Ethereum

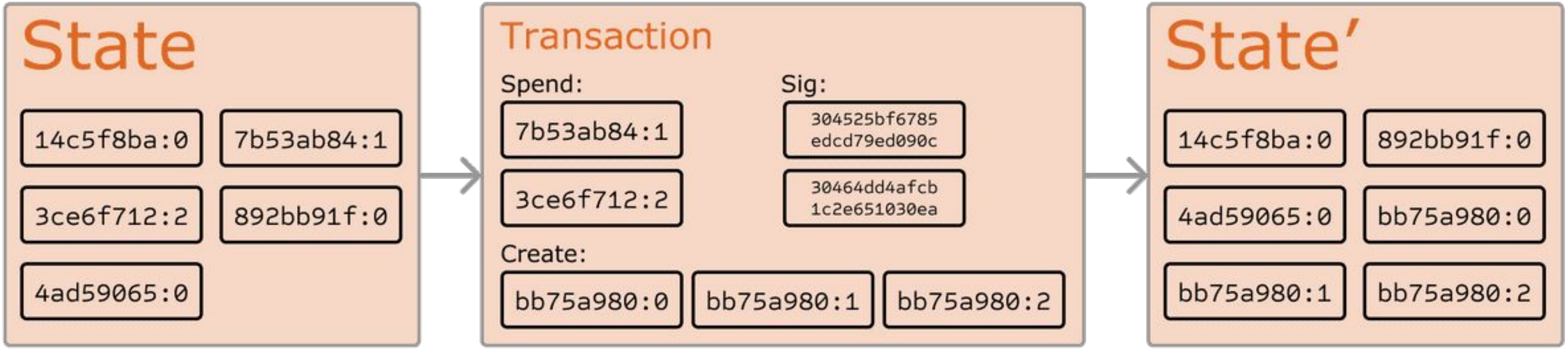
Created by: Vitalik Buterin
Presentation by: Wesley Tsai

History

Bitcoin

- Introduced by Satoshi Nakamoto in 2009
- The first decentralized currency system that actually WORKS
    - Nodes have consensus on the Blockchain
    - Impossible to hack: Attacker would need more power than 51% of nodes
        - Better to just play the game than to cheat
- Introduced the concept of “Blockchain”
    - Proof of work
    - State transition system
    - Mining by “guessing” the hash of the next block
    - A block is stored as a multi-level data structure (Merkle Tree)

Bitcoin as a State Transition System



State

14c5f8ba:0
7b53ab84:1
3ce6f712:2
892bb91f:0
4ad59065:0

Transaction

Spend:
7b53ab84:1
3ce6f712:2

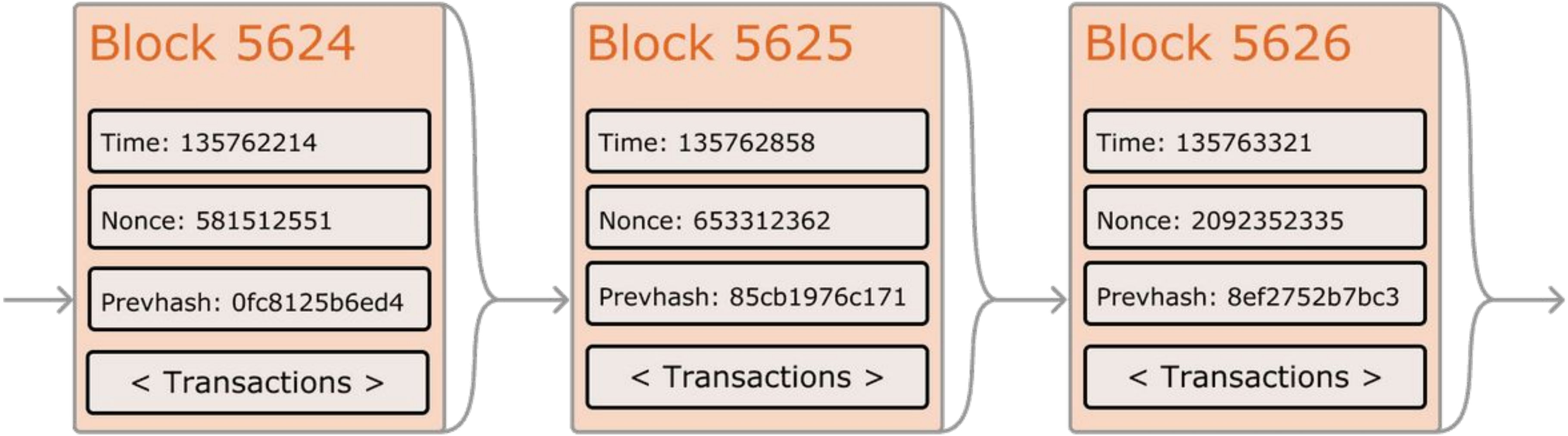
Sig:
304525bf6785
edcd79ed090c
30464dd4afcb
1c2e651030ea

