Cardano, Ouroboros and Proof of Stake

Richard Munson

Rochester Institute of Technology

rem3830@g.rit.edu

April 26, 2018

Overview

1. Introduction
2. Proof of Stake - Issues
3. Basic Protocol
4. Incentive Structure
5. Attack Resistance
6. Other Implementation Details
7. Performance of Cardano

Introduction

Proof of Work

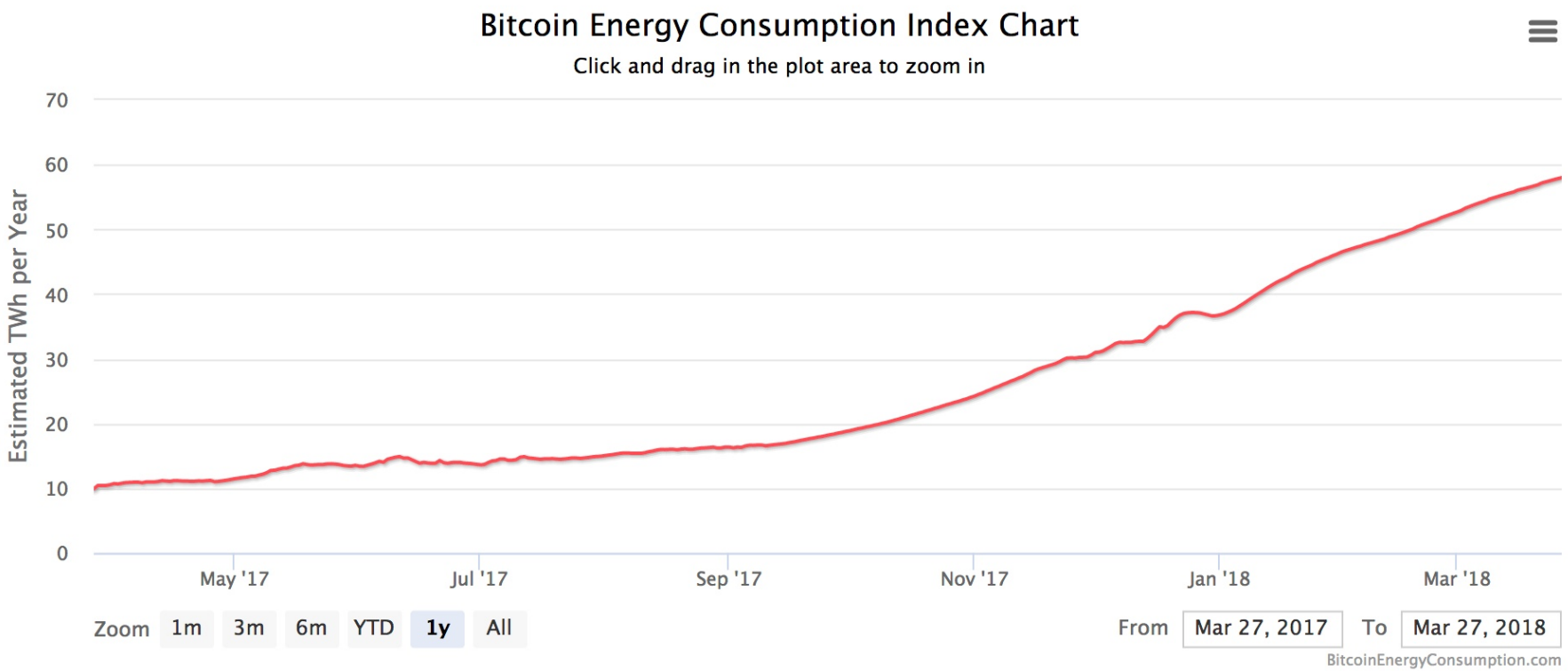
- Block signer chosen by randomized process based on computational power of miners
- Miners given expensive computational puzzles (often hashing-based) to solve
- Blockchain protocol used by many cryptocurrencies including Bitcoin and Ethereum

Proof of Work - Issues

- Typically very computationally intensive - requires a vast amount of energy to mine
- "Arms race" competition makes mining even worse computationally for cryptocurrencies like Bitcoin!
- Naïve implementations protect against some forms of cheating (double spending) only with the difficulty of mining (although Bitcoin implements further protection).

