Objective Functions

Making the Subjective, Objective

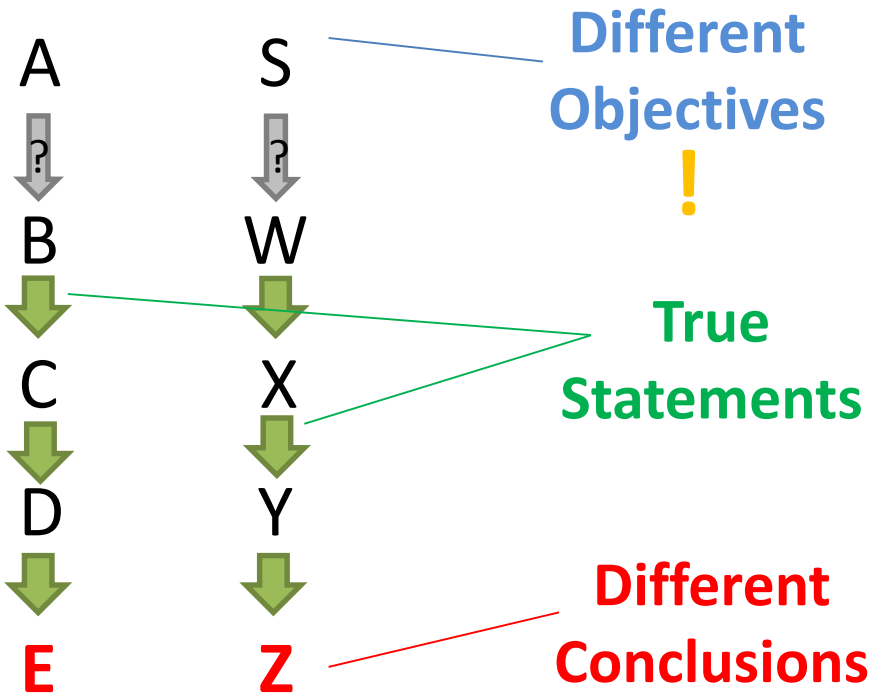
Paul Sztorc
truthcoin.info
Yale Econ Department
September 13th, 2015

Agenda

1. Emergency **discussion assistance** (2 Slide)
2. Can we **measure decentralization** (with a number)? (3 Slides)
3. **P2P Governance** / Measuring Bitcoin's Objective(s) (18 slides)

Principles of Discourse

- Without an **agreed OF** , all conversation is **meaningless**.
- If reasoning is tied to **objective principle**, conclusion will always be true.



Flowchart

Has speaker stated ***what they believe the blocksize does for Bitcoin***?

No

(Believe it or not) impossible to tell if speaker's reasoning is *even related* to "Improving Bitcoin".

Yes

Has speaker stated ***conditions under which blocksize should decrease?***

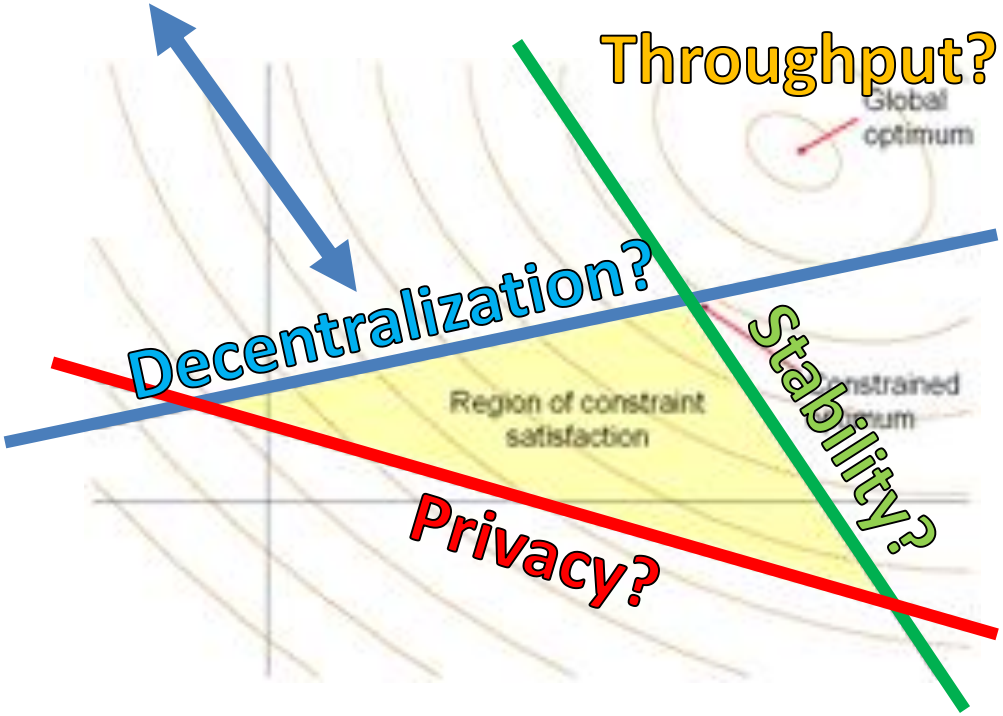
No

(Believe it or not) speaker hasn't expressed a thought related to *increasing* blocksize, either.

Yes

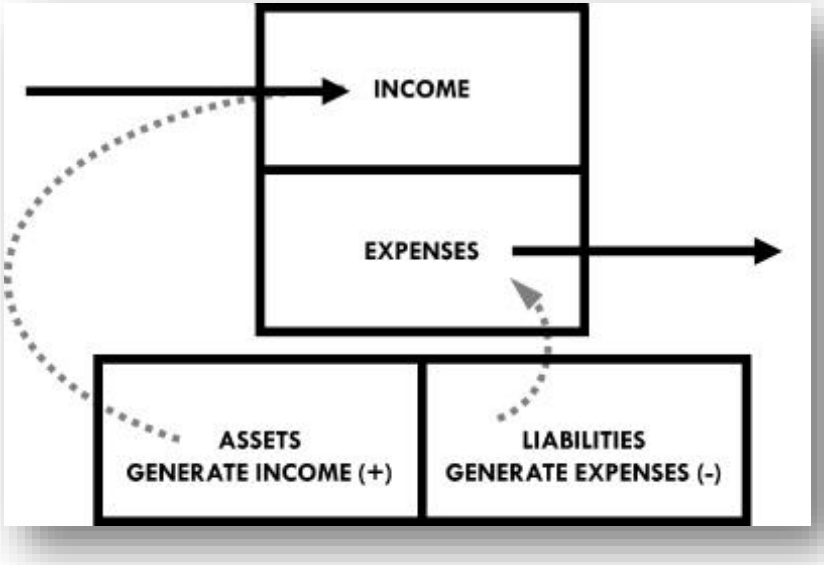
Measuring Decentralization (3 Slides)

- "Not agreeing on an objective function"?
- Almost as bad: "not agreeing on a constraint".
- "Decentralized Payments"
  - What is "Payments"?
  - What is "Decentralized"?

