Blockchains and economics

Why are blockchains interesting?

The “academic” reasons

- Blockchains are a very “pure” playground for implementing applications that run on economic incentives, experimenting and seeing the results
- Community with existing interest in market mechanisms, auctions, etc
- Very easy to test and deploy

The “social” reasons

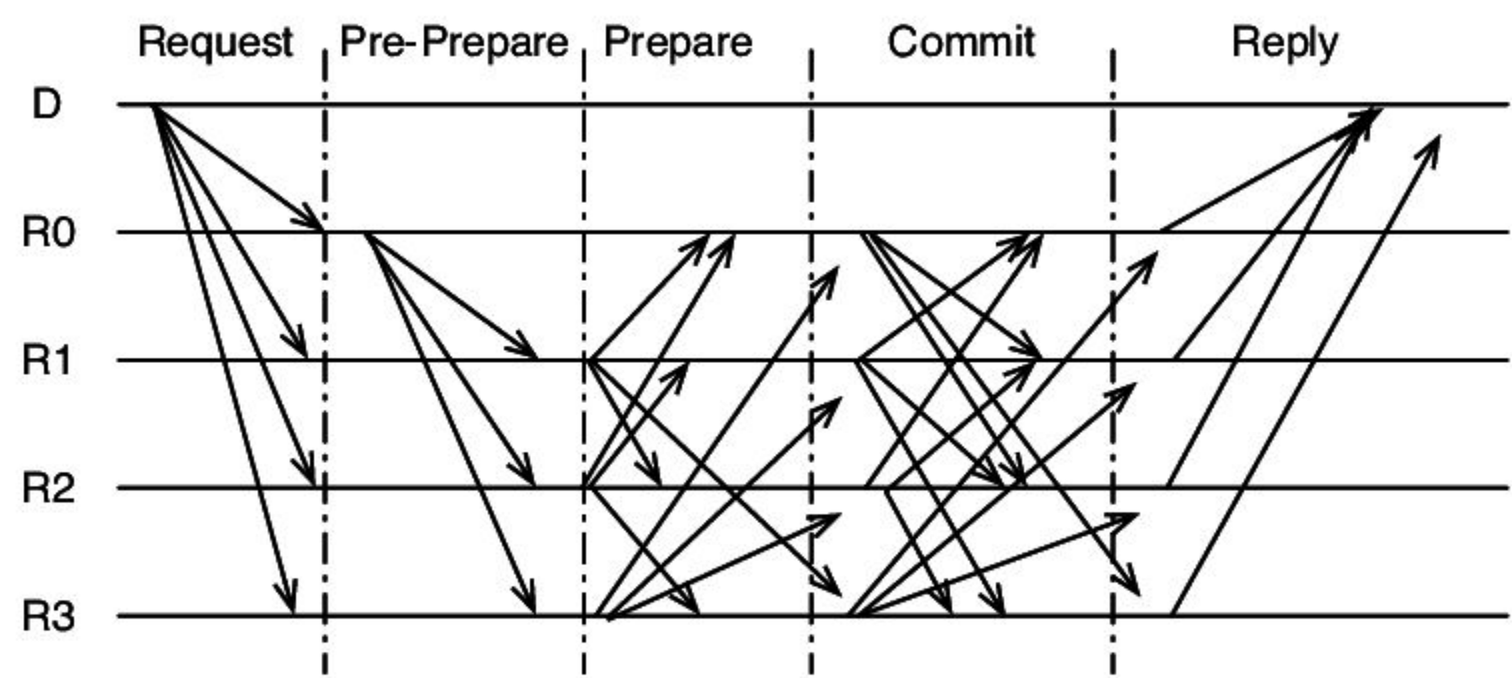
- Blockchains allow us to build an entire new class of applications that are not like anything else that existed before
- Digital institutions with no central coordinator and not bound to any single jurisdiction
- Smart contracts as special-purpose “legal system” with very low enforcement costs… in some cases
- More open, free, inclusive alternatives to centralized apps and platform monopolies
- Community excited about using technology for positive social transformation

Economics and public blockchain design

Important goal of a blockchain: be decentralized.

