interfluidity

a presentation
@hackerdojo lightning talks
february 6, 2015

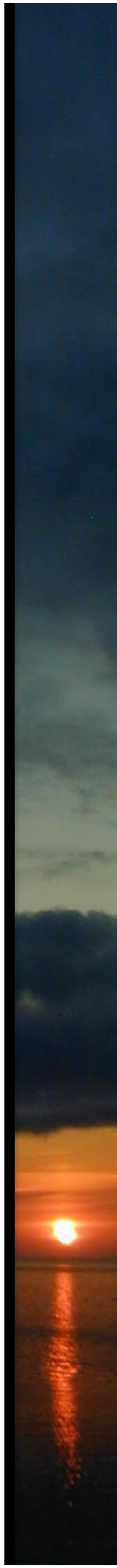
Steve Randy Waldman
http://www.interfluidity.com/
@interfluidity

"It's people.
It's made of people.
The blockchain is made of people!"

SOYLENT BLOCKCHAINS

What is a blockchain?

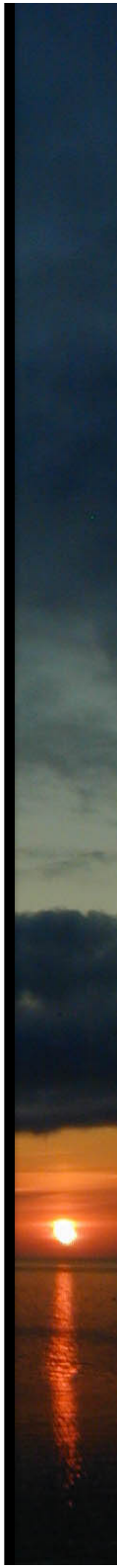
- Some Bitcoin thing
- A distributed “ledger” that tracks transactions and account balances of a cryptocurrency.



What is a blockchain?

- Some Bitcoin thing
- A distributed "ledger" that tracks transactions and account balances of a cryptocurrency

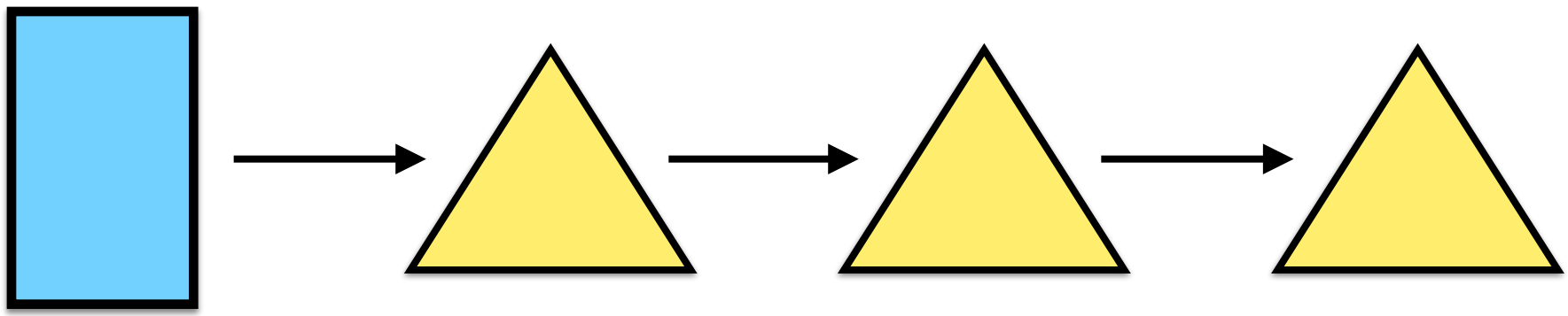
NO!
THESE ARE APPLICATIONS OF A BLOCKCHAIN.
MORE ABSTRACT PLEASE!



