FUQINTRD 697: Innovation and Cryptoventures

Ethereum

Campbell R. Harvey*
Duke University and NBER

*Prepared with the help of Joey Santoro, Ashwin Ramachandran and Brent Xu

Overview

- Ethereum Basics
- The Ecosystem
- dApp deployment and connections
- Appendix

History of Ethereum

- Russian-Canadian Vitalik Buterin co-founded Ethereum at 19 years old
- Whitepaper in 2013
- Genesis block July 2015

Important Concepts

- Blockchain
  - Accounts
  - Wallets
  - Transactions
- Smart Contracts
- Tokens
- Decentralized Applications

Ether Denominations

- Wei - lowest denomination
  - Named after Wei Dai - author of b-money paper (1998), many core concepts used in BTC implementation
  - 1/1,000,000,000,000,000,000 (quintillion)
- Szabo - next denomination
  - Named after Nick Szabo
    - author of Bit-Gold
- Finney – 2nd highest denomination
  - Named after Hal Finney
    - received first Tx from Nakamoto

Multiplier	Name
10^0	Wei
10^{12}	Szabo
10^{15}	Finney
10^{18}	Ether

http://www.weidai.com/bmoney.txt

Blockchain

Blockchain as a Fully Distributed Database

- Stores data
- Transactions/messages alter the data

Ethereum

- The “data” can be any digital asset/token
- Ethereum uses smart contracts to dramatically expand transaction capabilities

Accounts

- All accounts have equal access to interacting with Ethereum
- External Owned Accounts (EOA)
  - Human account
  - Public/private keys used to send/validate transactions
- Contract Accounts
  - Completely run by code once deployed
  - Can hold and transfer ETH or other tokens
  - Unchangeable outside of what is coded

Wallets

- A set of one or more external accounts
- Used to store/transfer ether
  - Can also hold other tokens
- Manages Public/Private keys for you
  - Usually opened with a password
  - Provides back up phrase for keys
- X of Y Multisig wallets (e.g., need 2 of 3 to sign off)

Transactions

- Only way to update Ethereum State
  - Transfer ETH
  - Change contract data
- All transactions begin from an External Account
  - Contracts do not run in background, must be called by a transaction from an EOA or other contract

Smart Contracts

- Programatically enforced state updates
  - Can add any functionality you want
- Can facilitate access to and distribution of funds based on specified conditions
- Can create, transfer, and alter arbitrary digital assets
- Interact with other contracts to create robust interoperable applications
- Base layer for the Internet of Value

Token

- In the context of a blockchain
- Digital assets which live on a blockchain not its own
- Can have utility in context of a dApp, represent a physical good, or be a digital collectible
- ERC-20: Fungible Ethereum Token spec
  - All tokens interchangeable (like money)
- ERC-721: Non-Fungible Ethereum Token spec
  - Each token unique (like collectibles or title deeds)

Decentralized Applications (dApps)

- Goal is totally distributed application
  - No point of failure
  - No censorship
  - Totally transparent
- App Logic via smart contract
- App data via decentralized storage like IPFS or Swarm
- Frontend via IPFS or Swarm as well
- Name resolution via ENS (Ethereum Name Service)
- Messaging via Whisper (decentralized SMS - or message calls between applications)

Big Idea

Ethereum is a **smart contract** enabled **blockchain** which can act as the **base layer** for an interoperable **internet of value** and **decentralized applications**

The Ecosystem

- Many different applications are being built on Ethereum
- Some aim to decentralize/tokenize things we already do:
  - Gambling/Games, file storage, Dharma, dYdX, 0x
- Others completely new crypto-native applications:
  - MakerDAO, Augur, Decentraland

Under the Hood

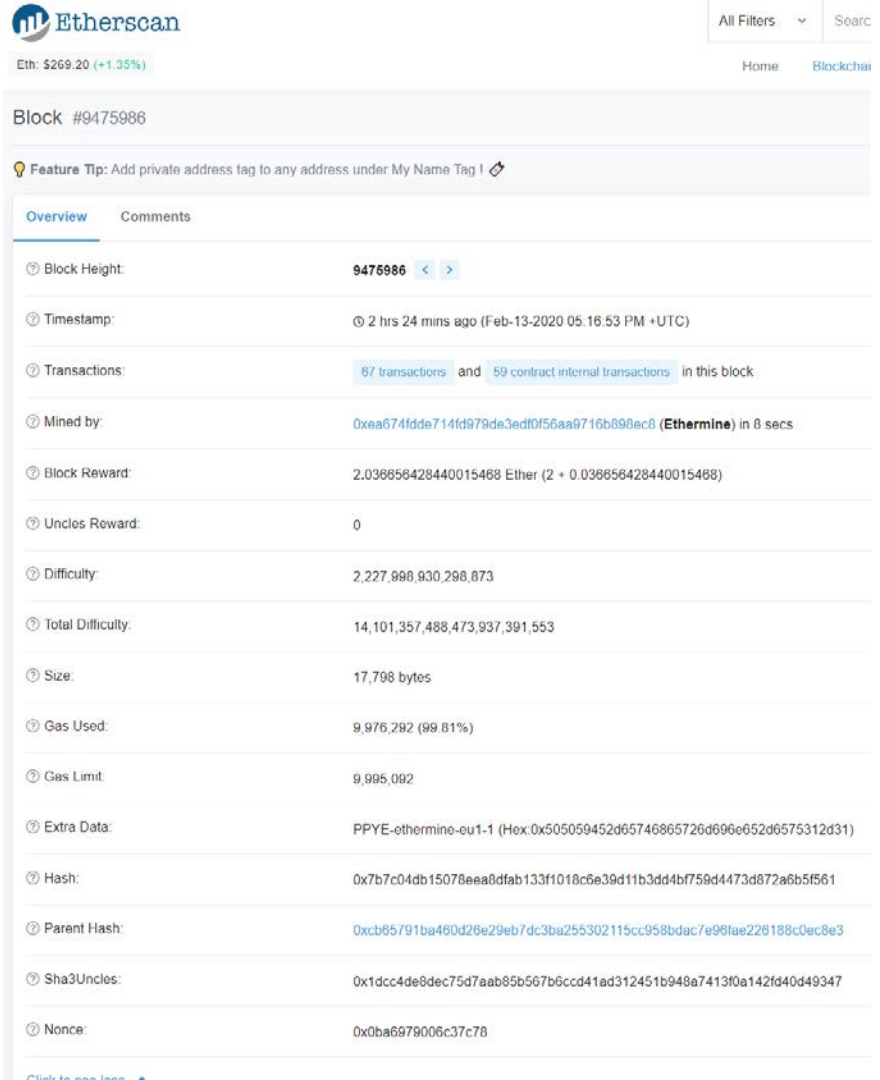
Blocks faster than BTC and reward is different