Byzantine Generals Problem (Lamport, 1982)

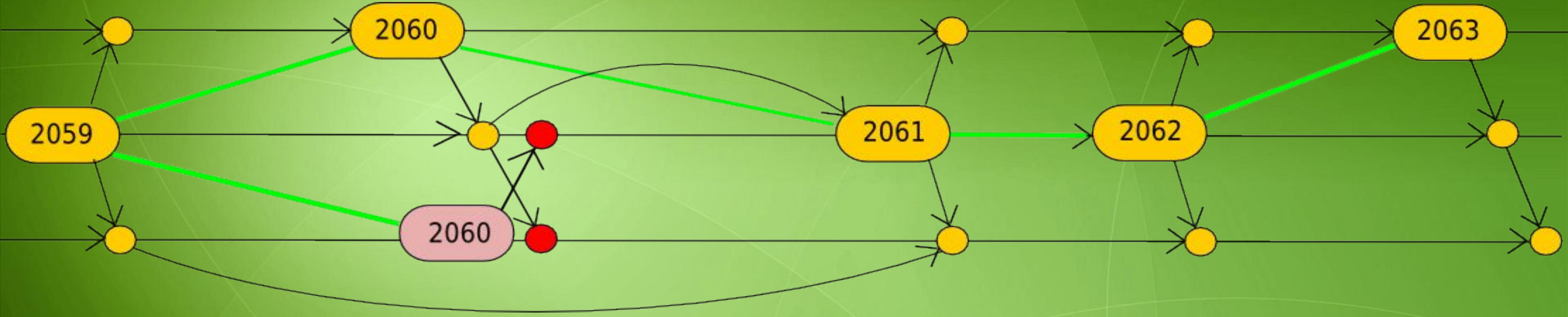
Traditional BFT consensus, eg. PBFT



Important goal: **really** be decentralized.

Challenges

- **The weight assignment problem**: given a set of actors, how do we assign them weights?
  - Cryptographic protocols have no access to roots of trust, legal identity, etc etc. Anyone can create as many "accounts" as they want.
- **The incentive problem**: how do we encourage the actors to (i) participate (as opposed to not participating), and (ii) honestly follow the protocol (as opposed to acting in some faulty manner)



