

Taking a Stroll through Ethereum



More than just NFTs

\$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. Kechak256

“hello” => 1c8aff950685c2ed4bc3...

“hello “ => 40000f84265ae2330b1336cd8fce...

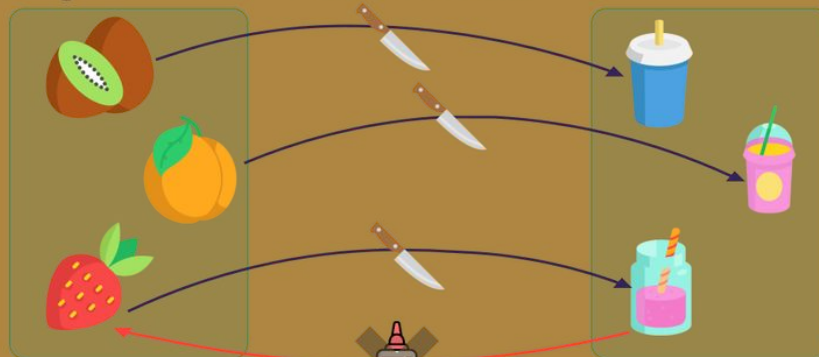
- certain properties needed:

- deterministic
- pre-image resistant
- correlation-resistant
- collision-resistant
- fast

Hashing

A hash function takes any input, and produces a fixed-length output (hash)

Ingredients Hash Function Smoothies



Deterministic

The same ingredients always yield the same smoothie

Pre-Image Resistance

You can't glue together a strawberry when given a smoothie

Collision Resistance

It's hard to find different ingredients for a smoothie that result in the exact same one

Correlation Resistance

Changing the ingredients a little results in a completely different smoothie

Speed & Verifiability

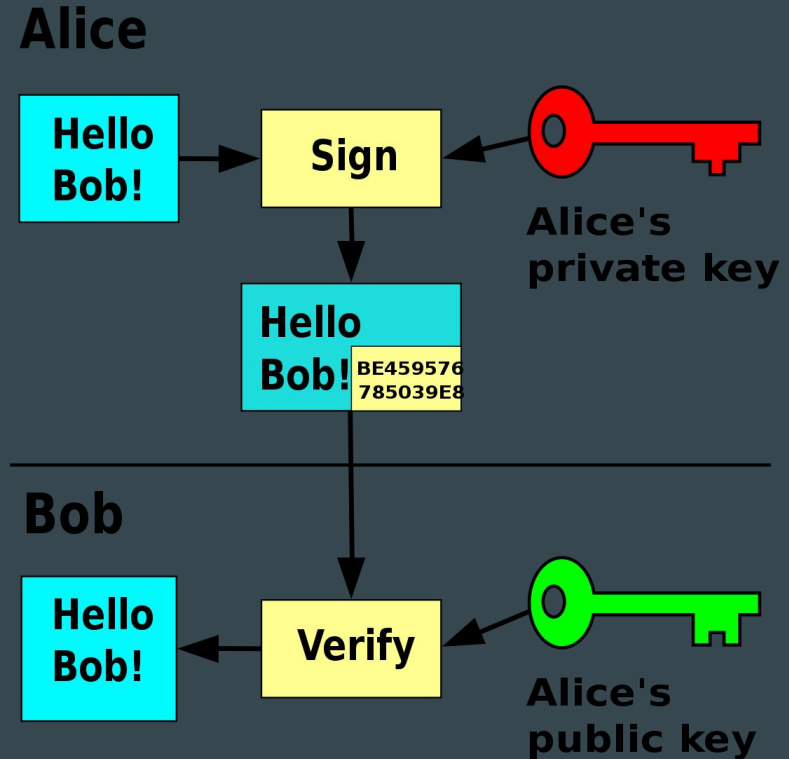
Throw fruit into the mixer. It's fast and what comes out for sure is a smoothie

