Discussion

Crytpocurrency, Imperfect Information and Fraud

(Li & Wang)

Thorsten Koeppl

Queen's University

JEDC Conference

October 9, 2020

Question

Can Double Spending (DS) be an equilibrium in a cryptocurrency transaction?

Assume **"consensus" is exogenous** (NOT about the ledger).

Think of DS as a race attack in Bitcoin.

Ownership of crypto becomes stochastic in attack.

Key:

No double spending on the ledger

Main Result

Only two trading mechanism can be optimal in a “cryptocurrency” transaction.

Honest mechanism: costly on and off equilibrium

- message costs (PoW?)
- collateral (PoS?)
- destroy crypto in fork

DS mechanism: accept probabilistic settlement

- no direct costs
- sub-optimal terms of trade
- destroy crypto in fork

Relative costs determine which mechanism is best for transaction.

Consensus?

Cryptocurrency is a **distributed (payment) system**; hence, agreeing on the state matters.

With DS on the ledger level, finality is pretty much impossible.

Why?

- DS attempt has to compete with other DS attempts.
- Successful DS can be undone by future DS.
- Forks sow confusion.

Key: **success of DS & consensus are both endogenous**

Very difficult to get a handle on.

Double Spending and Consensus

Consider DS in the form of “Secret Mining”.

One cycle only (no catch up) with fixed mining power.

- M miners; fraction ϕ double spends (“1”)
- N required confirmations
- R mining reward & V extra value from DS

Do not consider vested interest.

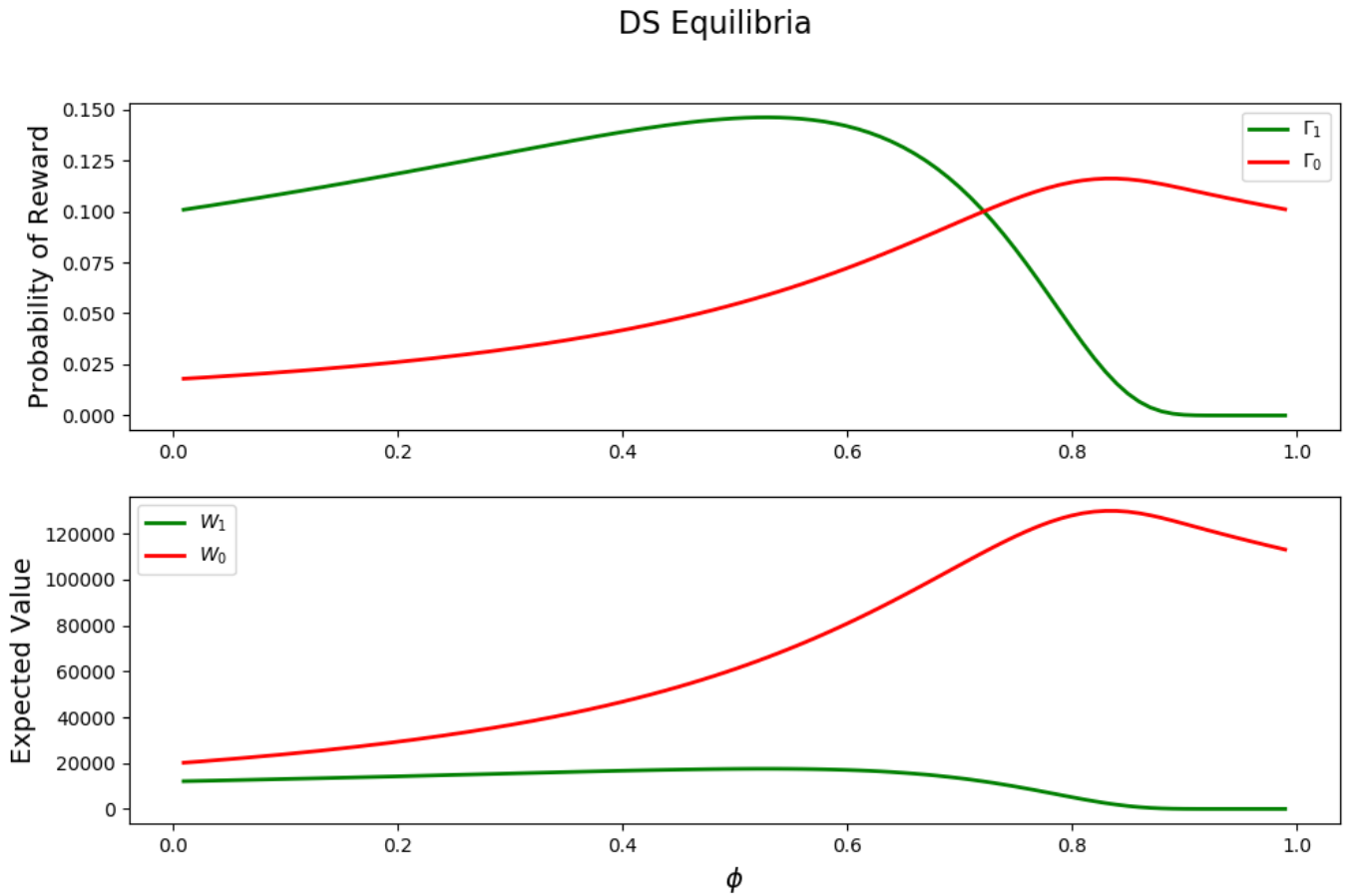
Idea:

DS equilibrium as a Nash equilibrium with strategic miners.

Poisson race against sequence of exponential races

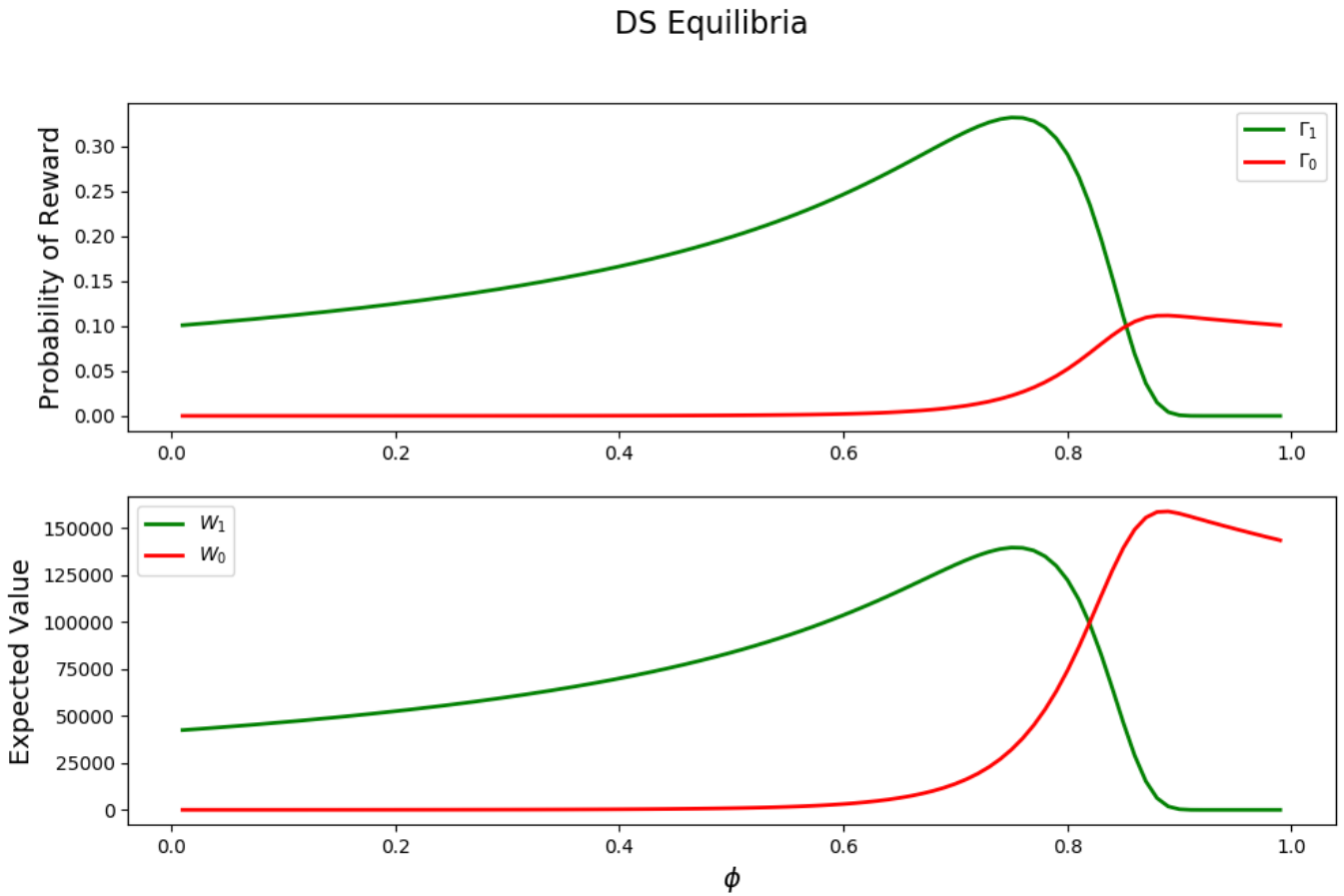
$W_1(\phi)$ vs. $W_0(\phi)$?

Bad news?



For low N ($N = 1$), all miners always try to DS.

Good news?



For high N ($N = 6$), there is a NoDS equilibrium.

We need to switch a fairly large amount of mining power for DS.