Taking a Stroll through Ethereum

...

More than just NFTs

06/2021 Dominik Muhs

$whoami

- CS @ TU Dresden
- Working with Ethereum since 2018
- Background: Data Science and Backend
- Now: Security Engineering with ConsenSys Diligence

If you have questions: @lethalspoons

Our Tour

1. Introduction to Blockchains
2. What are Smart Contracts?
3. What has been built so far?
4. What is being built right now?
5. How do I join in on the action?

Introduction to Blockchain Technology

- Key ingredients
  - Cryptographic hash functions
  - Public key cryptography
  - Merkle trees

Cryptographic Hash Functions

- e.g. Kecchak256

“hello” => 1c8aff950685c2ed4bc3...

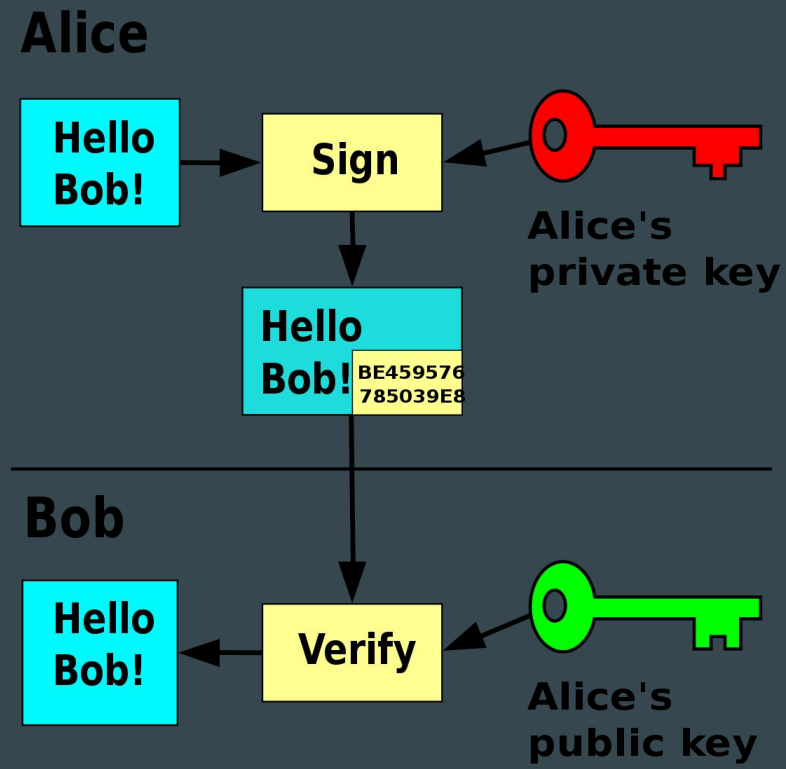
“hello “ => 40000f84265ae2330b1336cd8fce...

- certain properties needed:
  - deterministic
  - pre-image resistant
  - correlation-resistant
  - collision-resistant
  - fast

https://dmuhs.blog/2018/10/15/explain-like-im-five-cryptographic-hashing/

Public Key Cryptography

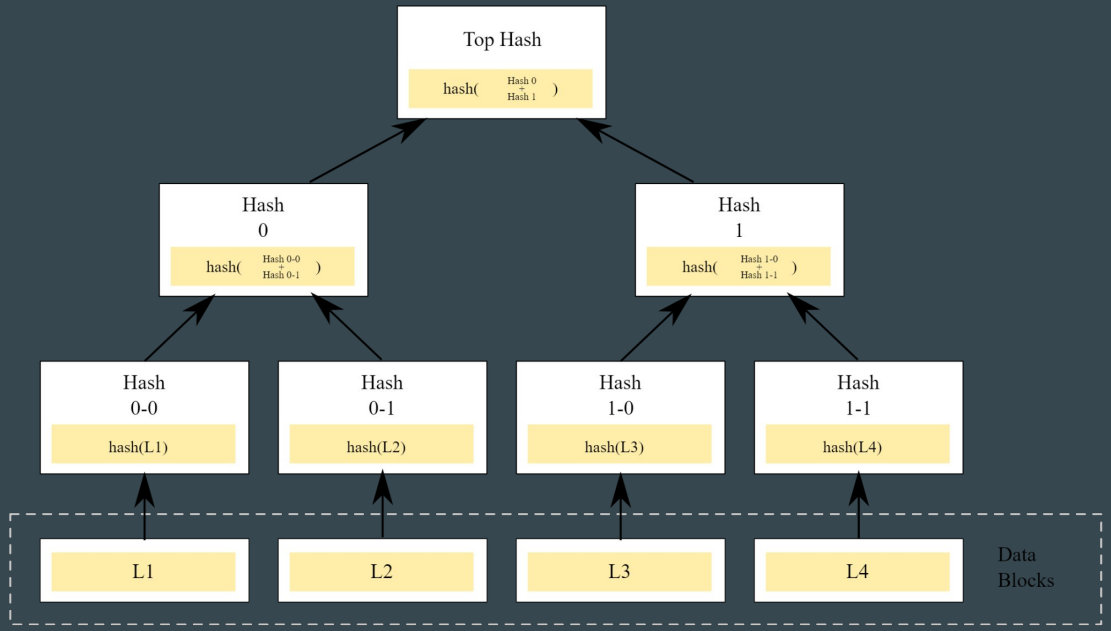
- Public/private key pairs
- We need to sign things!
- Most common: ECDSA