Dominik Muhs

Images from FreePik and Smashicons at flaticon.com

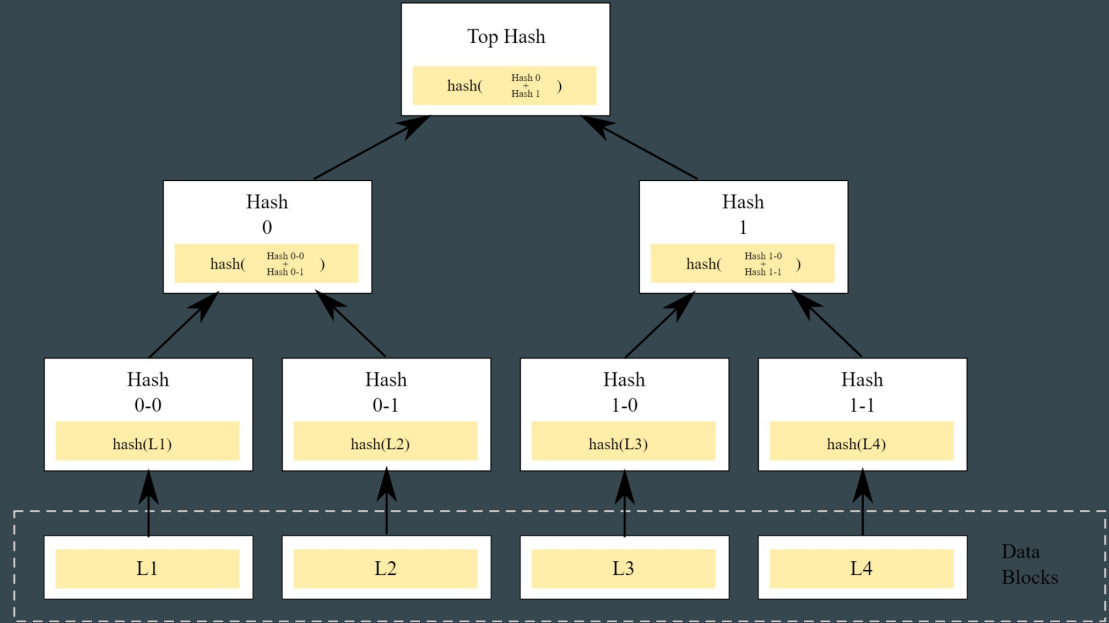
Public Key Cryptography

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



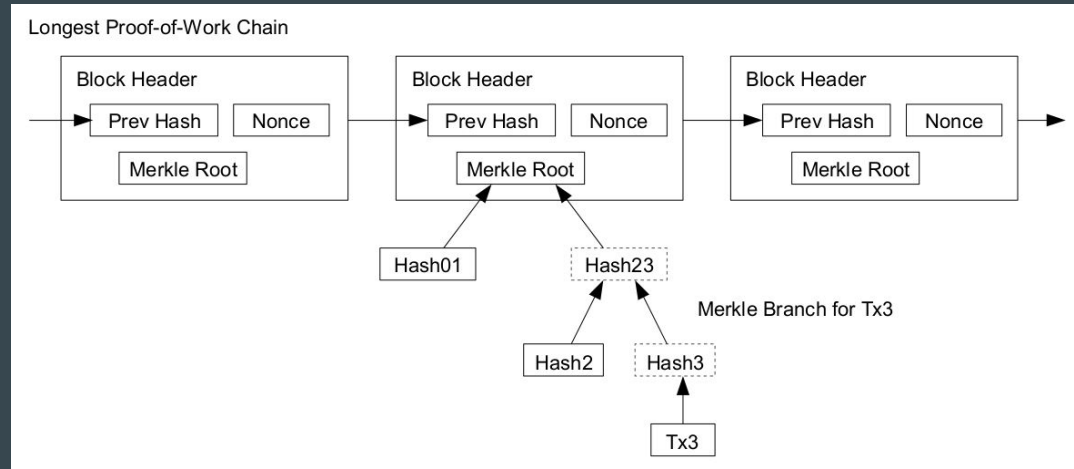
Merkle Trees

- 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



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

```
6080604052604051620021b9380380620021b9833981810160405260c081101562
00002957600080fd5b810190808051604051939291908464010000000082111562
00004a57600080fd5b838201915060208201858111156200006157600080fd5b82
518660018202830111640100000000821117156200007f57600080fd5b80835260
20830192505050908051906020019080838360005b83811015620000b557808201
518184015260208101905062000098565b50505050905090810190601f16801562
0000e35780820380516001836020036101000a031916815260200191505b506040
52602001805160405193929190846401000000008211156200010757600080fd5b
838201915060208201858111156200011e57600080fd5b82518660018202830111
640100000000821117156200013c57600080fd5b80835260208301925050509080
51906020019080838360005b838110156200017257808201518184015260208101
905062000155565b50505050905090810190601f168015620001a0578082038051
6001836020036101000a031916815260200191505b506040526020018051906020
019092919080519060200190929190805190602001909291908051906020019092
9190505050620001e3336200029660201b60201c565b8560049080519060200190
620001fb9291906200070e565b5084600590805190602001906200021492919062
