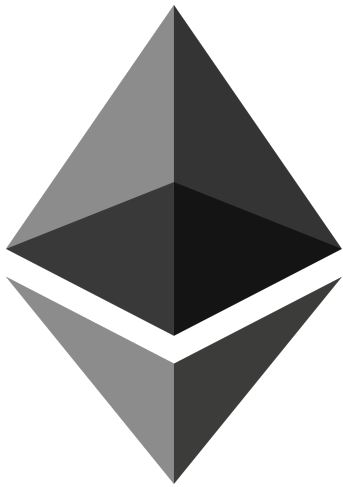




Ethereum and Smart contracts

Module 2 (part 1)

"On the Blockchain, no one knows you're a fridge"

Richard Brown

Part 1

- Much of what we've discussed so far has been primarily based on *Bitcoin* because it was the **first well-known blockchain** and a great introduction to the topic because of its foundational *character* in the industry.

Ethereum Blockchain

<https://www.ethereum.org/>

About Ethereum

Crowdfunded ~\$20M in ~ a month
Popularized a grand vision of
“generalized” cryptocurrency

[\[Ethereum Whitepaper\]](#)



The Constantinople 'Network Upgrade' is scheduled to take place at Block #7280000 in (~33 d



MARKET CAP OF \$12.195 BILLION

\$116.68 @ 0.03278 BTC/ETH ▼ 1.36%

LAST BLOCK

7105975 (16.8s)

TRANSACTIONS

380.05 M (5.7 TPS)

Hash Rate

177,117.11 GH/s

Network Difficulty

2,840.02 TH

<https://etherscan.io/>

Ethereum

A decentralized platform designed to run smart contracts

- The Ethereum platform is similar to a **world computer** that executes code and maintains the state of all smart contracts
- The latest block stores the latest local states of all smart contracts
- Transactions result in executing code (calling a function) in target smart contracts
- Transaction change the state of one more contracts
- Ethereum smart contracts are Turing-complete

Bitcoin vs. Ethereum

Bitcoin

Bob owns private keys to a set of unspent transactions

5 BTC => Bob

2 BTC => Bob

3 BTC => Bob

Easy to make transactions and prevent double-spending attacks

Ethereum

Bob owns private keys to an account

Address: 0xfa34...

Balance: 10 ETH

Code: `f() {c := a + b}`

Has executable code

Update balance instead of storing unspent transactions

Ordinary contracts between two parties

- Civil courts are available to mediate, but typically don't get involved
- Parties responsible for their own accounting:
 - “Double entry accounting”

Third-party services

E.g., Paypal, Kickstarter, ...Piazza?

- Transactions are automatically processed by the third party
- Formal intermediary to finance network (help with taxes)
- Settles disputes through mediation

Smart Contract dApps “decentralized apps”

- Transactions typically go through the blockchain
- App developers do not receive custody of funds
- Developers limited in ability to change the rules
- Settles automatically via cryptocurrency
- Auditing may be simplified by public transparent log

What is ETH?

- ETH is Ethereum's native currency. It is "digital money" that can be sent over the internet instantly and cheaply, and also be used in many Ethereum-based applications

Potential Ethereum Applications

<https://github.com/ethereum/wiki/wiki/White-Paper#applications>

- Tokens
- Lotteries
- Cryptocurrency exchanges
- Marketplaces
- Insurance / hedging
- Supply-chain management
- “Self-sovereign” identity management
- Sharing economy

And many more!

Two types of client applications

- There are generally two essential types of client applications to meaningfully interact with any blockchain including Ethereum Blockchain: **wallets** and **full nodes**

Ethereum wallets

- Ethereum has several wallets:
 - [MetaMask](#) (browser-based, and the one we will use in this class)...



[What is a wallet, and which one should I use?](#)

Full node Ethereum clients

- A full node is required for **mining** purposes.