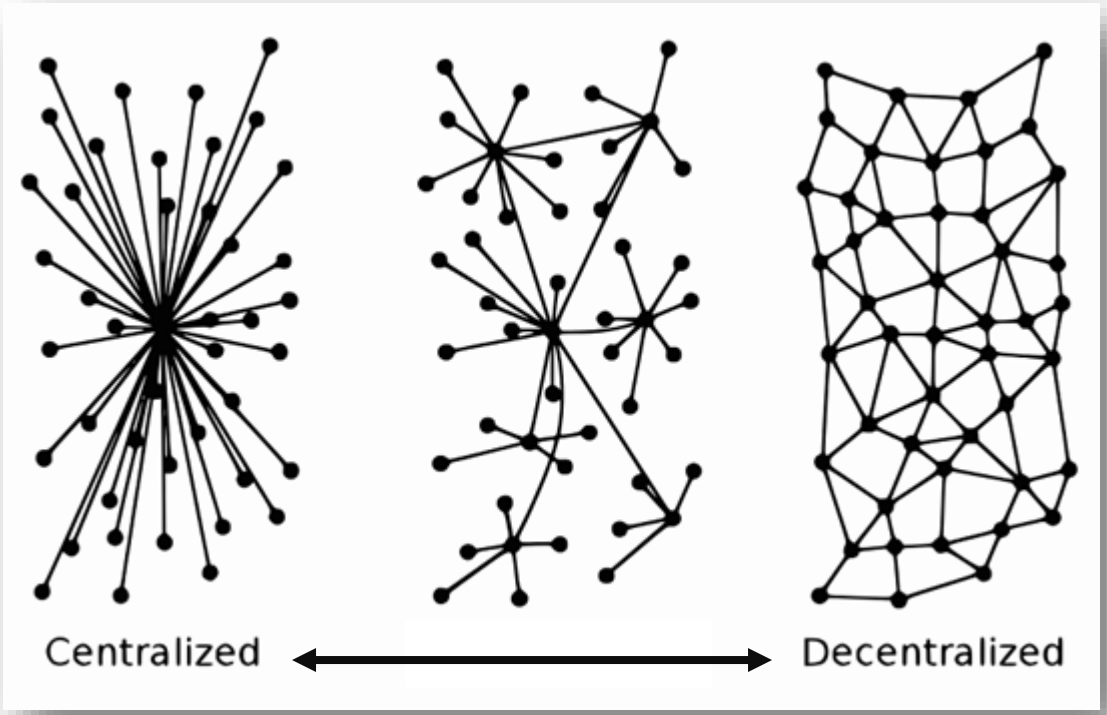


Money

- Abstraction of “favors”.
  - “Know you’ve gotten ‘credit’ for your favor”.
  - “Convince trading-partner they’ll get ‘credit’ for their favor.”
  - Those ^ ^ are actually mirrors (the same).
- We need the system to show us “we’ve been paid”. (“Paid” = finality).

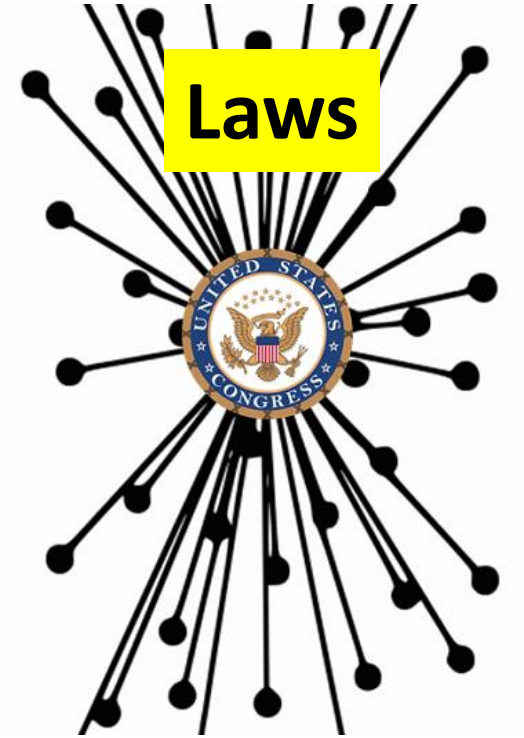


When is Money Decentralized?



Who knows ("decides") who's been paid?
1 person ---------- "Everyone"

Who *can or can't* know?
(Who can afford to *run a full node*?)



Privacy constraint: tor bandwidth.

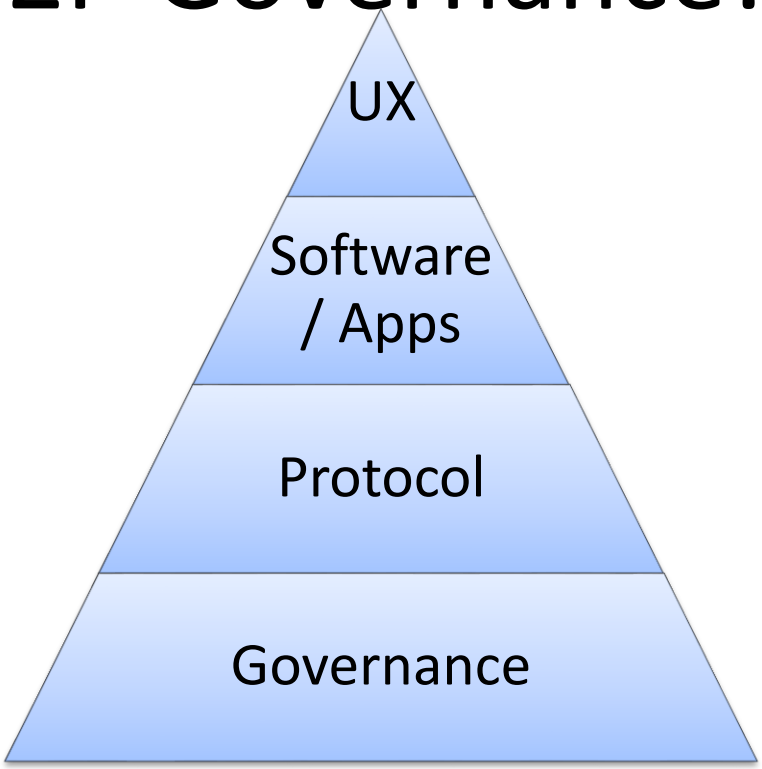
Tor Metering with Bitcoin:

1. Be able to measure decent.
2. Vastly improve decent.
3. (Improve all upstream bandwidth)

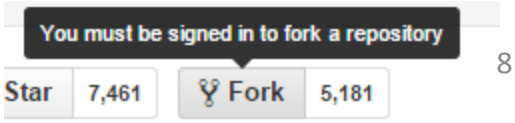
A P2P System *needs* P2P Governance!