00070e565b5083600660006101000a81548160ff021916908360fff160217905550
620002428184620002f760201b60201c565b8173fffffffffffffffffffffffffff
ffffffffffffffff166108fc349081150290604051600060405180830381858888f1
935050505015801562000289573d6000803e3d6000fd5b50505050505050620007
bd565b620002b1816003620004c160201b620016db1790919060201c565b8073ff
ffffffffffffffffffffffffffffffffffffffff167f6ae172837ea30b801fbfcdd4
108aa1d5bf8ff775444fd70256b44e6bf3dfc3f660405160405180910390a25056
5b600073ffffffffffffffffffffffffffffffffffffffff168273fffffffffffff
ffffffffffffffffffffffff1614156200039b576040517f08c379a0000000
0000000000000000000000000000000000000000000000000000000000000000
```

Meet Solidity

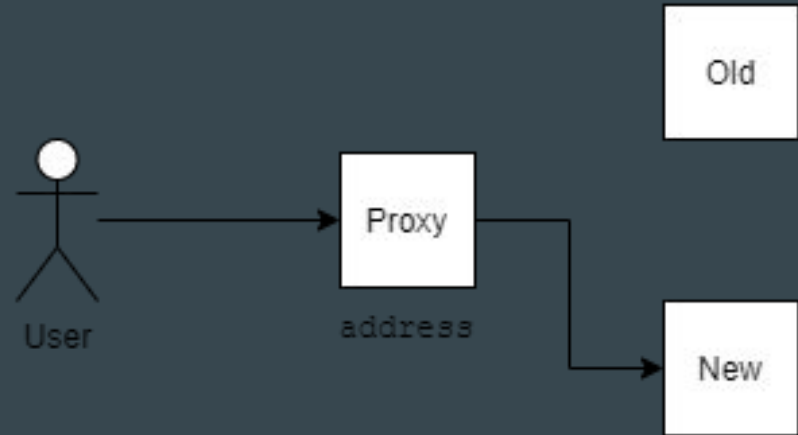
- Inspired by JavaScript
- Compiled, statically typed
- A bit wacky in some places

Go have fun: remix.ethereum.org

```
1 // SPDX-License-Identifier: GPL-3.0
2
3 pragma solidity >=0.7.0 <0.9.0;
4
5 /**
6  * @title Storage
7  * @dev Store & retrieve value in a variable
8  */
9 contract Storage {
10
11     uint256 number;
12
13     /**
14      * @dev Store value in variable
15      * @param num value to store
16      */
17     function store(uint256 num) public {
18         number = num;
19     }
20
21     /**
22      * @dev Return value
23      * @return value of 'number'
24      */
25     function retrieve() public view returns (uint256){
26         return number;
27     }
28 }
29
30
```