What is a blockchain?

definition #1

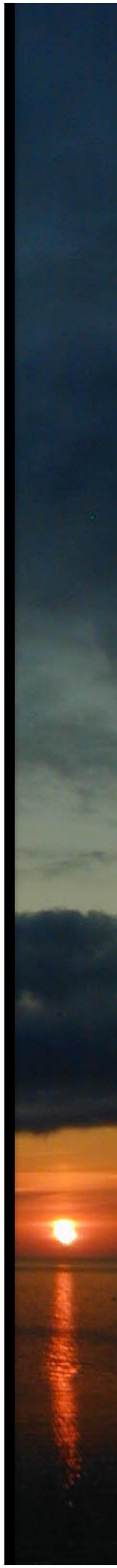
- A ***blockchain*** is a ***description of application state*** defined in terms of a ***genesis state*** and an ***append-only series of deltas***, the integrity of which is ensured by cryptographic hashes of each delta and its parent state.



What is a blockchain?

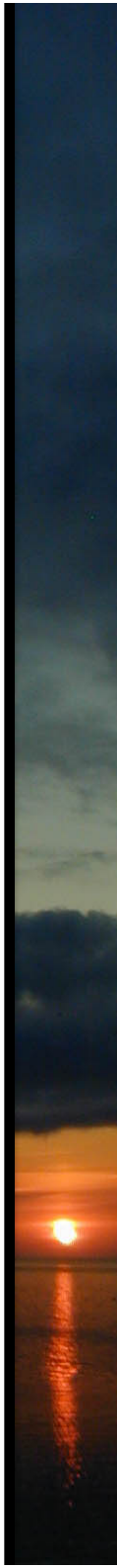
definition #2

- A ***blockchain*** is a ***parliament*** which issues an ***ordered series of "resolutions"*** each of which modify the previously-agreed arrangements and behavior of a ***community***.
- A ***blockchain*** is a ***parliament without a parliamentarian***, for which there is ***no single "true", "canonical" record*** of which resolutions have passed, but about which individual "members" are likely to converge to ***nearly universal consensus.***



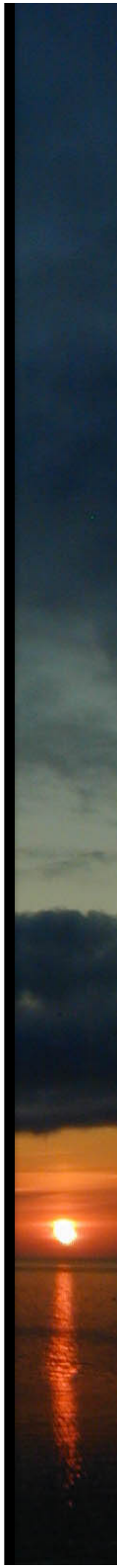
What is a blockchain?

- These two definitions, um, ***synergize***.



What is a blockchain?