Proof of work uses economic tools to solve both of these challenges

Economic security properties

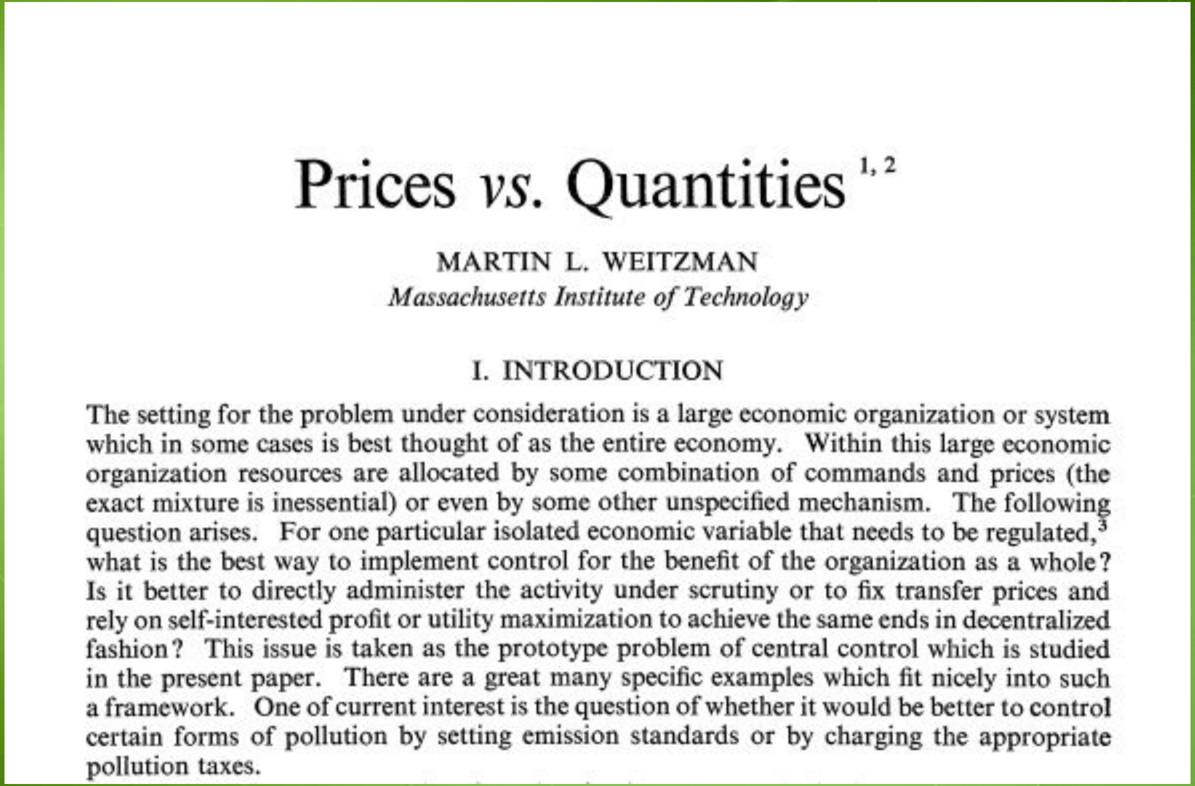
- Fairness
- Maximize cost of attack

Economic security models

- **Honest majority:** at least X% follow the protocol
- **Uncoordinated majority**: all actors make choices independently, no actor controls more than X%
- **Coordinated choice**: most or all actors are colluding, though in second-layer systems we may rely on free entry from non-colluding actors
- **Bribing attacker:** all actors make choices independently, but an attacker can add their own money to influence participants' payoff matrices

Subproblem: block size / transaction fee economics

- Any transaction that gets included in a block has several consequences:
    - Utility to the sender
    - Direct processing costs to nodes [externality]
    - Impacts to “decentralization” [externality]
- Problem: how to price externalities?



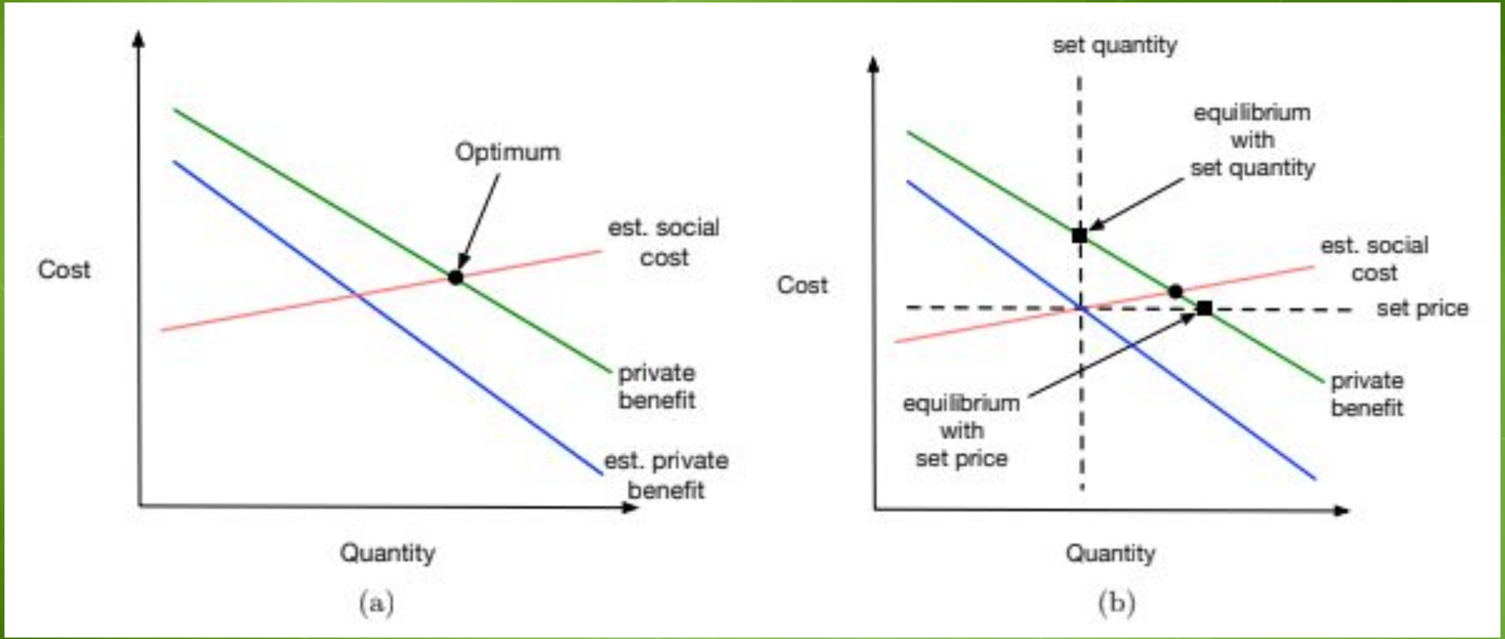
Prices *vs.* Quantities[1, 2]

