Understanding Decentralization in Proof-of-Stake Blockchains: An Agent-Based Simulation Approach

Jungpil Hahn

National University of Singapore
jungpil@nus.edu.sg

Joint work with Christoph Müller-Bloch, Jonas Valbjørn Andersen and Jason Spasovski

Understanding Blockchain Governance Decentralization: An Agent-based Simulation Model

National University of Singapore

Joint work with Christoph Müller-Bloch, Jonas Valbjørn Andersen and Jason Spasovski (IT University of Copenhagen)

the rise of algorithmic operations

tripadvisor.com.sg

Tripadvisor

Review | Trips | Alerts | Sign in

Athens | Hotels | Things to do | **Restaurants** | Flights | Holiday Rentals | Package Holidays | Cruises | Car Hire | •••

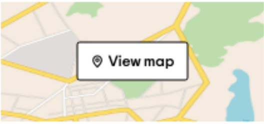
United States > Georgia (GA) > Athens > Athens Restaurants

Best Restaurants in Athens, GA

Restaurants in Athens

Filter and search through restaurants with gift card offerings. ⓘ

See restaurants with gift cards



Establishment Type

- [x] Restaurants
- [ ] Quick Bites
- [ ] Dessert
- [ ] Coffee & Tea

Show more

Restaurant features

- [ ] Delivery
- [ ] Takeout
- [ ] Gift Cards Available
- [ ] Wheelchair Accessible

Show more

Meals

- [ ] Lunch
- [ ] Dinner

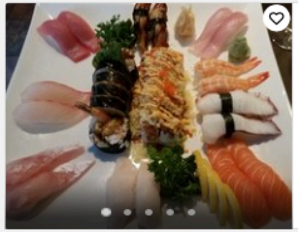
Price

- [ ] Cheap Eats
- [ ] Mid-range

29 results match your filters **Clear all filters**

Sort by: Relevance

Restaurants ✕ | Asian ✕



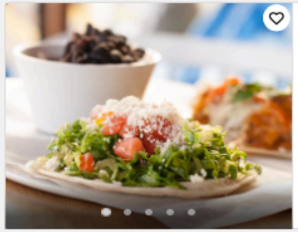
1. Shokitini

80 reviews · Closed Now

Japanese, Sushi · $$ - $$$ · **Menu** ↗

"I am not a fan of sushi and ordered the cooked salmon with steamed **rice** and v..."

"Good Sushi Downtown"



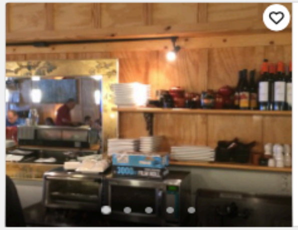
2. Taqueria Tsunami

121 reviews · Closed Now

Latin, Asian · $$ - $$$ · **Menu** ↗

"Good food and service"

"Great service during busy time!"



3. Thai Spoon

83 reviews · Closed Now

Asian, Thai · $$ - $$$ · **Menu**

"Chicken **Pad Thai**, Pad See Ew, and Thai Spicy Noodles were all delicious and a..."

"So the wife and I are pretty big fans of **Thai Food** and I almost always stick..."

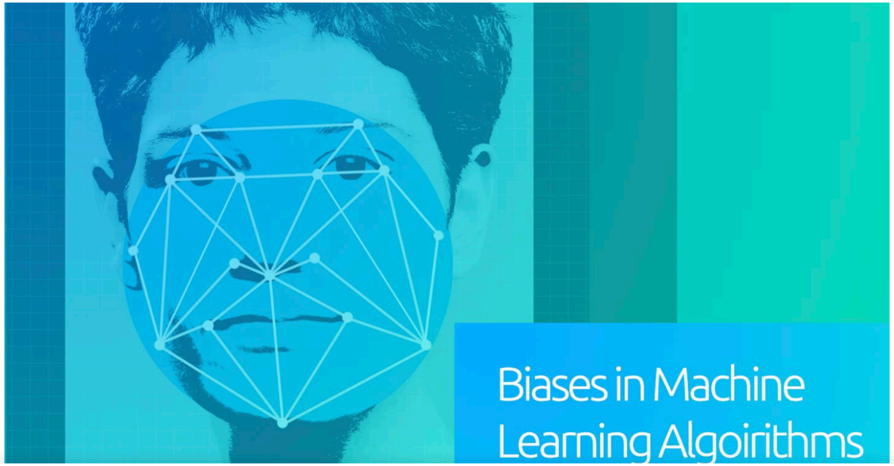
Amazon Scraps Secret AI Recr

A Medium Corporation [US] | https://medium.com/datadriveninvestor/amazon-scraps-secret-ai-recruiting-engin...

Amazon Scraps Secret AI Recruiting Engine that Showed Biases Against Women

AI Research scientists at Amazon uncovered biases against women on their recruiting machine learning engine

October 11, 2018 by Roberto Iriondo



algorithms are everywhere!

algorithms have real-world consequences that are materialized in practice algorithms have real-world consequences that are materialized in practice

- unintended consequences
- opaque connection between process and outcome

how can we design more predictable algorithm-driven systems?

how can we design more predictable algorithm-driven systems?

& *explainable*

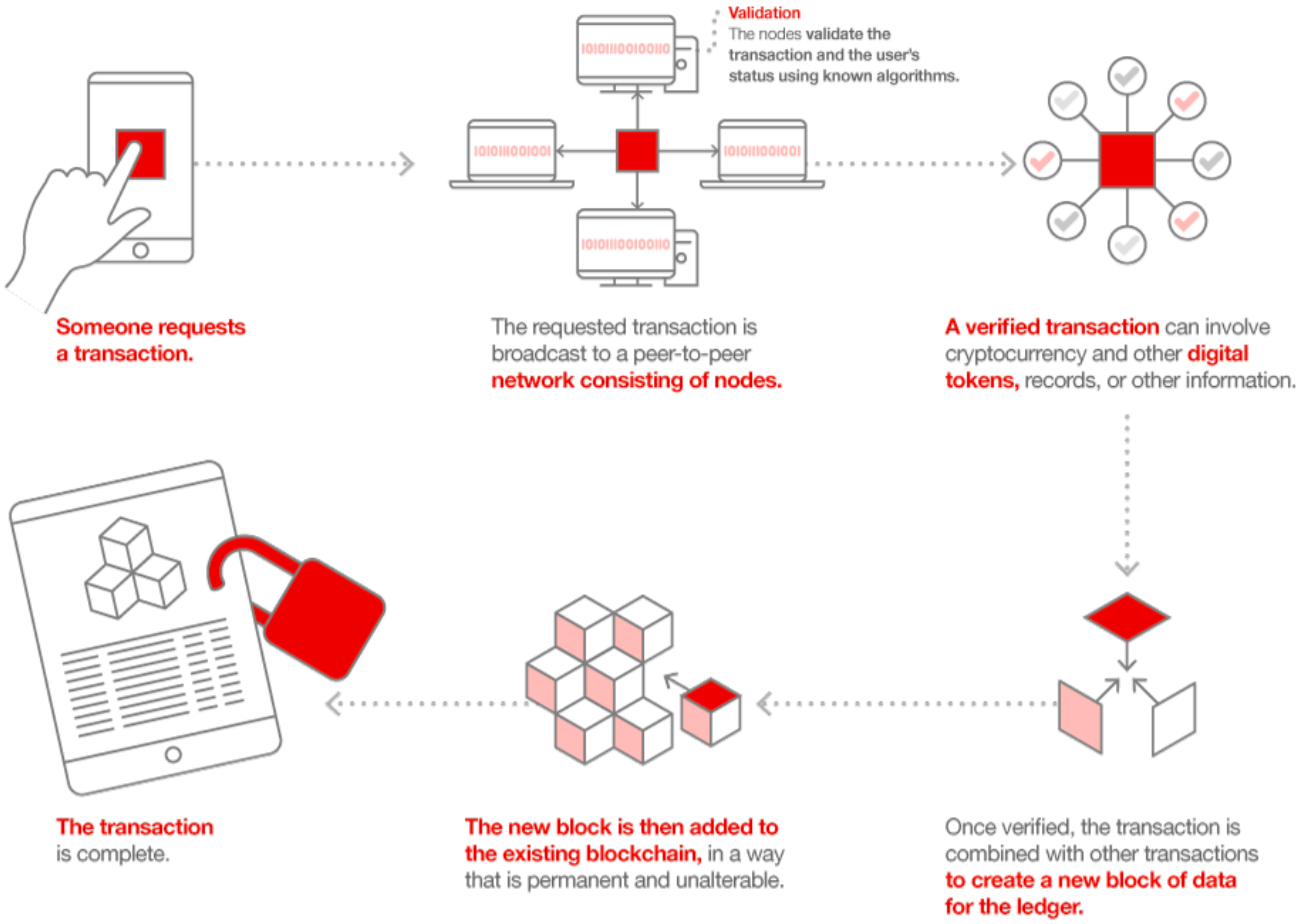
how can we design more predictable
algorithm-driven systems?

& explainable

how can we design more predictable
algorithm-driven systems?

designer's intention

… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …


Someone requests a transaction.
Validation
The nodes validate the transaction and the user's status using known algorithms.
The requested transaction is broadcast to a peer-to-peer network consisting of nodes.
A verified transaction can involve cryptocurrency and other digital tokens, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

