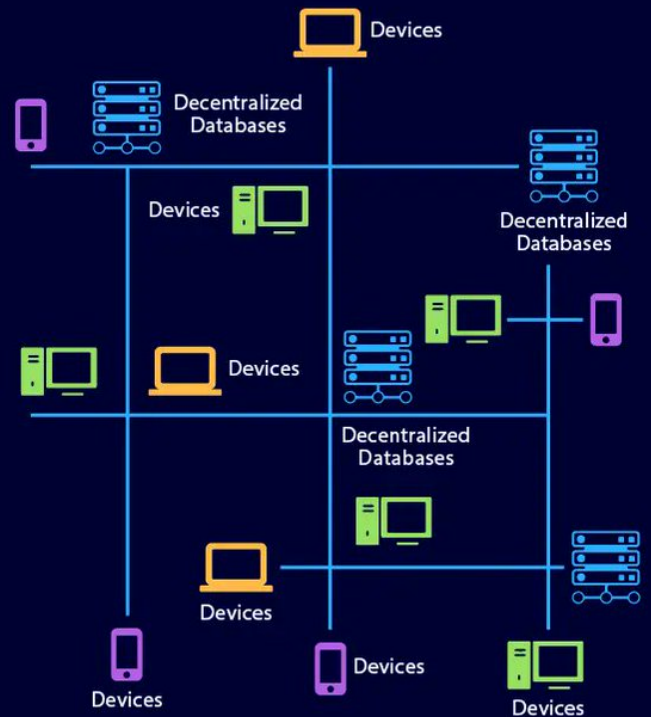
It decentralizes the internet, eliminating Big Tech and middlemen.

# Centralized vs Decentralized Internet

BEFORE



AFTER



Decentralization causes a radical shift from the status quo and allows us to build peer-to-peer organizations and social structures.

Here's Why the future will be decentralized from [@bigthink](#)

<https://t.co/IFmkTortsU>

The norm: everything we do passes through some centralized organization that controls most aspects of how we live.

The shift: computer code replaces centralized control, opening opportunities and activating massive latent talent and human potential.



PERMISSIONLESS blockchains are decentralized and open to the public.

There are no gatekeepers.

Anyone who wants to access the blockchain does not need to pass Know Your Customer (KYC) requirements or provide identification documents.

Key characteristics of a permissionless system are:

- full transparency
- open source
- anonymity
- lack of a central authority

This means many more people have access.



## PERMISSIONLESS BLOCKCHAIN

### WHAT ARE PERMISSIONLESS BLOCKCHAINS?

Permissionless blockchains are blockchains that require no permission to join and interact with.

### CHARACTERISTICS

- Truly decentralized
- Transparent network
- Immutability



### ADVANTAGES

- Open to all
- Brings trust to all users
- Offers high security



### DISADVANTAGES

- Slow transaction speed
- Harder to scale
- Not energy efficient



### USE CASES

- Digital Identity
- Voting
- Fundraising



## PERMISSIONED BLOCKCHAIN

### WHAT ARE PERMISSIONED BLOCKCHAINS?

Permissioned blockchains are blockchains that require permission to join and participate in consensus.

### CHARACTERISTICS

- Governance structure
- Private transactions
- Authentication process



### ADVANTAGES

- Extremely fast output
- Scalable network
- Offers energy efficiency



### DISADVANTAGES

- Not truly decentralized
- Less transparent
- Partial immutability



### USE CASES

- Food tracking
- Banking and payments
- Supply chain management



The norm: a central authority controls who can use the system, some have access many do not.

The shift: no one is excluded, allowing billions more to:

- participate in the economy
- expand creative opportunity
- build more useful product/Dapps.