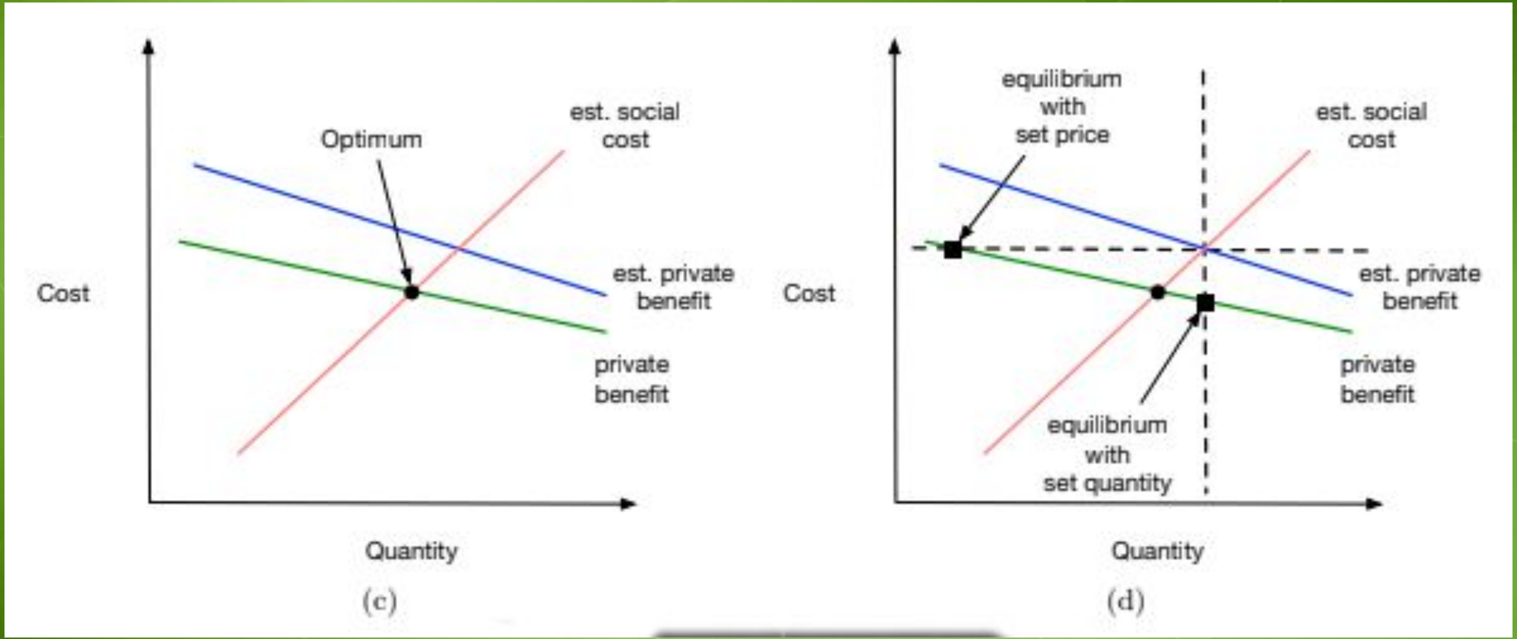
MARTIN L. WEITZMAN

Massachusetts Institute of Technology

I. INTRODUCTION

The setting for the problem under consideration is a large economic organization or system which in some cases is best thought of as the entire economy. Within this large economic organization resources are allocated by some combination of commands and prices (the exact mixture is inessential) or even by some other unspecified mechanism. The following question arises. For one particular isolated economic variable that needs to be regulated,[3] what is the best way to implement control for the benefit of the organization as a whole? Is it better to directly administer the activity under scrutiny or to fix transfer prices and rely on self-interested profit or utility maximization to achieve the same ends in decentralized fashion? This issue is taken as the prototype problem of central control which is studied in the present paper. There are a great many specific examples which fit nicely into such a framework. One of current interest is the question of whether it would be better to control certain forms of pollution by setting emission standards or by charging the appropriate pollution taxes.


Optimum
est. social cost
Cost
private benefit
est. private benefit
Quantity
(a)
set quantity
equilibrium with set quantity
est. social cost
Cost
set price
private benefit
equilibrium with set price