[Running an Ethereum Node](#)

Ethereum accounts



Externally owner accounts

- Owned by some external entity (person, corporation, ...)
- Can send transactions to transfer ether or trigger contractcode
- Contains:
 - Address
 - Ether balance

Controlled by public-private key pairs
(i.e. humans)



Contract accounts

- “Owned” by contract
- Code execution triggered by transactions or function calls
- Contains:
 - Address
 - Ether balance
 - Associated contract code
 - Persistent storage

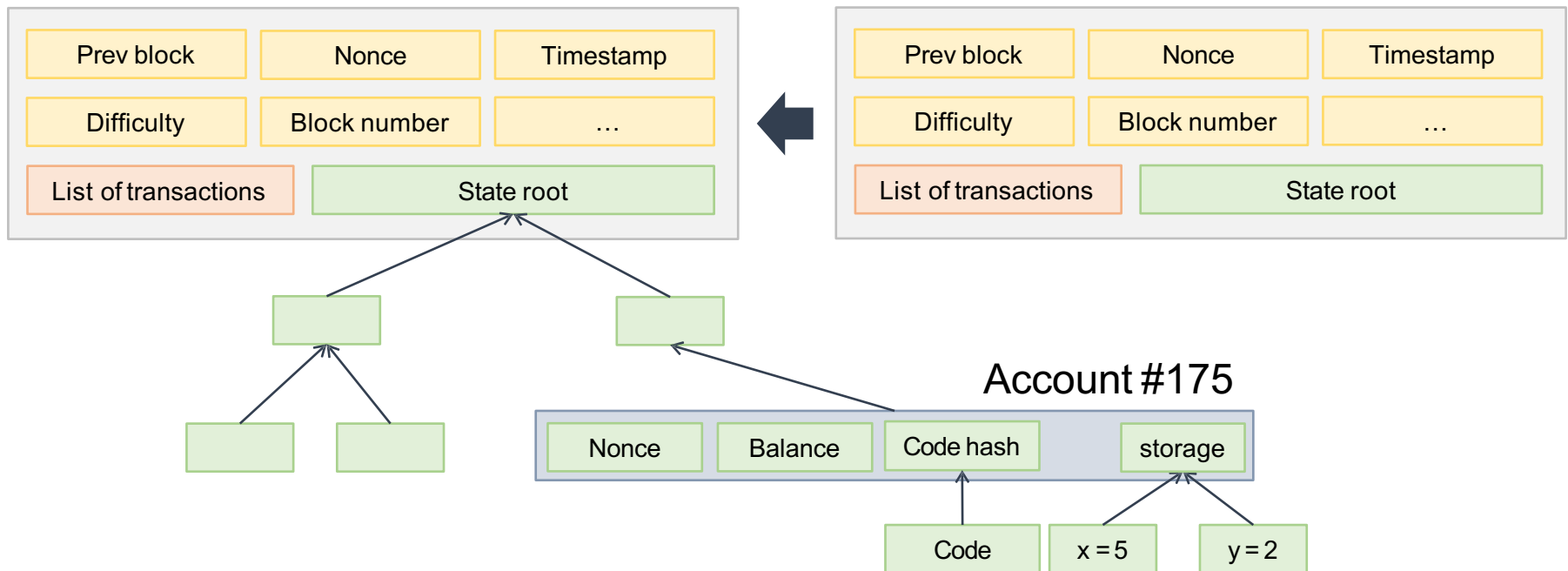
controlled by the code
stored together with the account.

Differences between accounts

- The address of an **external account** is determined from the public key while the **address of a contract** is determined at the time the contract is created (it is derived from the creator address and the number of transactions sent from that address, the so-called “nonce”).
→ Regardless of whether or not the account stores code, the two types are treated equally by the EVM.

Ethereum blocks

More complex than Bitcoin...



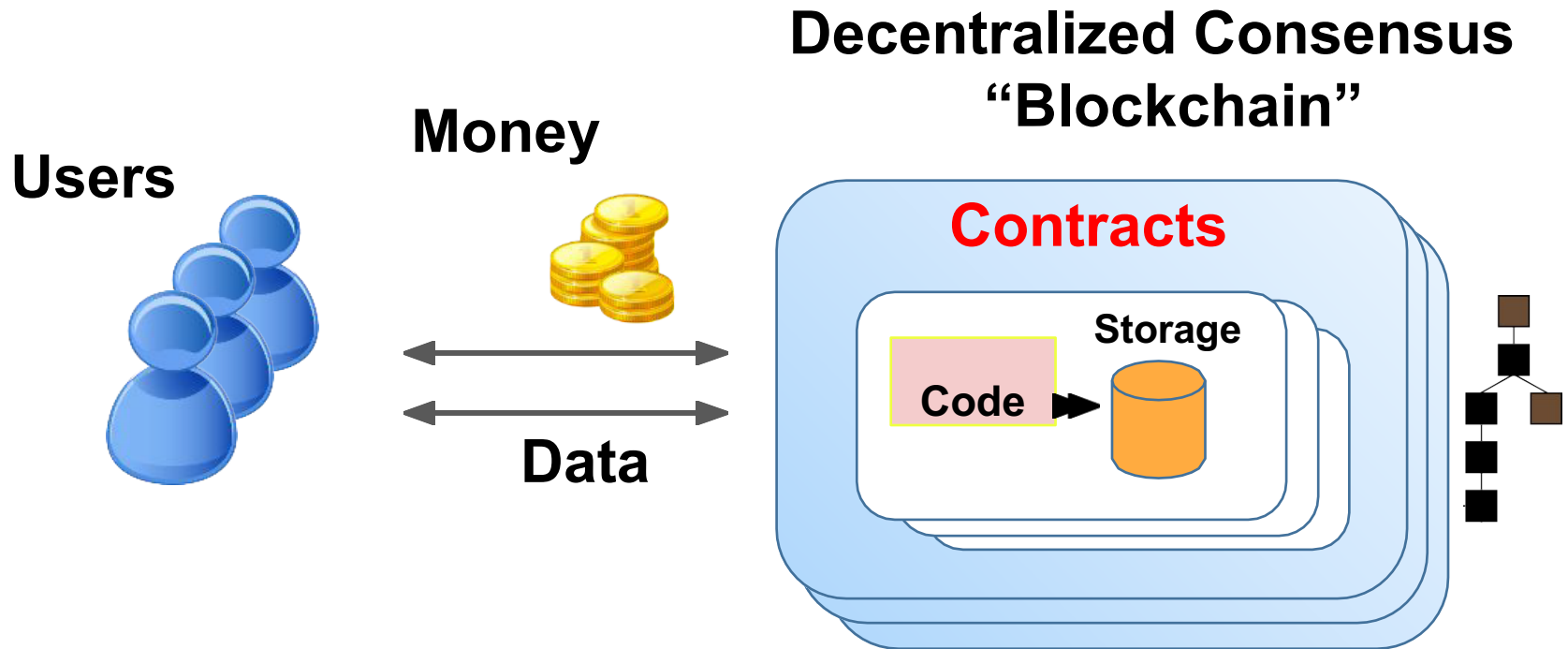
Browse the Ethereum blockchain: <https://etherscan.io/blocks>

Smart Contracts

What is a smart contract?

- Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

Smart Contracts: user-defined programs running on top of a blockchain



KICK STARTER



SUPPORTERS



PRODUCT TEAM

SUPPORTERS

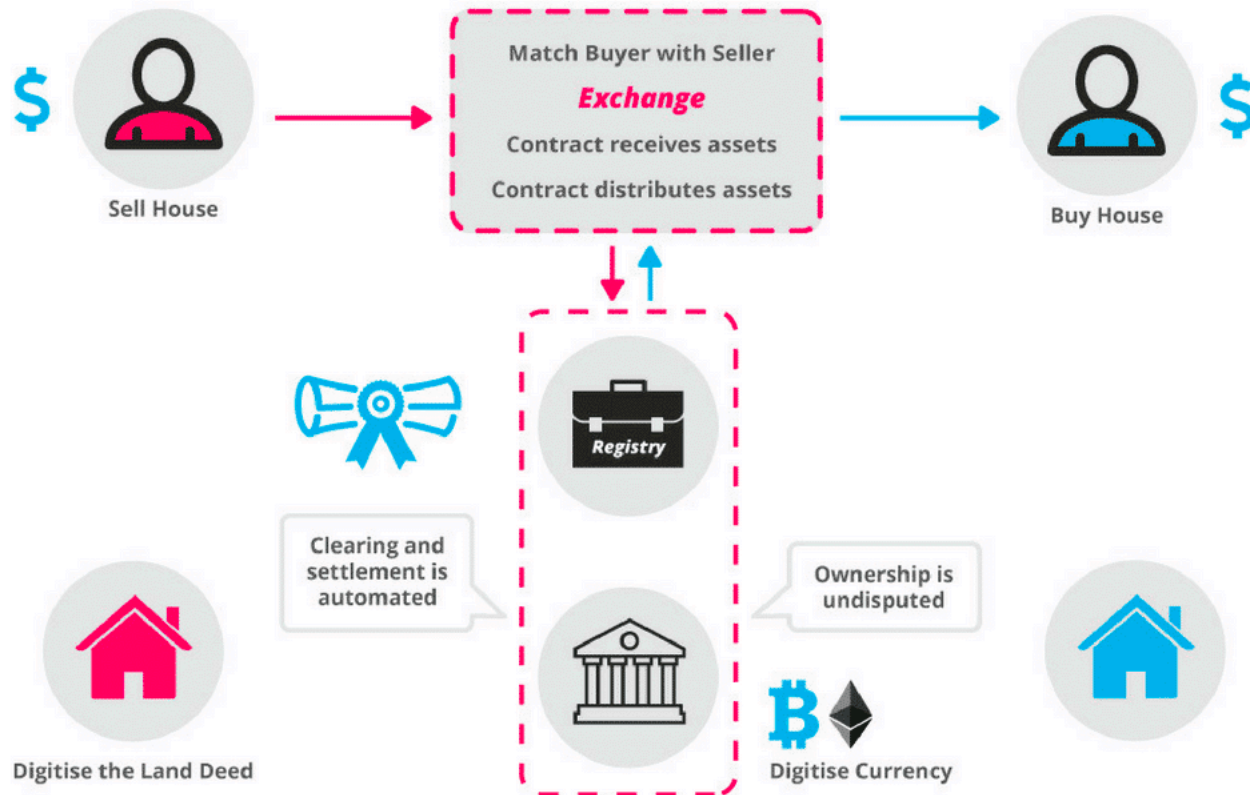


PRODUCT TEAM



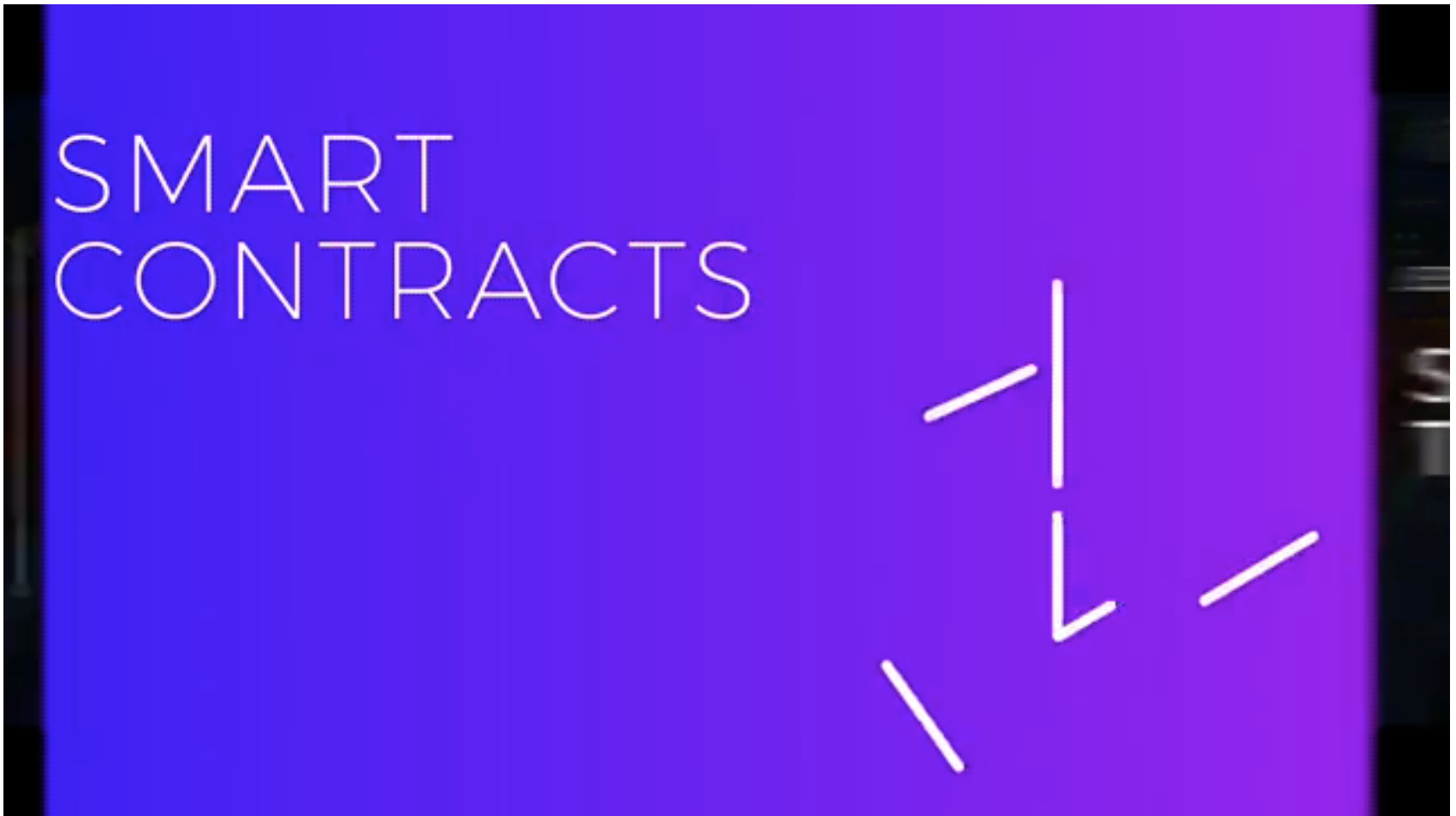
Why trust a Smart Contract?

How Smart Contracts Works



Smart contracts and EVM

[Source from ConsenSys]



The idea of smart contracts

A smart contract is a **computerized transaction** protocol that executes the **terms of a contract**. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and **minimize the need for trusted intermediaries**. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

-Nick Szabo “The Idea of Smart Contracts”

A smart contract formalizes the terms of a contract in code

Smart Contract Example (very high level)

If GOOG rises to \$1,000 by
30 June 2015, assign 10
shares from Alice to Bob and
pay Alice \$10,000

Other examples abound:

Auctions, elections, lotteries, escrow, ...

Traditional vs smart contracts

	Traditional	Smart
Specification	Natural language	Code
Identity & consent	Signatures	Digital signatures
Dispute resolution	Judges, arbitrators	Decentralized platform
Nullification	By judges	????
Payment	As specified	built-in
Escrow	Trusted third party	built-in

Does Bitcoin support smart contracts?

Bitcoin features a simple scripting language

Example

OP_DUP OP_HASH160 69e...3d42e OP_EQUALVERIFY OP_CHECKSIG

256 instructions

- Arithmetic
- Logic/data handling
- Cryptographic operations

Restrictions

- No loops
- Not Turing-complete



Are you bored?

Learn to Code Ethereum DApps By Building Your Own Game

CryptoZombies is an interactive code school that teaches you to write smart contracts in Solidity through building your own crypto-collectables game.

Get Started, It's Free

Learn More

CRYPTOZOMBIES

<https://cryptozombies.io/>



SPACE DOGGOS

Learn Solidity by creating your own game!

START NOW



<https://www.bitdegree.org/courses/learn-solidity-space-doggos/>