https://medium.com/mycrypto/the-magic-of-digital-signatures-on-ethereum-98fe184dc9c7

Merkle Trees

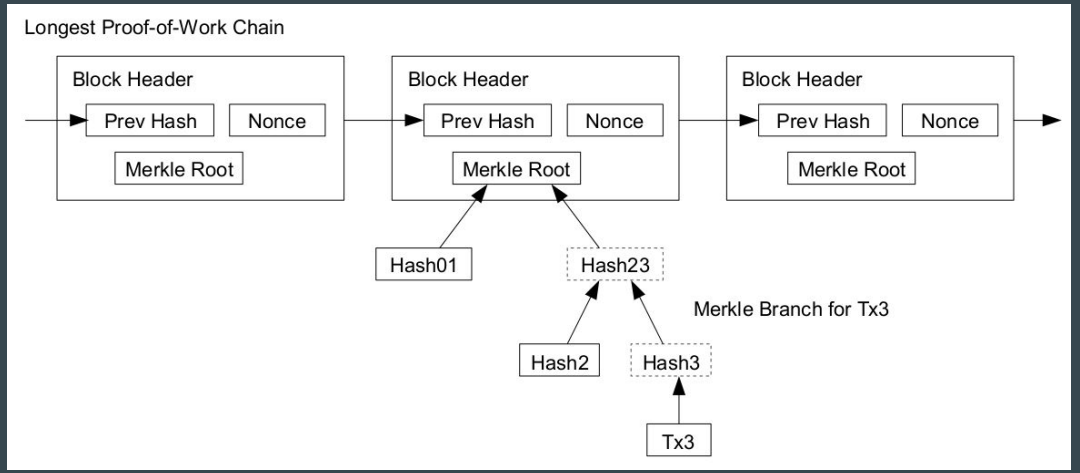
- Only thing I didn't learn about in uni
- chunk data, sort into buckets
- hash buckets, repeat process
- Merkle Proofs!
- Allows for very fast queries without downloading all data



https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/

Mixing it Together...

- Now we have a way to..
  - validate authenticity of data
  - query lots of data efficiently
- Let's link it!



Side-Track: Miners

- Miners do a proof-of-work
- Calculation of hashes
- Collaborate in pools
- Get rewarded for “finding” new blocks
- Sometimes they are mean

Introduction to Smart Contracts

So far we only built Bitcoin. :(

- global shared state
- cryptographically secured
- ordered, transactional state changes

If we can store anything on a blockchain, why not code?

That's what Ethereum is all about!

What Makes Contracts Smart?

- Metaphor: vending machine
- Code executed by every participant
- Result of code is the new state

“But what if I build an infinite loop?”