Security Aspects of Smart Contracts

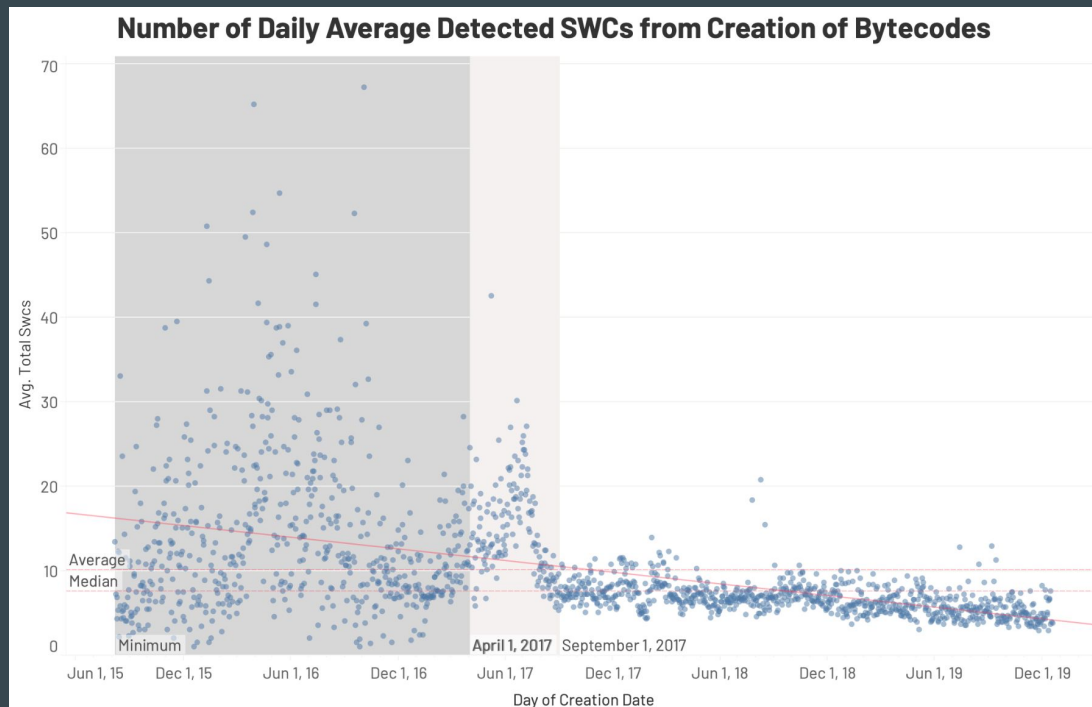
- Immutability can be problematic
- Upgradeability as well
- QA and audits are a must-have
- Formal verification very popular as well



Security in Ethereum

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

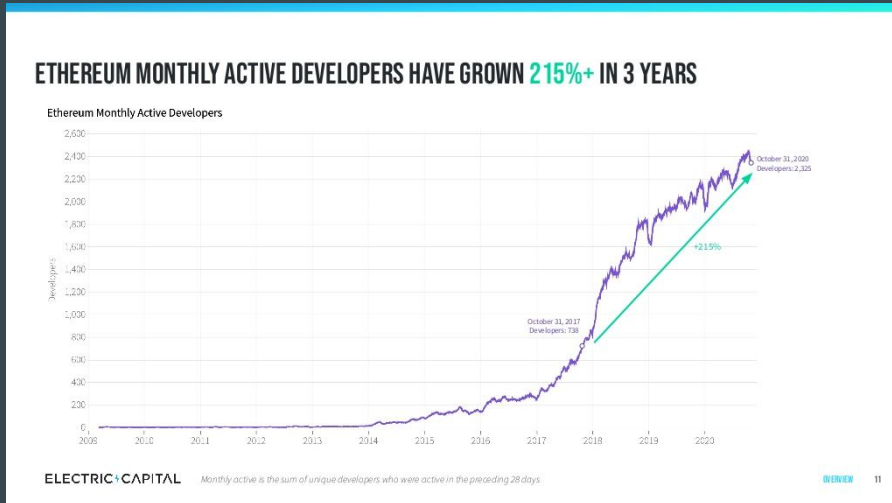
Based on SWC registry: swcregistry.io



What has been built so far?