Create:
bb75a980:0
bb75a980:1
bb75a980:2

State’

14c5f8ba:0
892bb91f:0
4ad59065:0
bb75a980:0
bb75a980:1
bb75a980:2

Blocking and Mining



Block 5624

Time: 135762214

Nonce: 581512551

Prevhash: 0fc8125b6ed4

< Transactions >

Block 5625

Time: 135762858

Nonce: 653312362

Prevhash: 85cb1976c171

< Transactions >

Block 5626

Time: 135763321

Nonce: 2092352335

Prevhash: 8ef2752b7bc3

< Transactions >

Alternatives Bitcoin Applications

- **Goal:** Take the blockchain concept and apply it to other concepts
- Namecoin
  - Name registration system
- Colored Coins
  - Other digital tokens on the Bitcoin blockchain
- Metacoin
  - Protocol on Bitcoin Blockchain
  - Use Bitcoin transaction to store transactions but have a different state transition function

Issue with these alternatives...

- Build an independent network (*NameCoin*)
  - Difficult to implement
  - Sometimes it's not even worth having its own Blockchain
- Build a protocol on Bitcoin (*Colored Coins / Metacoin)*
  - Doesn’t get the simplified payment feature of blockchain
  - Not Scalable
  - Need a trusted server for data, so not really centralized

Another Alternative: Scripting

- Bitcoin supports a weak version of the smart contract
- Scripts can own unspent transaction output
- Enables cross crypto-currency exchange

Scripting still has problems...

- Lack of Turing - Completeness
    - No loops allowed
- Value Blindness
    - No fine grained control on what can be withdrawn
- Lack of State
    - Only spent and unspent
- Blockchain blindness
    - No source of randomness, which means no gambling

Bitcoin

Applications on Bitcoin

???

18:01
MON
20
1
13,926
FaceTime
Calendar
Photos
Mail
Clock
Maps
Weather
Reminders
Notes
News
App Store
Podcasts
tv
TV
Settings
Google apps
Pocket Casts
1
1
Messages
Twitter
Instagram
Words 2
Todoist
Spotify
Citymapper
The Guardian

Enter Ethereum

Overview

- 2013: White Paper written by Vitalik Buterin (who was 19 at the time!)
- 2015: The project was launched
- Goals:
  - An alternative protocol for building decentralized applications (DApps)
  - A blockchain with a Turing-complete programming language
  - The be able to build smart contracts on top of the protocol
    - Namecoin can be written in 2 lines of code in Ethereum!