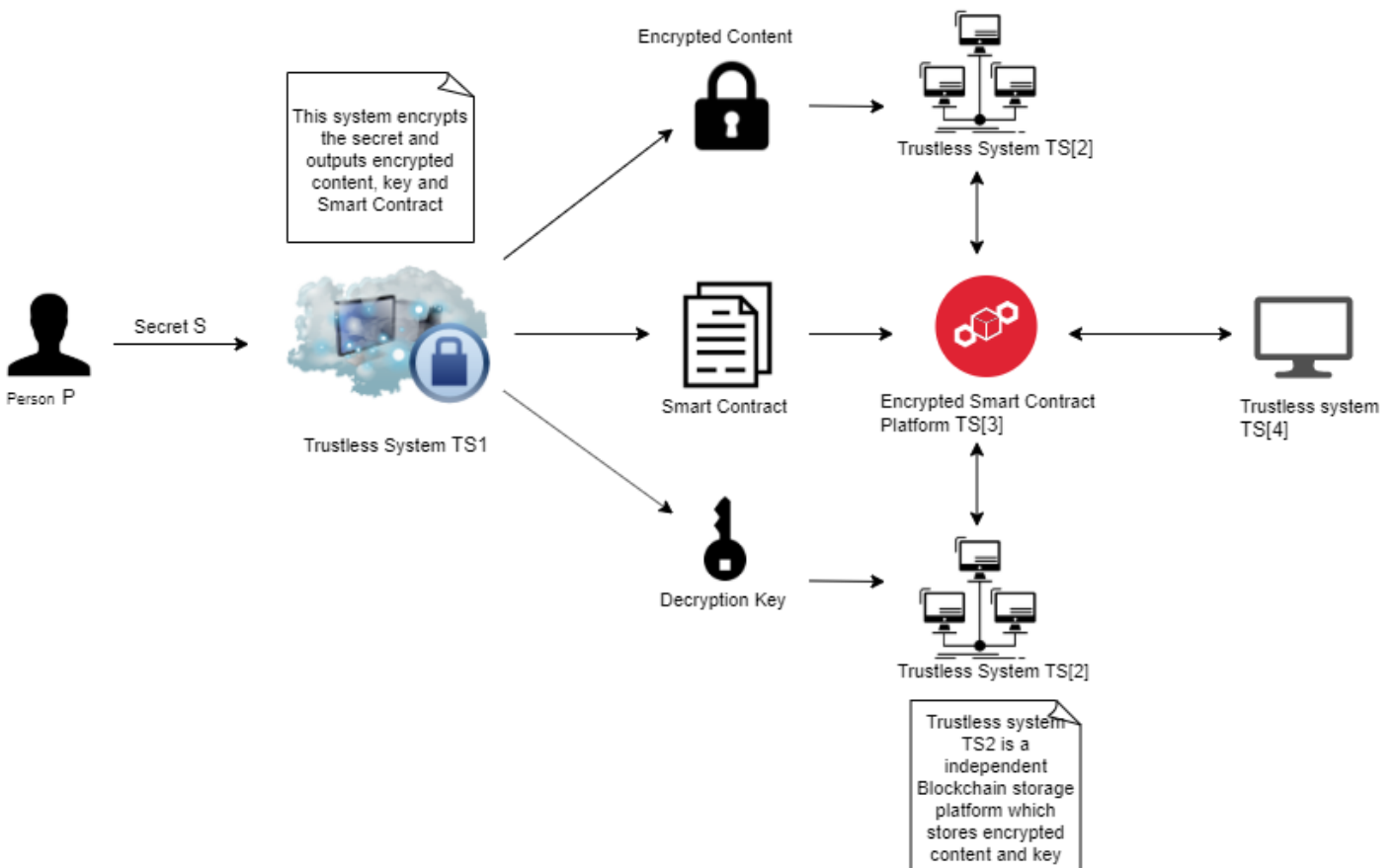
Here's a video on what permissionless means and why it matters from [@DefiantNews](#)

<https://t.co/WuaVbNmCob>

A TRUSTLESS system executes a transaction without any need for the humans involved to trust each other.

The system creates the trust.

And eliminates the need for an intermediary, such as a bank or exchange, to ensure the outcome.



Blockchain technology uses smart contracts to facilitate trustless interactions between users.

Computer code executes the task.

This allows total strangers from anywhere on the globe to do business without an intermediary.

# A WALK THROUGH A SMART CONTRACT EXECUTION PROCESS

Source: Global X ETFs.



## Contract

Bob and Alice want to make sure the conditions of an agreement are met. If met, Alice owes Bob \$20 in value.

Alice locks \$20 in a smart contract and submits the pre-defined contract to the blockchain.



## Event

Let's assume the condition is met.

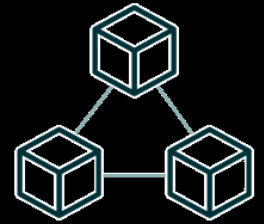
The smart contract can verify the validity of the terms via decentralized data oracles such as Chainlink.



## Outcome

The contract is triggered because it meets the conditions outlined when the contract was created.

A value of \$20 is transferred from the smart contract to Bob.



## Settlement

Settlement occurs once the block of transactions is added to the blockchain.

The distributed ledger recognized Bob's \$20 credit to his address.

