Digital Currencies

Jack & Sam

Digital Currencies

- An “Internet-based medium of exchange”
- No need for a physical representation
- Allow for untraceable* and **borderless** transactions
- Digital Currencies can fall into several categories, including:
  - Virtual Currencies
  - Cryptocurrencies

Bitcoin

- Bitcoin was the first decentralized digital currency
  - Classic example of a cryptocurrency
  - Transactions secured and **verified** using cryptography*
- Invented by an unidentified group known as Satoshi Nakamoto
  - Introduced originally in October, 2008, released in 2009
  - Original paper can be found https://bitcoin.org/bitcoin.pdf
- Currency based entirely on its own ledger
  - A cryptographically secured history of transactions as a **blockchain**

Bitcoin - The Blockchain

- A distributed database recording **every** bitcoin transaction ever made
    - Consists of blocks, with timestamps and a link to a **previous** block
    - Think linked-list
- The Blockchain is the core of Bitcoin
    - The Blockchain is constantly **verified** and
    - **extended** with a process called **mining**

Bitcoin - Mining

- New blocks added to the Blockchain must contain a **proof-of-work**
  - Miners must find a “nonce”, a number such that when the block is hashed with the nonce, the result is smaller than the network’s difficulty target (using SHA-256)
  - The bitcoin network updates its difficulty target roughly once every 2 weeks to keep the time between Bitcoin creation roughly 10 minutes
- The proofs are easy to verify, but hard to produce
  - In March 2015, the number of nonces miners had to attempt before succeeding in generating a valid hash was about **200.5 quintillion per block**

Bitcoin - Mining Pools

- Seeing as the amount of work to mine a single block is unfeasibly high for a single person, mining pools formed
    - Shared computational power to try to mine a block, distributing the resulting Bitcoins to all those involved in the mining
    - Allowed for more consistent income without necessarily earning less than if you mine a block on your own

Bitcoin - Supply

- Where do the Bitcoins come from?
  - **Mining** a block technically secures and verifies all the transactions the underlying chain represents
- When a block is created, a special coinbase transaction is included, granting some amount of Bitcoins plus all the transaction fees encoded in the block to the miner who created it
  - As of July 2016, this amount was roughly 12.5 Bitcoins*

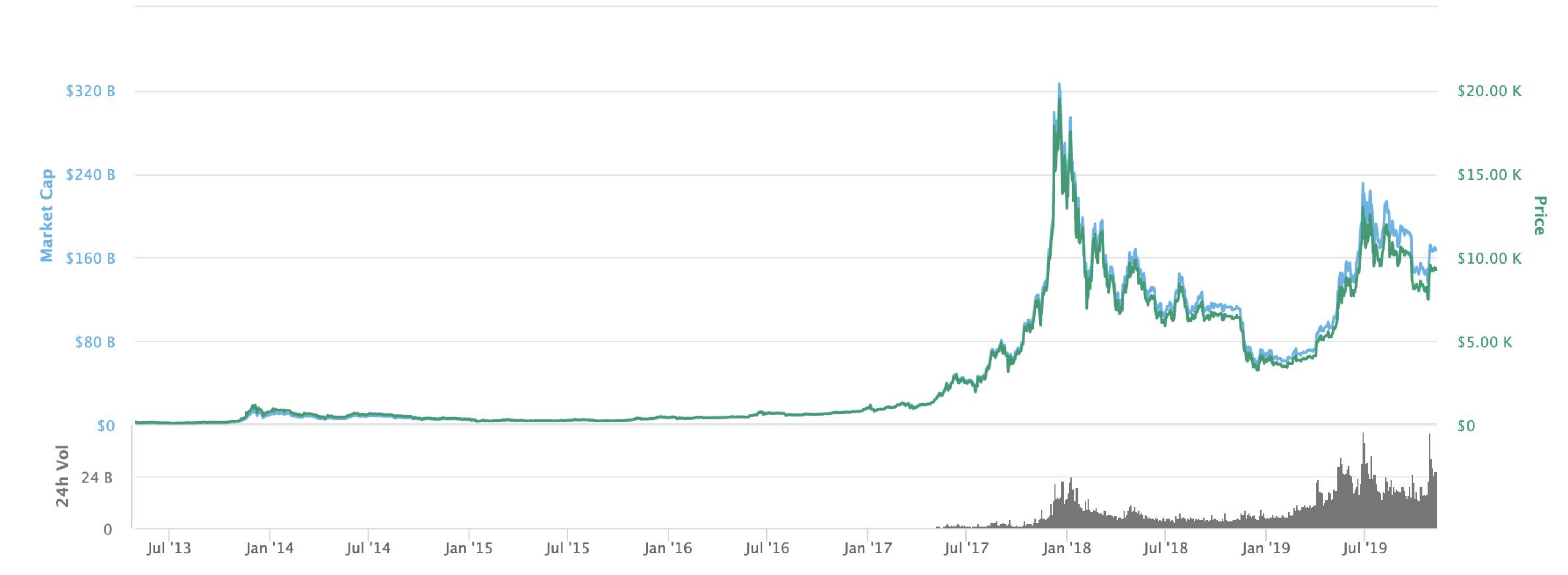
Bitcoin - Supply (cont.)