18 slides

- Governance > Software
  - Can *break* software rules!
    - Privacy?
    - 21 million coin limit.
  - Can *allow* Bitcoin to become obsolete!
  - Bitcoin's weakest link (?)
  - LR Scaling? Likely only gov.



- But How to Govern?
  - Trade-offs: Censorship vs Spam, Coercion vs Sybil, Groupthink vs Review-Cycle Burnout. (As hard as BTC ?)
  - "Experts?", Who chose them? "Who watches the watchers?" (vs. Foolish non-experts). Excluded people.
- **No one has ever done this before.**



Markets: Proof of Expertise

WIKIPEDIA
The Free Encyclopedia

Article Talk | Read Edit View history | Search

Economic calculation problem

From Wikipedia, the free encyclopedia

The **economic calculation problem** is a criticism of using economic planning as a substitute for market-based allocation of the factors of production. It was first proposed by Ludwig von Mises in

Main page
Contents
Featured content
Current events
Random article
Donate to Wik
Wikipedia stor
Interaction
Help

Part of a series on the
Austrian School
Principal works [show]
[show]
[show]
[show]
[show]
portal
V • T • E

Price System: how individual subjective values are translated into the objective information necessary for rational allocation of resources in society.

In market exchanges, prices reflect the supply and demand of

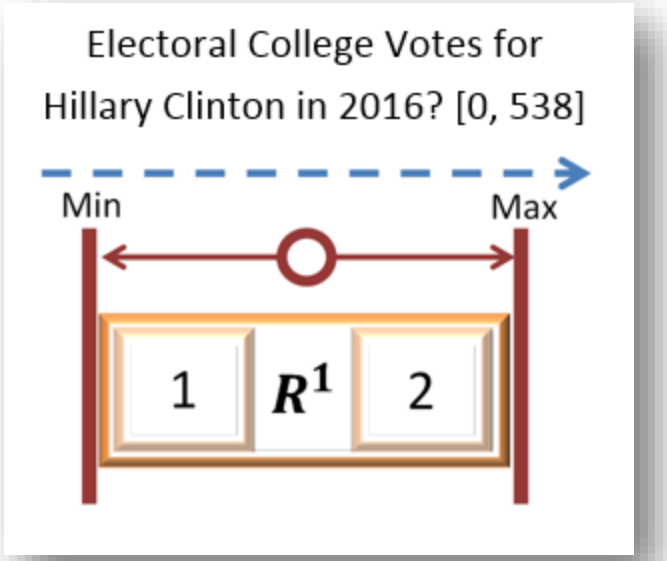
Trades:

1. Knowledge and meta-knowledge (#1).
2. **Constantly** and **unanimously** acceptable.
3. Prices are **common knowledge**.

Succinct, easily-verifiable "expertise proof".

Event Derivatives ("Prediction Markets")

(Only) one of these pays $1



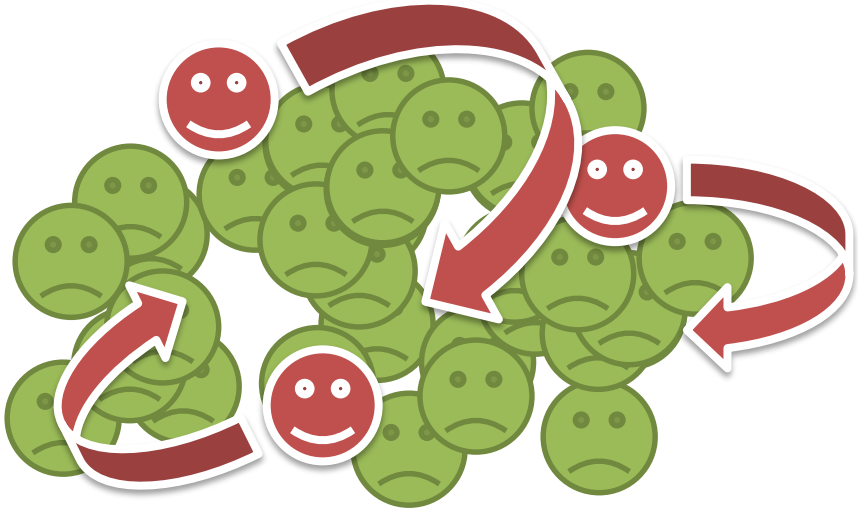
Splits a dollar and pays it proportionally.

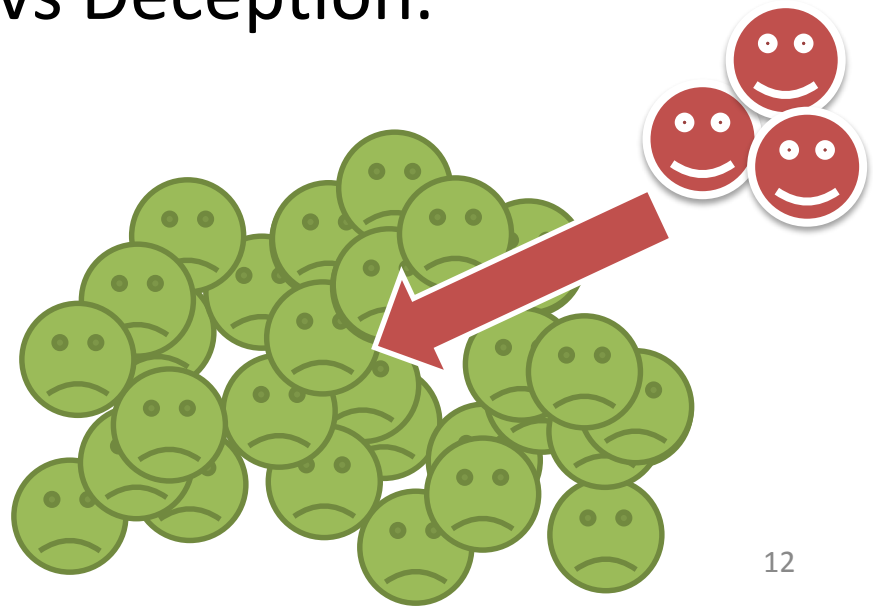
Prediction Markets: The Costs

1. **Oracle**
    1. …exactly once, we are going to need to have [easy-to-find] data be reported, honestly.
    2. OF reported…*after the fact*. (Not during.)
2. **Market Infrastructure**
3. **Traders**
    1. …to be interested enough.