Quantity
(b)


Optimum
est. social cost
est. private benefit
private benefit
Cost
Quantity
equilibrium with set price
est. social cost
est. private benefit
private benefit
equilibrium with set quantity
Cost
Quantity

(c)

(d)

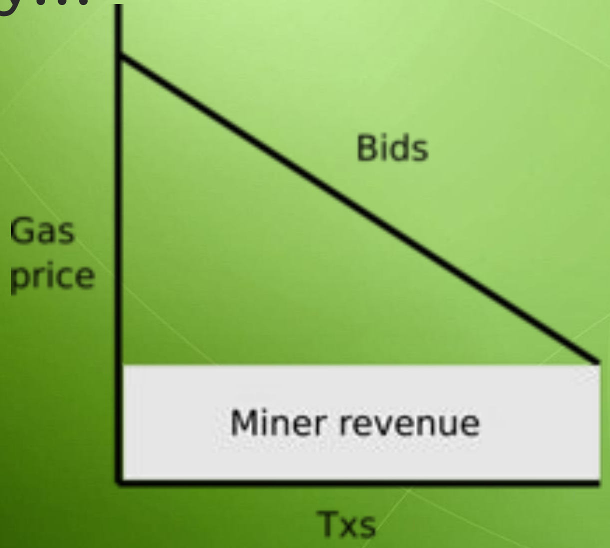
Transaction fee mechanism

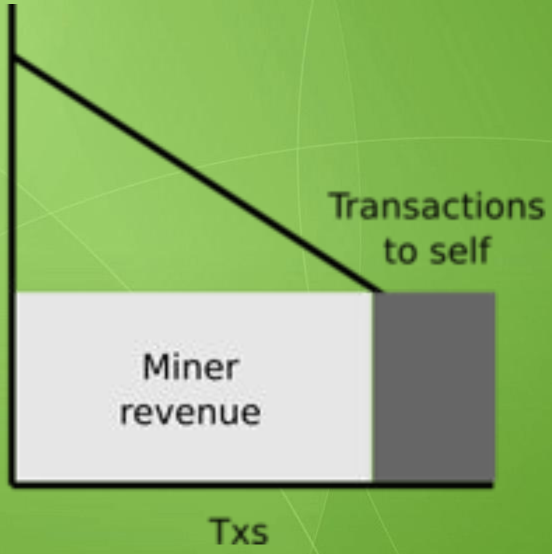
- Every transaction specifies a fee
- Miner chooses what transactions to include
- If a transaction is included, it pays the fee it specifies

This is equivalent to a first price auction (which is bad!)

Transaction fee mechanism

- Second price auctions near-optimal assuming non-coordination. Assuming coordination they can get nasty…





Using blockchains in the real world

Properties of blockchains

- Safety
    - Once a message is confirmed, it will not get un-confirmed
- Liveness
    - If you want to get a message confirmed, you can
- Validity
    - The chain only contains messages that are “valid” in their context

Blockchains vs cryptography

- Cryptography
  - Hide information
  - Prove that I made a message
  - Prove that I made a message after another message
- Blockchains
  - Prove *when* I made a message (upper bound)
  - Prove that I did *not* make a message
  - Prove that some set of messages is the entire set of messages that some set of participants made

Thinking about blockchains in terms of concrete added safety/availability guarantees….