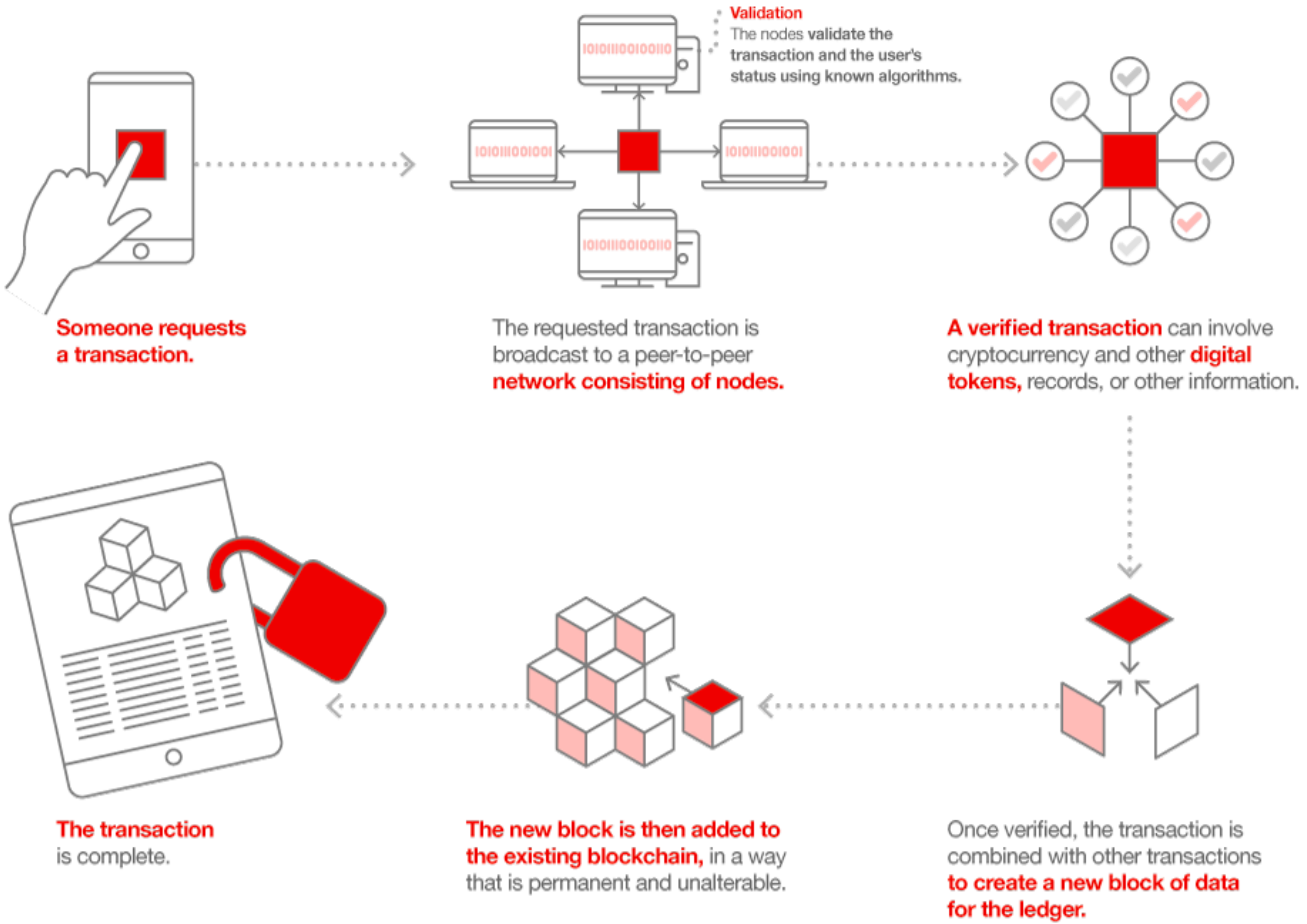
pwc

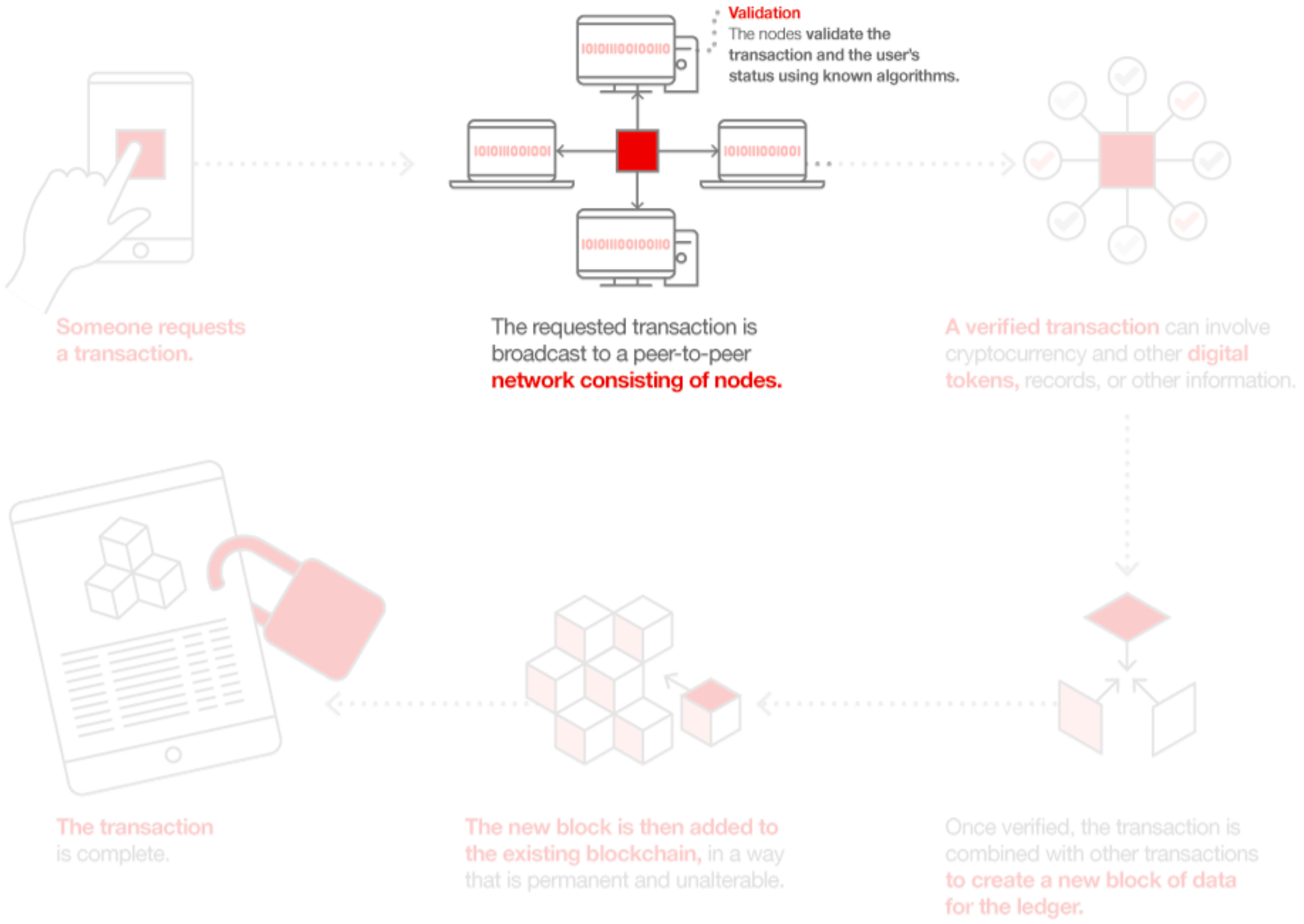
… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …

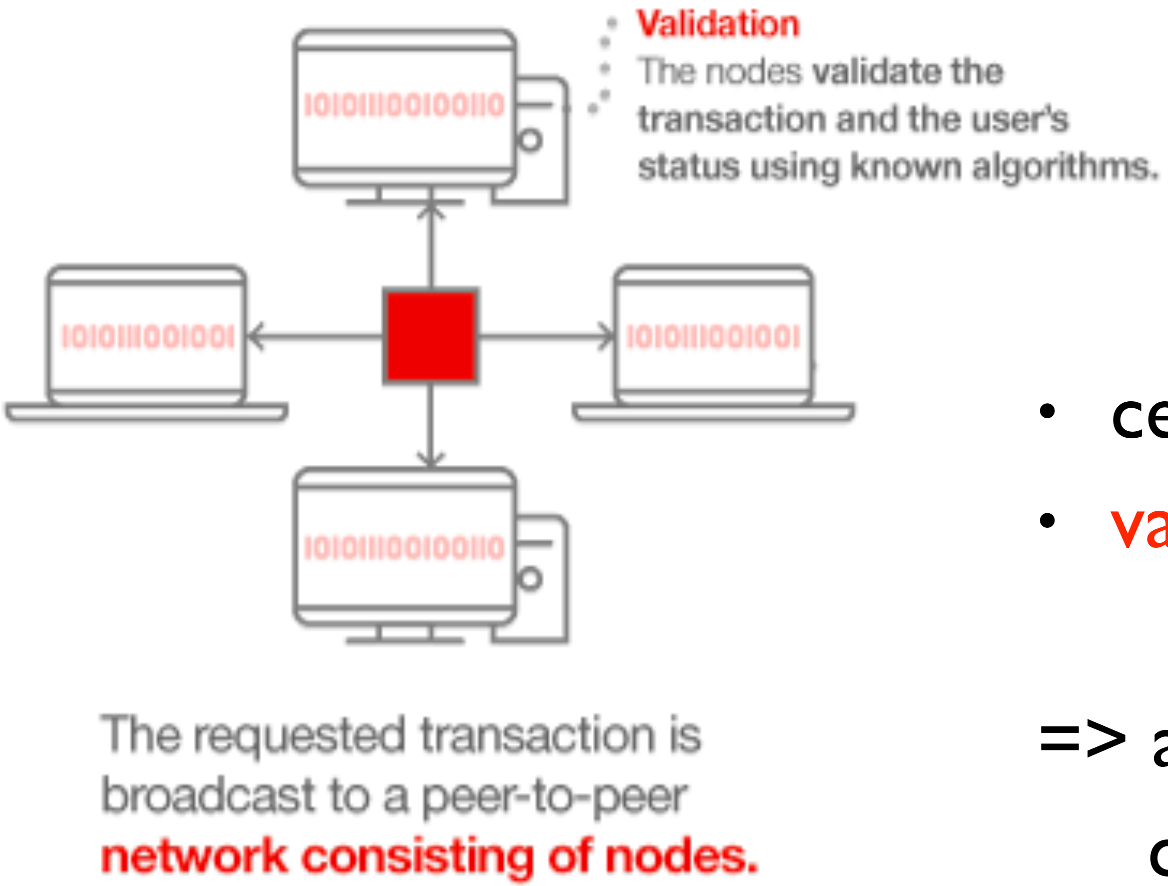
… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …

tamper-resistance

… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …


Validation
The nodes validate the transaction and the user's status using known algorithms.
Someone requests a transaction.
The requested transaction is broadcast to a peer-to-peer network consisting of nodes.
A verified transaction can involve cryptocurrency and other digital tokens, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
pwc


Validation
The nodes validate the transaction and the user's status using known algorithms.
1010111001001110
1010111001001
1010111001001
1010111001001110
Someone requests a transaction.
The requested transaction is broadcast to a peer-to-peer network consisting of nodes.
A verified transaction can involve cryptocurrency and other digital tokens, records, or other information.
The transaction is complete.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.



- central operator *not* needed
- validator node is selected

=> algorithmic governance via consensus mechanism (PoW, PoS, …)