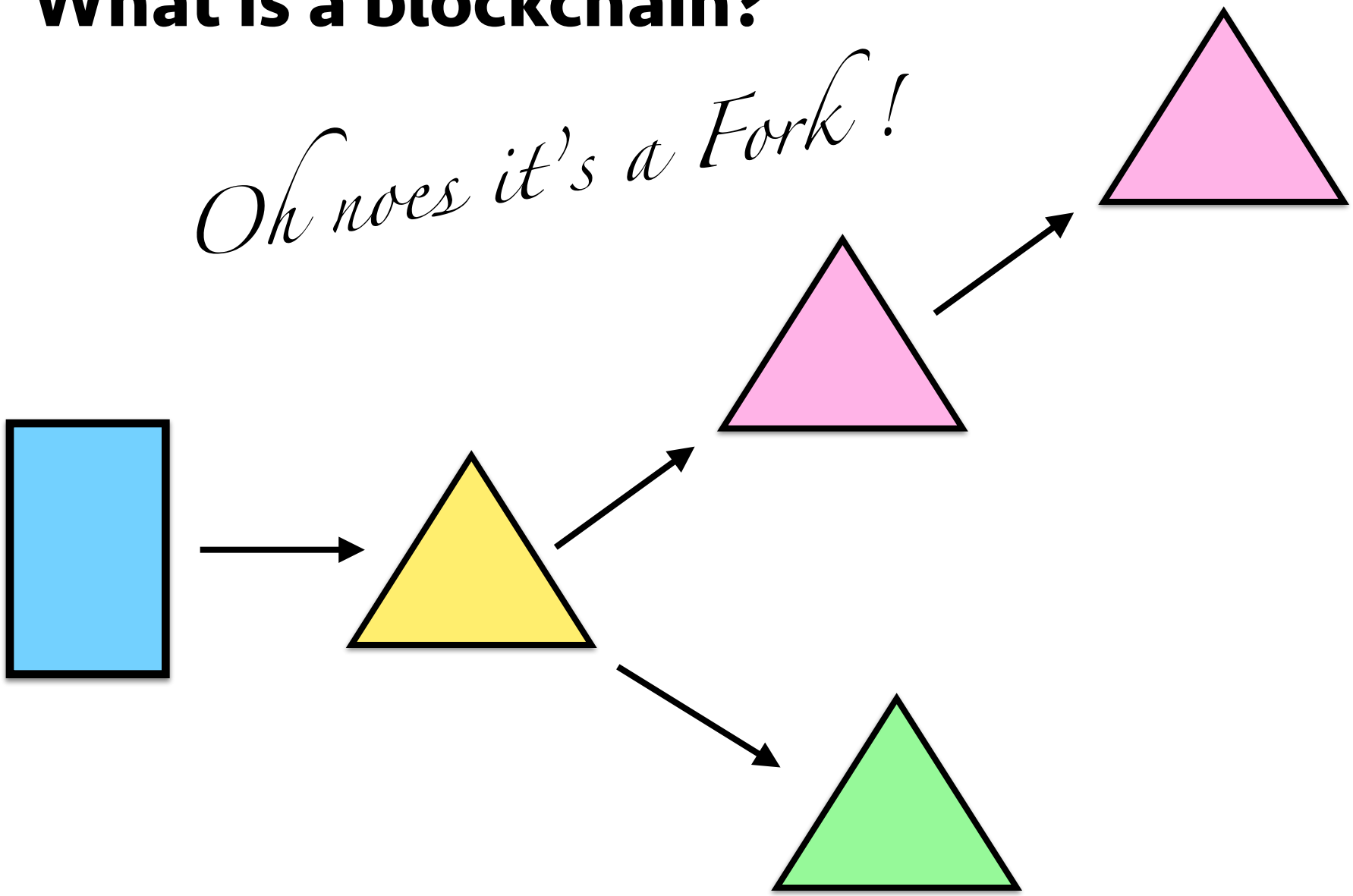
- These two definitions, um, ***synergize***.
- Yeah, dude. That's right. ***Synergy.***



What is a blockchain?

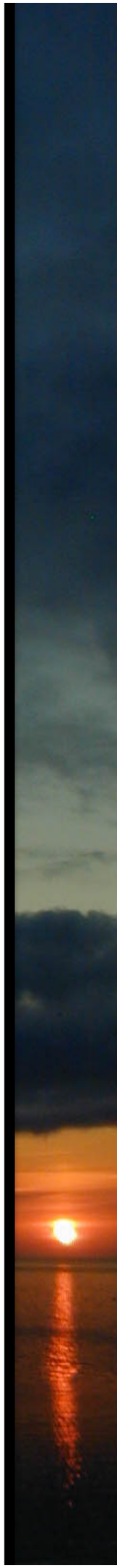
- These two definitions, um, ***synergize***.
- Yeah, dude. That's right. ***Synergy.***
- The data structure defined in ***definition 1***, if maintained by a "nodes" of a distributed system (or "members of a parliament") lends itself to consensus maintenance of ***definition 2***, because every state is uniquely identifiable and, from any "checkpointed" state, all that must be agreed are the ordering and identity of a series of deltas.

What is a blockchain?



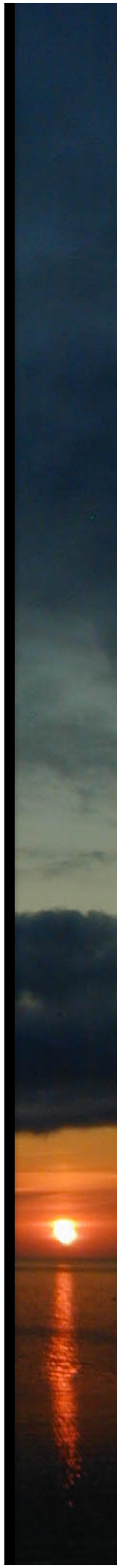
Two kinds of blockchains

- **Antidiscretionary blockchains**
  - Bitcoin
  - Ethereum
  - Nodes / members lack well-defined identity
  - Forks are technical glitches to be resolved mechanically, as fast as possible
  - Ideally, all nodes or members face incentives are to behave “correctly”, such that the behavior of the community is understood by and predicable to outside entities (“users”) who interact with the community.