Collectibles

- Cryptokitties are more valuable because I know I’ll always be able to trade them, even if the company disappears
    - (In theory. In practice the cryptokitties application depends heavily on centralized components which could shut down)

Auctions

- Possible attack: auction operator sees highest bid M, colludes with seller, inserts a bid for M-1, increases revenue for seller
- Mitigation: two-step auction
  - Step 1: everyone submits commitments to bids to chain
  - Step 2: everyone who committed can reveal bids
- Blockchain lets us check that some bid was not committed to

Certificates (eg. university degrees)

- When issuing a certificate, just sign it
- When revoking a certificate, publish to chain
- Checking the chain allows anyone to check that a certificate was *not* revoked

Uses by application category

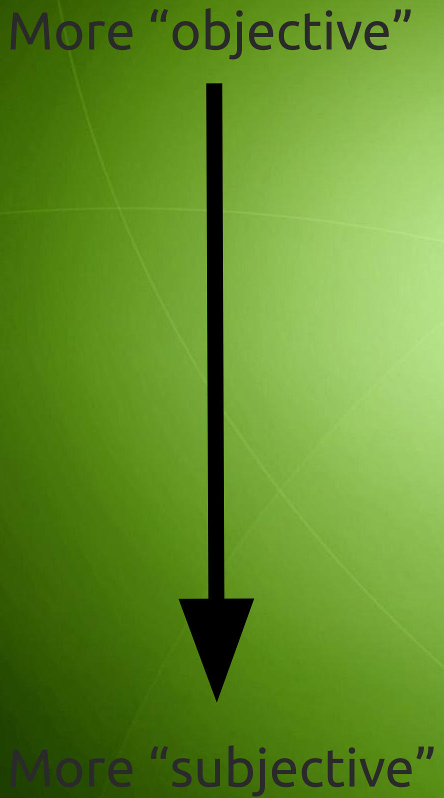
- Digital assets
  - “Purely cryptographic”
  - “Asset-backed”
- More complex applications involving digital assets
  - Smart contracts
- Non-asset-related applications (eg. certificate revocation)

Smart contracts

- “If X happens, then send asset Y to address Z”
- Benefits
  - Can represent many kinds of economic activities
  - Easy to cheap to deploy
  - No dependence on trusted third parties

Smart contracts

- Limitations
    - Can only effect transfer of assets under their direct control, cannot compel outside behavior (ie. can’t enforce loans)
    - Usually depend on data from the outside world (“oracles”); work less effectively the more subjective the data is