tamper-resistance

… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …

tamper-resistance

requires

decentralization of decision making power

… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …

decentralization of decision making power

is the intended outcome of the

consensus mechanism

… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …

(de)centralization of decision making power

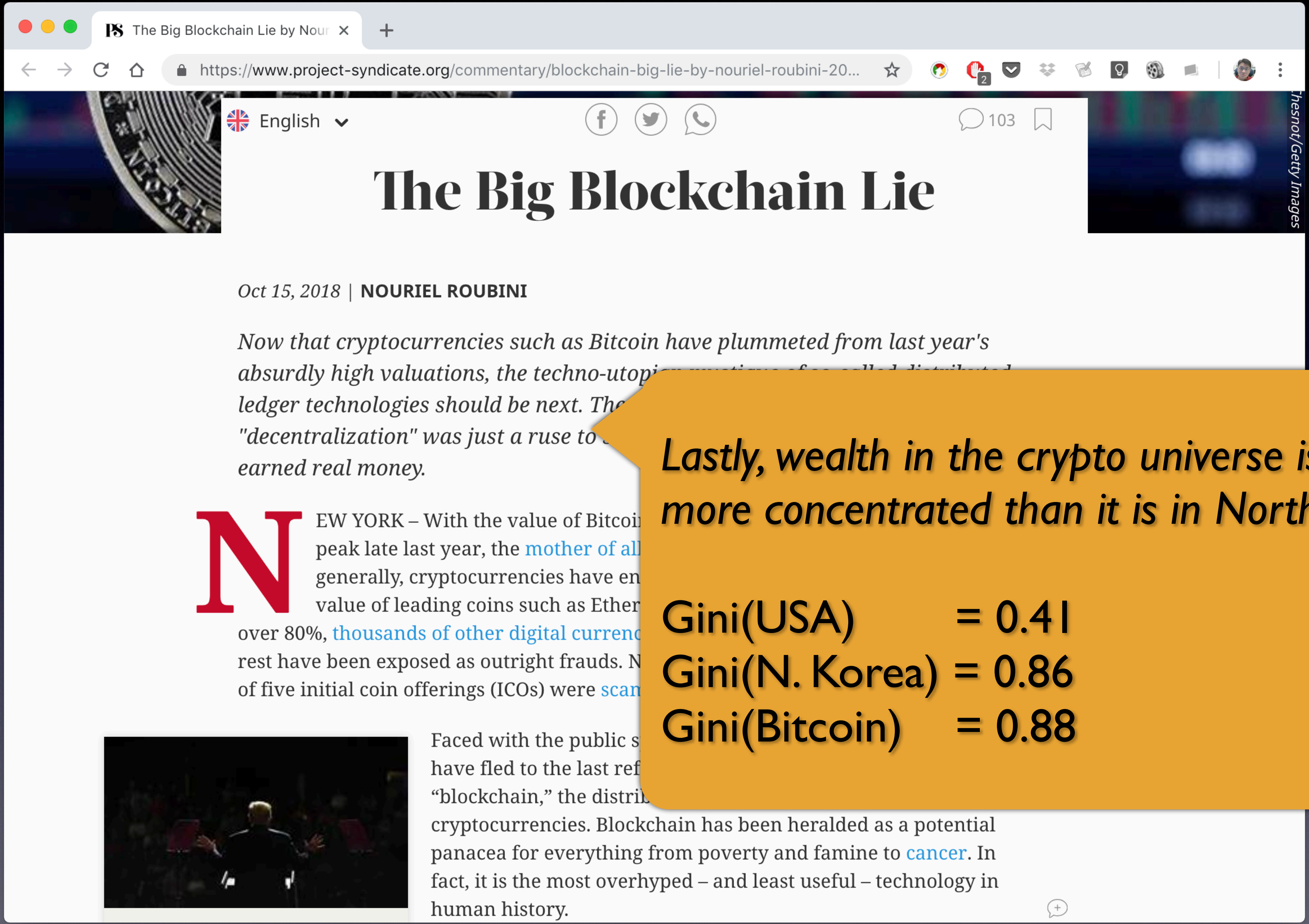
emerges from

network of nodes + interactions

… distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism …

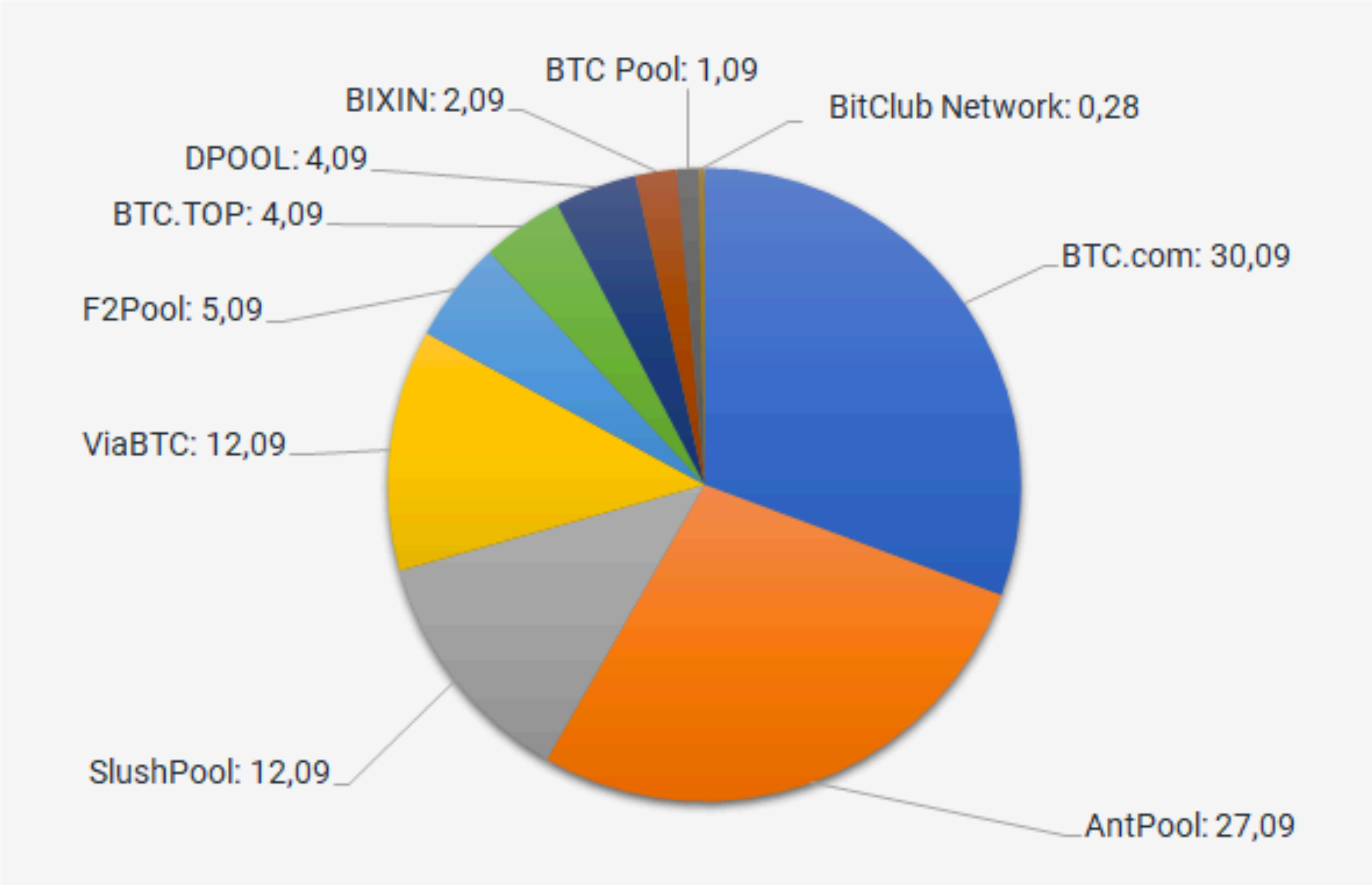
algorithms have real-world consequences that are materialized in practice

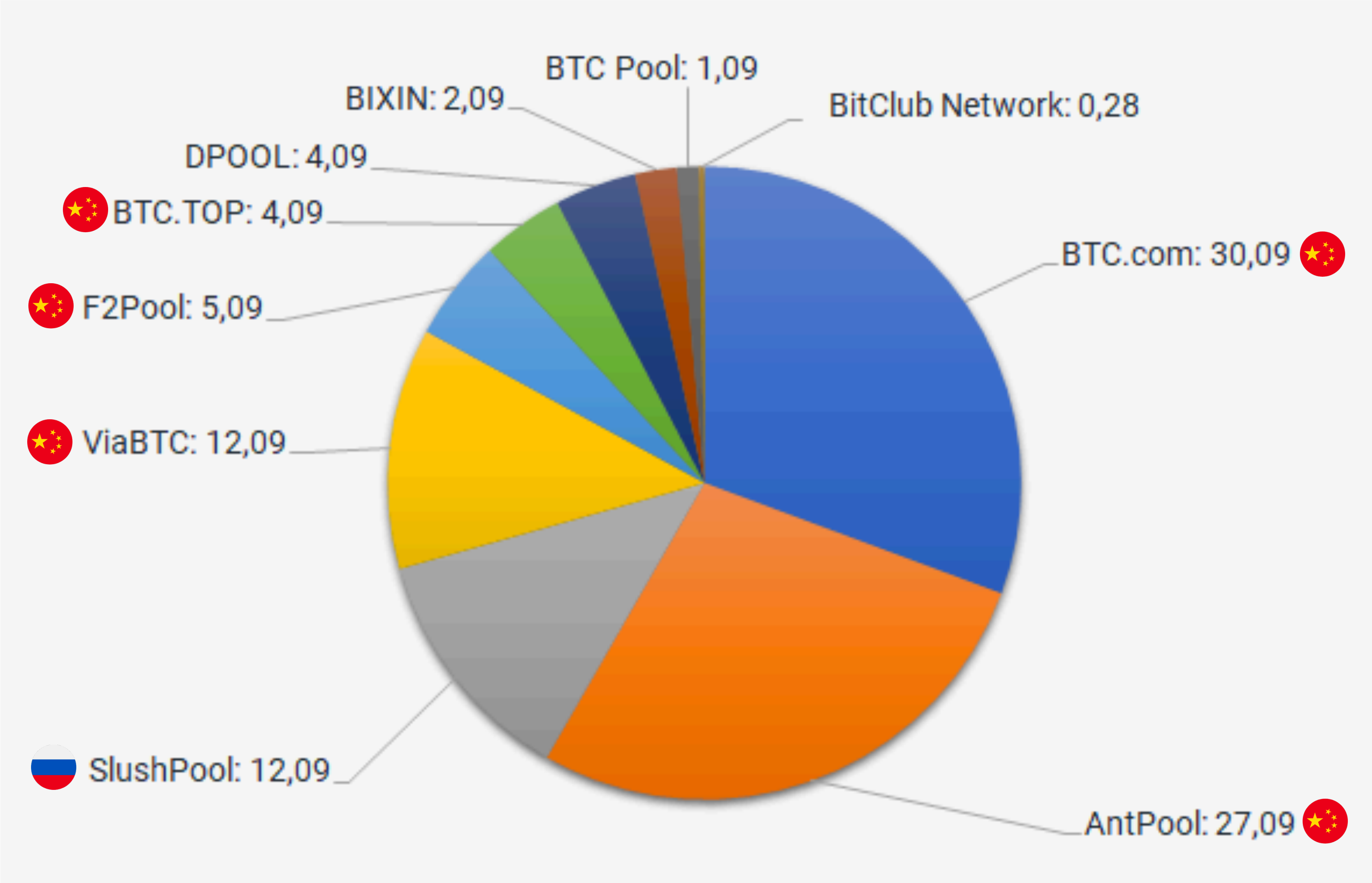
- unintended consequences
- opaque connection between process and outcome

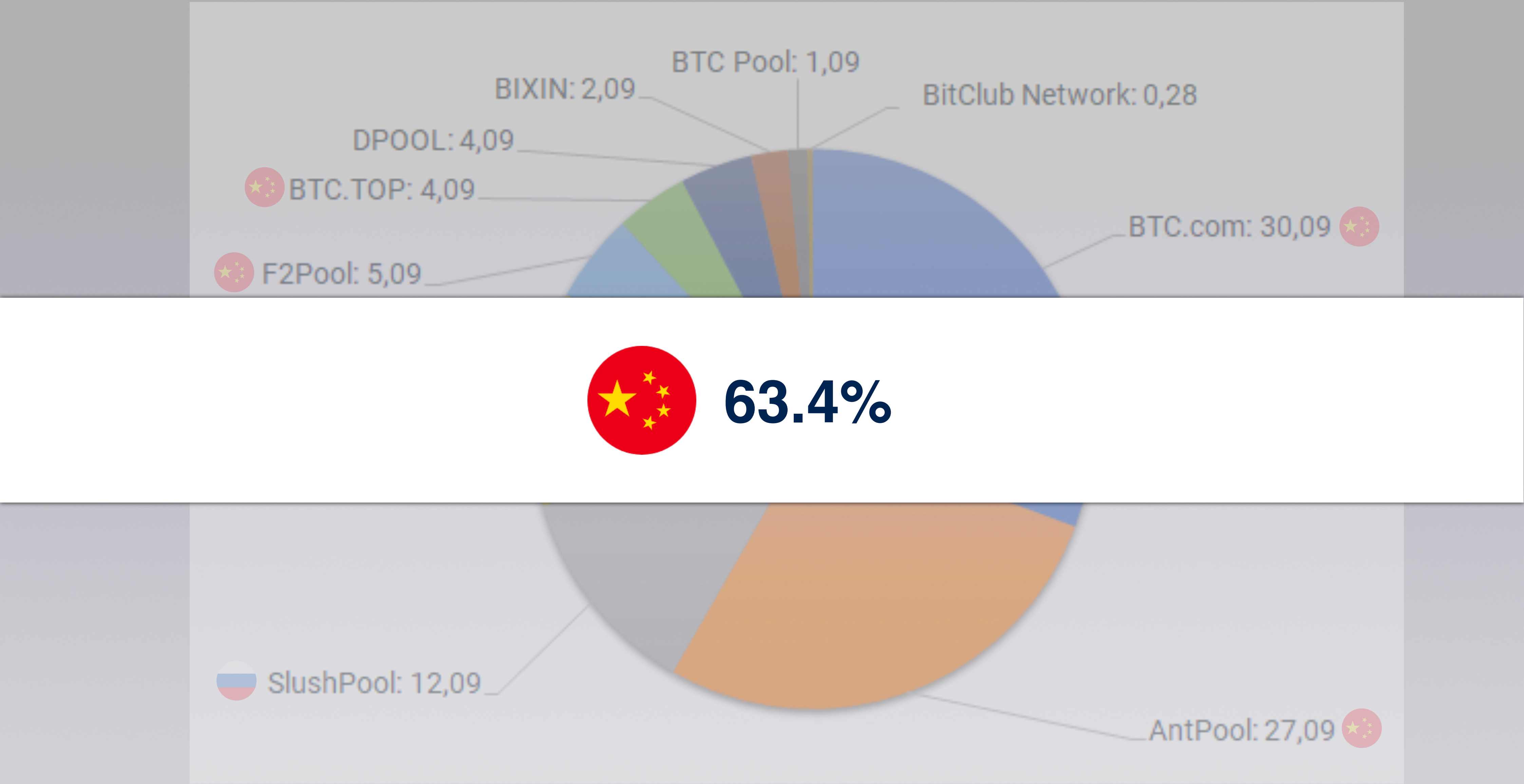


Lastly, wealth in the crypto universe is even more concentrated than it is in North Korea.