Home / Bitcoin Energy Consumption Index

Bitcoin Energy Consumption Index



Proof of Stake

- Block signer random selection process dependent on the *stake* (wealth) a participant holds in the current ledger (a modified "interest" system)
- Requires much less computational power to participate effectively (no "artificial" computational cost placed on participants)
- More complicated to implement properly!

Cardano

- New cryptocurrency (block chain launched on the 29th of September)
- Written in Haskell (a purely functional ML-style programming language)
- Based on the Ouroboros protocol (designed by the Cardano foundation) - a proof of stake algorithm with rigorous, peer-reviewed proofs of security

Adversaries

- The reason for our security concerns!
- Attempt to disrupt the network or corrupt it for their own gain
- May attempt to corrupt other users in order to modify the blockchain at will or create false transactions
- May disrupt network by cutting off user access to various important aspects of the protocol

"Covert" Adversaries

- Broadcast only one block per slot
- Broadcasting more than one block per slot can benefit user by allowing them to extend several chains at once
- Covert adversaries can blame issues with their performance on network delays rather than displaying suspicious "audit trails" that more clearly deviate from the protocol

Proof of Stake - Issues

Issues with Proof of Stake

- "Proof of stake is non-trivial - so non-trivial that some even consider it impossible." - Ethereum developer on the official Ethereum blog in 2014
- Ethereum are currently developing their own PoS protocol.

Building Blockchain is Easy

- Costs of working on several chains at once minimal (if no incentive to prevent it)
- Can lead to attacks
- Nothing at Stake Attack
  - Adversary maintains multiple versions of the blockchain - optimal for users to vote on any chain that can be found
- "Grinding" attack
  - Adversary "tests out" different chain heads to finding one that increases chances of being elected as the signer for the next block

Basic Protocol

Setup

- Time divided into *slots*; each associated with at most one block of the ledger

- Ledger should satisfy:
  1. *Persistence:* A transaction declared *stable* will be reported stable by honest parties.
  2. *Liveness:* If all honest parties attempt to include a transaction, it will be reported as stable after at most a certain (fixed) number of slots