Ethereum Account

- Two types of accounts
  - Externally owned account (User) - controlled by keys
  - Contract account - controlled by code
- Account has four fields
  - Nonce
  - Ether balance
  - Contract code (If contract account)
  - Storage (mainly for contract account)
- Ether is the fuel that pays transaction fees

Transactions

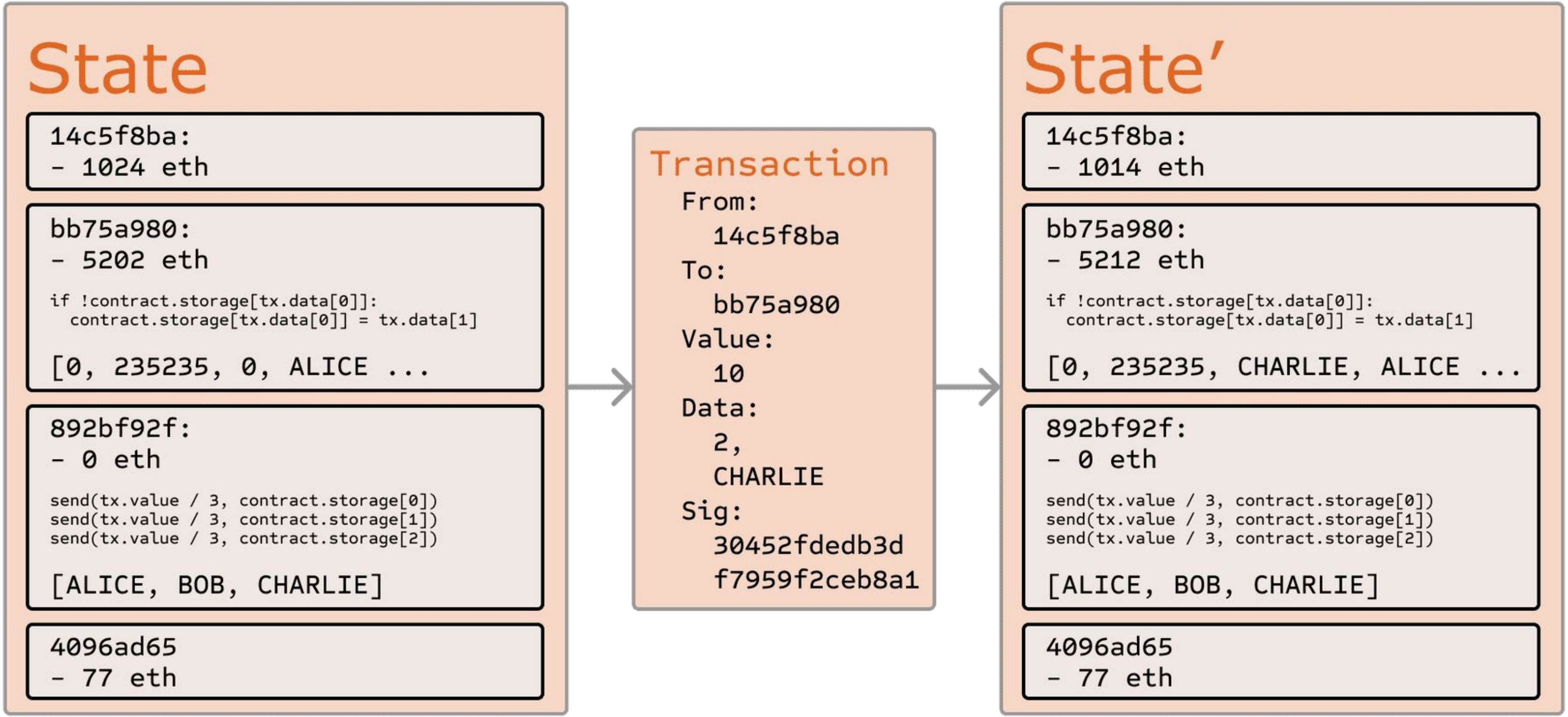
- Signed data pack that stores a message that was sent from an externally owned account
- Transactions contain
  - Recipient of message
  - Sender’s signature
  - Amount of ether to send
  - Maximum number of gas
  - Price of gas

Messages

- Sent between contract accounts
- Virtual objects that are not serialized and only exist in ethereum
- Message contains
  - Sender
  - Recipient
  - Amount of ether
  - Start gas
- Basically like a transaction, but made by a contract

Ethereum State Transition Function

1. Check for well written form, valid signature, and matching nonce.
2. Calculate the transaction fee and find the destination address. Subtract the fee and increment nonce for sender
3. Start the gas, and use some of it to pay for transaction
4. Transfer value from the sender's account to the receiving account
5. If the value transfer failed, revert all changes except the fee payment, which is added to miner’s account
6. Otherwise, refund remaining gas to the sender, and send the fees paid for gas consumed to the miner.



