bitcoin

CS1699: Blockchain Technology and Cryptocurrency

17. Bitcoin As a Platform

Bill Laboon

Bitcoin… More Than Just a Currency

- **Bitcoin is…**
  - *an append-only log which stores data "permanently"*
  - *a timestamping service*
  - *a means for value transfer*
  - *a way to cryptographically commit information*
  - *a way to prove "identity"*
- Can we do anything with these features besides move money?

Secure Timestamping with Bitcoin

- Proving that you know a block hash shows that whatever event occurred after that block - computationally infeasible to know block hashes ahead of time

Proof of Life

https://twitter.com/VitalikButerin/status/879127496024772610

https://etherscan.io/block/3930000

Commitment Scheme

- Recall that the SHA-256 hash function *H()* is collision-resistant (i.e., given $x \neq y$, it should be computationally infeasible to find $H(x) = H(y)$) and hiding (i.e., given a high min-entropy distribution, given $H(r \mid\mid x)$, it is infeasible to find x).
- Thus we can use our commitment scheme to commit to messages in the blockchain at a *specific (+/- 2 hours)* time

"Proof of Clairvoyance"?

- Not foolproof - what if I commit to several messages on the blockchain, but only reveal ones that are correct?
- Example: I commit three messages on Friday, one saying that the Steelers will win on Sunday, one saying they will lose, one saying they will tie. On Monday, I claim that I had "seen the future" on three days ago by only revealing whichever commit message was correct.
- How can we stop this and/or work around this?

"Permanently" Storing Data

- Recall that the blockchain is stored in numerous locations (every full node), and said locations have every reason to maintain the copy permanently (or until such time as Bitcoin becomes unprofitable)
- By using OP_RETURN, can store up to 80 bytes of arbitrary data, enough for a short message, link or hash
- Quite controversial! Some argue that this is "cheating" - Ethereum specifically discourages this through their design

Illicit Content Attack

- If anyone can push arbitary data onto the blockchain, what is to stop them from sending illegal data? *(and what do we mean by "illegal data", anyway?)*
- Nothing - and if you search the blockchain, you will find plenty of unusual/illicit arbitrary data
  - See "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin" by Matzutt *et al* - https://fc18.ifca.ai/preproceedings/6.pdf
- Wedding images, chat logs, doxxing, backups of Wikileaks dumps, backups of news articles covering pro-democracy protests in Hong Kong, several links to obscene images

Smart Property

- Bitcoin by themselves do not represent anything (unlike pre-Bitcoin attempts at a cryptocurrency such as e-Gold or Liberty Reserve)
- But they could… if we all came to a consensus on what they represent!

Smart Property

- Assume that we associate a particular UTXO with ownership of something (e.g., the ownership of this bike is whoever can prove ownership of a particular UTXO)
- UTXO can be used in a transaction to transfer ownership (with some technical help)
- Now provides perfect traceability! *(Bye-bye, title insurance…)*

Fungibility

- *Fungibility*: in economics, a good where all units are exactly equivalent and can be substituted for each other
- Example: if I want to buy an ounce of gold, I don't generally care about its provenance. An ounce of gold that came from melting down a Nobel prize is generally treated the same as an ounce of gold straight from a mine.
- Bitcoin is NOT fungible - one UTXO is NOT like another!
- This has benefits and drawbacks!

Bitcoin as a Platform

Can we use the strengths of Bitcoin to "overlay" our own services or represent other things?

Overlay Currencies

- An overlay currency uses the underlying Bitcoin network but re-uses specific bitcoin for non-Bitcoin related purposes
- Imagine extra credit points based on dollar bill serial numbers - I have a list of the serial numbers on certain dollar bills that can be redeemed for extra credit
- You can always use the dollar bill as “just” a dollar bill, but if it is one of the ones on my list, you could redeem it for extra credit in my class

Colored Coins

- Add some metadata to a particular UTXO (called a "color", but really just a sequence of bits)
- We can still transfer, split keys, combine transactions, etc., but we now have "tokens" on top of the Bitcoin network
- Security of Bitcoin but additional functionality for tracking property or other information

How is Smart Property Useful?

- **Securities** (*e.g. stocks, bonds, annuities, tontines*)
- **Physical property tokens** (e.g. real estate, vehicles)
- **Virtual property tokens** (e.g. CryptoKitties, domain names)

Secure Multiparty Lotteries

- Round 1: Each party picks a large, unique, randomly or pseudorandomly-generated number, x, and publishes $h = H(x)$
- Round 2: Each party reveals x (others can verify that $H(x)$ equals the originally published h)
- Winner: $(\sum x) \% n$, where n is the number of parties

Bitcoin as a Source of "Randomness"

- Problems with sources of randomness: how random are they?
- Stories abound about people who broke systems that were supposed to be random: The Eudaemonic Pie, Busting Vegas, Bringing Down the House (made into the movie "21"), Beat the Dealer, McDonald's Monopoly (https://www.newsweek.com/mcdonalds-monopoly-game-was-scam-truth-revealed-new-movie-1057001), Iowa lottery rigging (https://www.chicagotribune.com/news/nationworld/ct-lottery-rigging-scam-sentence-20170822-story.html) …
- But Bitcoin block hashes come pretty close to being random… could we use them (or use them as a seed for a PRNG) to replace these?
- Similar to how church raffles use the daily lotto numbers - outsource randomness generation

Cryptographic Beacon

- NIST (and others) provide randomness beacon as a way to "inject" randomness into a system.. but we have to trust NIST!
- Recall that computers cannot generate random numbers, best they can do is pseudo-random
- https://www.nist.gov/programs-projects/nist-randomness-beacon
- https://beacon.nist.gov/home
- https://beacon.nist.gov/beacon/2.0/pulse/last

Oracles

- Also called a *data feed* - an injection of external data into the blockchain
- Useful for many projects - e.g. tracking information, markets, futures, weather, etc.
- But very difficult to do in a trusted way!

The Oracle Problem

- The "**Oracle problem**" - how do we trust data coming in from off the blockchain?
- Possible ameliorations:
  - Market for oracles
  - Punishment for violations (bitcoin in escrow)
  - Multiple oracles must agree (within ε)

Prediction Markets

- Just like you can invest in stocks, can you invest in something to occur?
- Imagine sports betting: I get $100 if the Steelers
- This not only interesting for the players but also outside observers! Look at the popularity of 538..
- https://projects.fivethirtyeight.com/2018-midterm-election-forecast

Decentralized Prediction Markets

- Can we run these on the blockchain?
- It would avoid some regulatory issues and reduce the trust necessary.
- Yes, assuming you can trust the oracles… people stake REP on Augur, and if there is disagreement, you can actually have a hard fork!
- https://www.augur.net/
- By far the most complex dapp running on Ethereum today