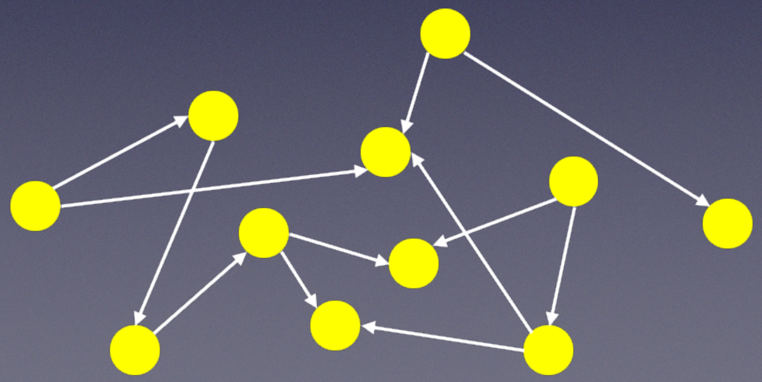
Gini(USA) = 0.41
Gini(N. Korea) = 0.86
Gini(Bitcoin) = 0.88

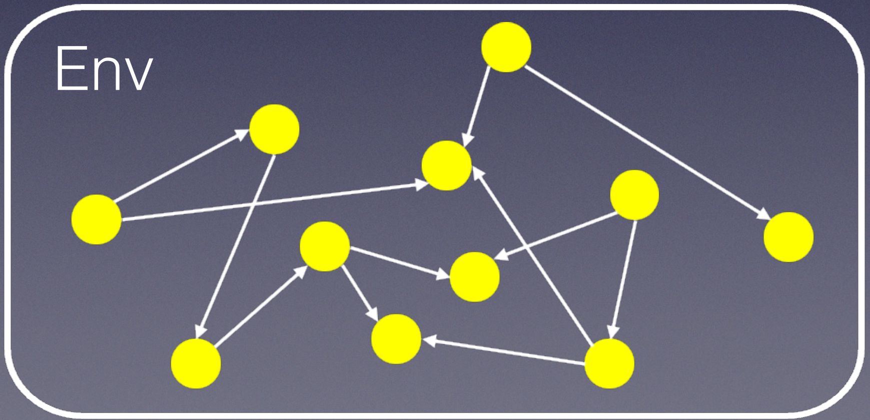

BTC Pool: 1,09
BIXIN: 2,09
BitClub Network: 0,28
DPOOL: 4,09
BTC.TOP: 4,09
BTC.com: 30,09
F2Pool: 5,09
ViaBTC: 12,09
SlushPool: 12,09
AntPool: 27,09

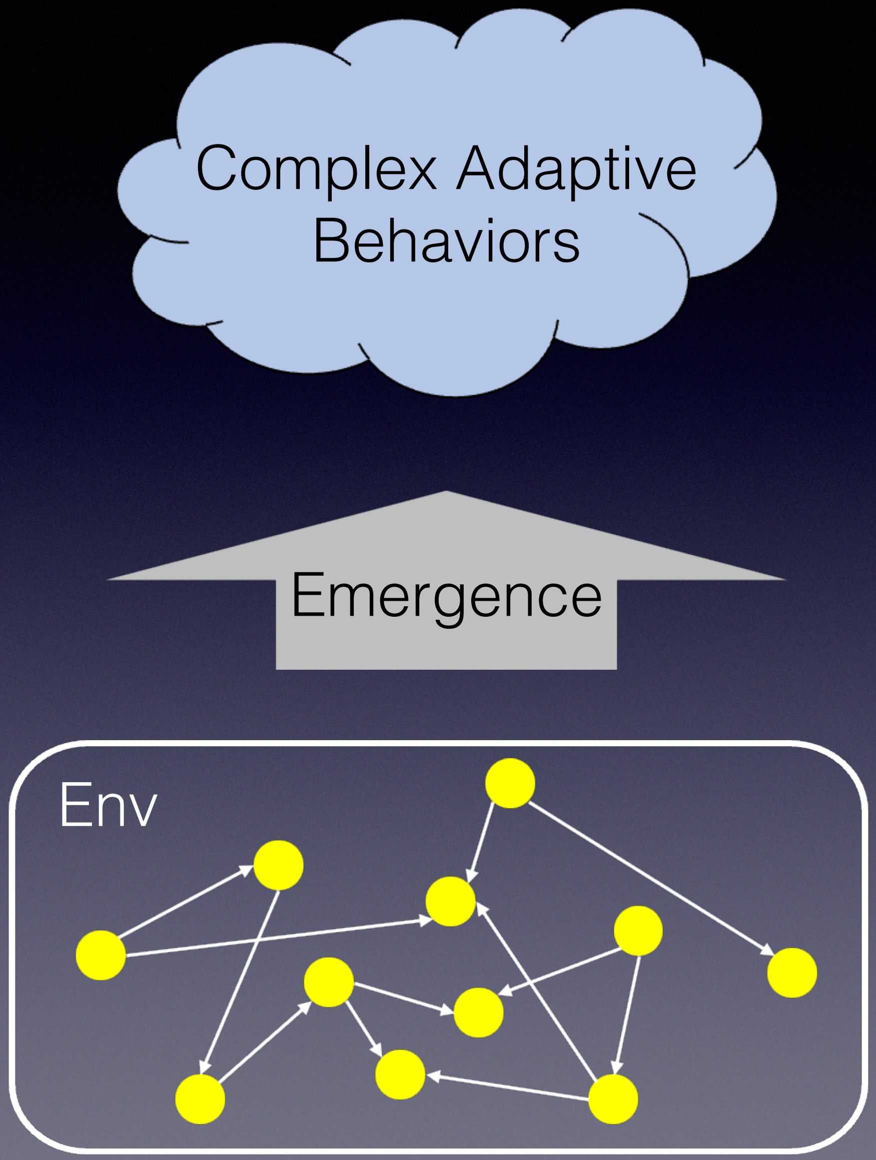

BTC Pool: 1,09
BIXIN: 2,09
BitClub Network: 0,28
DPOOL: 4,09
BTC.TOP: 4,09
BTC.com: 30,09
F2Pool: 5,09
ViaBTC: 12,09
SlushPool: 12,09
AntPool: 27,09

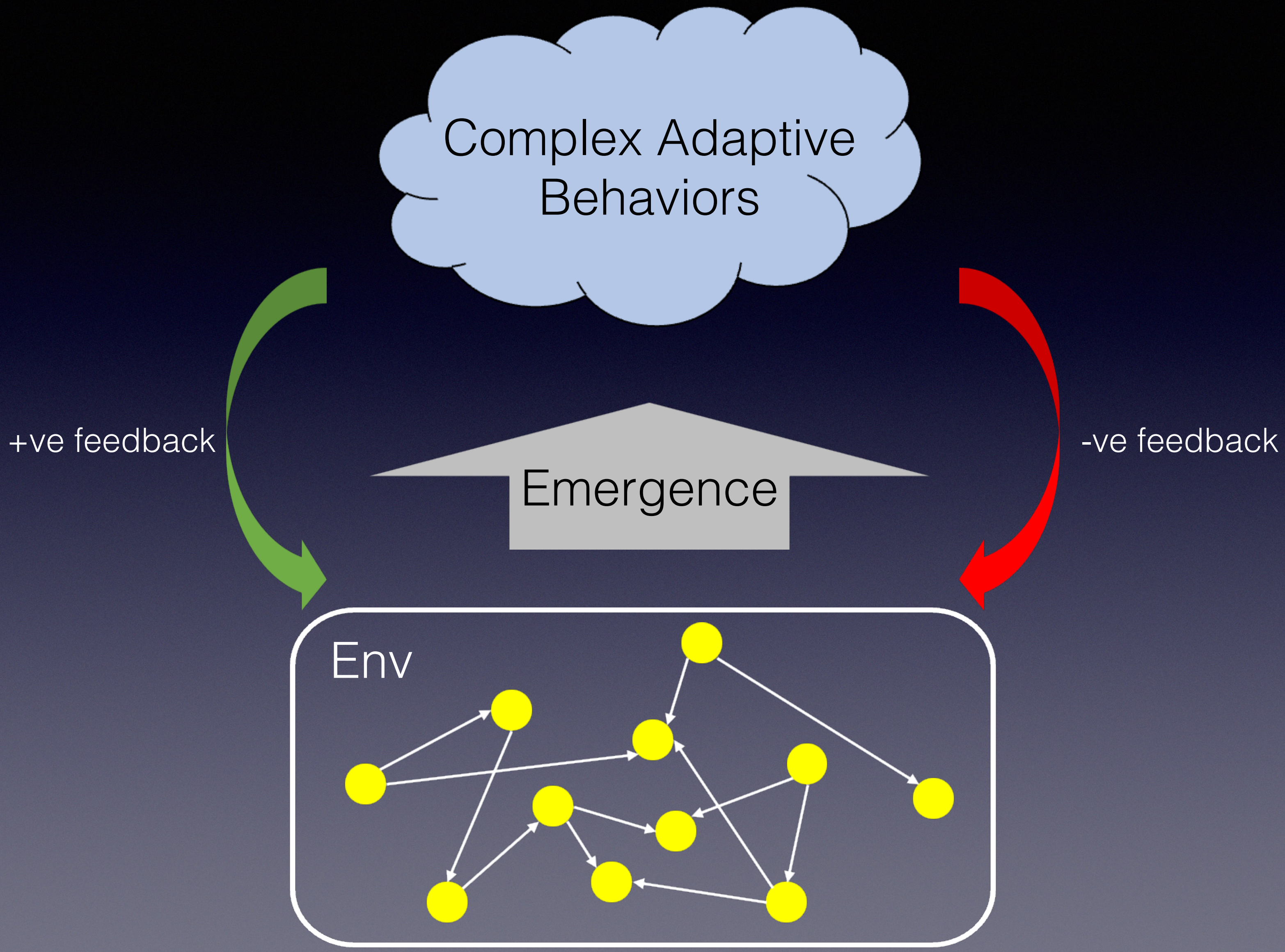

BTC Pool: 1,09
BIXIN: 2,09
BitClub Network: 0,28
DPOOL: 4,09
BTC.TOP: 4,09
BTC.com: 30,09
F2Pool: 5,09
63.4%
SlushPool: 12,09
AntPool: 27,09

