Oracles

Thus Far

- Bitcoin
- Ethereum

Recap

- Bitcoin Script:
  - Dest Address in UTXO
  - Timelock
  - What else?

Recap

- Ethereum
- Smart contracts
- Examples?

Real-World

- When the temperature hits X°F, pay $.
- When player X scores a home run, pay $.
- When Stock price hits 14, sell/buy.

In Our Setup

- Impossible
    - Can only reference on-chain information
        - Who puts this on chain?
        - What does the protocol need to allow?
        - What if you cheat?
- Today's Topic

Types

- What types of information do we reference?
- What types of trust / faith do we require?

Types

- Booleans:
  - `stock_price > 30`
  - `temperature > 20°`
- Time Series:
  - `[s1, s2, …, sn]`
- URLs
- Complex Schema

Real World

- Sports
- Gamble on next pitch
- TV / Radio

Real World

- Authoritative source
- News org
- TV
- Radio

Real World

- Sensor network (IoT)
- Readings on blockchain
- Trust?
  - Know their addresses a-priori
  - Stolen identity?

Real World

- I pay you when HTTP request returns response X

Real-World

- On receiving payment of 1 BTC, unlock next level on video game.

- Outbound

Storage?

- Where do you put this data?
  - Ethereum?
  - Bitcoin?
- Expensive!
  - Miners need to store the full chain
  - Cannot possibly service all the data-storage needs

Problem Dimensions

- Schema
- Inbound / Outbound
- Storage

Any Ideas?

Attempts

- Truthcoin
- Bitcoin Sidechain
- Prediction Market

Truthcoin

- PoW Blockchain
- 2 Types of Coin:
  - CashCoin
  - VoteCoin

Truthcoin

- CashCoin:
  - 1:1 redeemable for BTC
  - Use to create a prediction market (PM)
  - Buy/Sell PM shares
- VoteCoin:
  - Equity in “oracle corporation”

Truthcoin

- VoteCoin:
  - Corresponds to voting influence
  - Not really a store of value (or at least worse than CashCoin)
  - Rules to own them

VoteCoin

- If you own VoteCoin:
  - You must vote Y/N/Unk
  - On “Decisions”
  - Incentive mechanisms

VoteCoin

- Lost if you don't vote
- Lost if you vote against majority
- Gained if you tiebreak, pay attention to neglected decisions
- Incentive Model

Core Idea

- Create a market
- Ask for votes on “Decisions”
    - Oracle

Voters

- Incentivized to:
  - Vote with the rest (reality)
  - Vote on all decisions

VoteCoin

- Coin values = Reputatin

- Fixed # of coins - just exchanged based on voting activity

Issues?

- Can answer "some" kinds of questions:
  - POTUS on 11/08/2019?
  - Who will win the Superbowl 2020?

Issues?

- What do this sensor network say?

VoteCoin

- Sell your account (reputation) to someone?

Issues?

- Everyone *has* to vote.

- Additional “carrots” + “sticks” to make these prediction markets work.

Augur

- Similar incentive models
    - Incentive to vote
    - Penalty for abstaining
    - Reputation model
- Ethereum Dapp

Augur

- Final truth arbiter appointed at time of Q creation
- After event, arbiter has some time period to post result
- Can dispute this result

Those Were

- Consensus based
    - Voting
- Limited to certain types of facts

Sensors/IoT

- Hardware oracles
  - Cryptographic attestation of data
    - Make sure tampering is identifiable so you can reject data
    - Harder said than done
- Implications:
  - Insurance fraud

Centralized

- What if I just trust authority figures?
- Centralized oracle
  - One authoritative source of facts
  - Trust it in your smart contracts

Centralized

- Is the platform still decentralized?
    - If data providers are centralized?

ChainLink

- Decentralized

  - But different

Compared to Augur

- Decentralized in market creation time.
- Networks achieves consensus on truth source
- Truth source then delivers truth
- Dispute / Accept

Compared to Augur

- Here, multiple sources of truth
    - These sources then achieve consensus
- How?
    - At contract level

Chainlink

- Contract:
  - Reputation
    - Oracle performance tracking
  - Order-match
    - Collect bids from oracle providers
  - Aggregation
    - Aggregate results from oracle and produce final result

Chainlink

- Primitives for aggregation
- Schema dependent
- Some provided in chainlink

Chainlink

- Freeloading?
  - Lazy oracle just copies and sends response
- Solution:
  - Commit and reveal
  - Cryptographic commitment
  - Reveal responses

Chainlink

- Aggregate off-chain
    - Storage issues

Chainlink Reputation

- Publish user ratings of oracles
- Payment in LINK tokens

Outbound?

- Inform sidechains
  - Smart contract on chain 1 -> unlock payment on chain 2
- Inform outside world
  - Comes with own trust model
  - Do you trust the external aggregator?

Questions