- The reward in this coinbase transaction changes, such that it halves every 210,000 blocks (roughly 4 years)
  - This means the introduction of new Bitcoins will eventually reach 0, and there is a set upper limit on possible Bitcoins (about 21 million)
- These bitcoins will eventually be stored in wallets
  - Since bitcoins don’t exists outside of unspent transaction results in the leger, all a wallet is is a private key that can sign the transaction of a specific amount of bitcoin
  - Basically the leger says “This person (with this public key) received X amount of bitcoins”
  - That key pair is necessary to verify any transaction spending those bitcoins, so knowing that key is equivalent to owning the bitcoins

Bitcoin - Economic Value

- Bitcoin as a currency is secure, but its economic value is based entirely on what people are willing to exchange for it (basically, the market S/D)
- There is no centralized authority that can guarantee some service or good in exchange for bitcoins
- This makes the value of bitcoins unstable

Bitcoin - Economic Value (cont.)



Other Currencies

- The Market
- Ethereum, Libre, and Dogecoin
  - What are the differences?
    - Libra Facebook’s (sorta)
    - Ethereum Attempting to make work useful
    - Dogecoin a very expensive meme

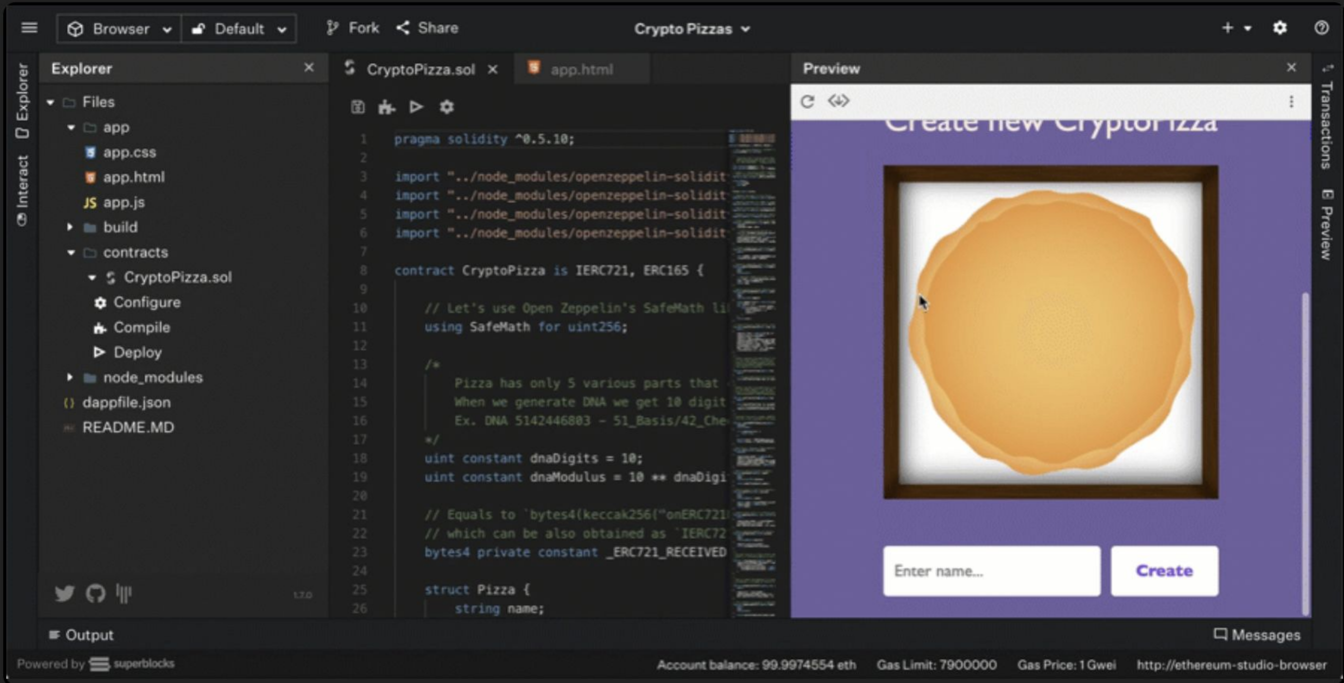
Libra is for the world

A stable global cryptocurrency built on a secure network.