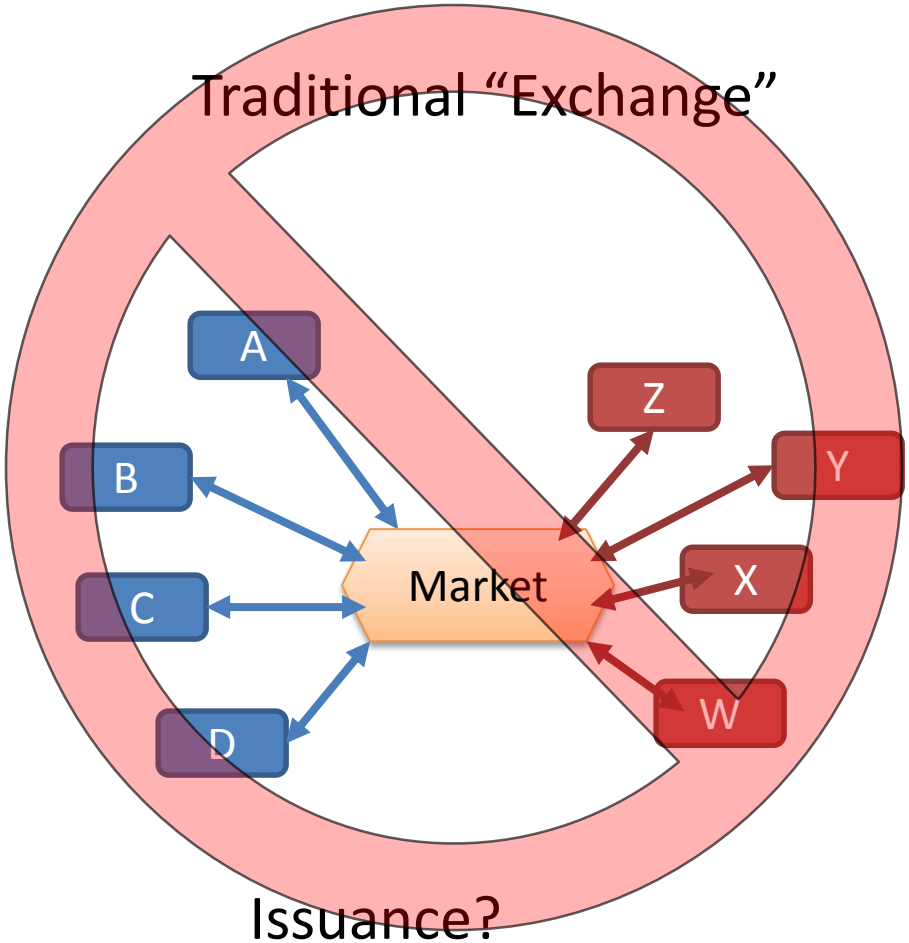
Worst News 1st: The Oracle

- Truthcoin (experimental, requires pegged sidechains)
- Federated Sidechain / Multisig Functionaries
  - People who own a lot of Bitcoin.
  - Bitcoin co's we plan to do business with.
- Trade-off: "Experts" (circular !) vs Representatives.
- Trade-off: Meta-Deception vs Deception.