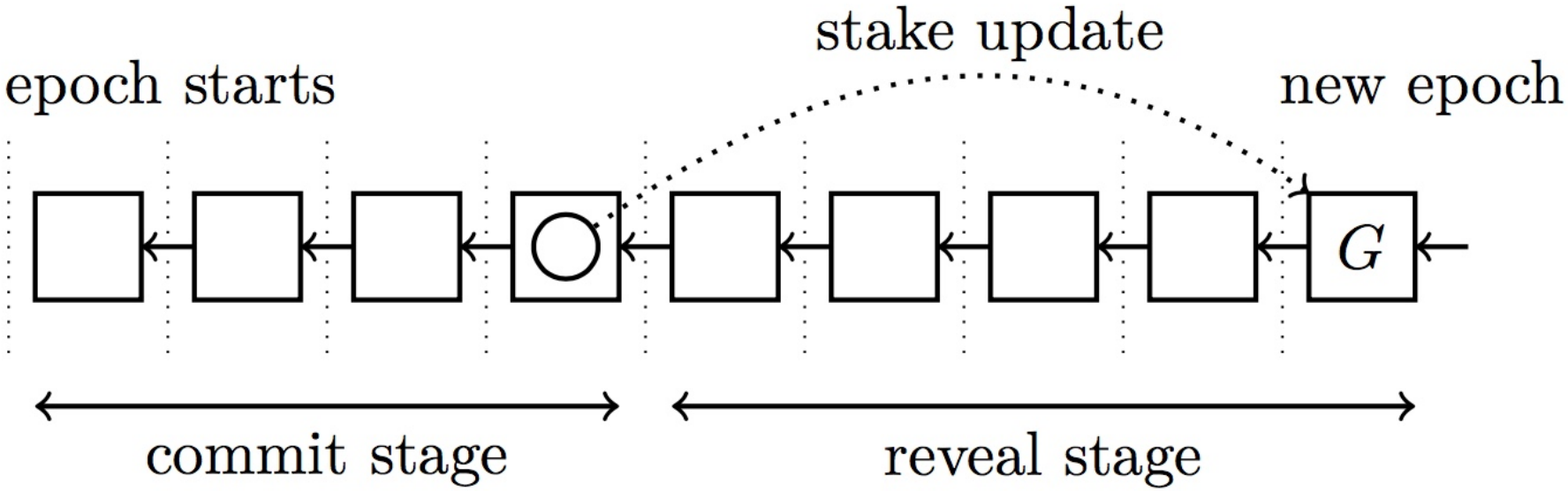
Important Parameters and Details

- Genesis block B_0 - the initial block in the system, containing the public keys and stakes of the users
- k - the depth in the ledger at which an entry becomes "stable"
- ϵ - The advantage of the collection of honest users over the adversary
- Keys generated randomly according to some encryption scheme, or *by adversary* if user has been corrupted
- Protocol divided into "epochs" of size $10k$

Stake Selection

- Random "coin toss" algorithm using publicly verifiable secret sharing system (PVSS)
- Users on committee in the previous stage divide a random "commitment" into shares and post both to blockchain
- Shares are signed with each users respective private key
- If user does not open the commitment in the reveal phase, a number of honest users greater than a certain threshold can recover the commitment
- Sum of commitments used as seed for random weighted stake-based selection

Stake Selection (cont'd)



Blockchain Protocol

1. Stake in epoch j drawn from at latest block in slot less than $jR - 2k$ (to preserve stability)
2. Valid chains collected and signed blocks verified - set maximal chain that does not fork from current chain more than k blocks as the new local chain
3. Endorser verifies the validity of the transactions to be included in the chain
4. Slot leaders (selected by coin toss) generate a new block with the endorsed input (or an empty block if no endorsement took place), append to the chain, and broadcast

Incentive Structure

Incentives

- Incentives chosen based on *slot leader*, rather than on the actual block minter
- Endorsers rewarded based on their contribution
- Given the sum of transaction fees P, input endorsers $E_1, ..., E_r$ and slot leaders $L_1, ..., L_R$ all in an epoch, claimable rewards for a given user U collected from transaction fees total (for some constant $\beta \in [0, 1]$)

$$\left(\beta \frac{|\{j|U = E_j\}|}{r} + (1 - \beta)\frac{|\{j|U = L_j\}|}{R}\right) P$$

- Rewards for epoch j claimable after slot $(j + 1)R + 4k$

Nash Equilibrium

- A strategy is a *Nash Equilibrium* if it does not benefit a party to change their strategy given knowledge of the other parties strategies
- Provable that the honest strategy is a δ-Nash equilibrium (may be some small benefit to deviate) for a reasonable constant δ.
- (Relative) stake of adversaries assumed to be reasonably small ($\frac{1-\epsilon}{2} - \sigma$ for some constant σ in $(0, 1)$ representing the expected change in stake over an epoch)

Attack Resistance

"Grinding" Attacks

- Rely on the adversary being able to determine the next slot leader from a given block in a slot
- Ouroboros is resistant to these attacks, as this information is not encoded in a block at all (the leaders are chosen using the coin-toss protocol)

"Nothing At Stake" Attacks

- Rely on adversaries maintaining false copies of the blockchain that "fork off" from the main blockchain
- Since optimal decision is to work on any blockchain that can be found, defense relies on difficulty of maintaining a fork
- Given that colluding slot leaders take up no more than $\frac{1-\epsilon}{2}$ slots among n, the probability of being able to maintain such a dishonest fork is very small - $2^{-\Omega(\sqrt{n})}$

"Double Spending" Attacks

- Involves an adversary reporting a transaction "twice" by causing the validity of a different transaction to be nullified or otherwise ignored
- The provable *persistence* of the ledger prevents this
- Impossible to bring system to state in which the confirmed transaction is invalid

Desynchronization Attacks

- Involve an honest party not being capable of behaving properly with the network
- Adversary can prevent honest parties from accessing the synchronized time or other synchronization mechanisms
- Protocol can fail... if over 50% of the stake's worth of parties are desynchronized