Two kinds of blockchains

- **Discretionary blockchains**



OH MY

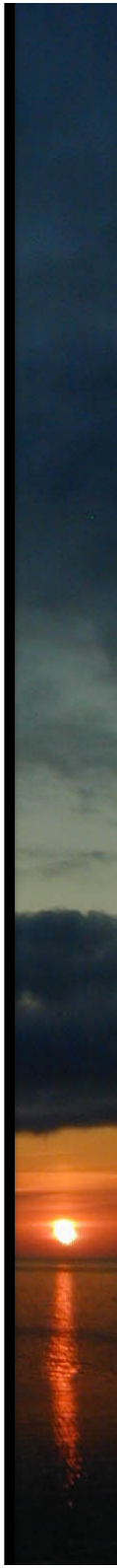
Two kinds of blockchains

- Dis[illegible]y [illegible]ha

GOD!

THEY'RE MADE OF

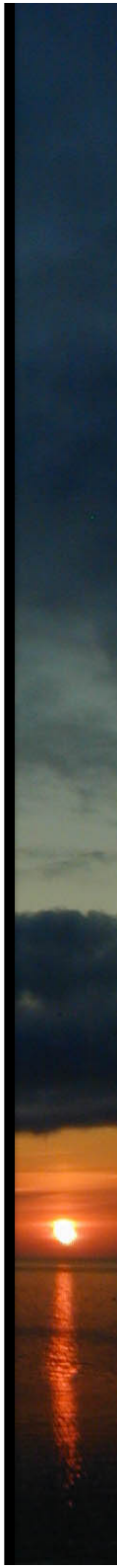
PEOPLE!



Two kinds of blockchains

- **Discretionary blockchains**

(sorry!)



Two kinds of blockchains

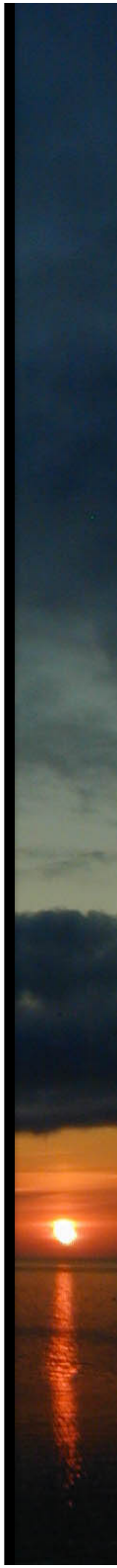
- **Discretionary ("soylent") blockchains**

  - Nodes represent identifiable members

    * *Note: Identity is a complicated problem, philosophically as well as technically. Each application must define its own notion of identity, perhaps piggybacking on meatspace definitions and institutions.*

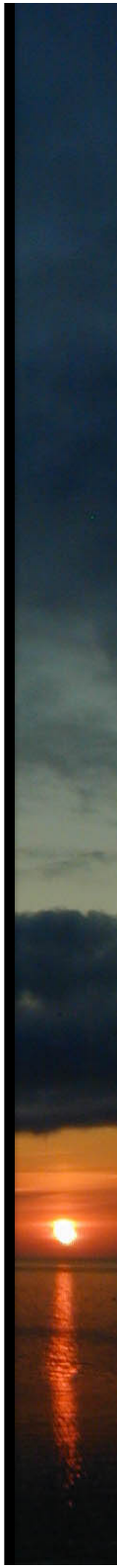
  - Forks represent disagreement. They must be resolved, but may persist a while.