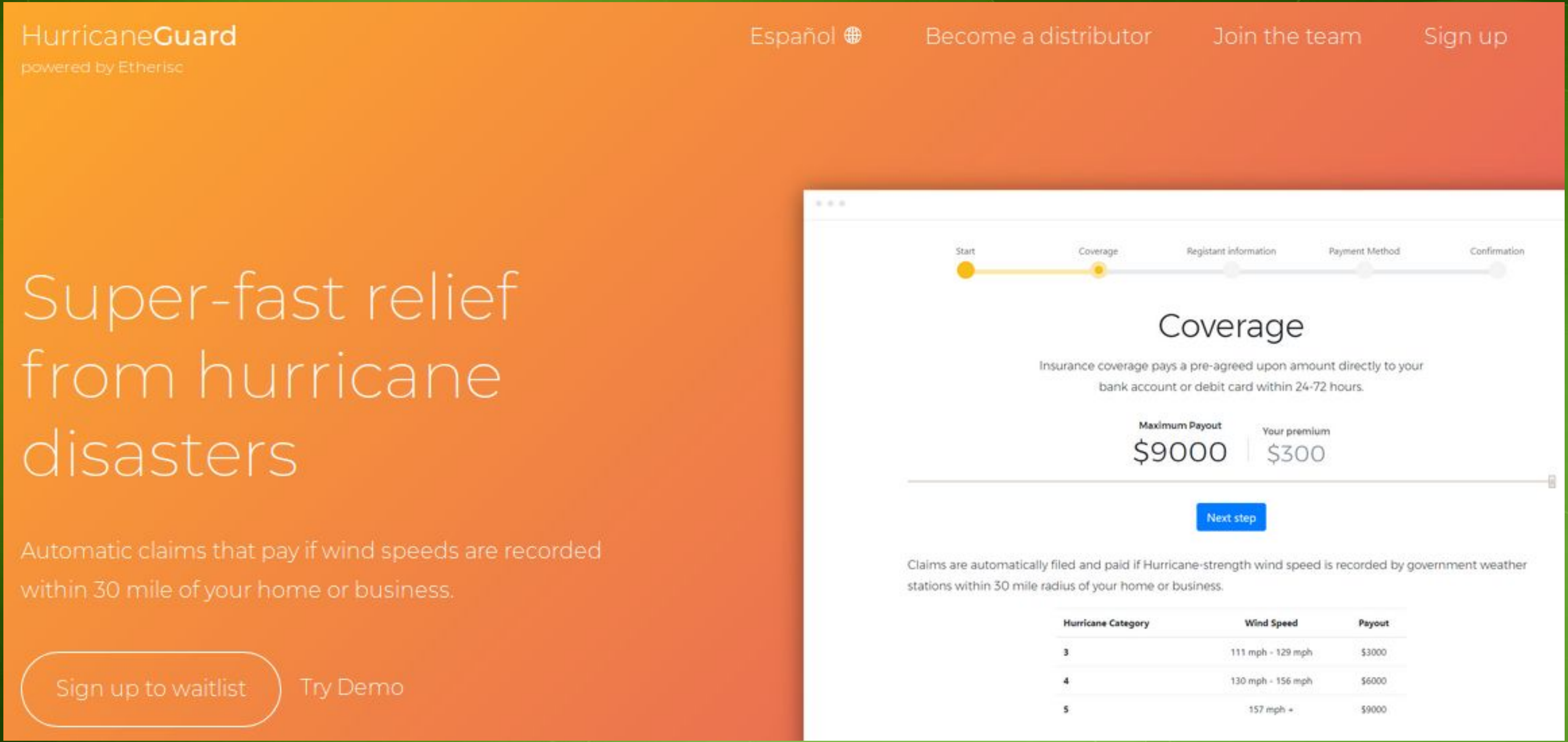
More “objective”

More “subjective”

- Verifying solutions to math problems, computation, file storage

- Derivatives on financial assets and indices
- Weather insurance

- Insurance on damage to specific objects
- Verifying completion of offline tasks (eg. building a road)



Super-fast relief from hurricane disasters

Automatic claims that pay if wind speeds are recorded within 30 mile of your home or business.

Coverage

Insurance coverage pays a pre-agreed upon amount directly to your bank account or debit card within 24-72 hours.

Maximum Payout $9000 | Your premium $300

Claims are automatically filed and paid if Hurricane-strength wind speed is recorded by government weather stations within 30 mile radius of your home or business.