- Gas is used up for each instruction
- More complexity -> more gas -> more cost
- Storage and memory access included


```
608060405260405162000021b9380380620021b98339818101604052 60c081101562
```


https://ethereum.github.io/yellowpaper/paper.pdf

Meet Solidity

- Inspired by JavaScript
- Compiled, statically typed
- A bit wacky in some places

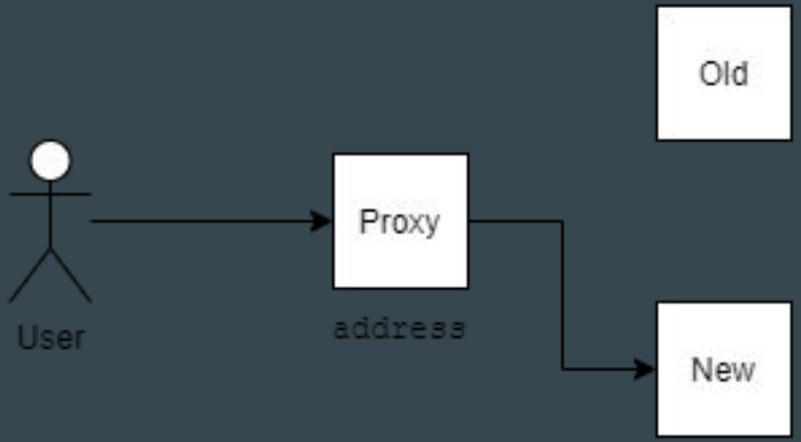
Go have fun: remix.ethereum.org

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

/**
 * @title Storage
 * @dev Store & retrieve value in a variable
 */
contract Storage {

    uint256 number;

    /**
     * @dev Store value in variable
     * @param num value to store
     */
    function store(uint256 num) public {
        number = num;
    }

