Discussion of

Economics of Proof of Stake Payment Systems

Fanti, Kogan, Viswanath

2019

Thought provoking paper on important issue

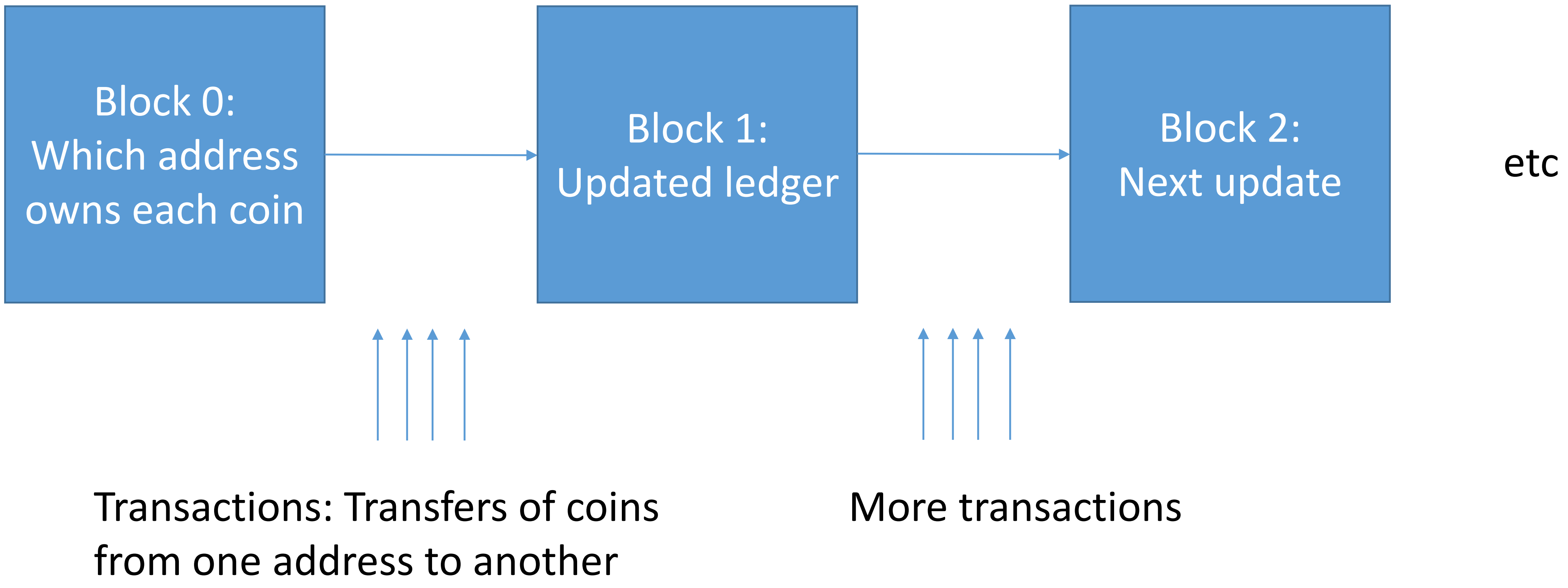
Ledger

Who owns assets (coins)

Transactions -> changes in ledger

Blockchain

Transactions grouped in blocks



Who maintains ledger ?

Who enters transactions ?

Distributed ledger

All network participants see ledger

All contribute to maintaining it

How can decentralised network participants maintain ledger ?

Voting ? Not easy to decentralize in open network

-> Random draws:

1 participant randomly drawn: proposes ledger update = new block

= transactions + to which previous block appended

Next randomly drawn participant, if agrees to block, chains to it, etc…

How are participants rewarded for maintaining ledger ?

Reward = newly minted coins (also fees but very small)

Reward written down in block added by the participant: valuable only if further participants chain to it

If fork: participants choose to which branch to chain

Biais et al (RFS 2019) -> coordination game: I attach my block to the branch I expect the others to follow -> multiple equilibria

How are participants randomly drawn ?

Proof of work protocol:

First one to find solution to complicated numerical problem

-> Waste of energy

(electricity spent to find solutions = electricity consumption of Switzerland)

How are participants randomly drawn ?

Proof of stake protocol:

Participants drawn with proba increasing in holdings of token

-> Vast reduction in energy consumption

Rewards in POS comparable to dividends in stock market

Larger coin holdings
$\Rightarrow$ More likely to be drawn
$\Rightarrow$ Larger expected reward

Coin give rewards // stocks give dividends

Fanti, Kogan, Viswanath (2019) model coin valuation in POS

Unit fixed supply of coins, flow of transactions Y

Risk neutral validators get fee c for each trade, willing to hold ϕ coins

$\Rightarrow \phi$ p = c Y /r (present value of rent cY, similar to dividend)

Users hold $1 - \phi$ coins they value at k Y (reduced form)

$\Rightarrow (1 - \phi)$ p = k Y

Combining the two: p = (k + c/r) Y

Proof of stake?

Does not directly/explicitly model individual choice:

If I hold one more coin

$\Rightarrow$ this increases the probability that I will be drawn as validator

$\Rightarrow$ and correspondingly my expected blowk rewards or transaction fees

Also does not model strategic interaction between validators in blockchain (Saleh 2018), which might impact validators’ valuation for coins

Extension

If transactions grow at rate g_y and supply at rate g_s

$$p = (k + (c+kg_s)/(r-g_y))\ Y$$

More transactions

$\Rightarrow$ more transaction fees

$\Rightarrow$ larger present value of transaction fees

Bring in some monetary economics to endogenise users' demand ?

OLG (Garatt and Wallace 2018, Schilling Uhlig 2018, Biais, Bisiere, Bouvard, Casamatta, Menkveld 2019, Saleh 2019)

« Lagos Wright » (Chiu Koeppl 2018, Fernandez Villaverde Sanchez 2018)

Network (Cong et al 2019, Pagnotta Buraschi 2019)

Indifference (equilibrium)conditions

Indifferent between holding risk free asset and coin:

$$r\, p_t\, dt \quad = \quad E[dp_t] + E[dV(p_t)]$$

invest p_t in riskfree

invest p_t in coin -> capital gain+ « dividend »

Fanti et al: $dV(p_t)$ reflects POS reward: $[p_t\,(c+kg_s)Y_t \,/\, (p_t - kY_t)]\,dt$

Cong et al: $dV(p_t)$ reflects network: U(holdings, network size) dt

Biais et al: $dV(p_t)$ reflects transaction benefits and hack risk: $p_t\, \tau_t\, dt - E[p_t\, dHt]$

Conclusion

Interesting first step towards understanding coin valuation in POS

Suggests potentially interesting further avenues of research:

- Monetary economics to endogenise users’ demand for coin
- Game theory to understand validators strategies in blockchain (Saleh, 2018)