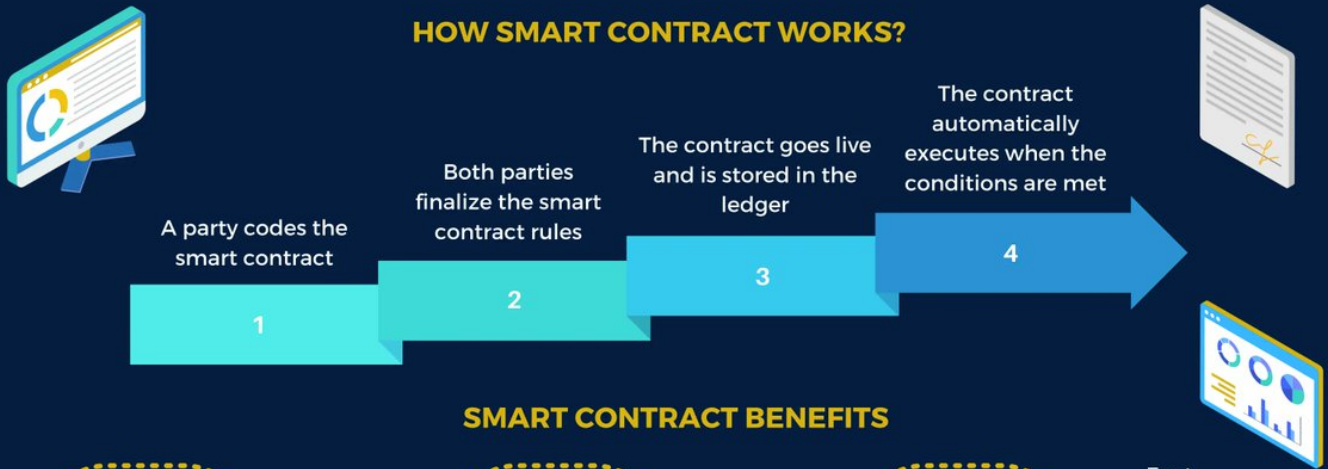
The norm: two strangers need an intermediary they both trust, like a bank, in order to do business.

The shift: users trust the code and the smart contract executes the transaction, eliminating the expensive, controlling middleman.

## WHAT IS A SMART CONTRACT?

A smart contract is a set of digital codes that is used to exchange assets including shares, money, or property without the need for any intermediates to function.

## HOW SMART CONTRACT WORKS?



## SMART CONTRACT BENEFITS



## USE CASES



Trustless systems transform business, finance and even voting systems.

In this video, Crypto, the Future of Trust

[@alive\\_eth](#) delves into the meaning, history and future of trust and how it changes the future.

<https://t.co/rglUx5ufM9>

ZERO KNOWLEDGE PROOFS are a way to prove knowledge of a particular set of information without actually revealing what that information is.

It's an authentication system without any exchange of sensitive data.



## WHAT IS ZKP?

A zero knowledge proof is a unique method where a user can prove to another user that he/she knows an absolute value, without actually conveying any extra information.

Here, the prover could prove that he knows the value  $z$  to the verifier without giving him any information other than the fact that he knows the value  $z$ .

## ZERO KNOWLEDGE PROOF PROPERTIES



### COMPLETENESS

If the statement is really true and both users follow the rules properly, then the verifier would be convinced without any artificial help.



### SOUNDNESS

In case of the statement being false, the verifier would not be convinced in any scenario. (The method is probabilistically checked to ensure that the probability of falsehood is equal to zero)



### ZERO-KNOWLEDGE

The verifier in every case would not know any more information.

## ZERO KNOWLEDGE PROOF: WHAT ARE THE USE CASES?

### MESSAGING

In messaging end-to-end encryption is necessary. Two users have to verify their trust to the server and vice versa. On the other hand, ZKP provides that end-to-end trust without leaking any extra info.



### SHARING DATA

Sharing data across the internet without a third party eye is exceptionally crucial. ZKP can definitely help out here too.



### SECURITY FOR SENSITIVE INFORMATION

Sensitive information such as bank statements or credit card info needs an added level of security. ZKP can provide that.



### AUTHENTICATION

ZKP can restrict any user from accessing complex documentation that he isn't authorized to see.



### STORAGE PROTECTION

It can provide greater protection for your storage utility. It's equipped with the protocol to keep the hackers away.



### COMPLEX DOCUMENTATION

Zero knowledge proof can help to convey sensitive information like authentication information with extra security.



### FILE SYSTEM CONTROL

Everything within a file system can be protected by the zero knowledge proof protocol. The files, the users and even every login can have different layers of security.