State

```
14c5f8ba:
- 1024 eth
```

```
bb75a980:
- 5202 eth

if !contract.storage[tx.data[0]]:
  contract.storage[tx.data[0]] = tx.data[1]

[0, 235235, 0, ALICE ...
```

```
892bf92f:
- 0 eth

send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])

[ALICE, BOB, CHARLIE]
```

```
4096ad65
- 77 eth
```

Transaction

```
From:
  14c5f8ba
To:
  bb75a980
Value:
  10
Data:
  2,
  CHARLIE
Sig:
  30452fdedb3d
  f7959f2ceb8a1
```

State’

```
14c5f8ba:
- 1014 eth
```

```
bb75a980:
- 5212 eth

if !contract.storage[tx.data[0]]:
  contract.storage[tx.data[0]] = tx.data[1]

[0, 235235, CHARLIE, ALICE ...
```

```
892bf92f:
- 0 eth

send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])

[ALICE, BOB, CHARLIE]
```

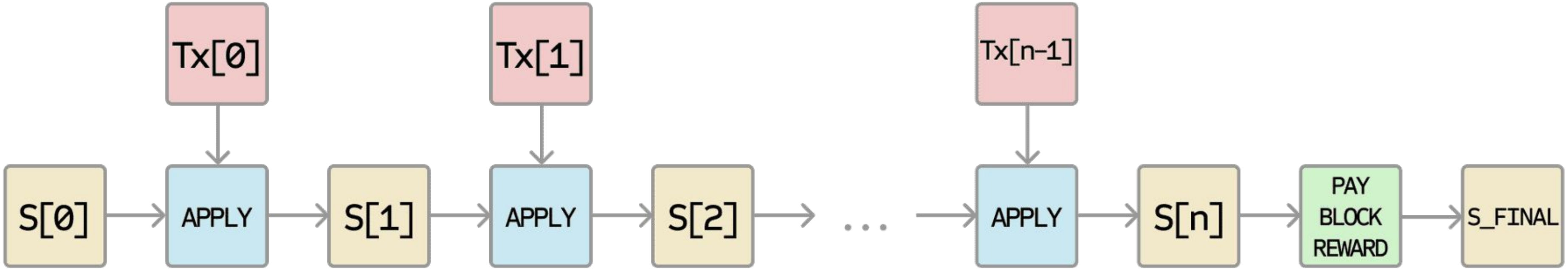
```
4096ad65
- 77 eth
```

Code Execution

- EVM (Ethereum Virtual Machine) Code
  - Low level, stack-based bytecode language
  - Can have infinite loops
- Three places to store data
  - Stack
  - Memory
  - Long term storage
- State: (block_state, transaction, message, code, memory, stack, pc, gas)

Blockchain and Mining

- Similar to Bitcoin’s Blockchain
  - Contains transaction list and most recent state
- Block Validation Algorithm
  - Check if previous block exists
  - Check if timestamp is correct
  - Check block number, difficulty, root, and gas limit
  - Check proof of work
  - Apply all transactions in transaction list
  - Add payment to the miner
- State can be stored Patricia tree
  - Like a merkle tree, but nodes can inserted/deleted efficiently


Tx[0]
Tx[1]
Tx[n-1]
S[0]
APPLY
S[1]
APPLY
S[2]
...
APPLY
S[n]
PAY BLOCK REWARD
S_FINAL

Smart Contracts

- CODE IS LAW
- Kind of like a real contract, but regulated by code instead of lawyers
- Users can create a decentralized application by defining it as a contract
    - People can write scripts using Solidity
- People pay Ether to run a Smart Contract on the Ethereum Supercomputer
- Why Smart Contracts?
    - Transparent: Anyone can look at its code and judge if it’s good or bad
    - Permissionless: Anyone can write as smart contract and deploy it
    - Immutable: Secured by blockchain so code can’t change
    - Distributed: Validated by all notes on network