Complex Adaptive Systems (CAS)
/
Agent-based Modeling



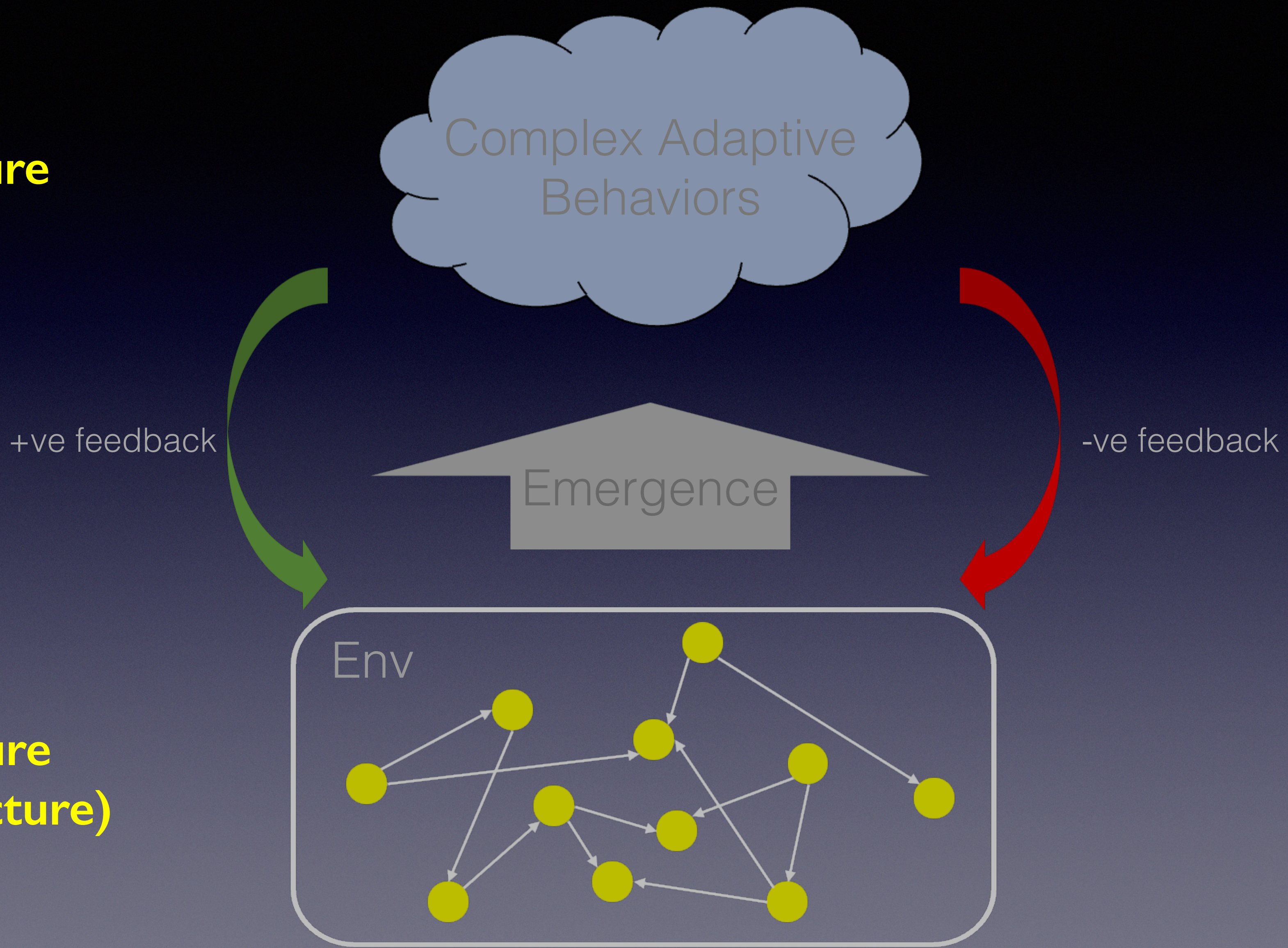

Env


Complex Adaptive Behaviors
Emergence
Env


Complex Adaptive Behaviors
+ve feedback
Emergence
-ve feedback
Env

Observed Structure

Elemental Structure
(Generative Structure)



Complex Adaptive Systems (CAS)

CAS Structure	CAS Component	CAS Component Elements	
Generative structure (unobserved)	Model Rule	The behavioral logic of the model specified at the model level	
Elemental structure (micro-level)	Agent	Identity	
		Attributes	
		Behavioral Rules	
	Interaction	Connection	
		Flow	
	Environment	Initial conditions, model parameters and settings	
Observed structure (macro-level)	Emergent Property	Output observations at the system level	

Blockchain as CAS

CAS Structure	CAS Component	CAS Component Elements	Equivalence in Blockchain Governance
Generative structure (unobserved)	Model Rule	The behavioral logic of the model specified at the model level	Consensus mechanism as an algorithm for choosing validator nodes
Elemental structure (micro-level)	Agent	Identity	A public address that identifies nodes
		Attributes	Currency stake
		Behavioral Rules	Make a transaction
	Interaction	Connection	Transactions on the blockchain, fee paid to winning validator nodes
		Flow	Amount and volume of transactions between agents
	Environment	Initial conditions, model parameters and settings	Number of available validator nodes, initial distribution of stakes
Observed structure (macro-level)	Emergent Property	Output observations at the system level	Distribution of decision making power, structure of the validation network

Complex Adaptive Systems (CAS)
/
Agent-based Modeling

Design Theorizing

Complex Adaptive Systems (CAS)

/

Agent-based Modeling

Design Theorizing

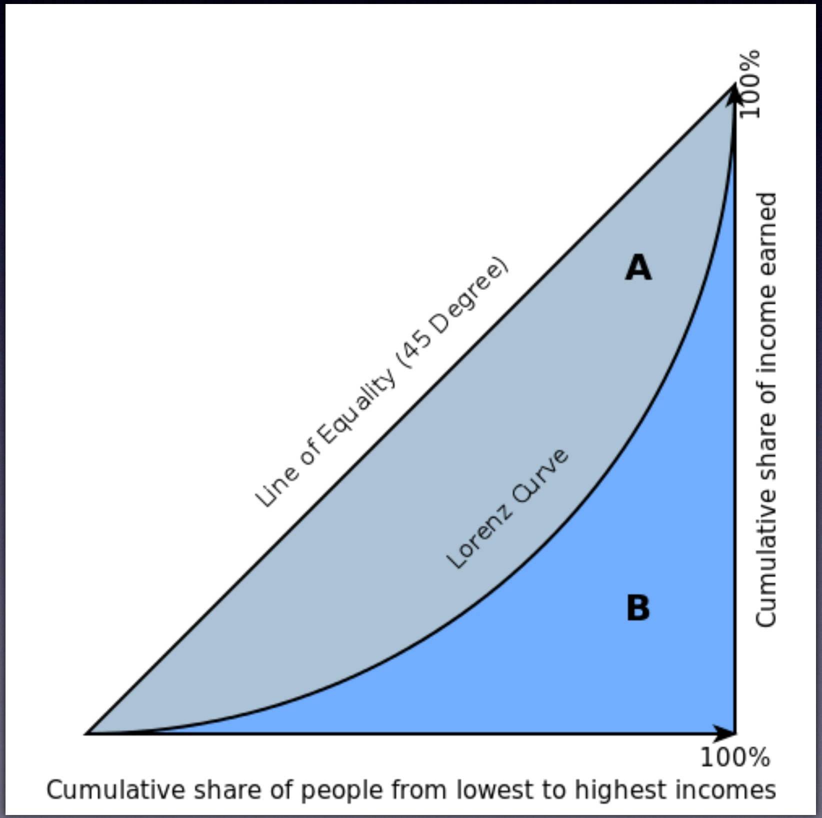
Agent-based model of PoS consensus mechanism

- Blockchain network consisting of A potential validator nodes
- Each agent a is assigned an initial currency balance b_a
- At each t, a random number V_t of transactions of size s_{at} ($< b_a$) between random pairs of nodes take places and a node is selected to be the validator; $s_{at} = 1$
- Likelihood of becoming the validator node depends on decision making power p_a which is proportional to b_{at}
- Validator node receives transaction fee F and is added to b_a

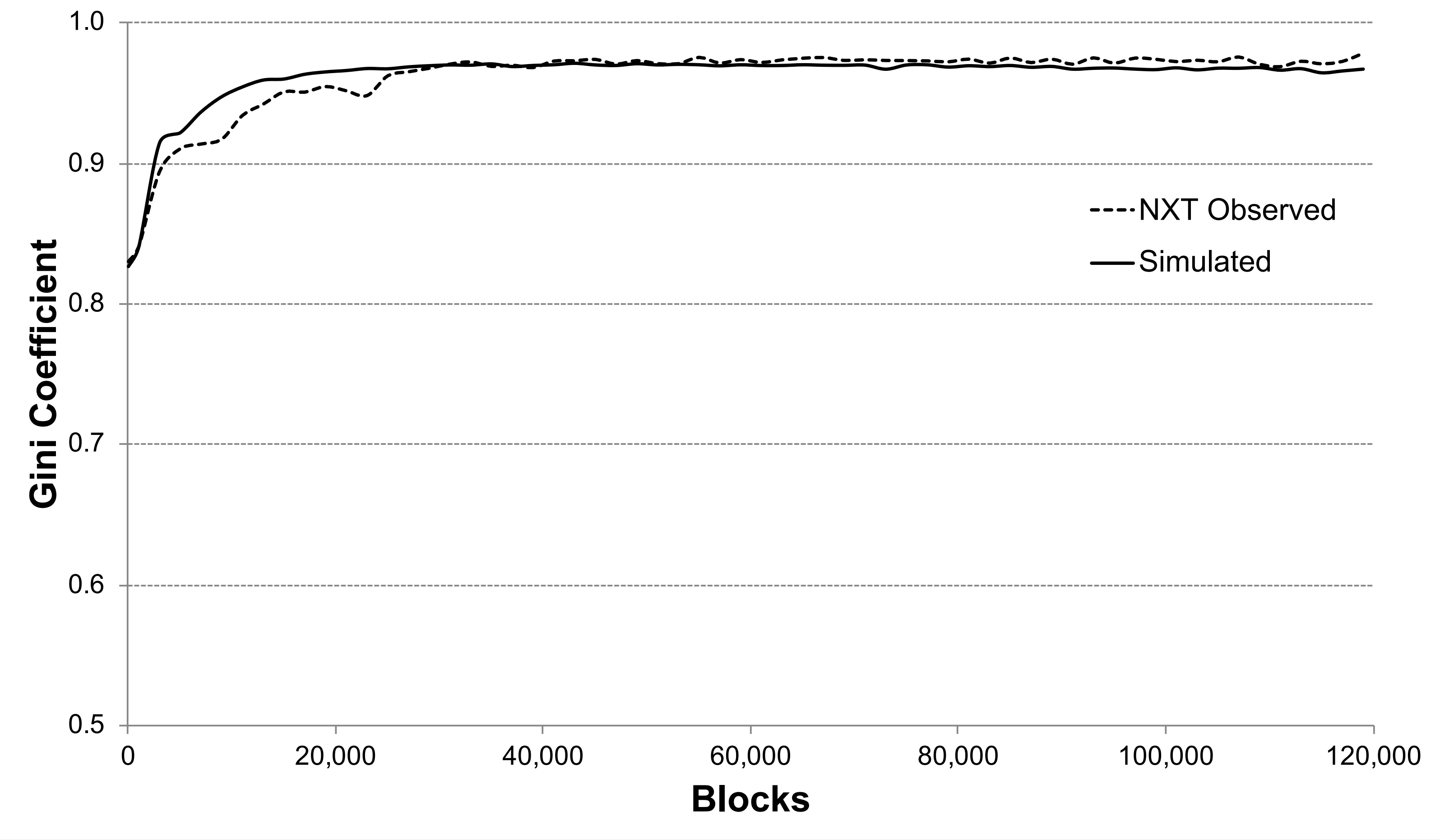
degree of (de)centralization

$$\text{Gini coefficient} = \frac{A}{A + B}$$

Gini = 0; no inequality; fully decentralized
Gini = 1; full inequality; fully centralized