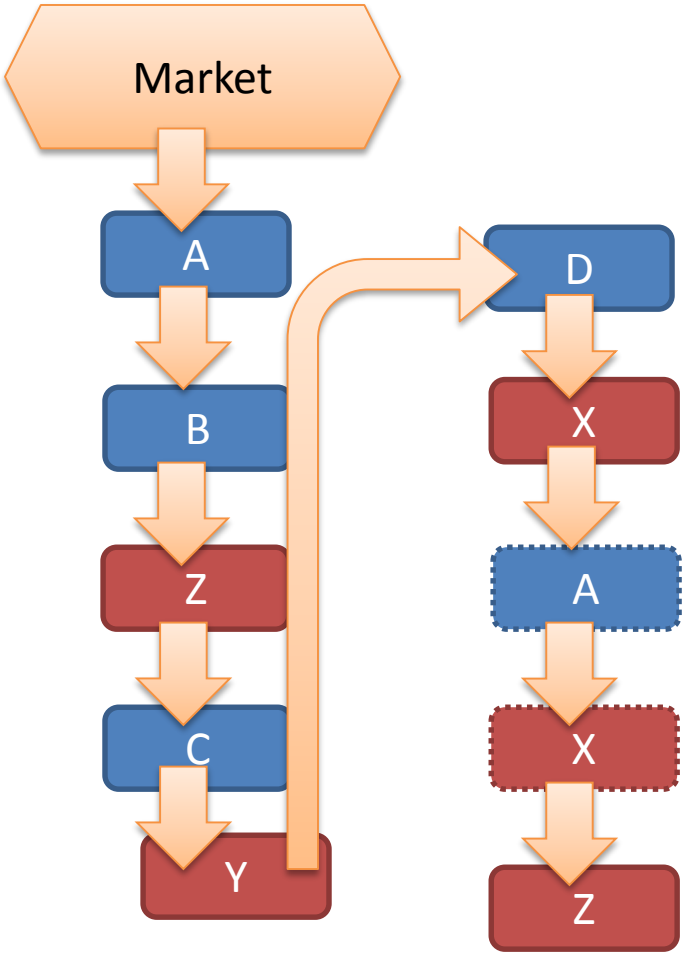




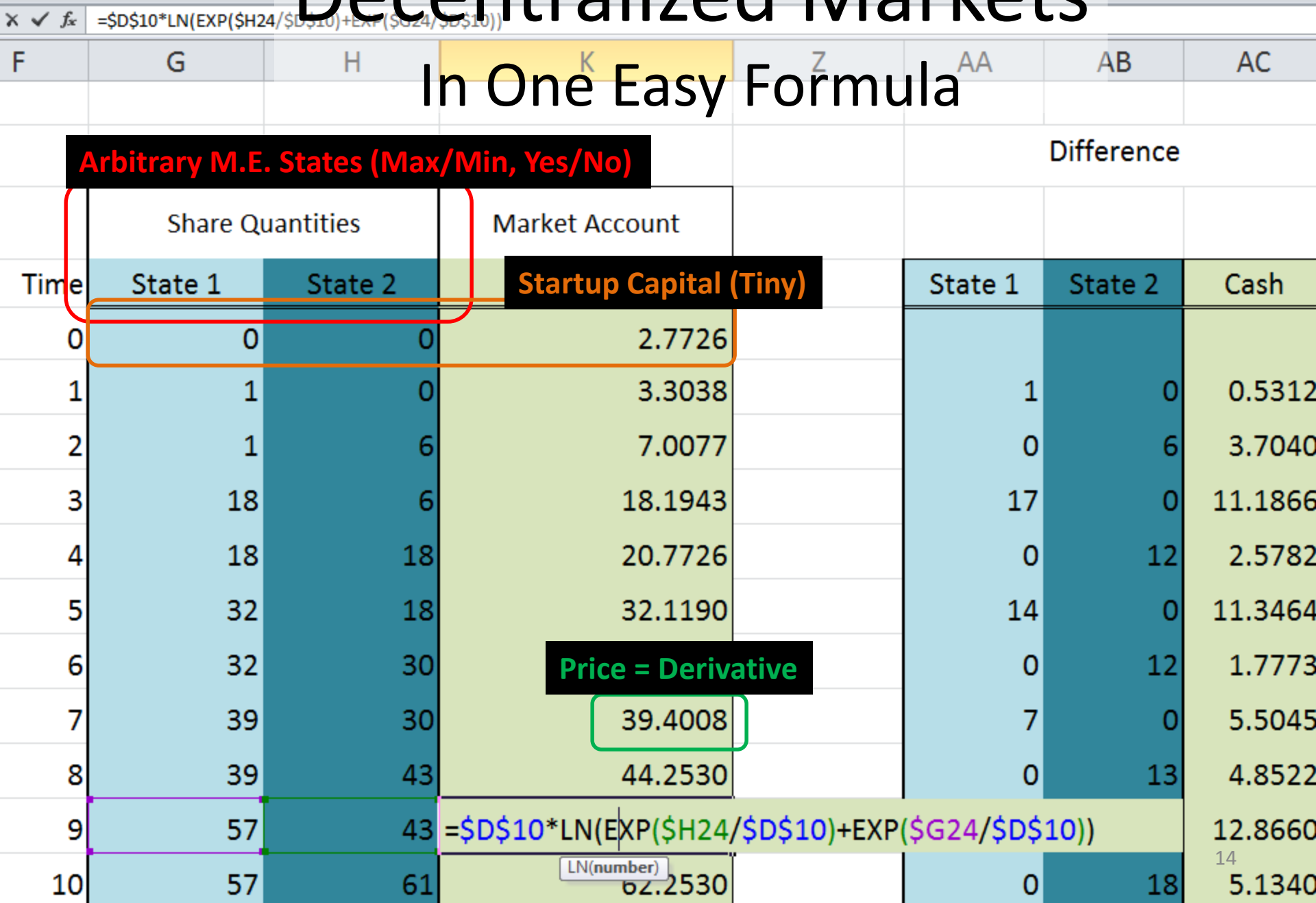
2. Market Infrastructure



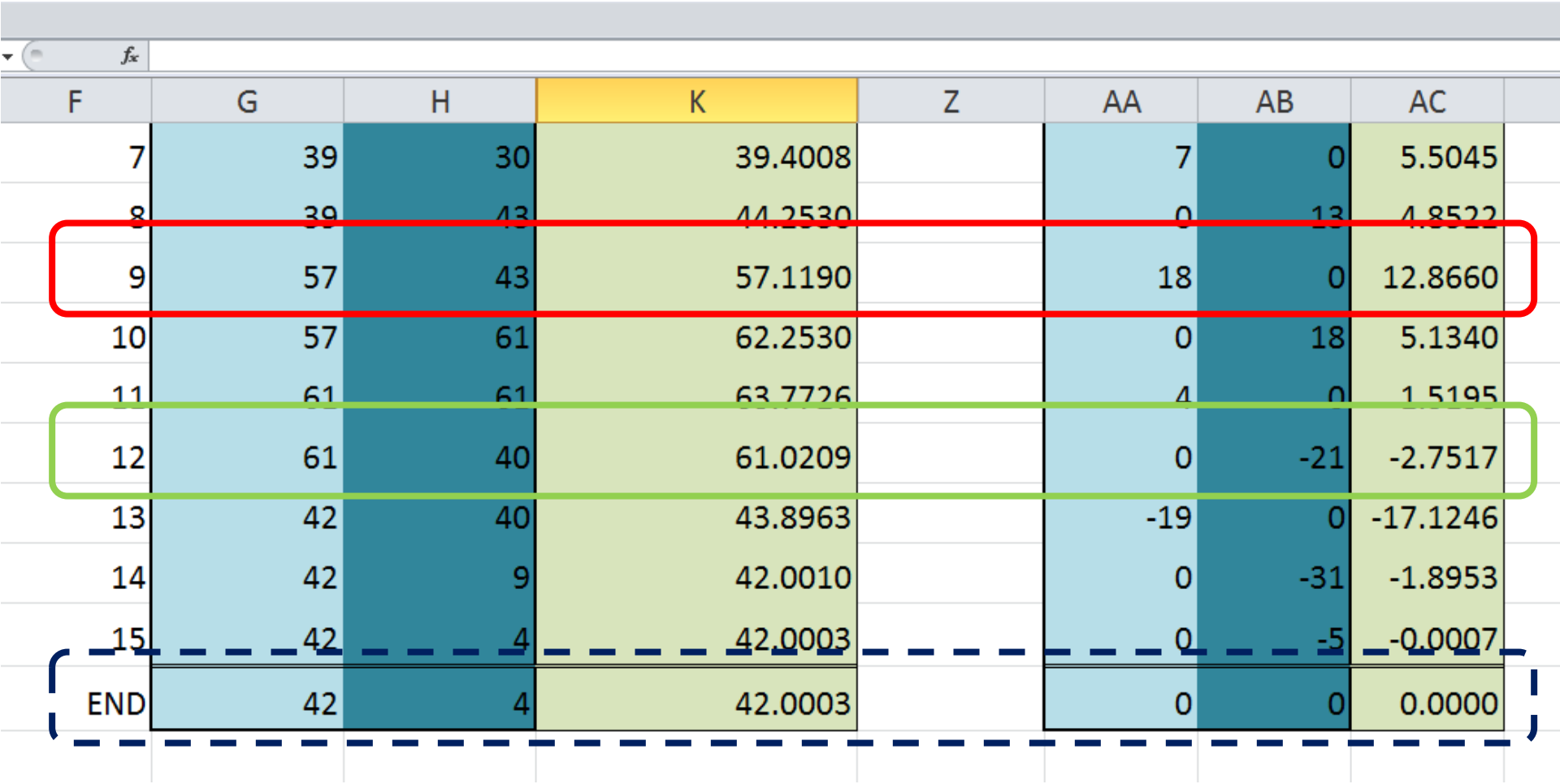
Issuance?
Exchange?
Redemption?



Decentralized Markets
In One Easy Formula



Issuance, Buying, Selling, Redemption

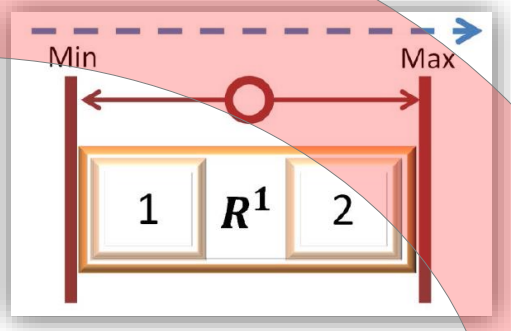


F	G	H	K	Z	AA	AB	AC
7	39	30	39.4008		7	0	5.5045
8	39	43	44.2530		0	13	4.8522
9	57	43	57.1190		18	0	12.8660
10	57	61	62.2530		0	18	5.1340
11	61	61	63.7726		4	0	1.5195
12	61	40	61.0209		0	-21	-2.7517
13	42	40	43.8963		-19	0	-17.1246
14	42	9	42.0010		0	-31	-1.8953
15	42	4	42.0003		0	-5	-0.0007
END	42	4	42.0003		0	0	0.0000