If you give me 2 Ether,

I will give you 1 can of coke

Miscellaneous + Concerns

Modified Ghost Protocol

- Ethereum has a fast block time compared to Bitcoin
  - 15 seconds
- GHOST protocol was used to solve the issue of lowered security
  - Has the concepts of uncles (stale blocks)
  - Uncles are calculated as part of the total proof of work for a chain
- Ethereum expands on it by
  - Giving some rewards to stale blocks
  - Simplifying it to to 7 cycles

Gas + Fees

- Used to address infinite loops
- There is a need for regulatory mechanism (fees) to prevent use of Ethereum
- The concept of Gas was created for that
    - Code on the contract will only run until all the Gas runs out
    - Will revert back to original state if incomplete
- Gas incentivise people to write good contracts that don’t use up a lot of gas
    - Miners will choose to run contracts that won’t take that much gas
    - Also ethereum has a hard cap on how big a block can be

Currency and Issuance

- Ether is the main currency
  - To pay transaction fees
  - Exchange for different assets
- Can be divided into many little parts
  - 1 Ether = 10^18 wei
- Permanent linear supply growth model to reduce risk of wealth concentration
- Supply growth rate will tend to zero over time
- Coins will be lost due to death, carelessness and coin loss

Sustainability

- Mining algorithm of Ethereum: Fetch some random data from state, compute some random transactions on the last N blocks, return hash
    - Lessen the need for ASICs
    - An adaptive solution
- To deal with an ever growing blockchain size:
    - Every miner will forced to be a full node,
    - Include an intermediate state tree root in the blockchain after processing each transaction

Applications

DECENTRALIZATION
DECENTRALIZATION EVERYWHERE
memegenerator.net

Decentralized File Storage

- Similar to Dropbox, but decentralized
- Individual users can earn money by renting out unused space in their own hard drives
- Possible thanks to smart contracts
- Split the file into many pieces to be stored

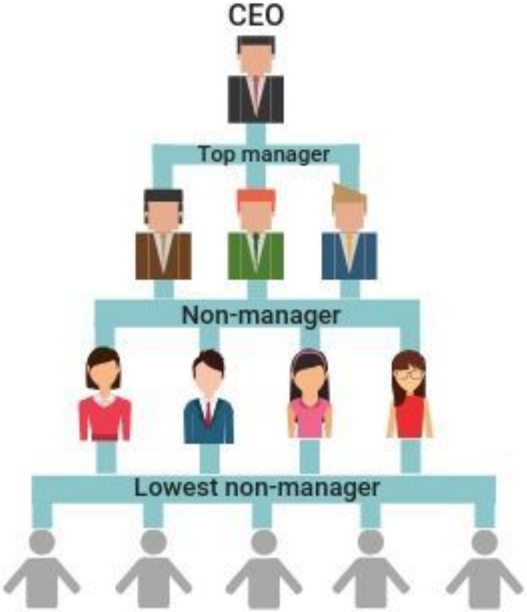
Decentralized Finance (DeFi)

- Collection of financial products on Ethereum
- No need to trust third parties to handle your money
    - YOU hold your money
    - YOU control where the money goes
- The future of banking?
    - Market is open to anyone
    - Transparency
    - Transfers happens in minutes
- Ethereum is a great foundation for DeFi
- Smart Contracts enable borrowing, funding, insurance, and portfolio managers

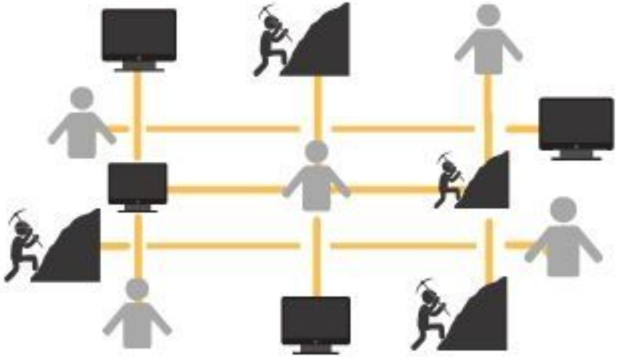
Decentralized Autonomous Organization (DAO)