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

Let's check out some history



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)
```


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)

BBC Sign in Home News Sport Reel Worklife Travel

NEWS

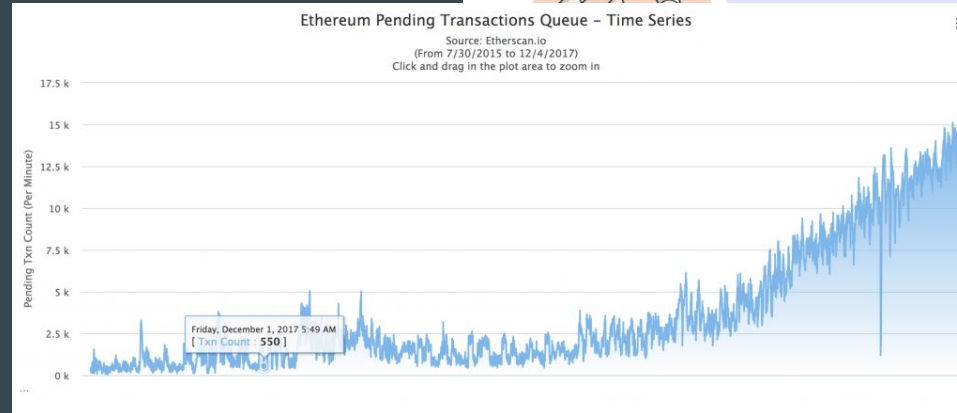
Home Coronavirus Video World UK Business Tech Science Stories Entertainment & Arts Health

Tech

CryptoKitties craze slows down transactions on Ethereum

5 December 2017

WWW.CRYPTOKITTIES.CO



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)

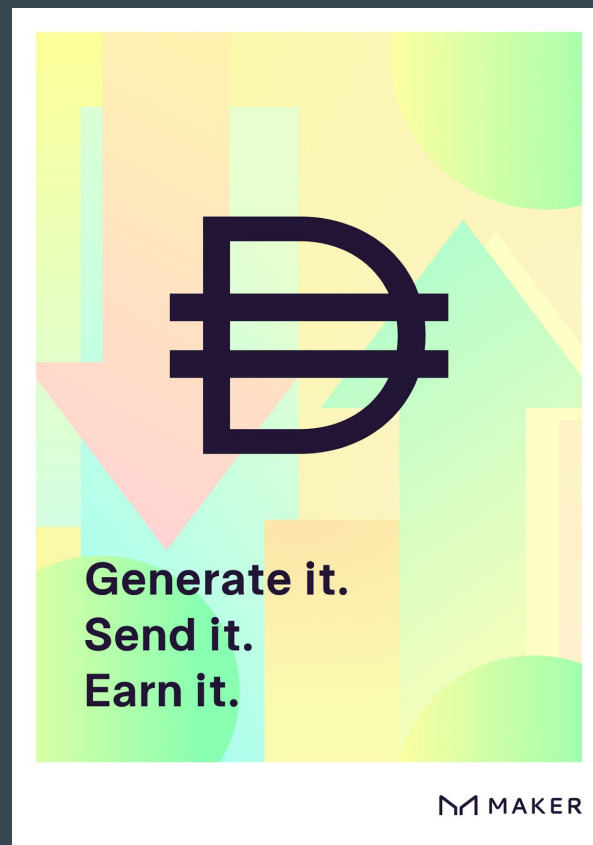
ApprovalForAll(owner, operator, approved)

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.



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



What is being built right now?

No one has an overview anymore. But people try.

Ethereum Ecosystem

The image displays a grid of logos categorized into several sectors of the Ethereum ecosystem:

- DeFi:** A large collection of logos for decentralized finance applications, including Aave, Compound, MakerDAO, and many others.
- Centralized Exchanges:** Logos for major exchanges such as Huobi, Bybit, and Coinbase.
- Data/Analytics:** Logos for data analysis and monitoring services like Nansen, Etherscan, and CoinGecko.
- Auditors:** Logos for security auditing firms such as Diligence and TRiBITS.
- Events:** Logos for community and industry events like ETHGlobal and ETHWaterloo.
- Corporate Testing:** Logos for companies that have been tested by Consensys and Forbes, including Ant Financial, Foxconn, and UBS.
- NFTs:** Logos for NFT marketplaces and projects, including OpenSea and SuperRare.
- Scaling:** Logos for scaling solutions like Loopring and Raiden.
- Infrastructure:** Logos for infrastructure providers such as Chainlink, Infura, and Covalent.

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



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



Thanks for listening!

Hit me up on Twitter or Telegram: [@lethalspoons](#)