Eteri234

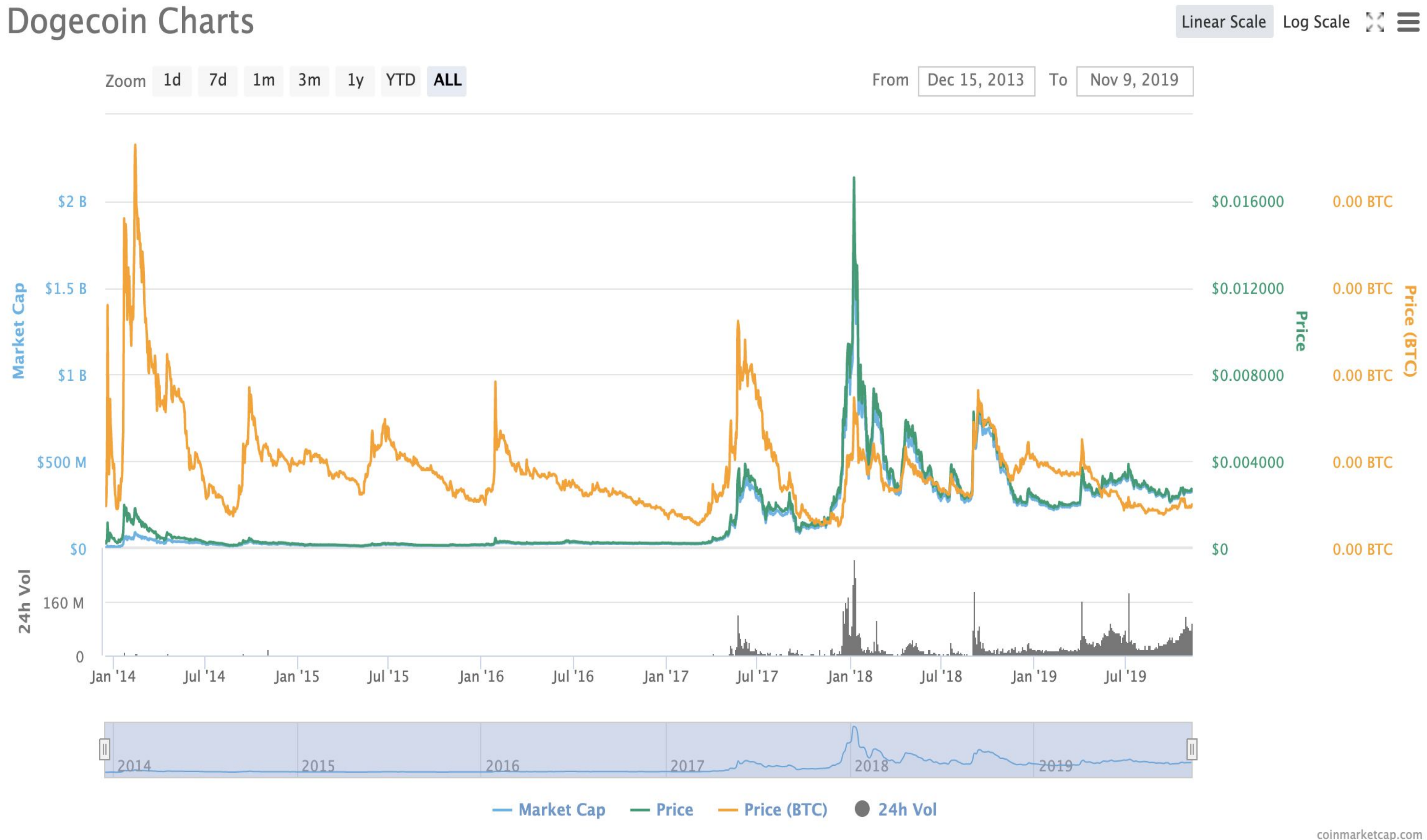
Ethereum is a global, open-source

On Ethereum, you can write code t
programmed, and is acc



```
pragma solidity ^0.5.10;

import "../node_modules/openzeppelin-solidit
import "../node_modules/openzeppelin-solidit
import "../node_modules/openzeppelin-solidit
import "../node_modules/openzeppelin-solidit

contract CryptoPizza is IERC721, ERC165 {

    // Let's use Open Zeppelin's SafeMath li
    using SafeMath for uint256;

    /*
        Pizza has only 5 various parts that
        When we generate DNA we get 10 digit
        Ex. DNA 5142446803 - 51_Basis/42_Che
    */
    uint constant dnaDigits = 10;
    uint constant dnaModulus = 10 ** dnaDigi

    // Equals to `bytes4(keccak256("onERC721
    // which can be also obtained as `IERC72
    bytes4 private constant _ERC721_RECEIVED

    struct Pizza {
        string name;
```

Account balance: 99.9974554 eth Gas Limit: 7900000 Gas Price: 1 Gwei http://ethereum-studio-browser



Dogecoin Charts

Zoom ALL

From Dec 15, 2013 To Nov 9, 2019

Notable Points

- Blockchain verified by cryptography
- Huge price fluctuation
- Additional materials
    - Three Blue One Brown
    - https://en.wikipedia.org/wiki/History_of_bitcoin