- An effective and safe way to interact with like-minded people
- Fully democratic: Just trust the DAO’s code
  - Changes to code determined by a vote
- Smart Contract makes the backbone for the trust
  - Also acts as a treasury
- Service handled automatically in a decentralized manner
- Use Cases
  - Charities
  - Freelance Network
- Membership
  - Token based or share based

Traditional centralized system

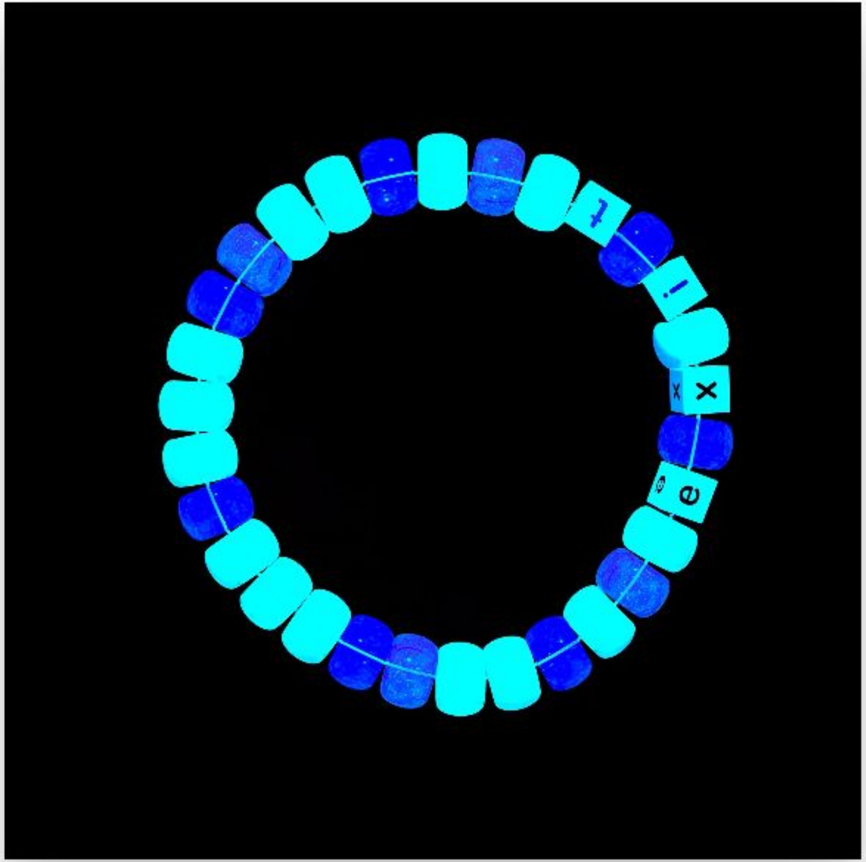


Decentralized Autonomous Organization



Non Fungible Token (NFT)

- Represent ownership of unique DIGITAL assets
- Only one official owner of a given NFT
    - Secured by the blockchain
    - Easy to prove ownership
    - Minted by smart contracts
- Not Interchangeable (aka Fungible)
- Digital creators can now have ownership of their work
- Digital work can also get auctioned
    - You can get the “original copy”



@LaTurbo

~*~ exit ~*~

Current Bid

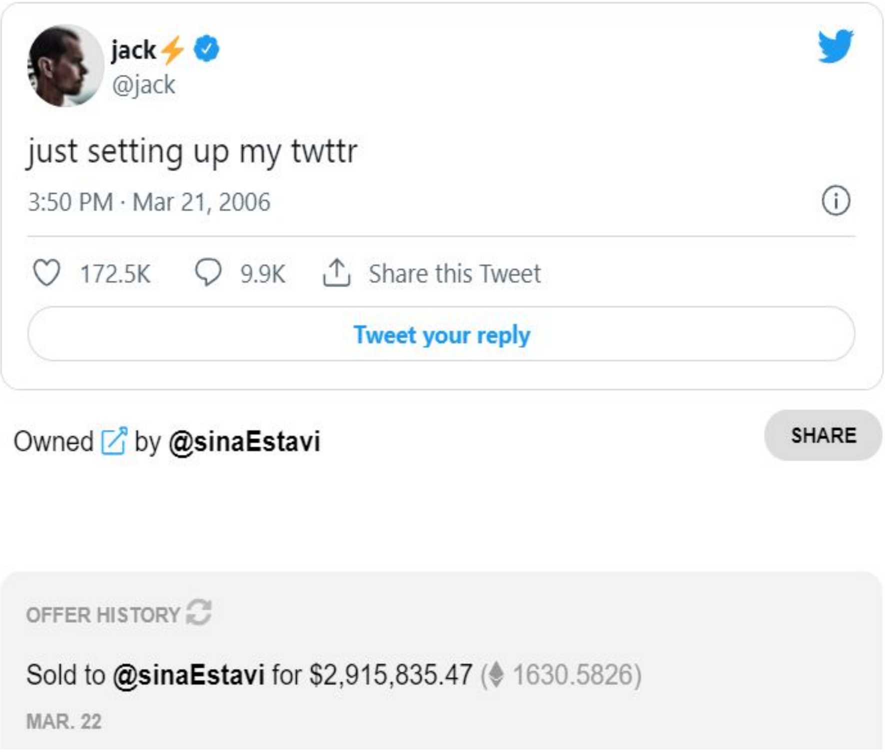
0.45 ETH

$2,013.95

Auction ending in

9	14	58
Hours	Minutes	Seconds

View artwork



jack⚡
@jack

just setting up my twttr

3:50 PM · Mar 21, 2006

♡ 172.5K 9.9K Share this Tweet

Tweet your reply

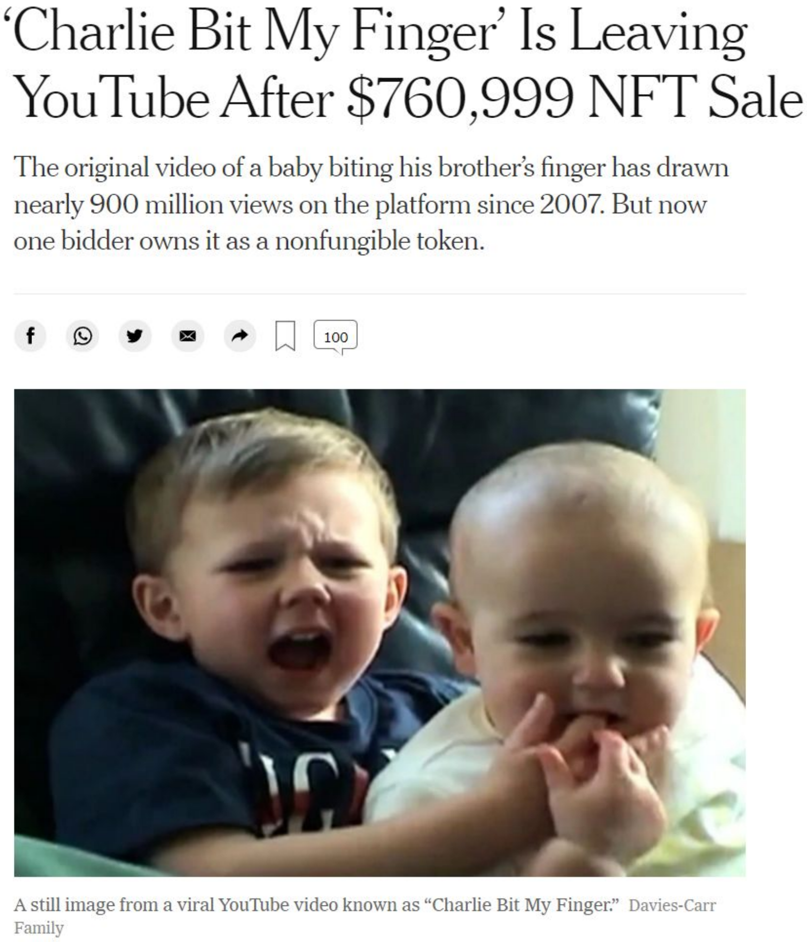
Owned by **@sinaEstavi**

SHARE

OFFER HISTORY

Sold to **@sinaEstavi** for $2,915,835.47 (1630.5826)