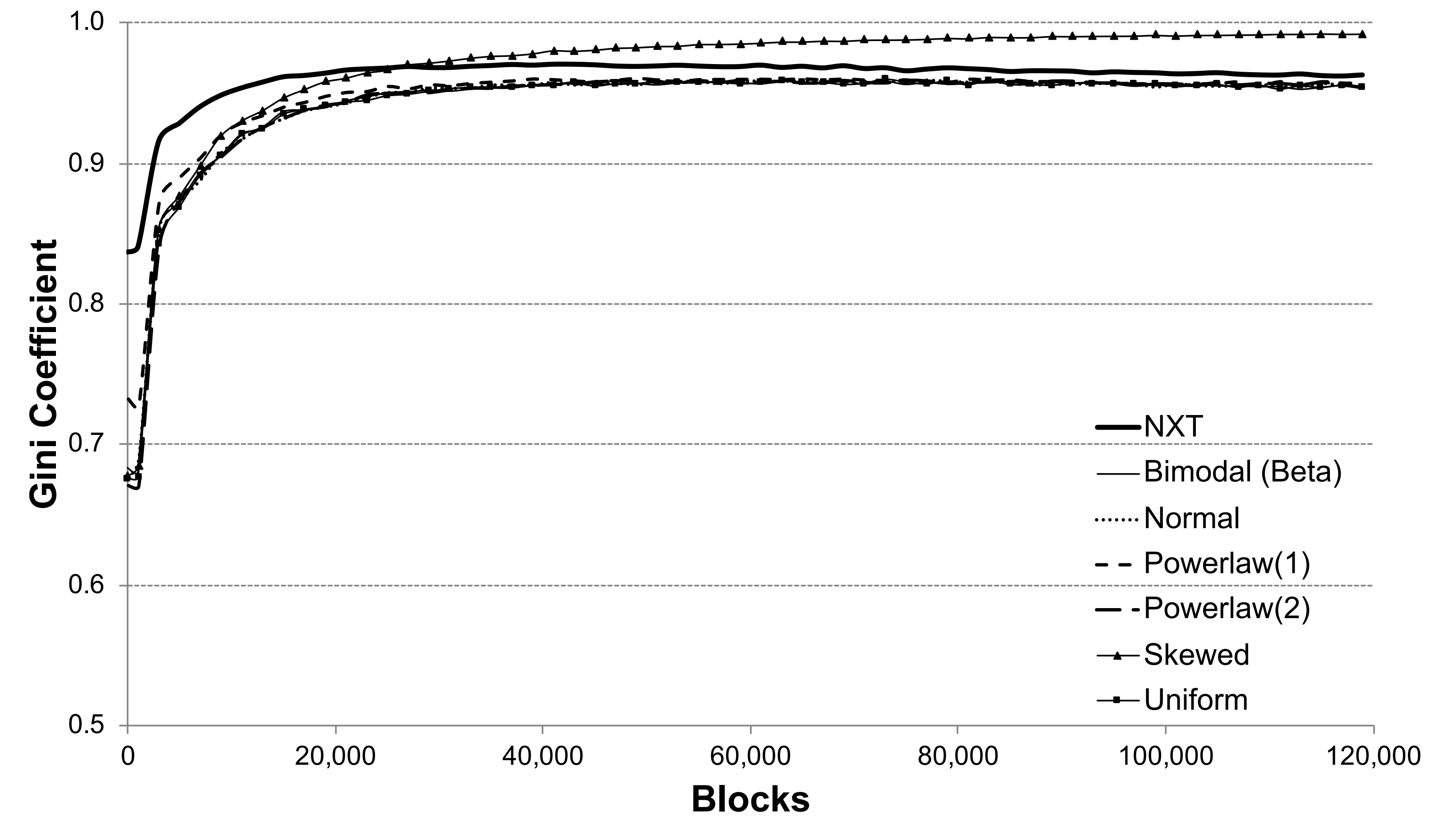
model validation



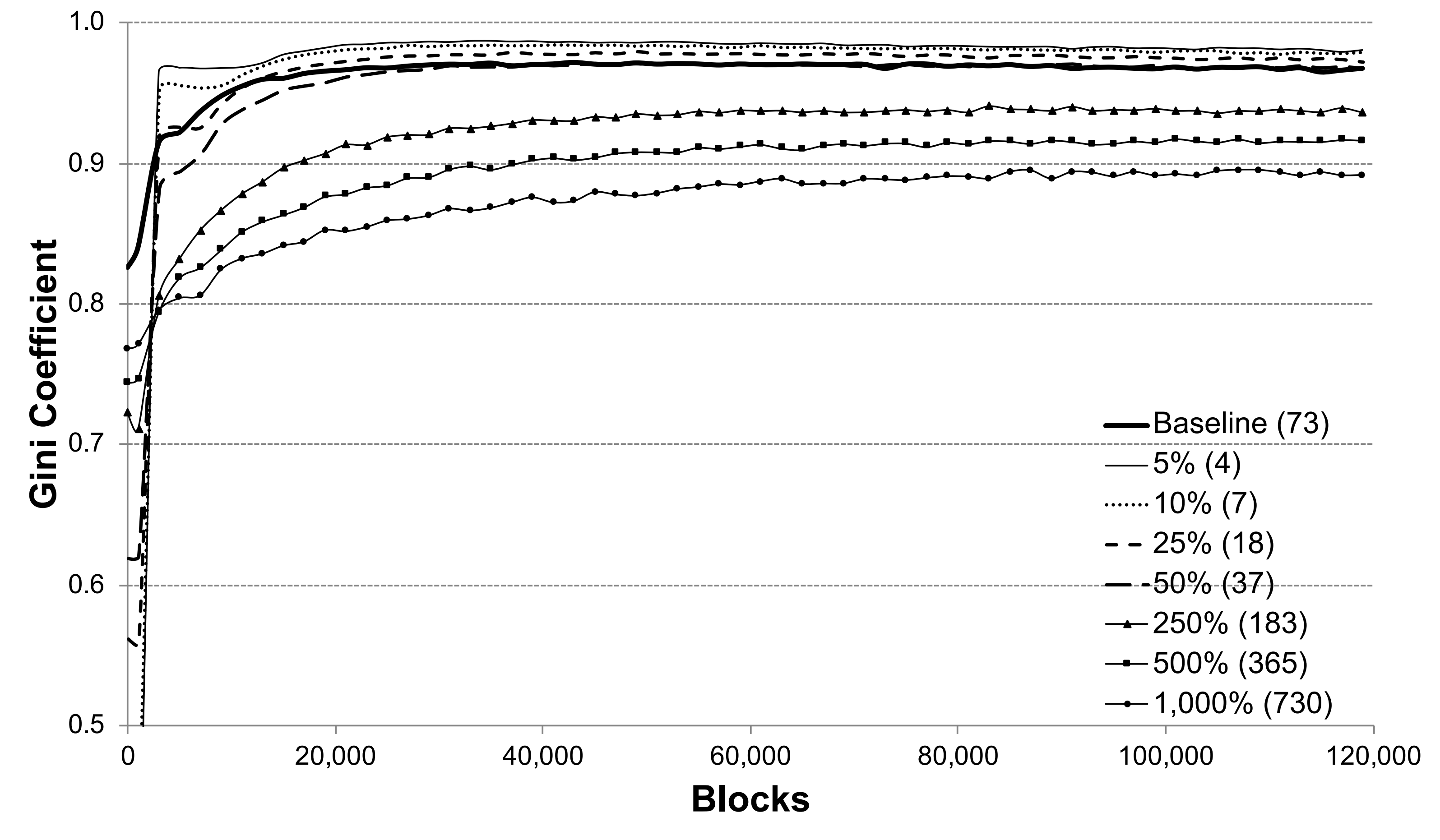
Simulation Experiments

	Parameter	Baseline	Experiments
Design Parameters	Initial Stake Distribution (*B*)	NXT Actual	N, Beta, Power-Law(2), U, Skewed
	Initial # of Validator Nodes (A_0)	73	5, 10, 25, 50, 250, 500, 1000% of NXT Actual
	Transaction Fee (*F*)	207	
Behavioral Parameters	Transaction Amount (*U*)	39,434	
	Transaction Volume (*V*)	2.54	
	Validator Network Growth (*G*)	0.0293	

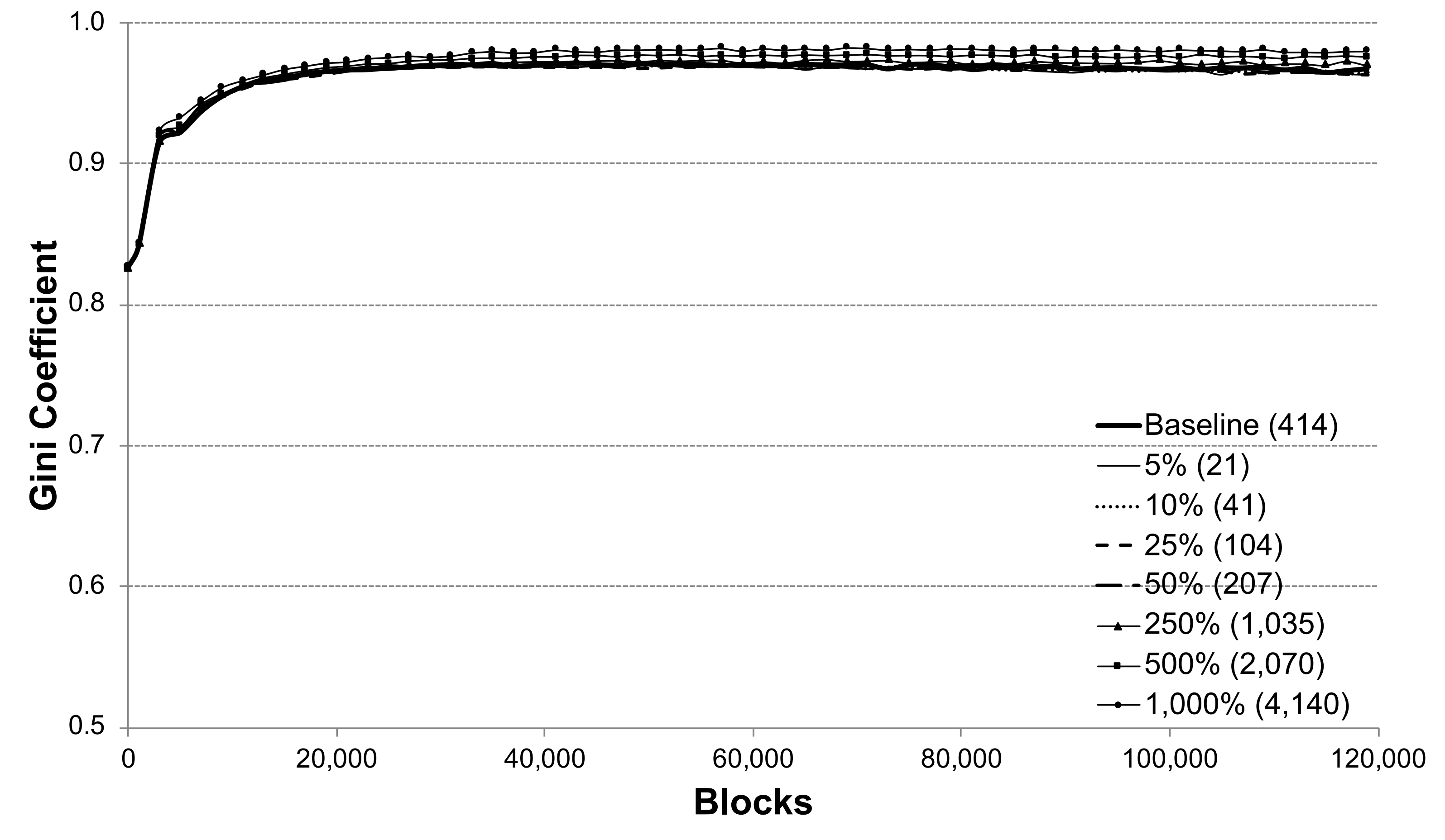
Initial stake distribution (*B*)