Other Implementation Details

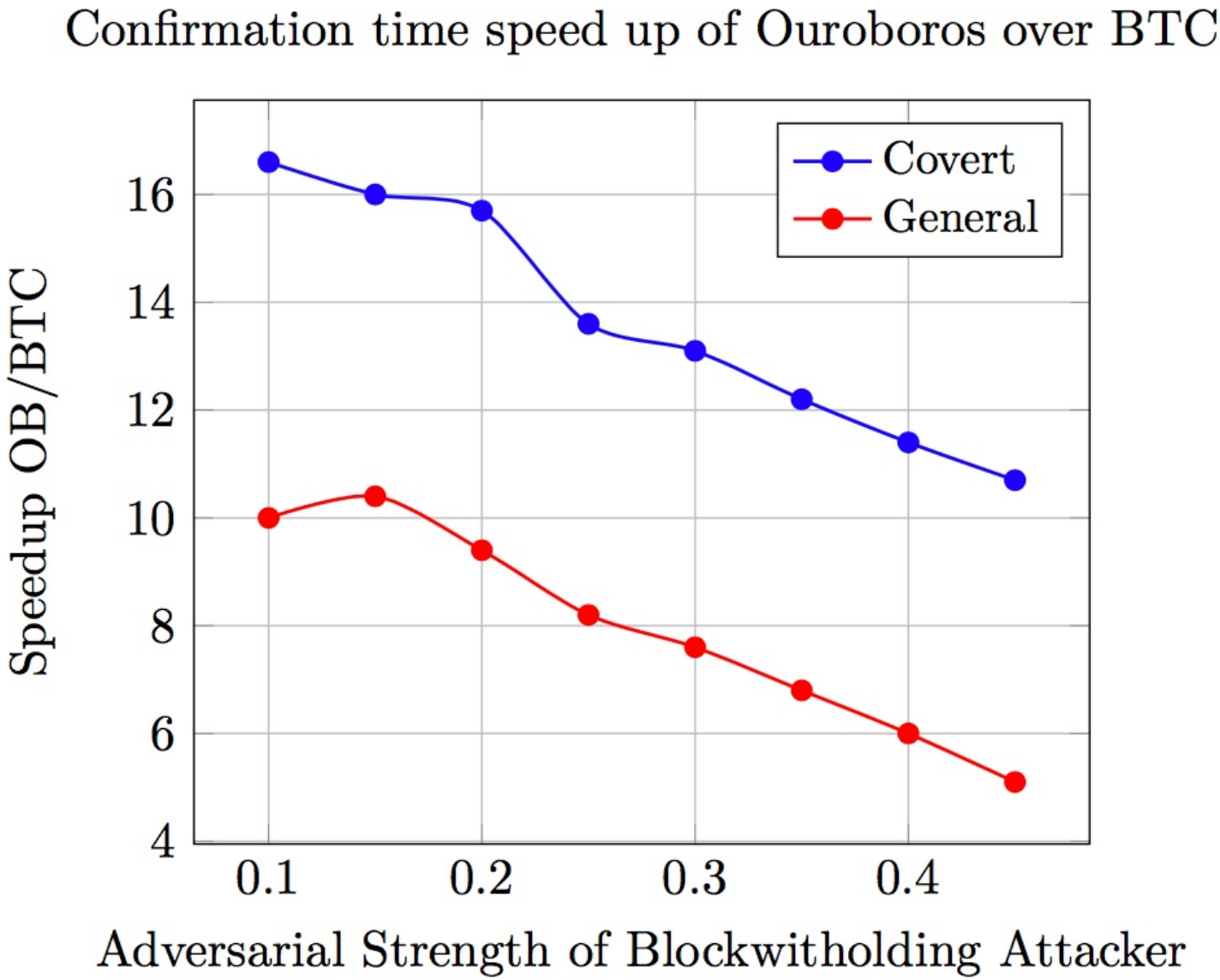
Elliptic Curves

- Elliptic curves used for signing system
- Tests run in the Amazon cloud were done over curve `secp256r1`

Comparisons With Bitcoin

- Tests of an implementation of the protocol were run in the Amazon cloud
- Comparisons of times required to confirm a transaction against covert / non-covert adversaries (with confidence 99.9%)
- 5 to 10 times faster than Bitcoin for non-covert adversaries (10-16 times faster for covert)

Comparisons with Bitcoin (cont'd)



Performance of Cardano

Price


1d
7d
1m
3m
6m
1y
All
Value
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Nov
Dec
2018
Feb
Mar
Apr
Volume
600M
400M
200M
0
Nov
Dec
2018
Feb
Mar
Apr

Thanks!