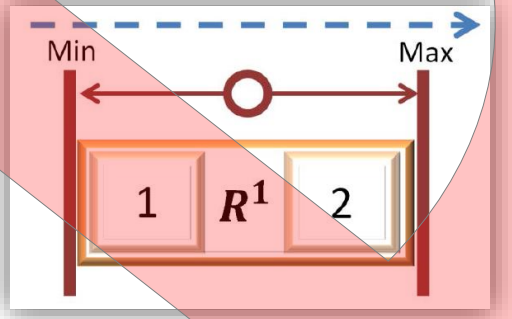
Simplicity = Maximized

3. Users

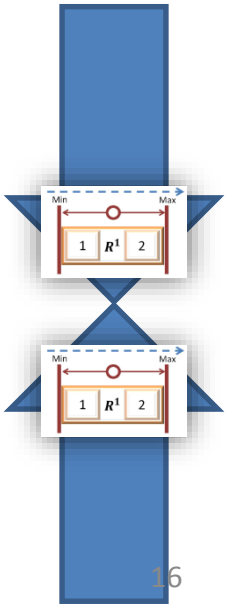
OF of 1 MB Blocksize Bitcoin:



OF of 20 MB Blocksize Bitcoin:



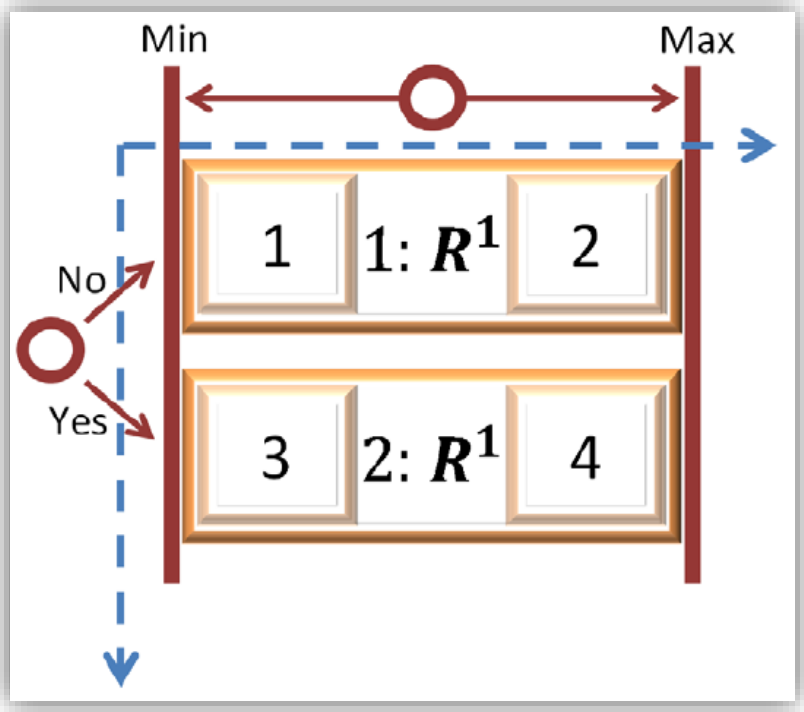
Compare



Combinatorial Markets
(Are Really Cool)

Blocksize > 1MB

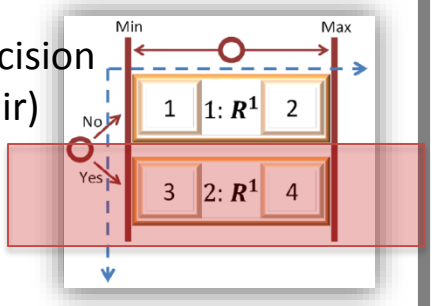
Exchange Rate



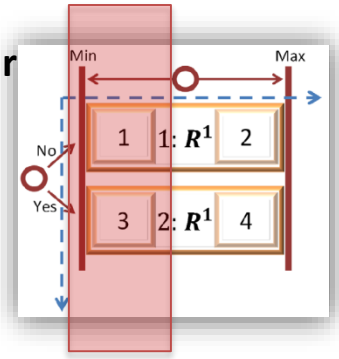
1. Simpler
2. More liquidity / better marketing.
3. For each n dimensions (blue arrows), we get (n-1) *relationships.*

Why?

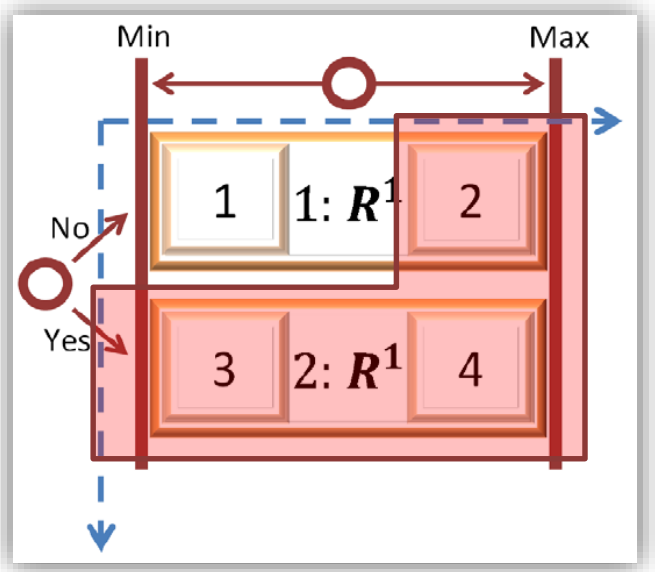
Decision Insurance
(pays if a specified decision is made, actuarially fair)

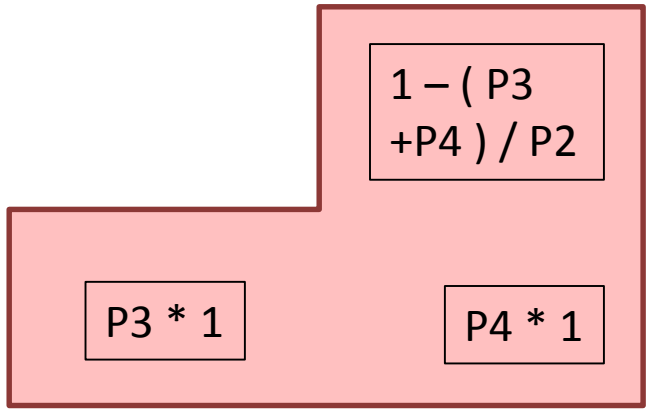


StableCoin / VolCoin Pair
("BitUSD")
(if OF = exchange rate)