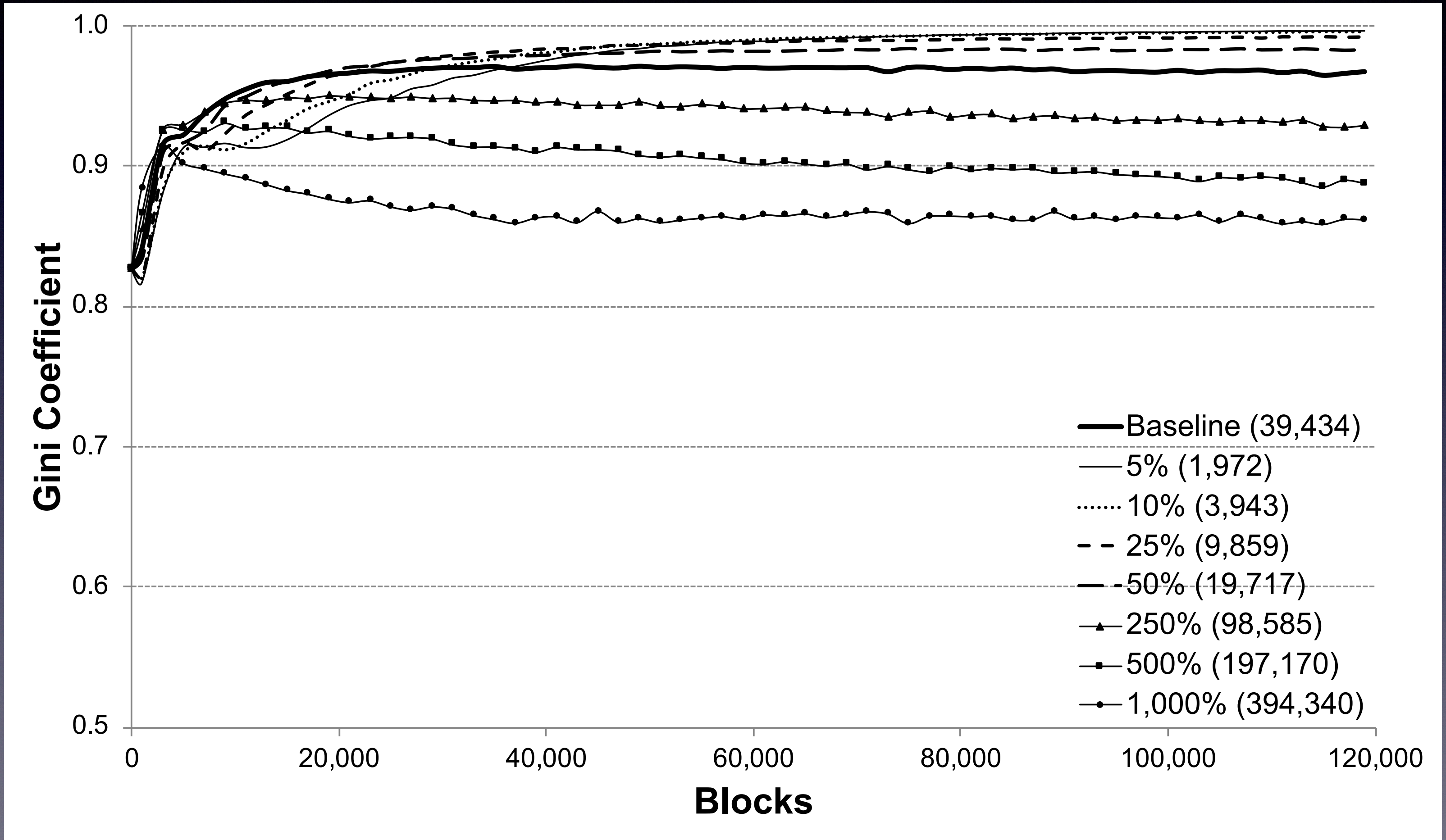
Initial validator nodes (A_0)



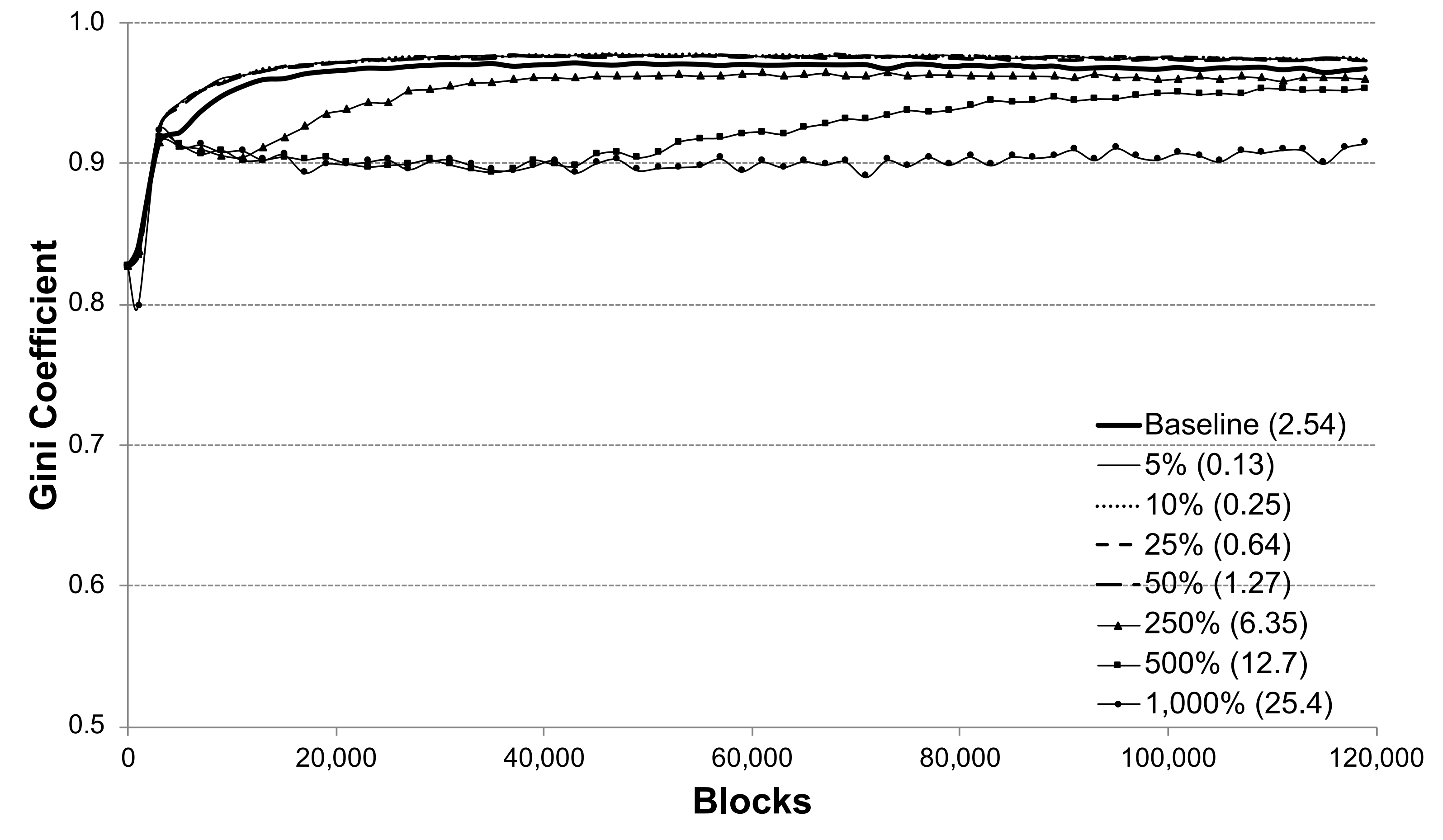
Transaction fee amount (*F*)



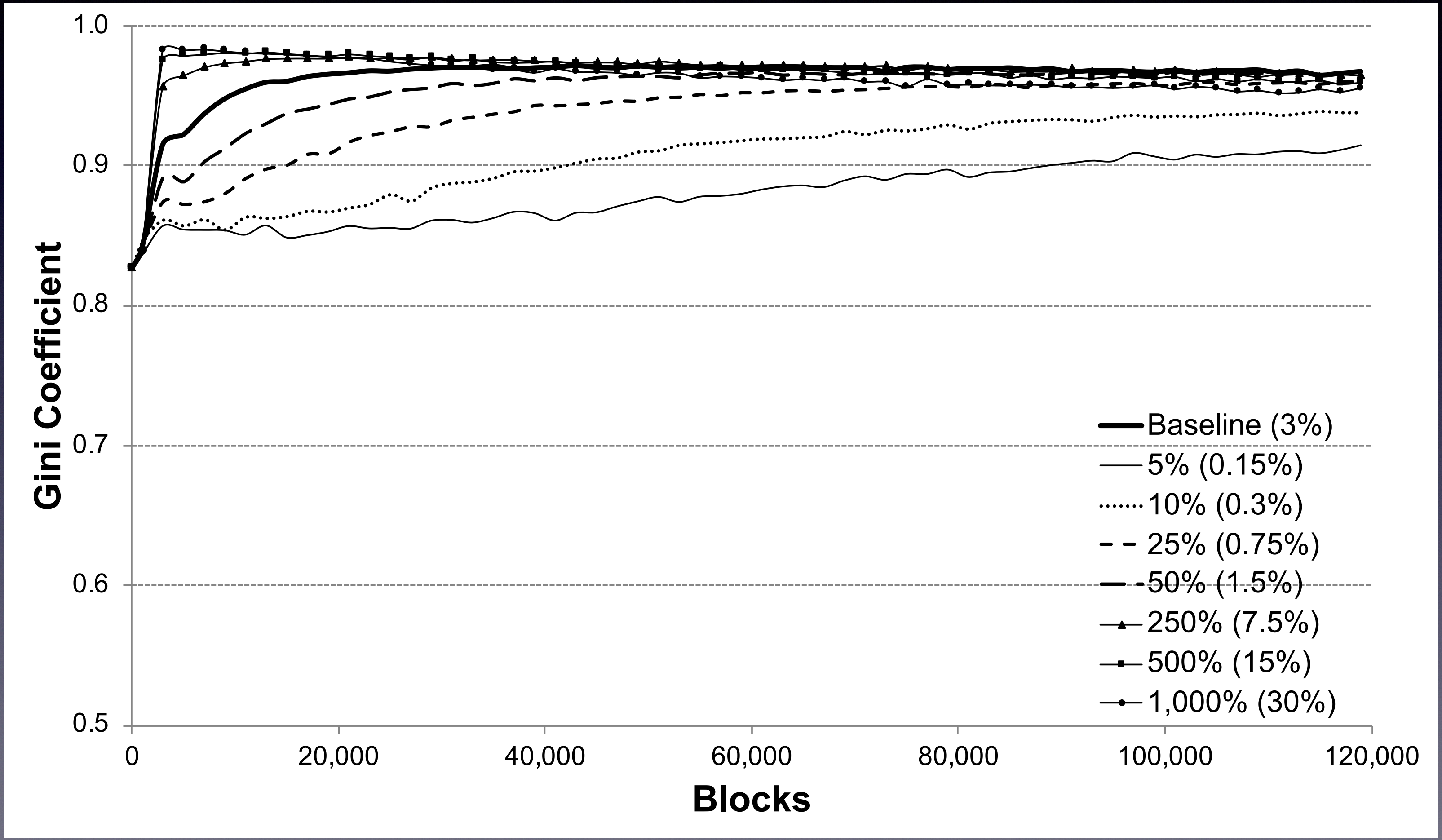
Transaction amount (*U*)