- Every 15 seconds
- 3 ETH main reward - reduced to 2 with Constantinople
- Different mining algorithm Keccak 256
- Same ECDSA used to generate public keys

- Blocks keep track of balances – not “unspent transaction outputs” like BTC
- Will transition from Proof of Work to Proof of Stake with Casper protocol

Under the Hood

- All blocks visible like BTC
- However, blocks have a different structure than BTC



https://etherscan.io/

Gas

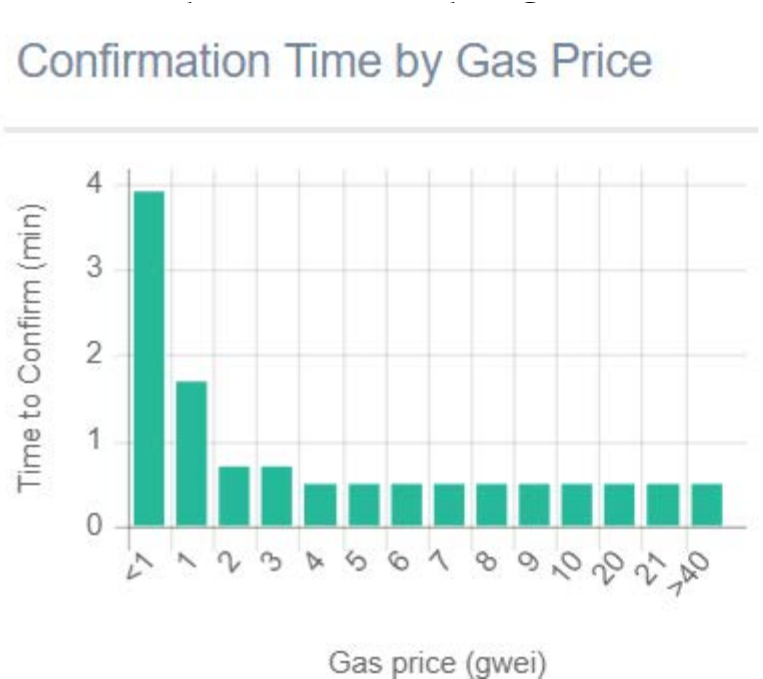
- Halting problem (infinite loop) – one reason for Gas
  - Problem: Cannot tell whether or not a program will run infinitely from compiled code
  - Solution: charge fee per computational step to limit infinite loops and stop flawed code from executing
- Every transaction needs to specify an estimate of the amount of gas it will spend
- Essentially a measure of how much one is willing to spend on a transaction, even if buggy

Gas Cost

- Gas Price: current market price of a unit of Gas (in Wei)
  - Check gas price here: https://ethgasstation.info/
  - Is always set before a transaction by user
- Gas Limit: maximum amount of Gas user is willing to spend
- Helps to regulate load on network
- Gas Cost (used when sending transactions) is calculated by gasLimit*gasPrice.
  - All blocks have a Gas Limit (maximum Gas each block can use)

Gas Cost

- Gas Price: current market price of a unit of Gas (in gwei)
  - Check gas price here: https://ethgasstation.info/



Recommended Gas Prices

(based on current network conditions)

Speed	Gas Price (gwei)
SafeLow (<30m)	1.1
Standard (<5m)	1.1
Fast (<2m)	4

PoW vs. PoS

Ethereum in the process of moving to Proof of Stake

- This approach does not require large expenditures on computing and energy
- Miners are now “validators” and post a deposit in an escrow account
- The more escrow you post, the higher the probability you will be chosen to nominate the next block
- If you nominate a block with invalid transactions, you lose your escrow

PoW vs. PoS

Ethereum in the process of moving to Proof of Stake

- One issue with this approach is that those that have the most ethereum will be able to get even more
- This leads to centralization eventually
- On the other hand, it reduces the chance of a 51% attack and allows for near instant transaction approvals
- The protocol is called Casper and this will be a hard fork

https://blockonomi.com/ethereum-casper/

Extra Material

- Highly recommended intro
- https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369
- I draw some graphics from the above article in the presentation