    /**
     * @dev Return value
     * @return value of 'number'
     */
    function retrieve() public view returns (uint256){
        return number;
    }
}
```

https://soliditylang.org/

Security Aspects of Smart Contracts

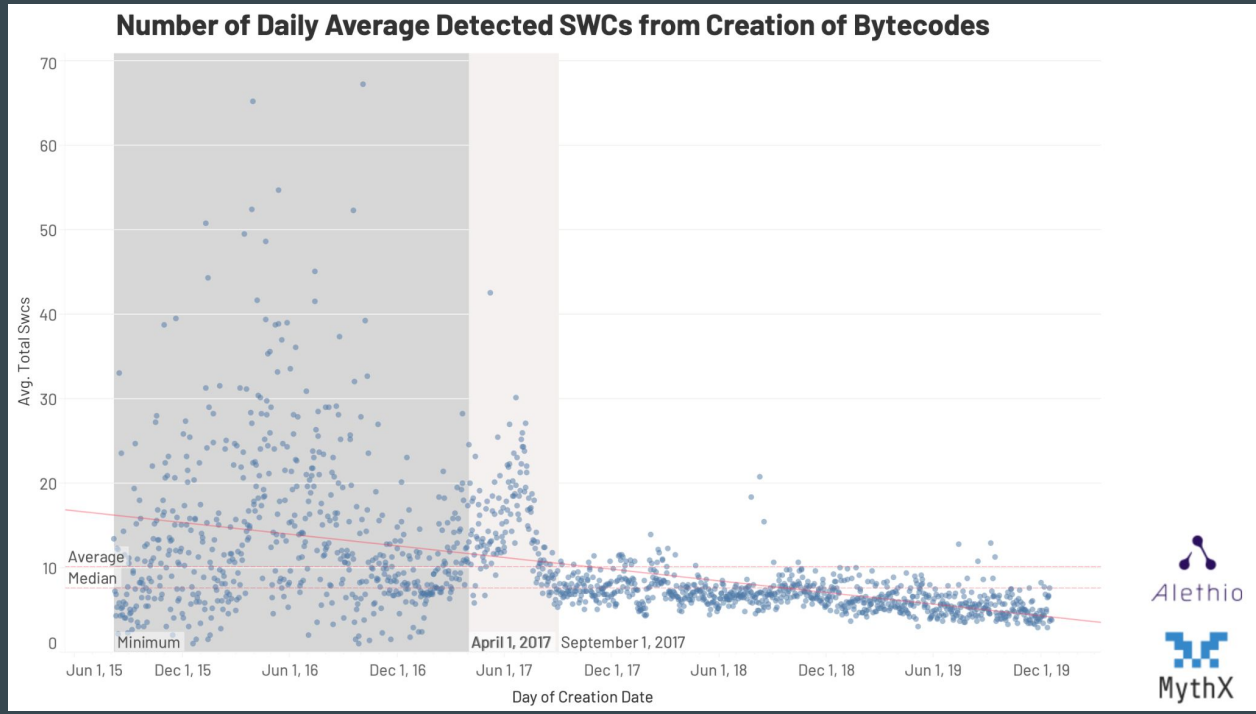
- Immutability can be problematic
- Upgradeability as well
- QA and audits are a must-have
- Formal verification very popular as well



Security in Ethereum

- We tried to measure it some time ago
- Purely based on bytecode

Based on SWC registry: swcregistry.io

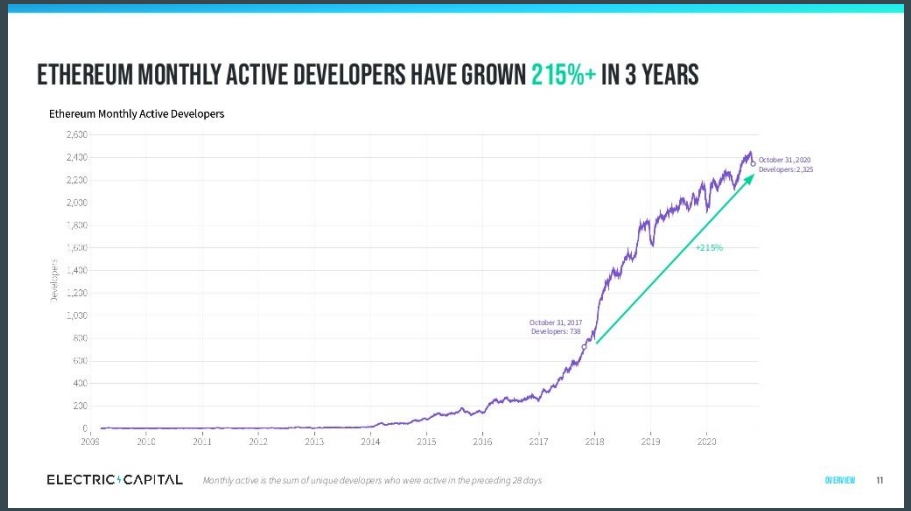


https://medium.com/alethio/the-security-series-a-look-at-ethereums-smart-contracts-4f096f48f2b

What has been built so far?

- largest developer community in blockchain space
- extremely fast-paced development
- incentivization experiments

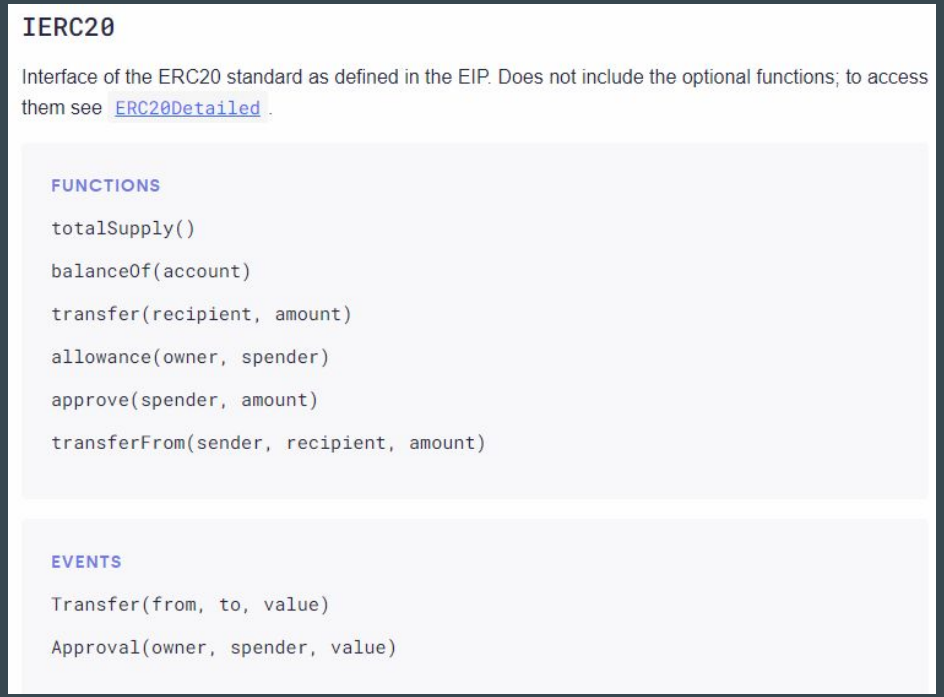
Let’s check out some history



https://medium.com/electric-capital/electric-capital-developer-report-2020-9417165c6444

ERC-20 Tokens

- Fueled ICO boom around 2017
- Smart contract implementing a fungible digital currency
- Highlights:
  - balanceOf()
  - transfer()
- Lots of early dev teams funded by token sales (and later investigated by SEC)
- Token economies, asset tokenization became popular



IERC20

Interface of the ERC20 standard as defined in the EIP. Does not include the optional functions; to access them see `ERC20Detailed`.

FUNCTIONS