Win-Win Trading

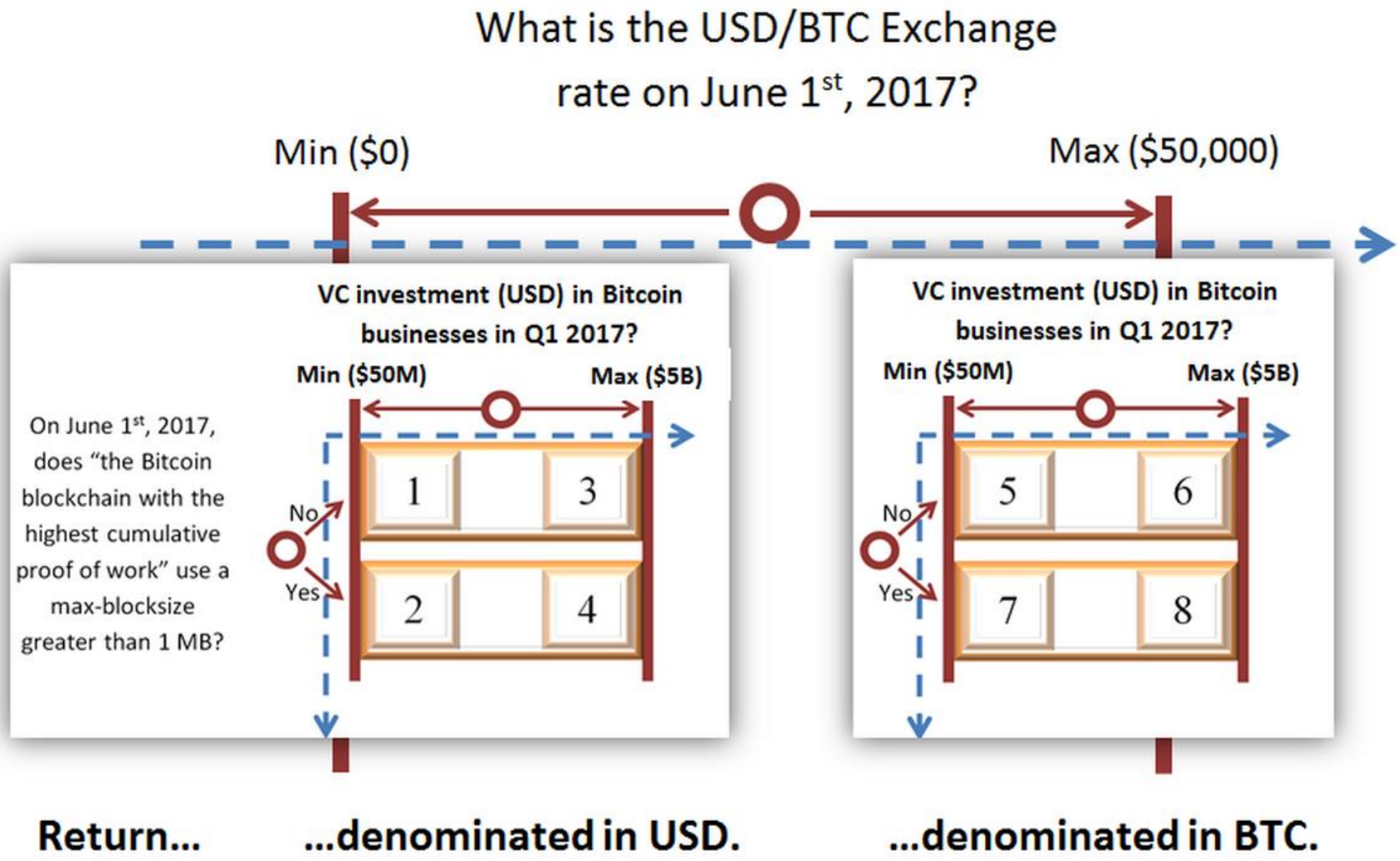




- Total cost must equal 1.
- Get 1 if “Yes”. (Min/Max ignore-able)
- Get ***r*** if “No”. ***r*** = Bitcoin return.

Buy a Bitcoin *that you can return* if Devs make a decision User doesn’t like.

Betting “in Fiat”



Full Refund ("Time Travel")

Principal
$500.0

Results

	Initial				Future				
	Cash	Invest	BTC	Shares	Shares	BTC	Sale ($)	Cash	Return
*	$469.3	$30.7	0.030	0.046545	0.046545	0.032102	$33.1	$502.4	100.5%
**	$469.3	$30.7	0.030	0.046545	0.046545	0.014745	$15.2	$484.5	96.9%

- "Lock in" getting 100% of your FIAT money back (or more!).
- If 'Good Decision' then User gets this, co-varies with OF.

- (Completely incentive compatible).
- Charge fee and amp. liquidity (?)

Costs Met

- ☑ Oracle **– Slightly annoying.**
- ☑ Market Infrastructure **– MSRs**
- ☑ Users **– Fully Incentive-Compatible**

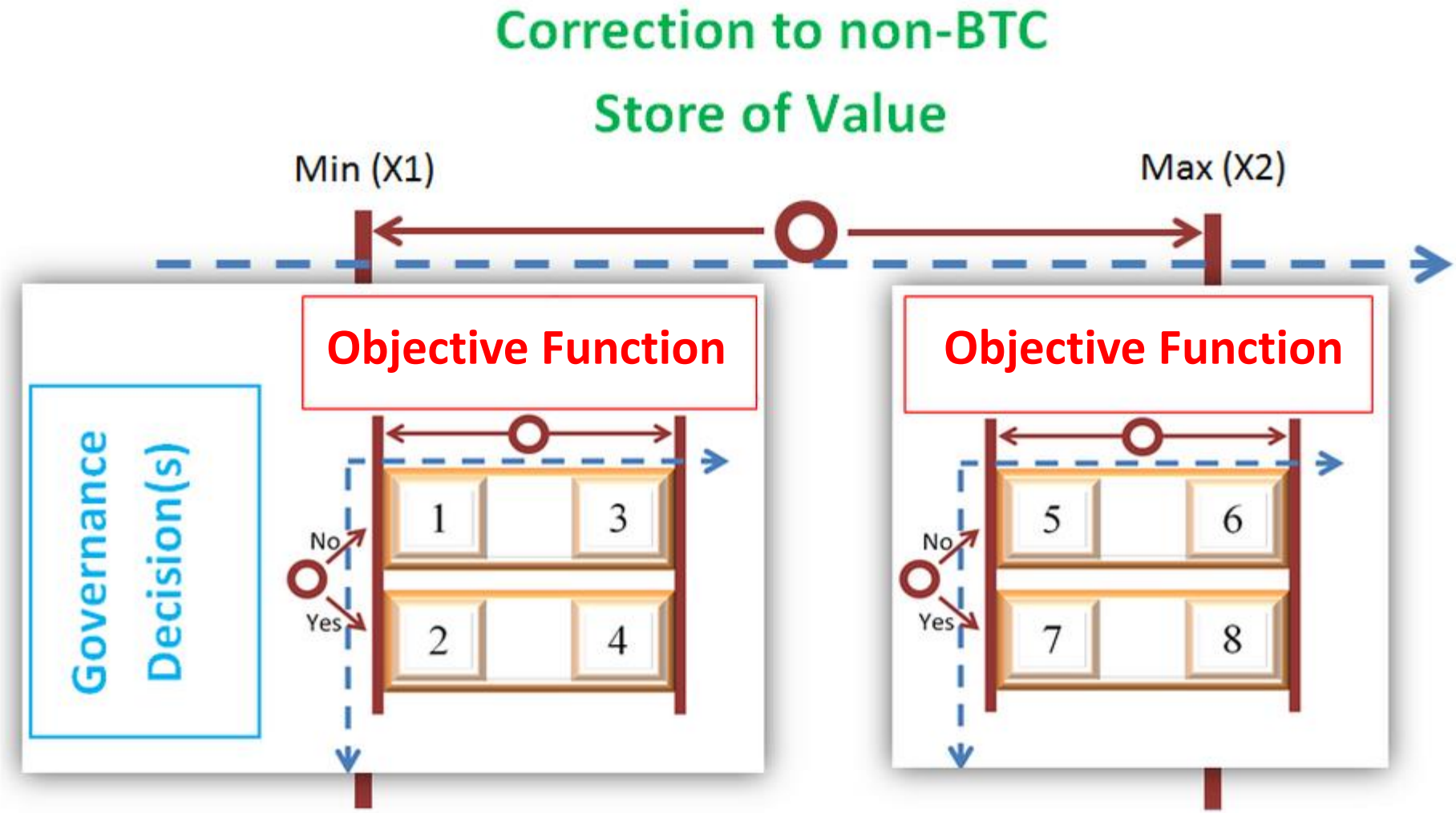
…what about **benefits**?