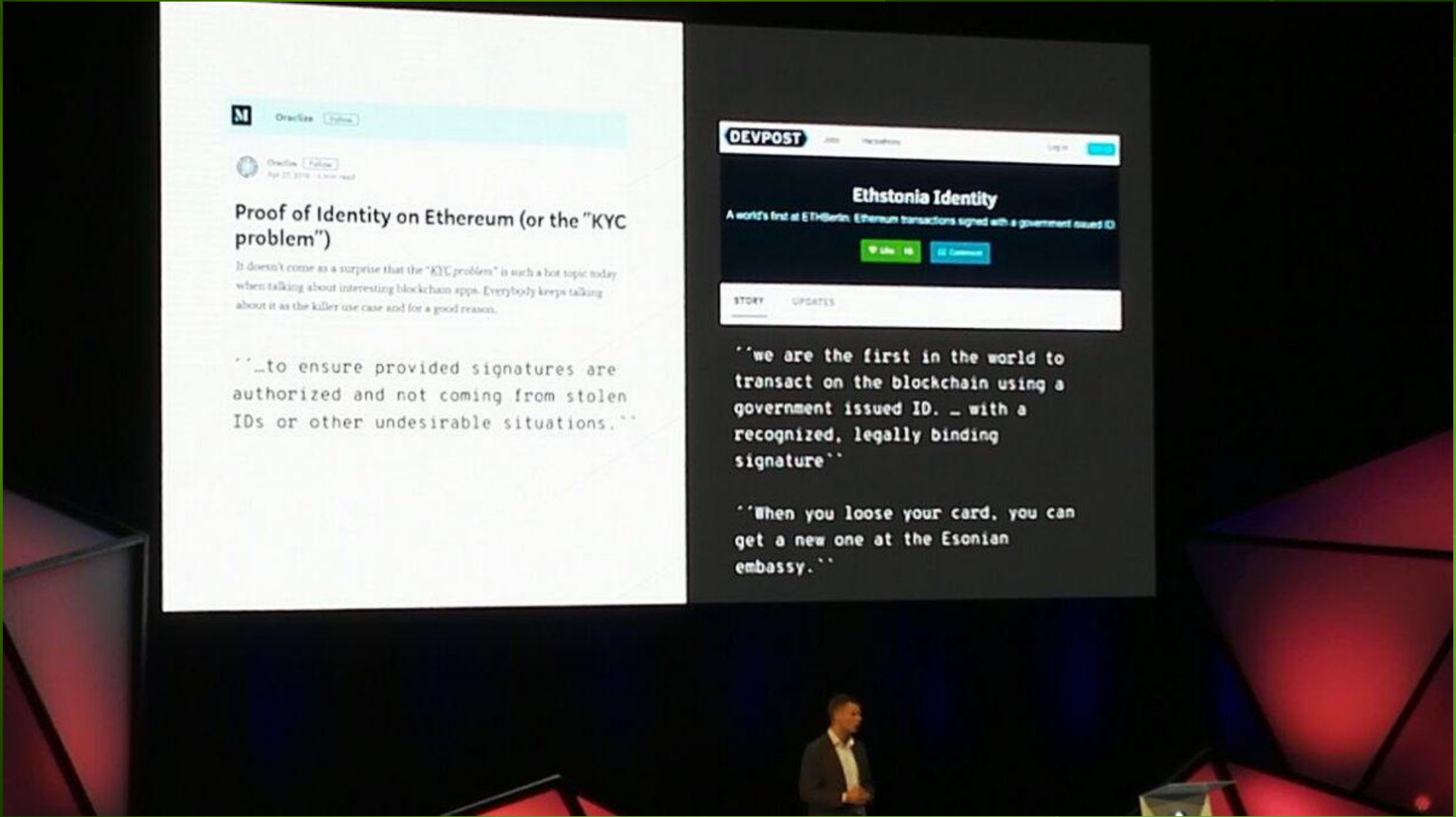
Hurricane Category	Wind Speed	Payout
3	111 mph - 129 mph	$3000
4	130 mph - 156 mph	$6000
5	157 mph +	$9000

Other projects (in the “pure crypto” category)

- MakerDAO (decentralized stablecoin)
- Augur (prediction market)
- Decentralized exchanges

Other projects (with more “real world integration”)

- Land registries (initially using blockchain only for added verification)
- Asset-backed “stablecoins” (USDC, USDT, TUSD… but also commodities and other assets)
- Publishing financial instrument life cycles onto the blockchain



Proof of Identity on Ethereum (or the "KYC problem")

It doesn't come as a surprise that the "*KYC problem*" is such a hot topic today when talking about interesting blockchain apps. Everybody keeps talking about it as the killer use case and for a good reason.

``…to ensure provided signatures are authorized and not coming from stolen IDs or other undesirable situations.``

Ethstonia Identity

A world's first at ETHBerlin: Ethereum transactions signed with a government issued ID

``we are the first in the world to transact on the blockchain using a government issued ID. … with a recognized, legally binding signature``

``When you loose your card, you can get a new one at the Esonian embassy.``

Sister technologies

- Zero knowledge proofs (privacy)
- Multi-party computation (privacy)
- Distributed identity (including “web of trust” systems)

Takeaways

- Blockchains are useful infrastructure for building and implementing many kinds of things, including economic mechanisms
- Blockchain communities are passionate about both the math of designing such mechanisms and the social transformative potential of partially replacing arbitrary authority with encoded rules
- Blockchains cannot do everything, and do not solve all trust problems. There are limits.