```
totalSupply()
balanceOf(account)
transfer(recipient, amount)
allowance(owner, spender)
approve(spender, amount)
transferFrom(sender, recipient, amount)
```

EVENTS

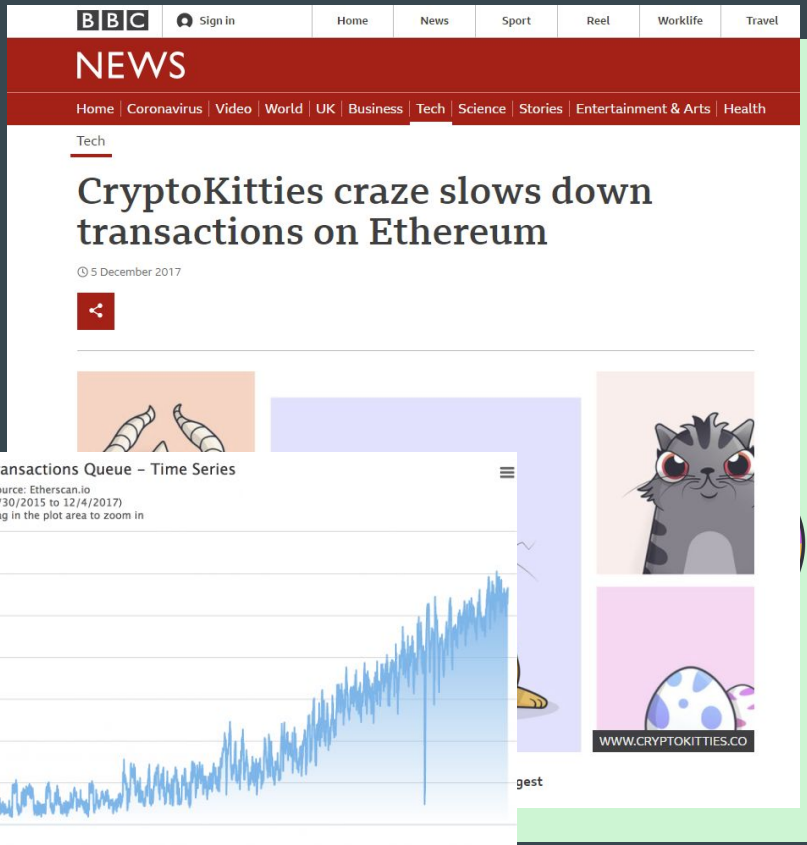
```
Transfer(from, to, value)
Approval(owner, spender, value)
```

https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

ERC-721

- Aka NFTs
- Similar to ERC-20 but non-fungible
- First real application: breeding kittens (2017)

Fun fact: CryptoKitties was almost too popular for Ethereum to handle (Dec 2017)

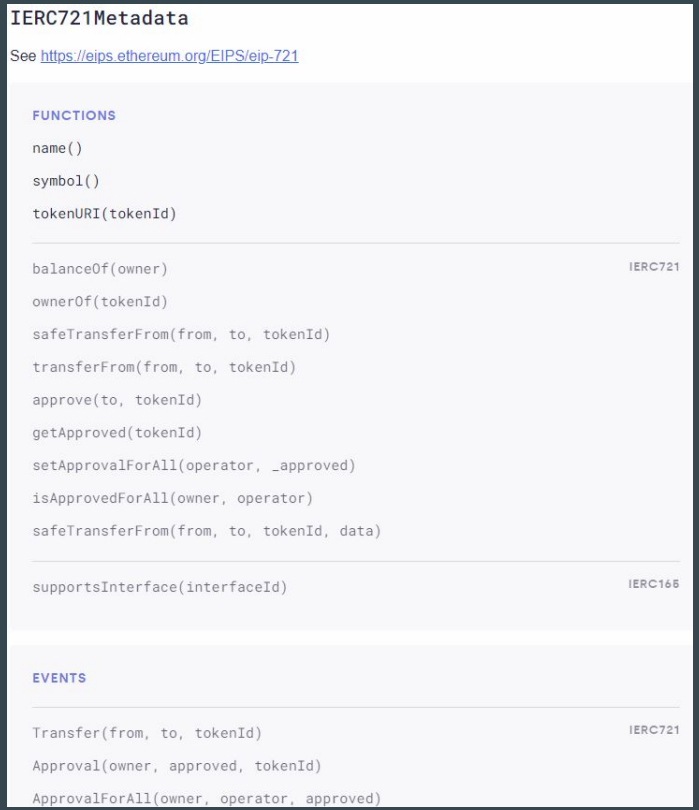


https://media.consensys.net/the-inside-story-of-the-cryptokitties-congestion-crisis-499b35d119cc

Debunking the Hype!!!1

- ERC-721 metadata extension
- mostly used to attach image assets
- main addition: tokenURI()
- e.g. tokenURI -> “cat1337.png” (or full URL)
- Mostly hosted on centralized servers
- So people buy the NFT but the underlying asset can change

Hype is annoying, but it brings attention, community growth, and money with it.



IERC721Metadata

See https://eips.ethereum.org/EIPS/eip-721

FUNCTIONS

name()

symbol()

tokenURI(tokenId)