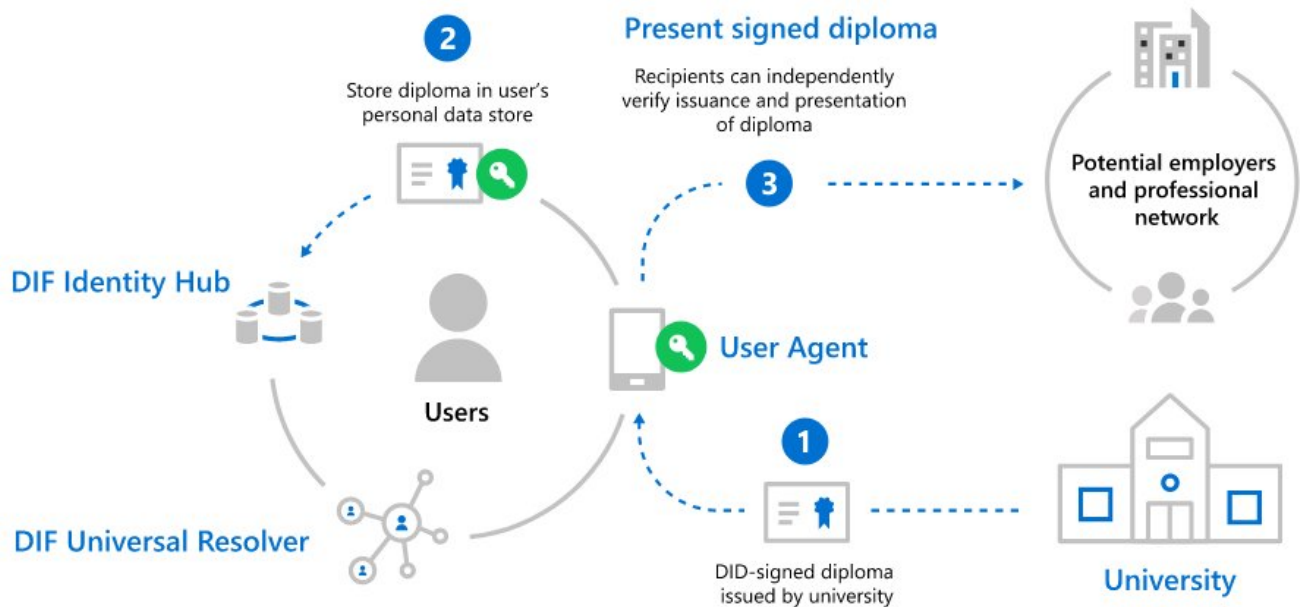


Created by 101blockchains.com

ZK Proofs are a powerful way to protect online security and privacy.

Say you need to be a certain age before you can sign up for a service.

With ZK you can deliver proof of age without sharing private info.



ZK Proofs will transform how we live.

It will allow anyone to make a completely private transaction on their mobile and then settle that on a trustless blockchain.

In this video from Wired, a computer scientist explains ZK ■

<https://t.co/4rz7Um8Wmd>

The norm: repeatedly revealing unnecessary sensitive personal data.

The shift: necessary proofs are provided while completely preserving your privacy.

For deeper study ■

The Zero Knowledge Canon from [@smc90](#) and the team [@a16zcrypto](#)

<https://t.co/L98izGJ9XW>

## RESOURCES

The best 2021 discussion of the new internet:

This still completely relevant convo between [@cdixon](#), [@naval](#) and [@tferriss](#) ■

<https://t.co/MM42T9pWVP>

Best 2022 discussion on where things are headed:

This must-listen convo between [@cdixon](#) and [@kevinrose](#) ■

Age of Wonders: NFTs, Art, AI, Cycles of Computing | web3 with a16z <https://t.co/NIYj2QXPx0>

Who to follow:

[@alive\\_eth](#)

[@bryanhpchiang](#)

[@CamiRusso](#)

[@cdixon](#)

[@eddylazzarin](#)

[@kevinrose](#)

[@naval](#)

[@smc90](#)

[@succinctjt](#)

[@VirtualElena](#)

That's it, folks. I hope this was useful.

If you enjoyed it, please share by retweeting the first tweet.

I write about the ideas, technology and people shaping web3 and the future. You can follow me [@MishadaVinci](#).  
<https://t.co/09hNhNs43V>

The future is already here.

The 1% who understand it will run the world.

Here's a thread of key concepts that will get you up to speed, quickly:

— Misha (@mishadavinci) [October 23, 2022](#)

My Future of the World newsletter is moments away.

It will be jam-packed with content to help you keep up with the future.

Subscribe here ■

<https://t.co/qpi7UDRqkx>