    * *Eventual consistency!*



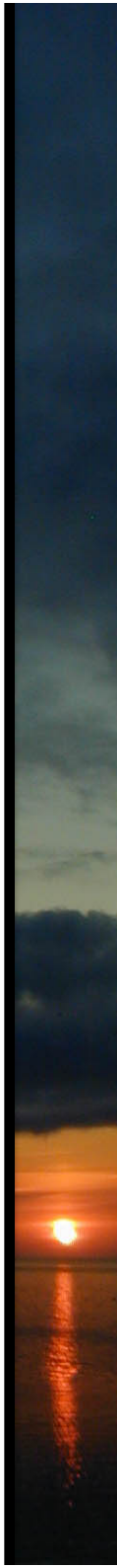
Two kinds of blockchains

- **Discretionary ("soylent") blockchains**
  - Outsiders that interact with the community may
    - tolerate a degree of temporary uncertainty
    - be offered a mechanism to try to force consensus
      - e.g. quorum and mutisig endorsement



Different tools for different purposes

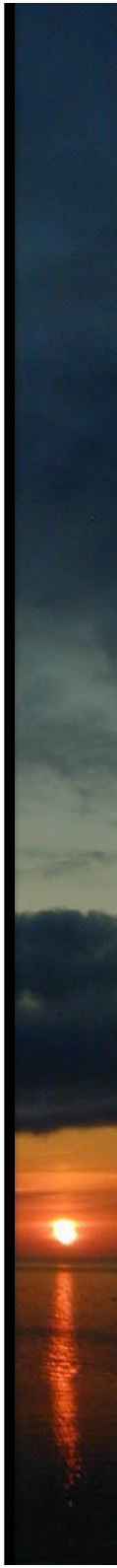
- Antidiscretionary blockchains prioritize values of *predictability* and *authority*
- Discretionary blockchains prioritize *participation*, *representation*, and *flexibility*.
- To some degree, there is a continuum between the two sorts of blockchains
  - Members express discretion in an "antidiscretionary" blockchain by gaming the intended incentive system and by choices made in software upgrades.
  - For many applications, disagreement will be rare or the scope for discretion will be small, in which case the two arrangements will behave similarly.



Different tools for different purposes

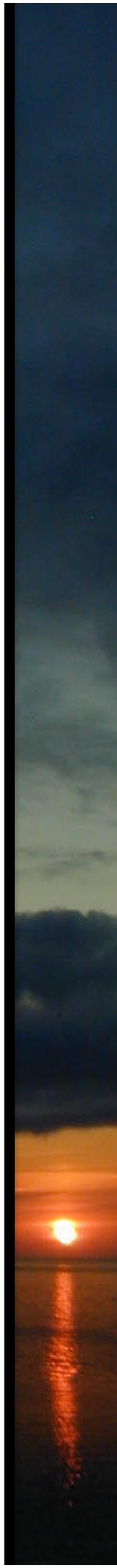
- ***Fundamentally, an antidiscretionary blockchain is a technique for deploying a long-running, predictable software application on top of a community of people whose role is merely to verify.***

- ***A discretionary blockchain is a technique for reifying and composing the ever-changing will of a community in the form of a distributed software application.***



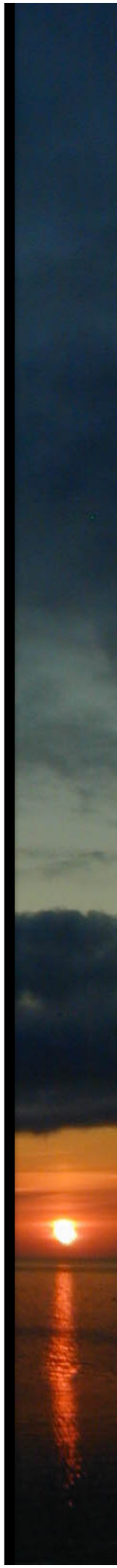
Very different security models

- Antidiscretionary blockchains try to rely on techniques like proof-of-work / proof-of-stake, game theory, and economic incentives.
- Discretionary blockchains rely on the value of relevance and participation, the costs of reputation and potential banishment, and sometimes enforcement of preagreed obligation and sanction for fraud.
- Each type of application can potentially be simulated atop the other, so different security characteristics might determine which architecture predominates.



Examples suited to “soylent” blockchains

- Online journals and publications
- Services like Yelp! or Facebook that rely upon algorithms that impinge upon the interest of application participants but whose details are inherently discretionary
- Explicit participatory membership organizations, e.g. neighborhood associations, civic and environmental groups, etc
- Shareholders of large business firms



THANKS FOR LISTENING !!!