balanceOf(owner) IERC721

ownerOf(tokenId)

safeTransferFrom(from, to, tokenId)

transferFrom(from, to, tokenId)

approve(to, tokenId)

getApproved(tokenId)

setApprovalForAll(operator, _approved)

isApprovedForAll(owner, operator)

safeTransferFrom(from, to, tokenId, data)

supportsInterface(interfaceId) IERC165

EVENTS

Transfer(from, to, tokenId) IERC721

Approval(owner, approved, tokenId)

ApprovalForAll(owner, operator, approved)

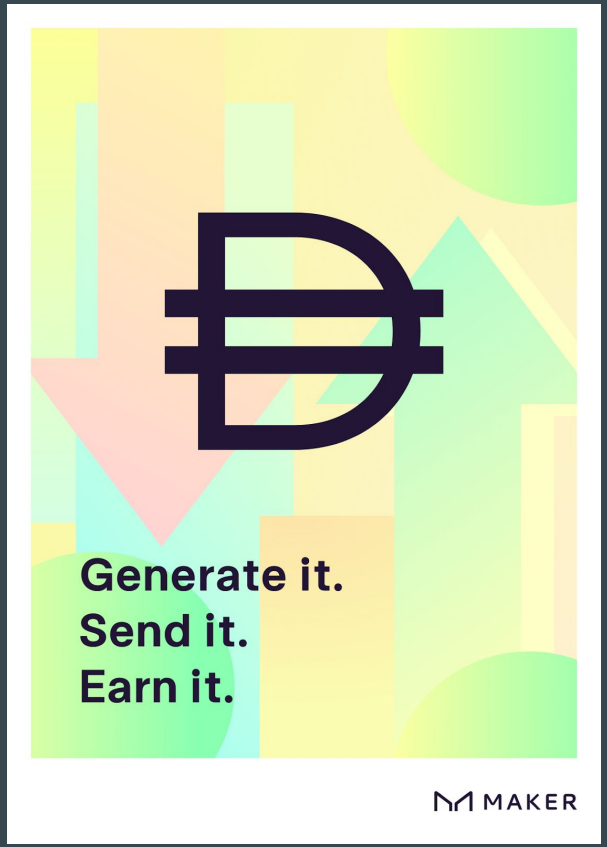
http://erc721.org/

Decentralized Finance

- MakerDAO built whole ecosystem
- Main product: DAI
  - decentralized
  - stable (dollar peg)
  - transparent

DAI to this day is invaluable to people living in inflation-plagued economies.

It also enabled a huge portion of what DeFi is today.



https://www.youtube.com/watch?v=ZEPx-iS7sz8

Decentralized Finance Cont.

- Aave: decentralized lending protocol
- Generates interest to those who provide liquidity
- Notorious for the invention of flashloans
- Instant, uncollateralized funds

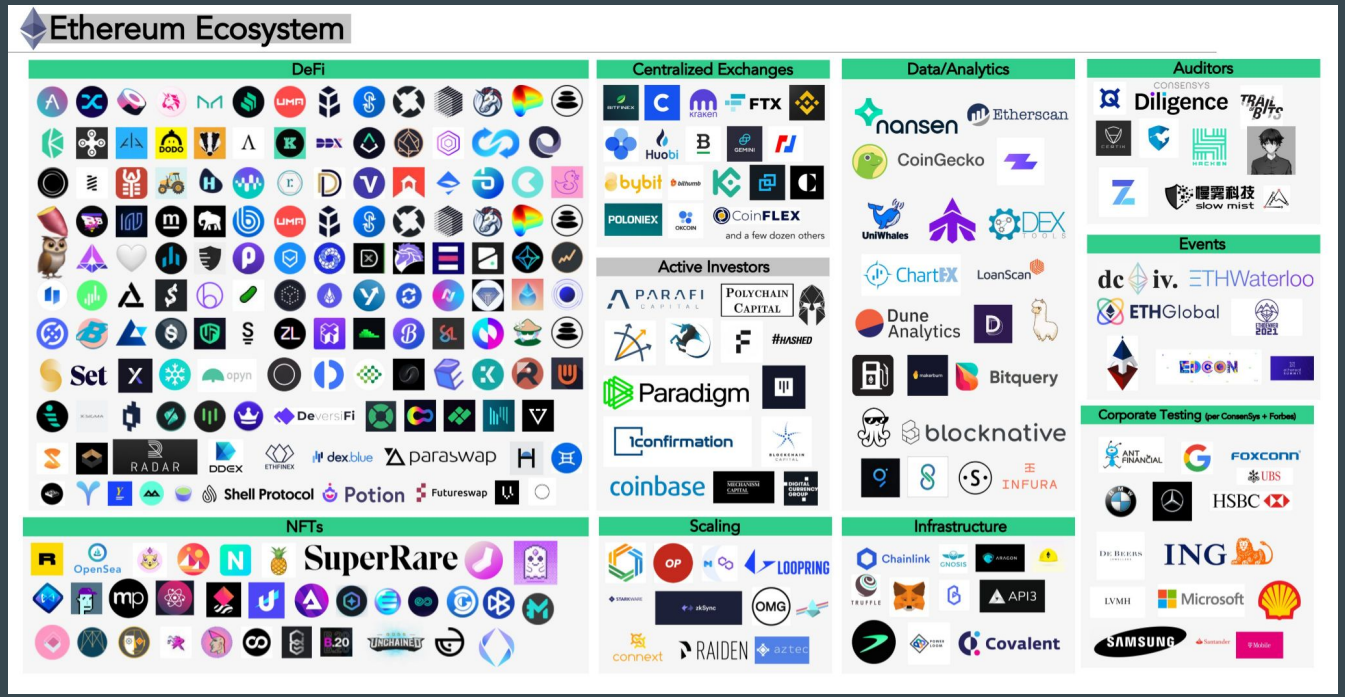
Flashloans have no equivalent in the traditional financial market.

it's also great for hacks

https://aave.com/

What is being built right now?

No one has an overview anymore. But people try.



https://consensys.net/blog/news/90-ethereum-apps-you-can-use-right-now/

https://www.reddit.com/r/ethereum/comments/m9sggj/ethereum_ecosystem/

Ethereum 2.0

- Significantly more:
  - Sustainable (PoS)
  - Scalable (Sharding/Rollups)
- Incredibly complex
- Much research still to be done

Check out ethresear.ch

For security fans: bounty.ethereum.org

Gitcoin

- Almost $20M funding to OSS
- Over 160k developers
- Do open-source work, get paid for it!
- DAO to distribute grants
- Quests to learn and get rewarded

https://gitcoin.co/

How do I join in on the action?

- Follow the news
- Ask about how things work
- Engage with people on Twitter
- Learn with friends and make friends learning
- Almost everything is open-source: Play around!

More officially: ConsenSys Academy

https://consensys.net/blog/developers/introducing-basic-training-a-free-consensys-academy-course-for-software-engineering-fundamentals/

Thanks for listening!

Hit me up on Twitter or Telegram: @lethalspoons