MAR. 22



‘Charlie Bit My Finger’ Is Leaving YouTube After $760,999 NFT Sale

The original video of a baby biting his brother’s finger has drawn nearly 900 million views on the platform since 2007. But now one bidder owns it as a nonfungible token.

100

A still image from a viral YouTube video known as “Charlie Bit My Finger.” Davies-Carr Family

Future for Gaming???

© 2021 Riot Games, Lnc.

Endless Possibilities...

- Crop insurance
- Cloud computing
- Peer to Peer gambling
- Prediction markets
- Data Feeds
- Lotteries

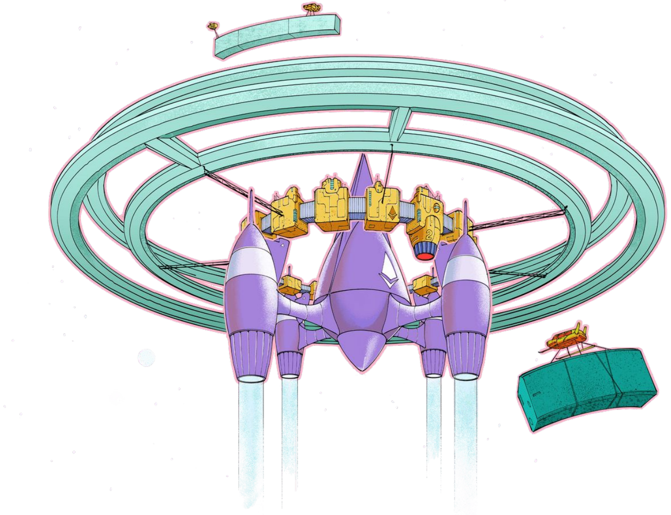
Ethereum Now

Ethereum Classic

- In 2016, “The DAO” was attacked
- 150 Million dollars lost!
- Ethereum Community decided to do a hard fork
    - Code is not law anymore
- Some Miners didn’t agree with the fork
- Thus, “Ethereum Classic” was created as the old fork

Ethereum 2.0?

- Started in 2020, will fully merge with Ethereum 1.0 in 2022
- Proof of Stake
    - Users stake their ETH to become validators
    - Validators selected at random to choose blocks
    - Much more eco-friendly
    - Encourages more participation
- The Beacon Chain
- Expected to merge with Ethereum 1.0 in 2022



Controversy

- Ethereum’s price is extremely volatile (as with other cryptocurrencies)
- Gas Fees are on the high end
- NFT’s are controversial as people debate its value
- Still requires a lot of energy for proof of work

Ethereum price (ETH / USD)
$4
D 1W 1
JAN
FEB 2017
MAR 2018
APR 2019
JUN 2020
JUL 2021
Stonks
Much profit
many gains
Buy low, sell high
imgflip.com

TO THE MOON!!!!!

Key Takeaways

1. Ethereum was proposed to take Blockchain Technology to the NEXT level
    a. Turing Complete Language
    b. Smart Contracts
    c. Ethereum Virtual Machine
2. The main goal of Ethereum is to provide a foundation for decentralized applications through smart contracts and blockchain tech
    a. DeFi
    b. DAO
    c. NFT
3. Ethereum is still growing, and in order for it to succeed, it needs to have support from the people
    a. Ethereum 2.0 in the future
    b. The rise of Ether's price indicates that Ethereum is growing in popularity
    c. Cryptocurrency is in a bull market, which means a lot of fluctuation

Thank you!