Transaction volume (*V*)



Validator network growth (*G*)



Statistical Validation

Variable	Coefficient	SE	*t*-value	*p*-value	Significance
Intercept	1.0309	0.0080	128.31	0.000	***
Bimodal	0.0003	0.0030	0.10	0.919	
Normal	0.0025	0.0030	0.82	0.411	
PowerLaw-1	0.0030	0.0030	0.96	0.337	
PowerLaw-2	0.0015	0.0030	0.48	0.635	
Skewed	0.0394	0.0030	12.77	0.000	***
Uniform	-0.0019	0.0030	-0.61	0.544	
$\ln(A_0)$	-0.0067	0.0006	-11.04	0.000	***
$\ln(F)$	0.0015	0.0006	2.49	0.013	*
$\ln(U)$	-0.0244	0.0006	-40.28	0.000	***
$\ln(V)$	-0.0082	0.0006	-13.52	0.000	***
$\ln(G)$	0.0451	0.0025	18.23	0.000	***
$\ln(G)^2$	-0.0052	0.0003	-18.05	0.000	***

$R^2 = 0.729$

Significance: *** $p<0.001$, ** $p<0.01$, * $p<0.05$

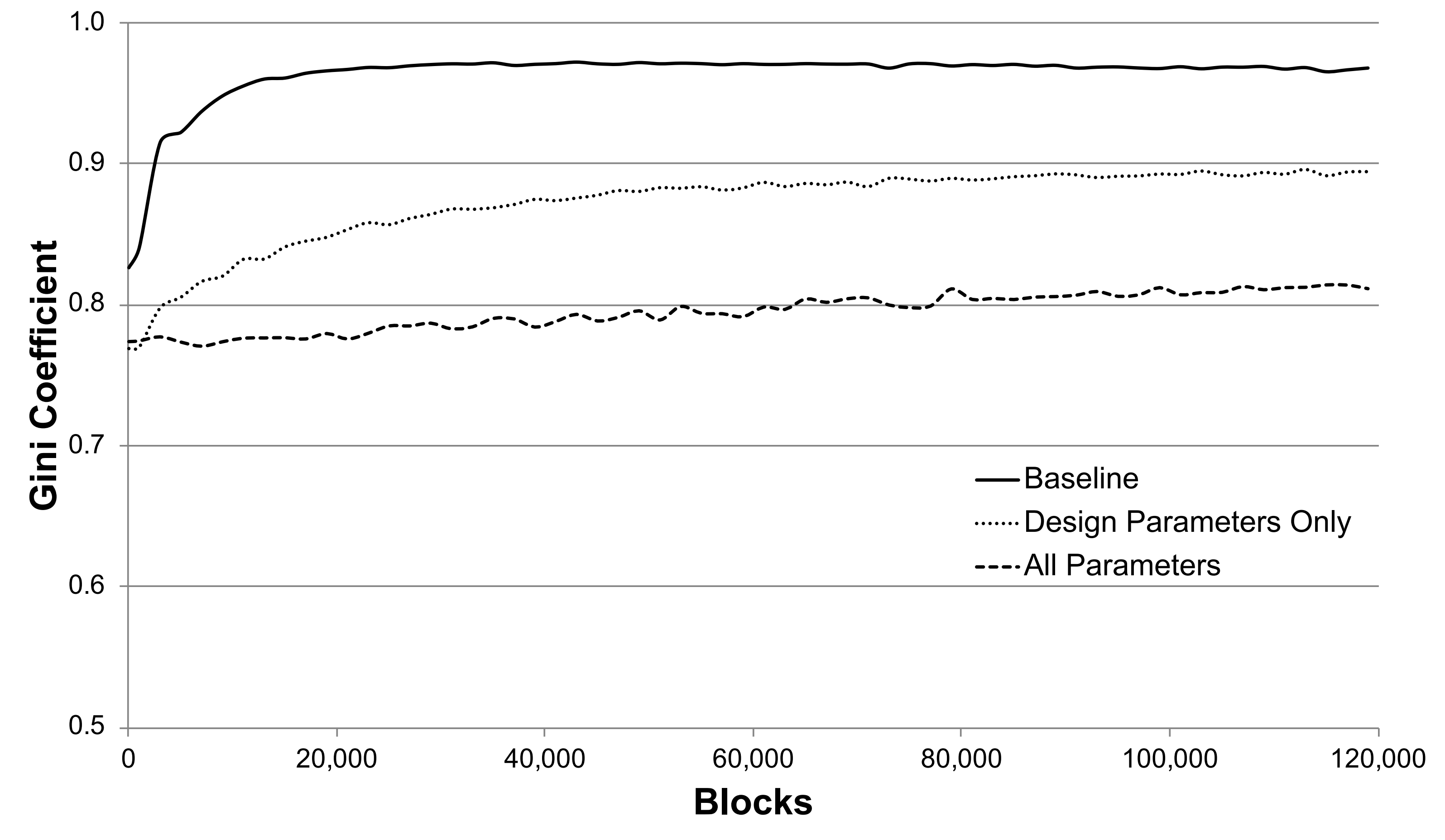
Notes: The dependent variable is the Gini coefficient, where higher values represent greater centralization and lower values represent greater decentralization. Therefore, coefficients that are negative are interpreted as increasing decentralization of decision-making power.

Summary:
A Design Theory of PoS Blockchains

Parameters	Greater decentralization with …
Initial Stake Distribution (*B*)	No impact of initial distribution, except when skewed
Initial Network Size (A_0)	Larger initial networks
Transaction Fee (*F*)	Smaller transaction fees (marginal)
Transaction Amount (*U*)	Larger average transaction amounts
Transaction Volume (*V*)	Larger transaction volumes
Validator Network Growth (*G*)	Very slow or very fast growth rates

Scenario testing

maximal decentralization scenario

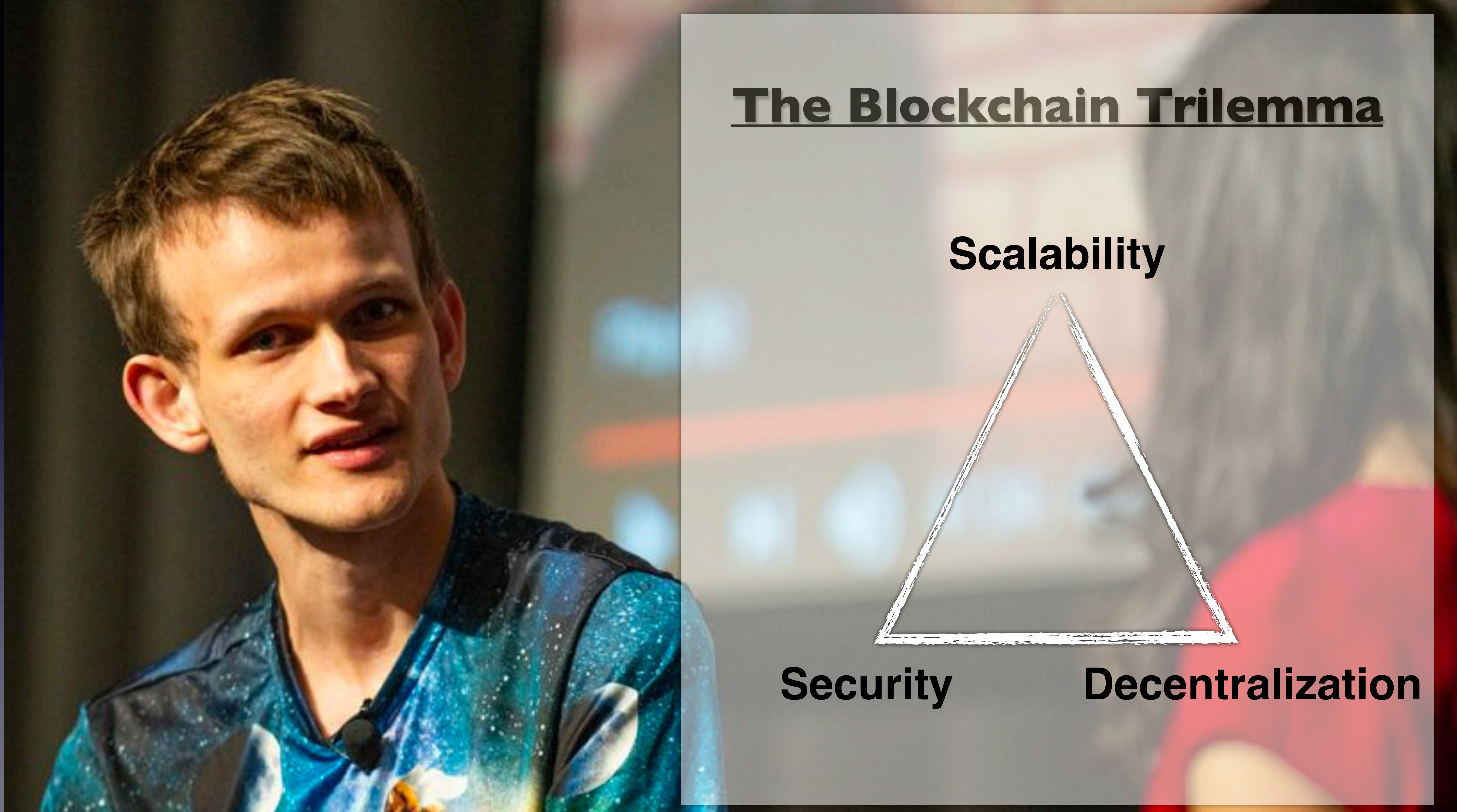


Conclusions / Contributions

- Well-intentioned designs of algorithmic governance may lead to unexpected (undesirable) outcomes

Conclusions / Contributions

- Well-intentioned designs of algorithmic governance may lead to unexpected (undesirable) outcomes
- Design theory of PoS consensus mechanism design for Blockchain networks
  - Identify model parameters (initial validator network, transaction fees) that are likely to lead to (un)desirable levels of decentralisation
  - Identify behavioural parameters (transaction volume, amount, validator nework growth) that are likely to lead to (un)desirable levels of decentralisation


The Blockchain Trilemma
Scalability
Security
Decentralization

Conclusions / Contributions

- Well-intentioned designs of algorithmic governance may lead to unexpected (undesirable) outcomes
- Design theory of PoS consensus mechanism design for Blockchain networks
  - Identify model parameters (initial validator network, transaction fees) that are likely to lead to (un)desirable levels of decentralisation
  - Identify behavioural parameters (transaction volume, amount, validator nework growth) that are likely to lead to (un)desirable levels of decentralisation
- CAS and agent-based modeling as a useful design theory building tool for algorithm-mediated decision making

Limitations and Future Work

- What are "acceptable" and/or "critical" levels of (de)centralization
- Study interaction effects of model and behavioral parameters
- Other consensus mechanisms? (e.g., variants of PoS, PoW, PoA)
- Endogenize behaviors / parameters