OF = The Price


Bitcoin Market Price
(Artist's Representation)


Secure – Will BTC become worthless?
Useful – Will BTC improve my life?
Growth – Is BTC different systems?
bottlenecks in the righ

“P2P Governance”



Users either indifferent to the **Dev-Decision**, or they’re not.
If not indifferent, have an incentive to trade.

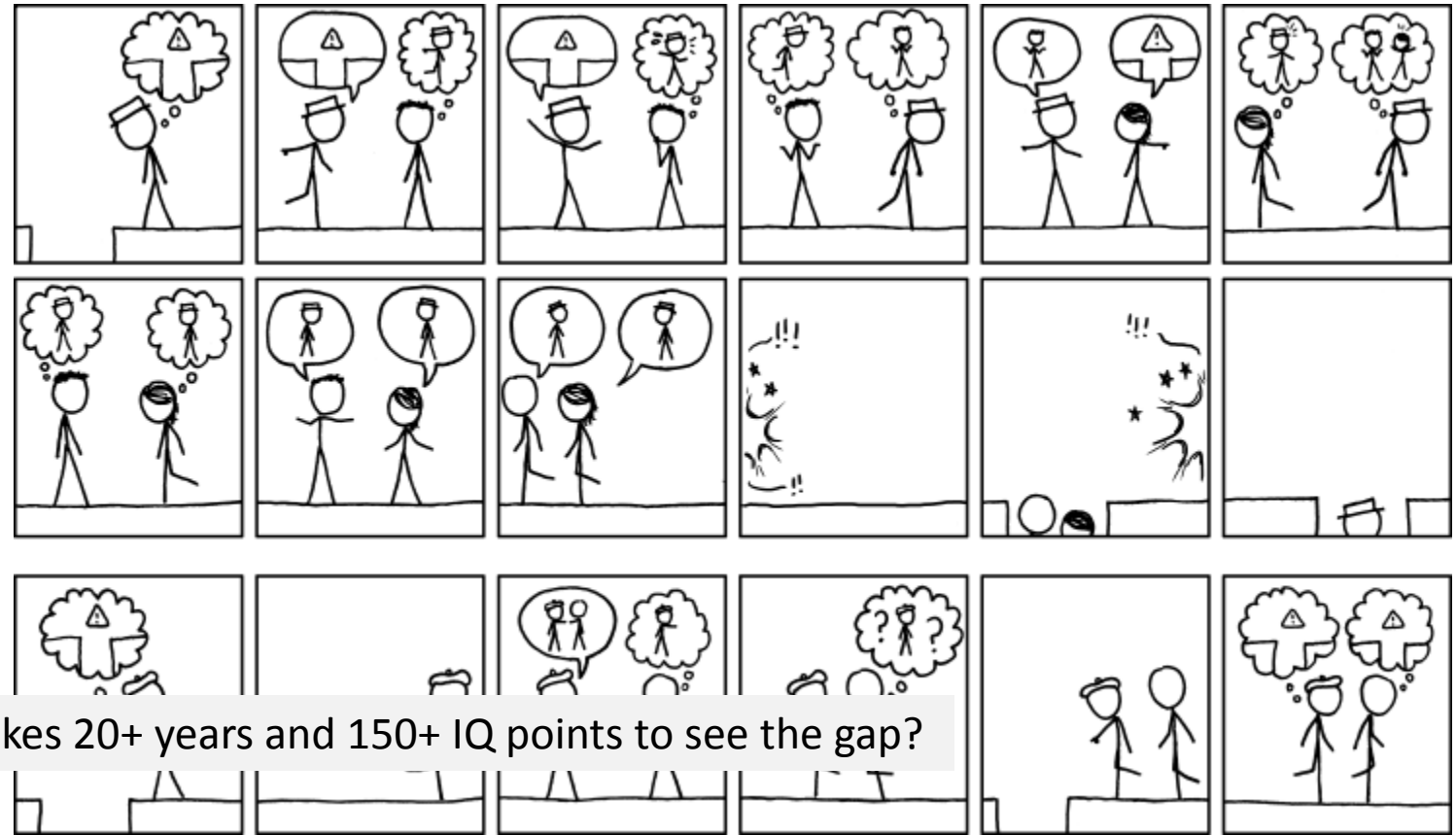
Manipulation

1. Key: what gov. is *least manipulate-able*?
2. Don't forget self-assessments.
    1. Plutocracy ("rule of the rich"): 1 dollar, 1 vote.
    2. Capitalism: 1 dollar *risked*, 1 vote.
3. Theoretical and empirical work.
    1. "Where the rich fool manipulates, the poor expert raises his head."
    2. Poker Sharks
    3. Iterative Cartel Betrayal

A Better Way (?)

1. Do research.
2. Carefully publish/write-up research.
3. Defend research against skeptics (who misunderstand it).
4. Edit / rewrite research to make it more persuasive.
5. Attempt to communicate research to public.
6. Defend against mis-interpretations of your point of view.
7. Spend all day responding to emails, walking people through (in a few minutes) jargon / multiple inferential steps (that you yourself learned over 10+ years in the field).
8. 12-year-olds on reddit call you names.
9. Spend all day responding to 12-year-olds. Meanwhile people accuse your work of being "too confusing" and go with politician/salesman type who is "more convincing".
10. Message does not get out. (No time to work on anything useful.)

1. …
2. Trade on that info.
3. (Optional) Partner with a rich person.
4. You get rich, your message gets out.



Where it takes 20+ years and 150+ IQ points to see the gap?

Thanks!

And remember: