

# The Governed Blockchain

Decentralized - Limassol

2nd November 2017

## Ian Grigg

- Financial cryptographer
- Inventor of Ricardian contracts
- co-Inventor of triple entry accounting
- Identity
- “EOS An Introduction”

## block.one

- Cayman Islands corporation
- Investors from finance & blockchain
- Fully funded
- Building the EOS.IO software
- Coin distribution on as we speak
- All details: <http://EOS.IO/>

I am contributing in EOS.IO, as are many others.

This is an interesting project - code, design, user needs.

I expect it to add value and benefit globally.



Crypto Ahead

But - Cryptocurrencies are dangerous places.

Not advocating an investment - Caveat Emptor

# I. Let's build a blockchain

**A blockchain for everybody**

**Establish from baseline or first principles**

**Who is everybody?**

**What do they need?**

**Can we provide it?**

**But 1st, review options**

# UNpermissioned Blockchains

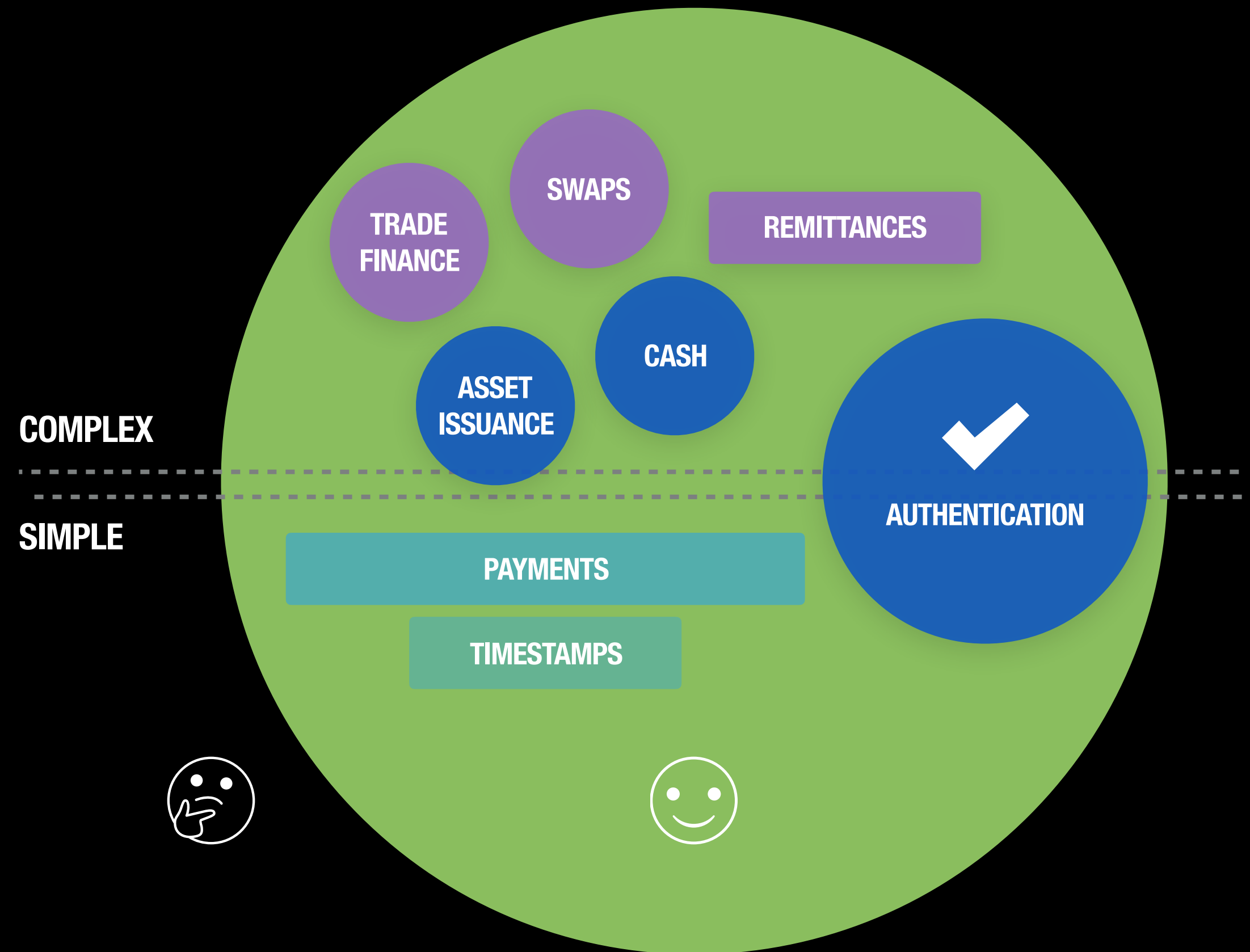
THE BUSINESS SPACE IN AN UNPERMISSIONED LEDGER



- (Swanson 2015) - two varieties
- Bitcoin & Ethereum  $\Rightarrow$  unpermissioned
- Simple things automated within the chain
- Complex things - left to users:  
smart contracts, external logic,  
Multisig, zkSNARKS, rings, etc.
- Wild west? Anarchy?

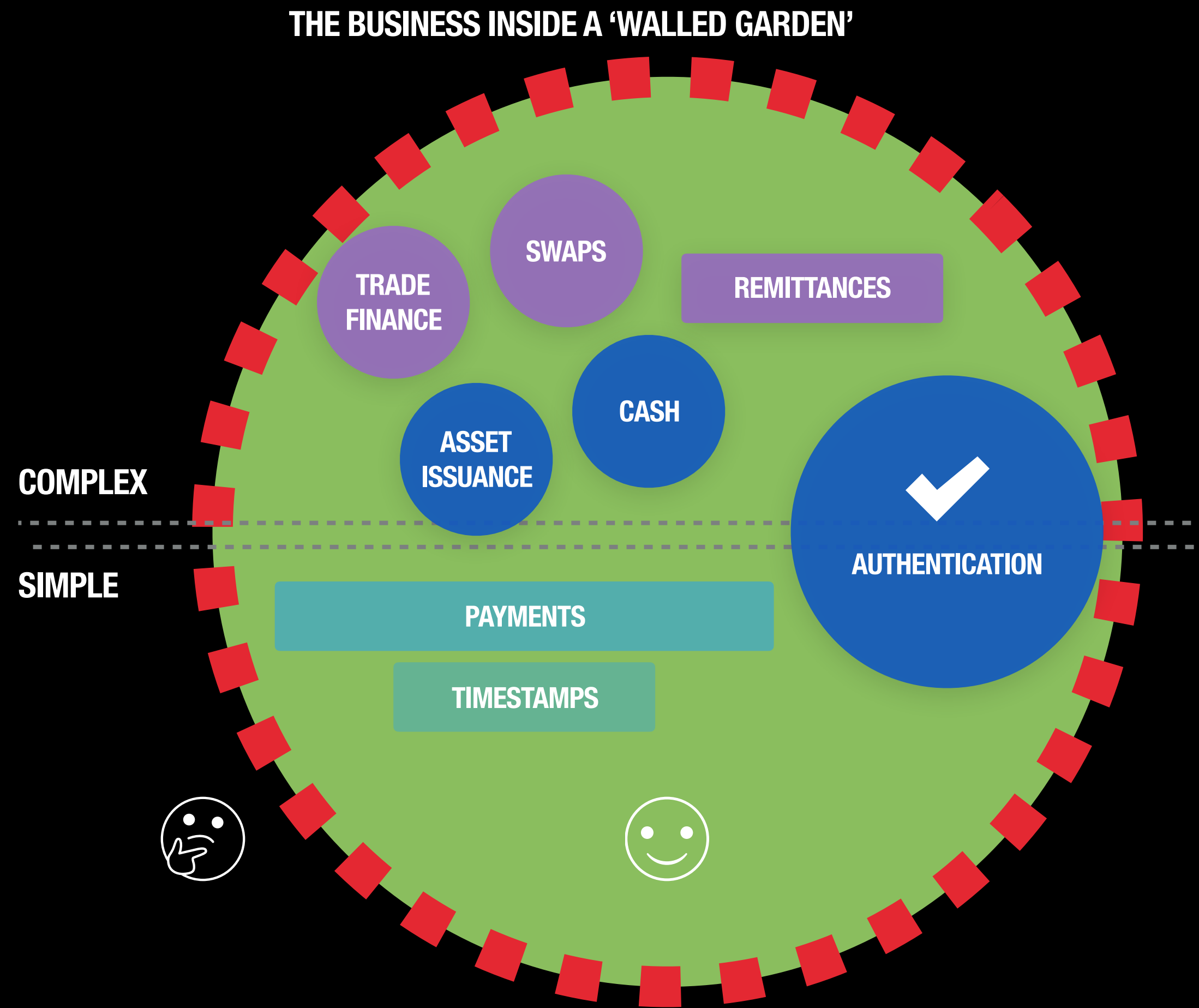
# Permissioned ledgers

## THE BUSINESS IN A PERMISSIONED LEDGER...



- Trade is more complex  
loans, swaps, trade finance
- Exposure  $\Rightarrow$  risk  $\Rightarrow$  protection

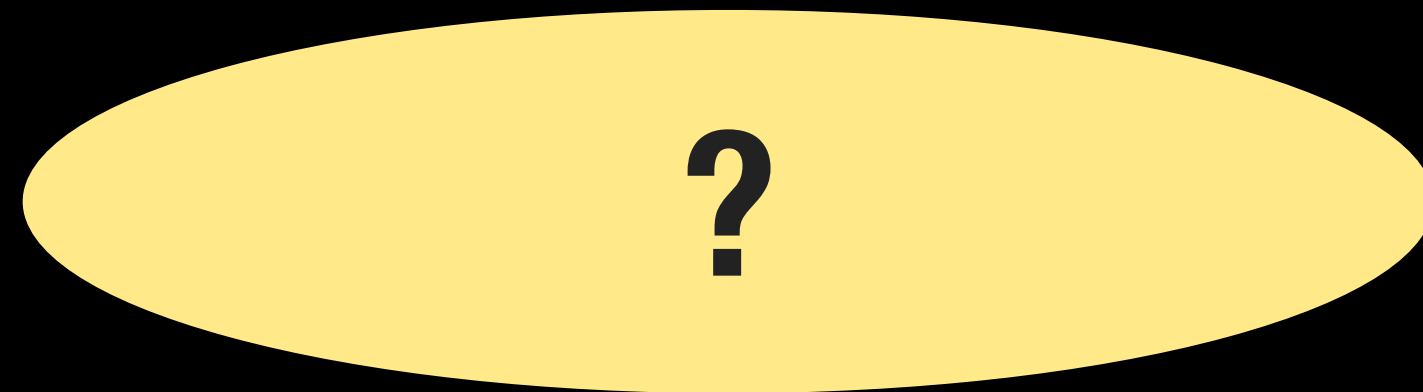
# Permissioned ledgers



- Trade is more complex  
loans, swaps, trade finance
- Exposure  $\Rightarrow$  risk  $\Rightarrow$  protection
- Cannot protect with free entry
- “Walled Garden” for insiders
  1. He who permits, extracts
  2. The cost rises,
  3. Small players excluded

# Between Anarchy and the Leviathan

*What do we do above the line?*



COMPLEX

SIMPLE

PAYMENTS

TIMESTAMPS

*(We agree to automate  
all below the line...)*

**WE AGREE:**

Automate below...

**BUT:**

above?

Context: What is a small business to do?



## II. What does Business do?

GlobalMegaCorp:

Don't Change

HNWI:

HODL



## II. What does Business do?



For The Rest Of Us:

**Trade!**

# Complexity...

**If trade were simple,**

It would be automated!

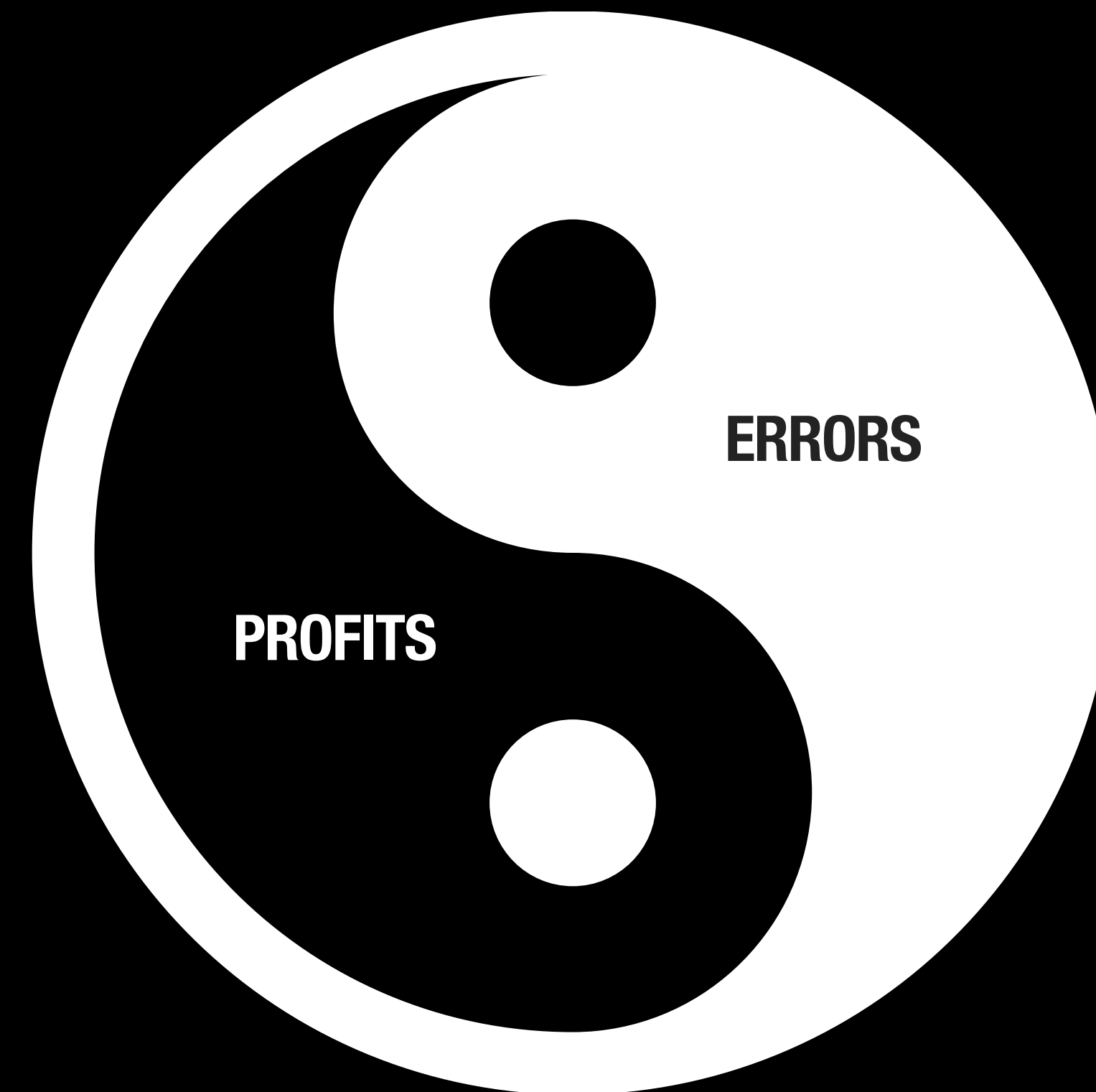
We would be competed out...

**Complexity  $\Rightarrow$  errors**

Unpredictability

$\Rightarrow$  need for care, and

$\Rightarrow$  profits :-)



# Errors

Errors are mostly  
unpredictable ⇒

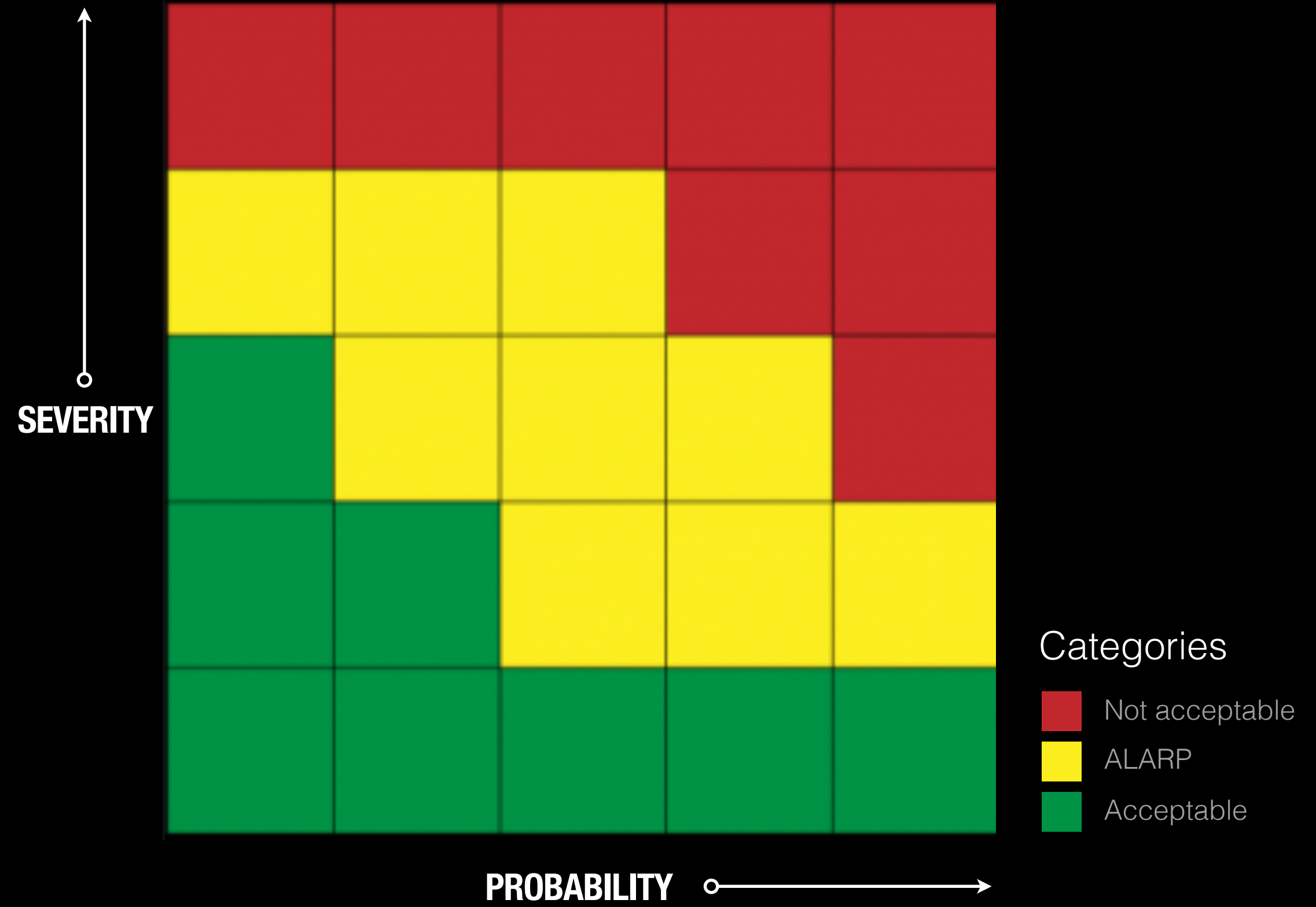
Business learns  
to live with risk

What does IT do  
with risk?

- Thefts of value - trading balances, capital
- Breaches of contract
- Extortions,
- Loss of customer data,
- Loss of faith, loss of reputation
- Fat fingers
- Regulation

# IT Bias

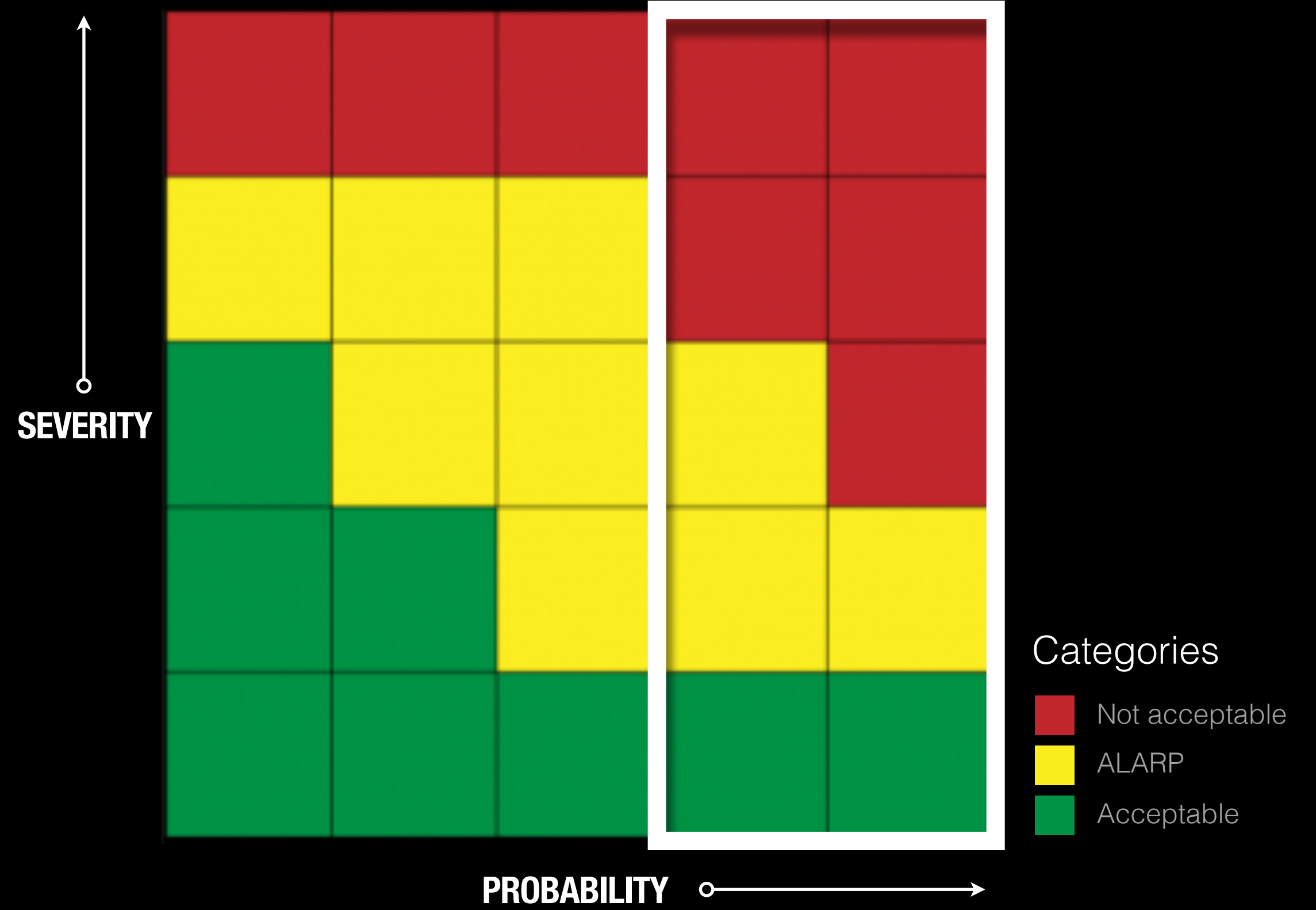
1. Against users



# IT Bias

1. Against users

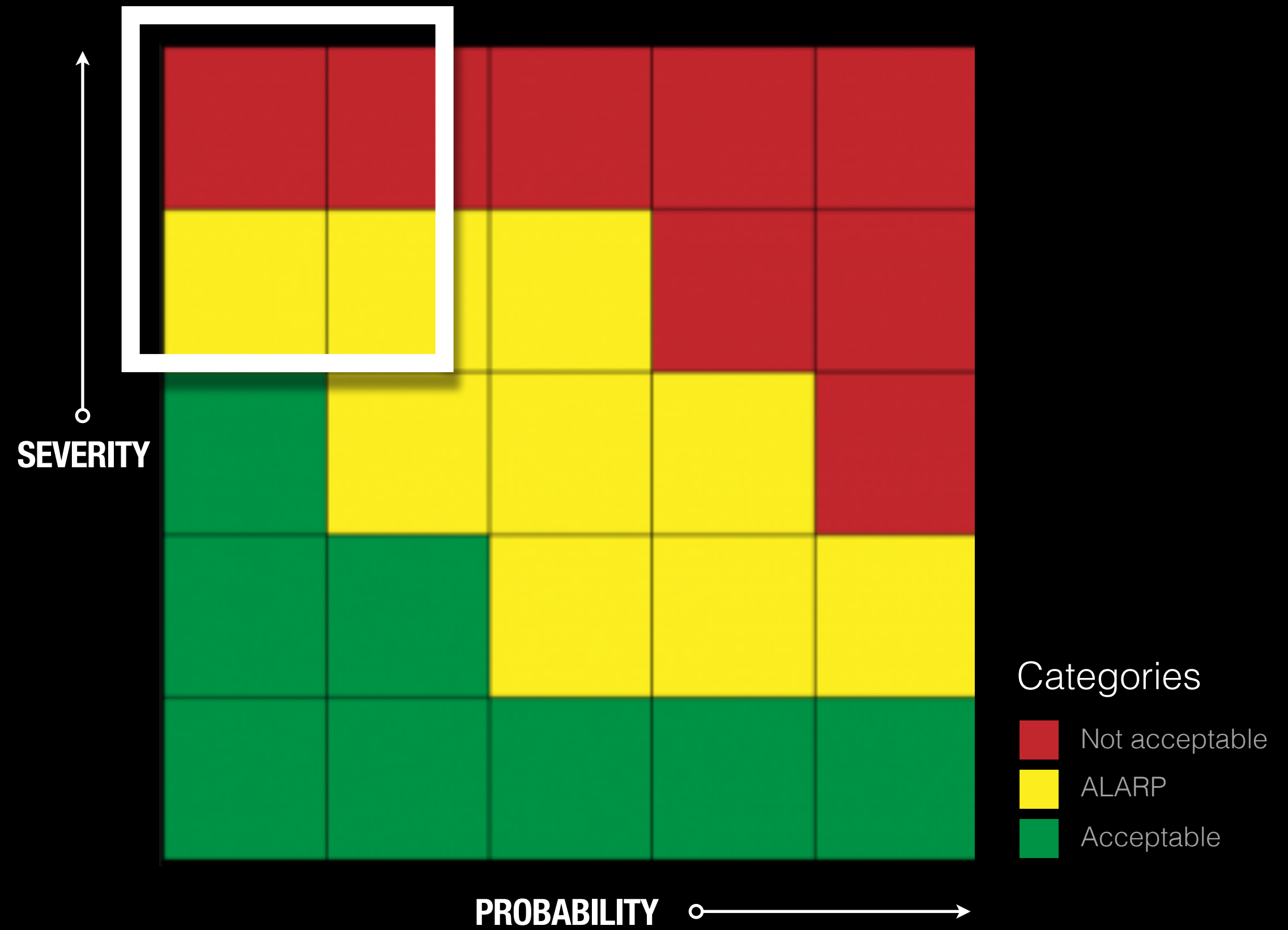
2. Knowledge



# IT Bias

- 1. Against users
- 2. Knowledge
- 3. Can't see?

Won't Happen!





2011  
500k stolen Mt.Gox

2013  
bug hard fork

2013  
179k 'Silk Road'

2014  
650k stolen Mt.Gox

2016  
I - 3.6mm ETH The DAO

2016  
II - Ethereum forks

2017  
I - Bitcoin forks

2017  
II - China forks...

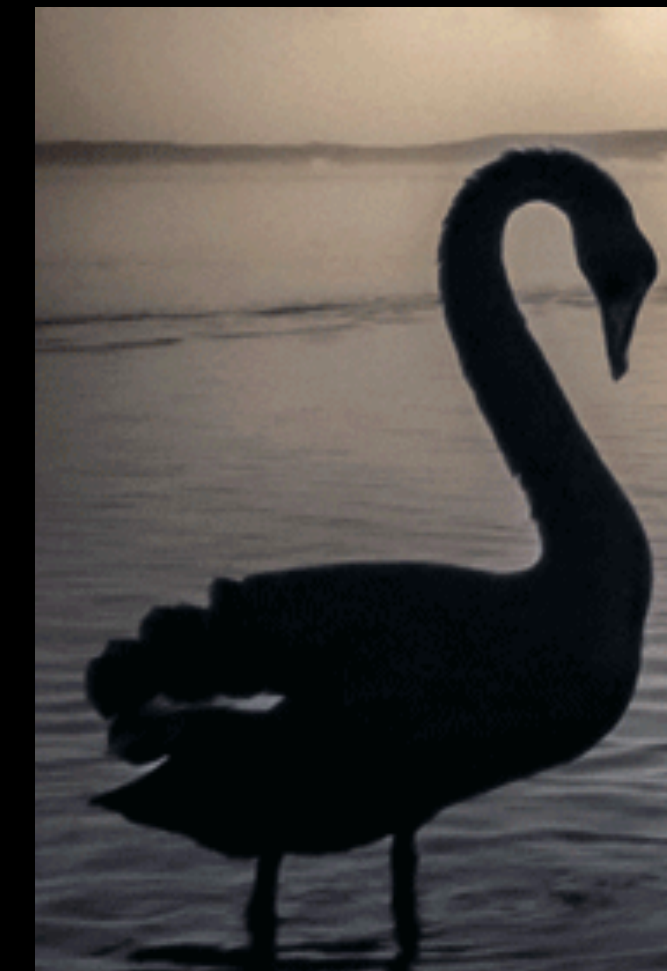


## The entrepreneur invests:

- Programmers, biz-dev, legal & accounting, web
- Cash - \$1mm and up?
- Time - 3m to 2 years

Question - why would entrepreneur invest if ...

**Black Swans ?**



## Proposal:

- the blockchain for business is
- the blockchain that solves the Black Swan

# Choice is Stark

Theft

Forks

Fat fingers

Sybils, trolls, spam

Privacy

Borked smart contracts

Disputes

Anarchy - but risk of loss

## IN REAL LIFE, WE USE TRUST

**Walled garden**

Trust outcompetes

**But excludes!**

**TRUST ! ?**

### **III. What is this thing called...**

## Trust is expensive - relationship, feedback

- Based on relationship  $\Leftrightarrow$  feedback
- Too expensive for one trade
- Trust  $\Leftarrow$  many many trades

## Game theory:

- Multiple rounds, no end in sight
- Shared profit from each round
- Punishments outside the game

**NOT JUST TODAY'S TRADE, BUT EVERY TRADE!**



## Negotiation theory:

- *(wants)* win-win
- *(gets)* win-lose

## Game theory:

- *(wants)* net-positive game
- *(gets)* Prisoner's Dilemma

## Negotiation theory:

- *(wants)* win-win
- *(gets)* win-lose

## Game theory:

- *(wants)* net-positive game
- *(gets)* Prisoner's Dilemma

	Stag	Hare
Stag	$a, a$	$c, b$
Hare	$b, c$	$d, d$

Fig. 1: Generic symmetric stag hunt

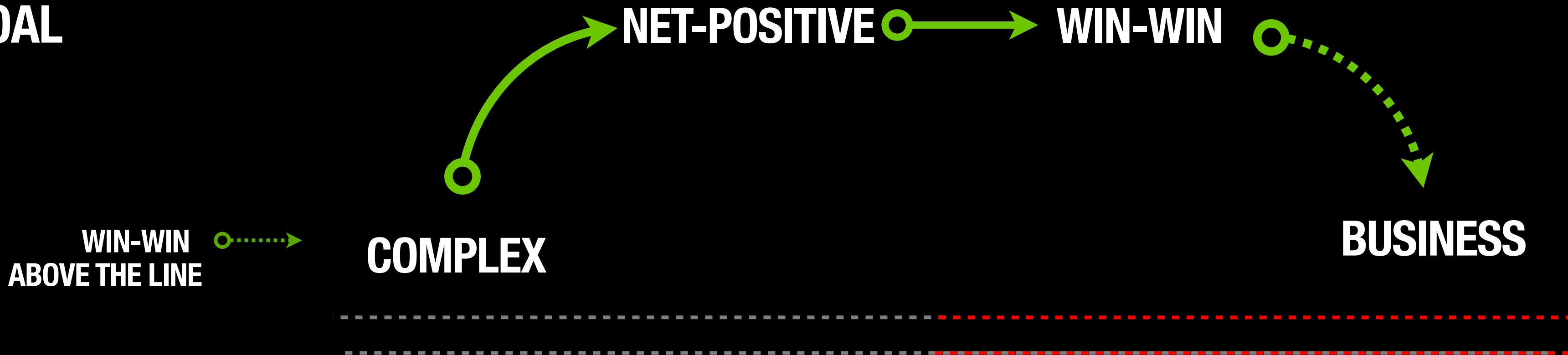
	Stag	Hare
Stag	2, 2	0, 1
Hare	1, 0	1, 1

Fig. 2: Stag hunt example

**Goal: THE BLOCKCHAIN WITH WIN-WIN**

# Let's Win above the line

**GOAL**



**SIMPLE**



**CONTENDERS?**

## Cultural opposition:

- Belief in the zero-sum game
- Suggests we export the win-lose to the business space - BAD.
- The DApps are all zero-sum: currency, ICOs, pumps&dumps, gaming, books
  - Get ahead in an ICO? *Fine, run a DDOS.*
  - See a fat contract? *Hack it.*
  - Don't like an opinion? *Call in a SWAT team.*

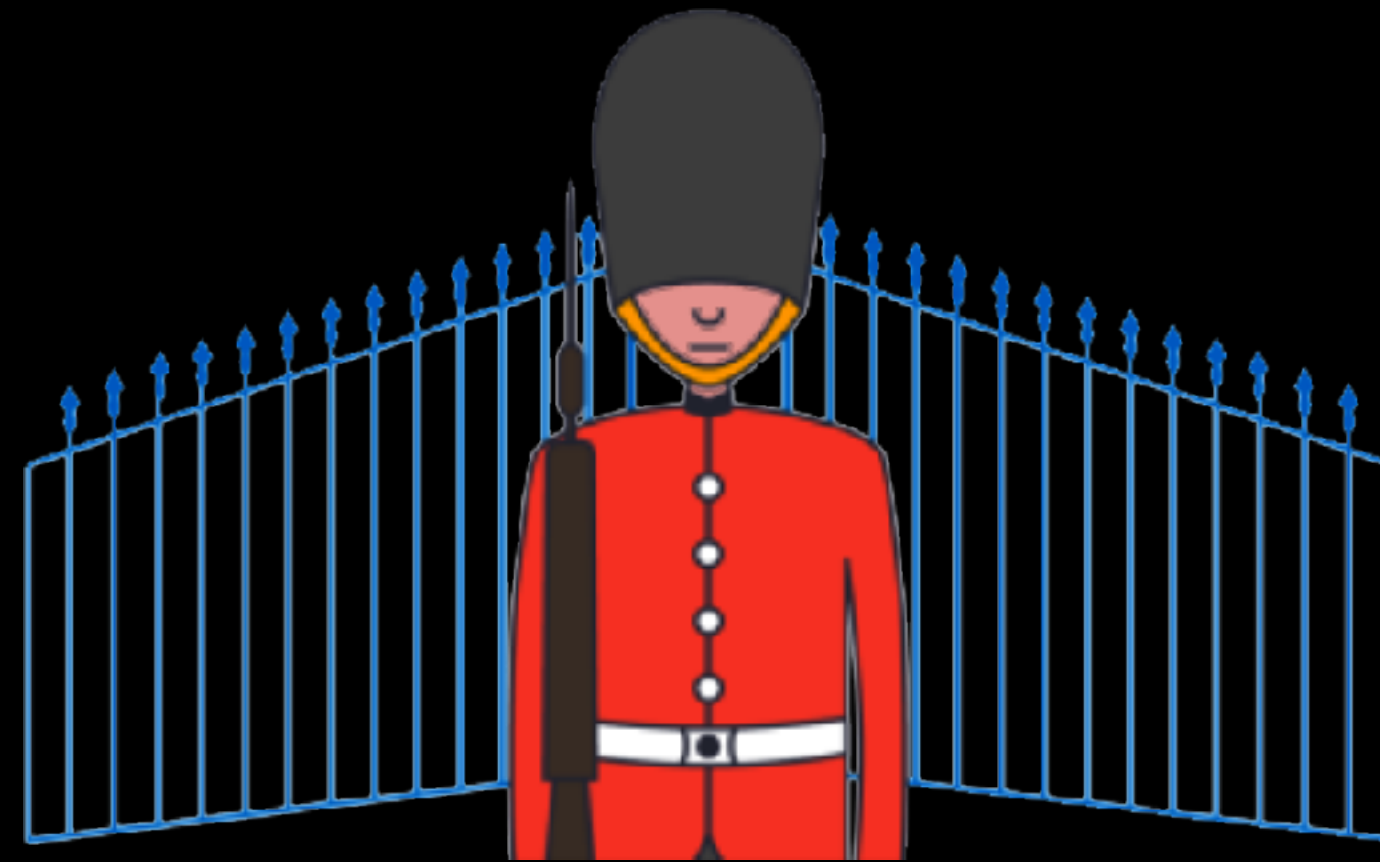
**ENTREPRENEUR WANTS  
MUTUAL PROFIT NOT  
EXTRACTION,  
PARTNERS NOT TOXICS.**

***Toxic customers***



## **The equation of win-win:**

- 1. A repeated round, no end in sight**
- 2. Remember who we are dealing with**
- 3. Rules of the game**
- 4. A way to trade (the blockchain thing, the smart contracts)**
- 5. A way to hold an aggressor to account...**



**A wall around the garden**

**A gate and a gate keeper**

*(Fees, fees, more fees)*

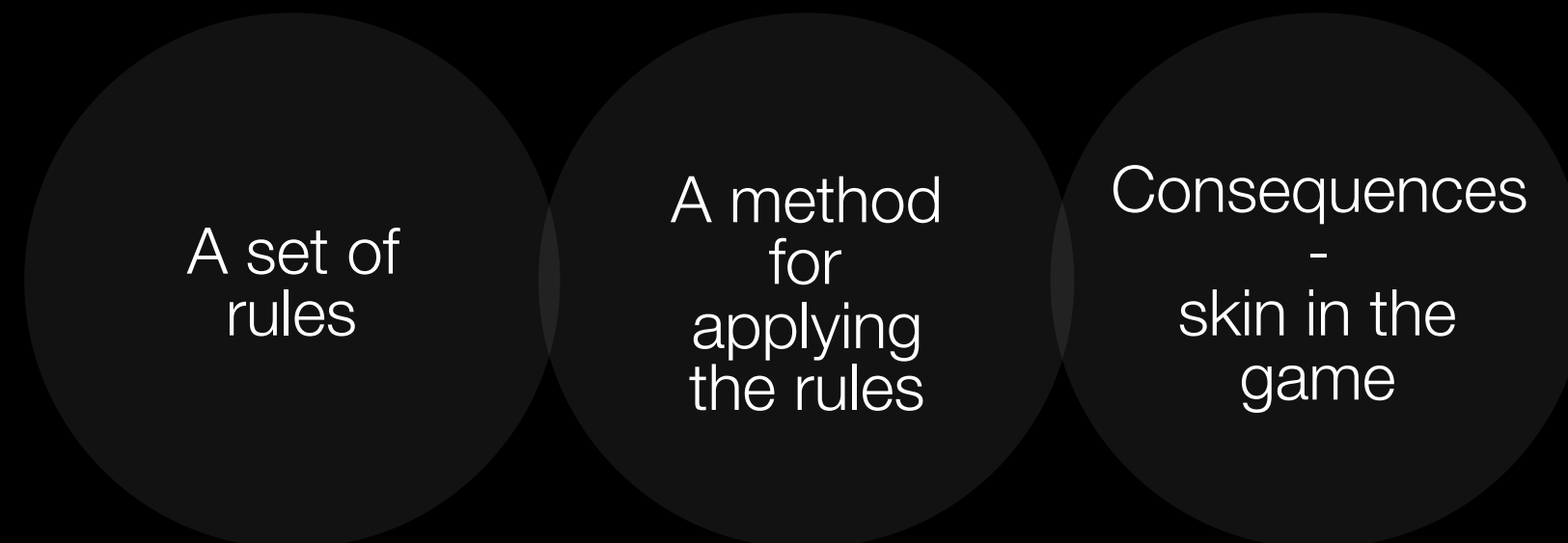
**A set of  
rules**

**A method  
for  
applying  
the rules**

**Consequences  
-  
skin in the  
game**

**A wall around the garden**

**A gate and a gate keeper**



**Many rounds, no end**

**Who we are dealing with**



# Tear down the wall

**We don't need it.**

**Proposal :**

- **A way of knowing who we're dealing with.**
- **Identity... (beyond scope of today)**

**(IDENTITY IS YOUR PERSONAL WALL)**

**Set of rules == Constitution**

**Entry agrees to Constitution**

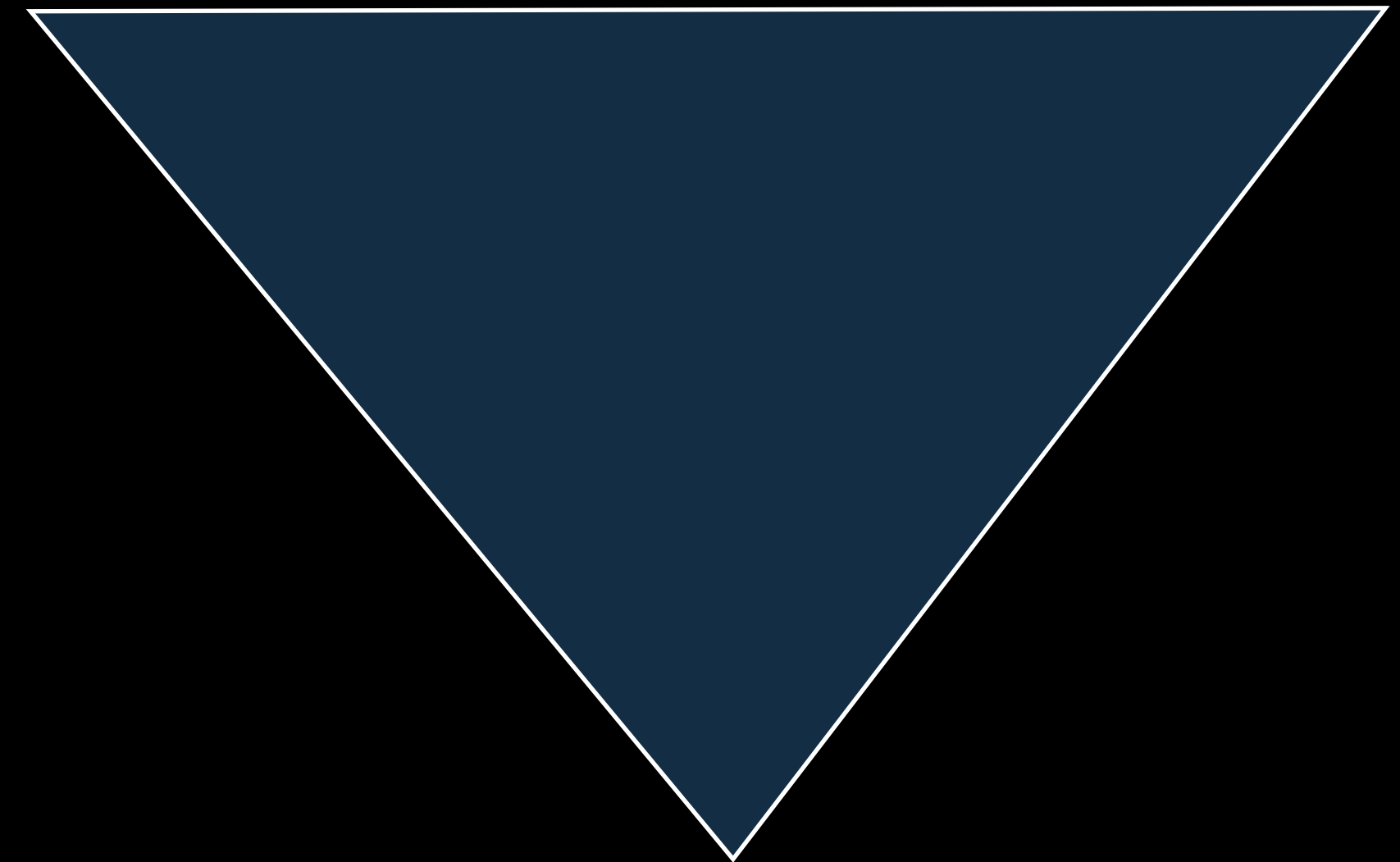
- *Preserves free entry*
- *Does not need a wall*

**Tx signs the Constitution**

**Community  $\Leftarrow$  Members' Intent + Constitution**

**INTENT**

**COMMUNITY**

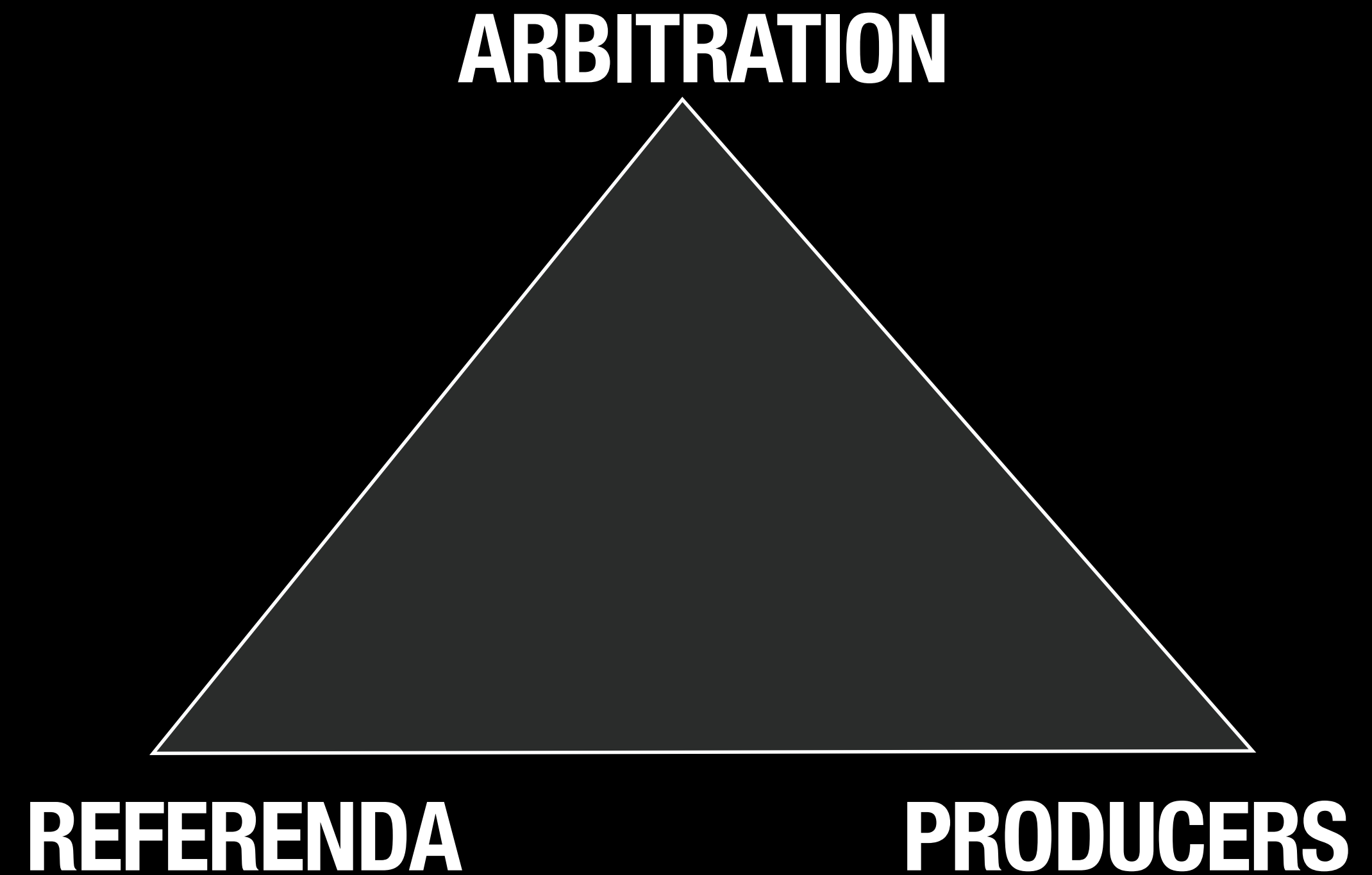


**CONSTITUTION**

## Baseline rules include:

- DPOS  $\Leftarrow$  delegated proof of stake
- referenda  $\Leftarrow$  to appoint roles
- Dispute Resolution  $\Leftarrow$  solve problems
- referenda  $\Leftarrow$  change the rules

**Community owns its Constitution**



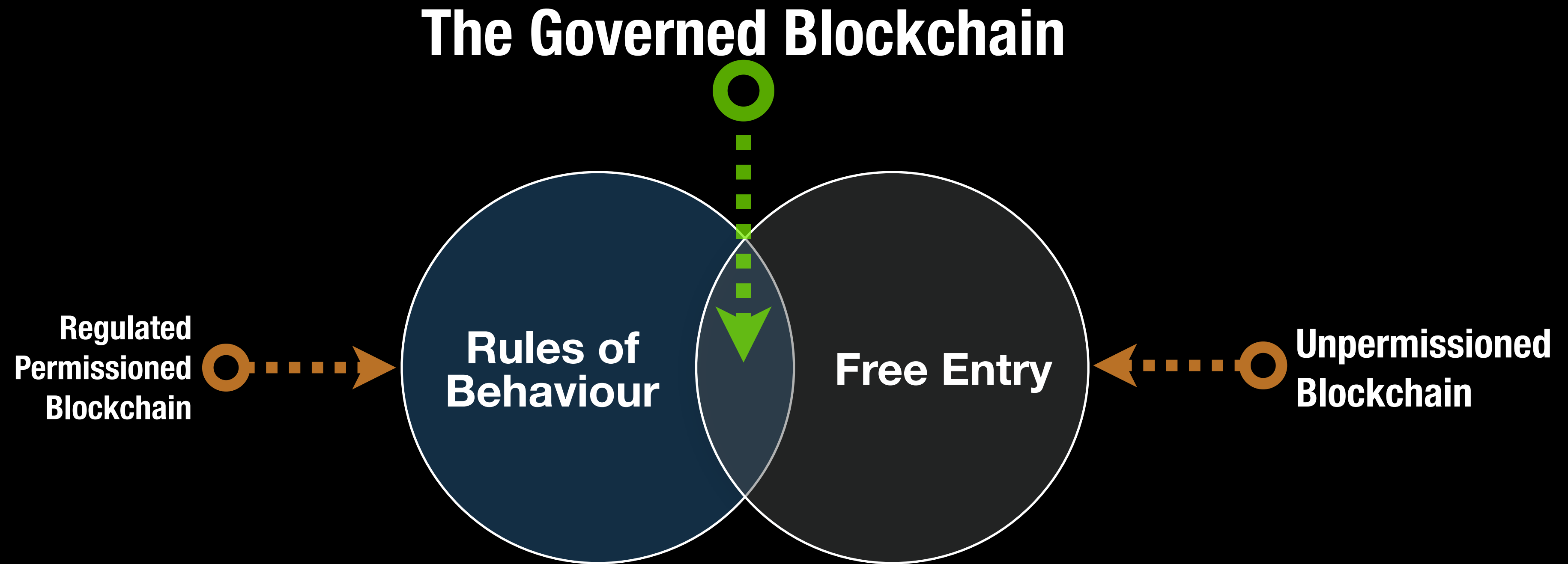
## V. Summary - (i) - Entrepreneur needs win-win

### Entrepreneur needs to make value not take value

- Unpermissioned  $\Rightarrow$  the taking of value, win-lose
- Permissioned  $\Rightarrow$  concentrates the value, excludes

—  
**Wanted: the freedom of one & protection of other**

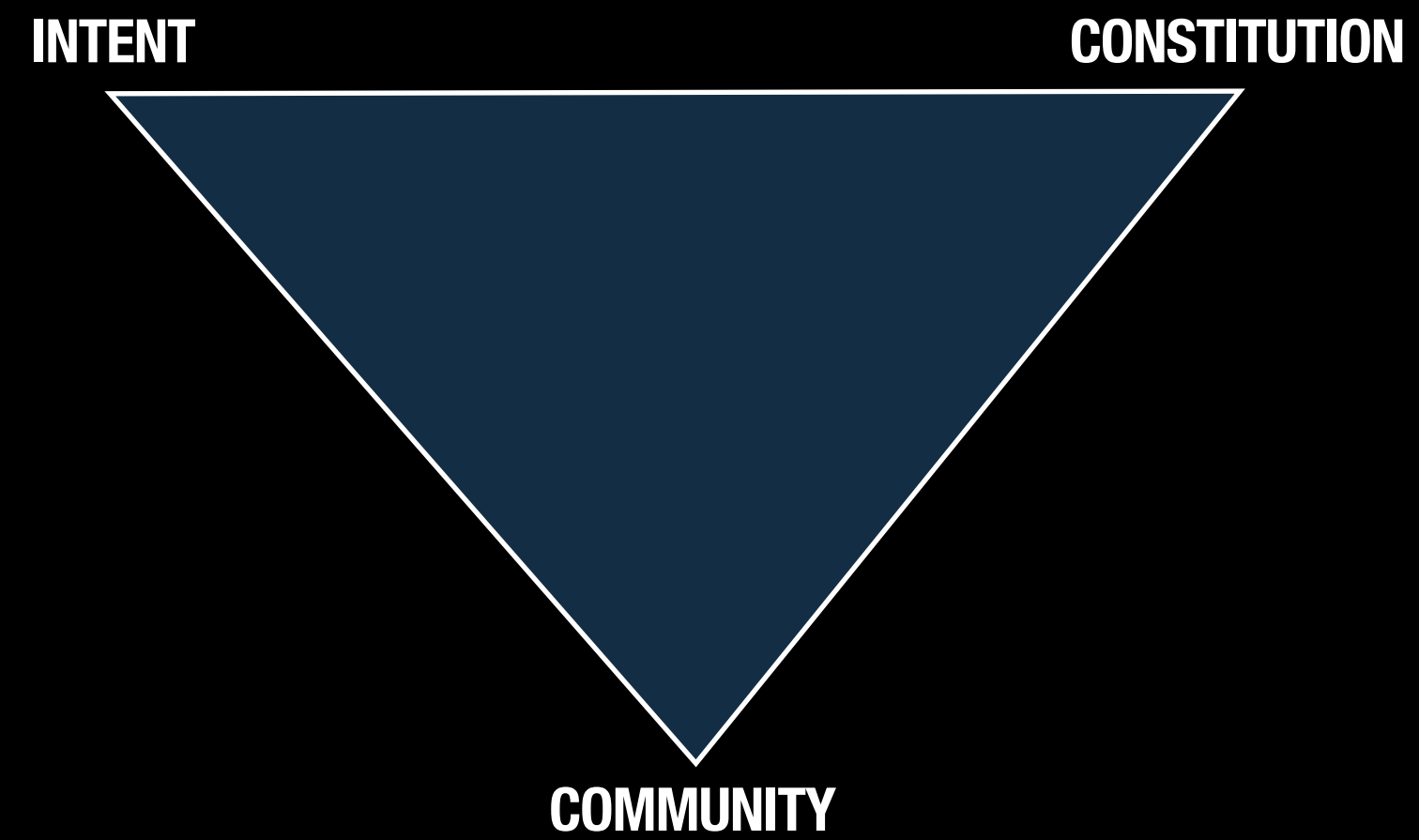
## Summary - (ii) - A third choice



**The fallacy is the wall:  
the real requirement is free entry**



## (iii) - The Governed Blockchain



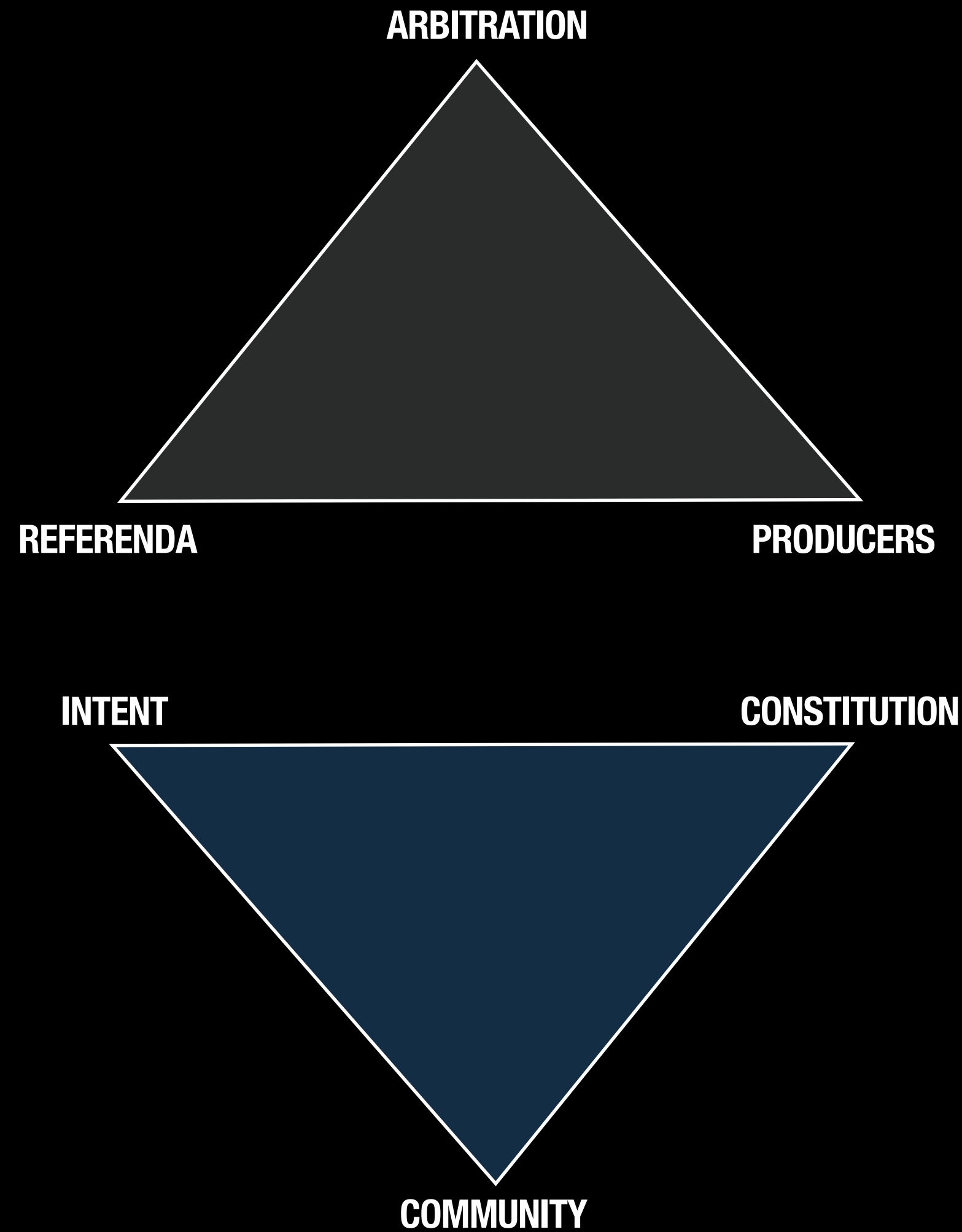
**Agree on entry:**

Intent + Constitution == Community

---

**Sets rules**

## (iii) - The Governed Blockchain



### Rules to resolve the Black Swan

- set roles: Producers, Changes
- resolve disputes: own forum

### Agree on entry:

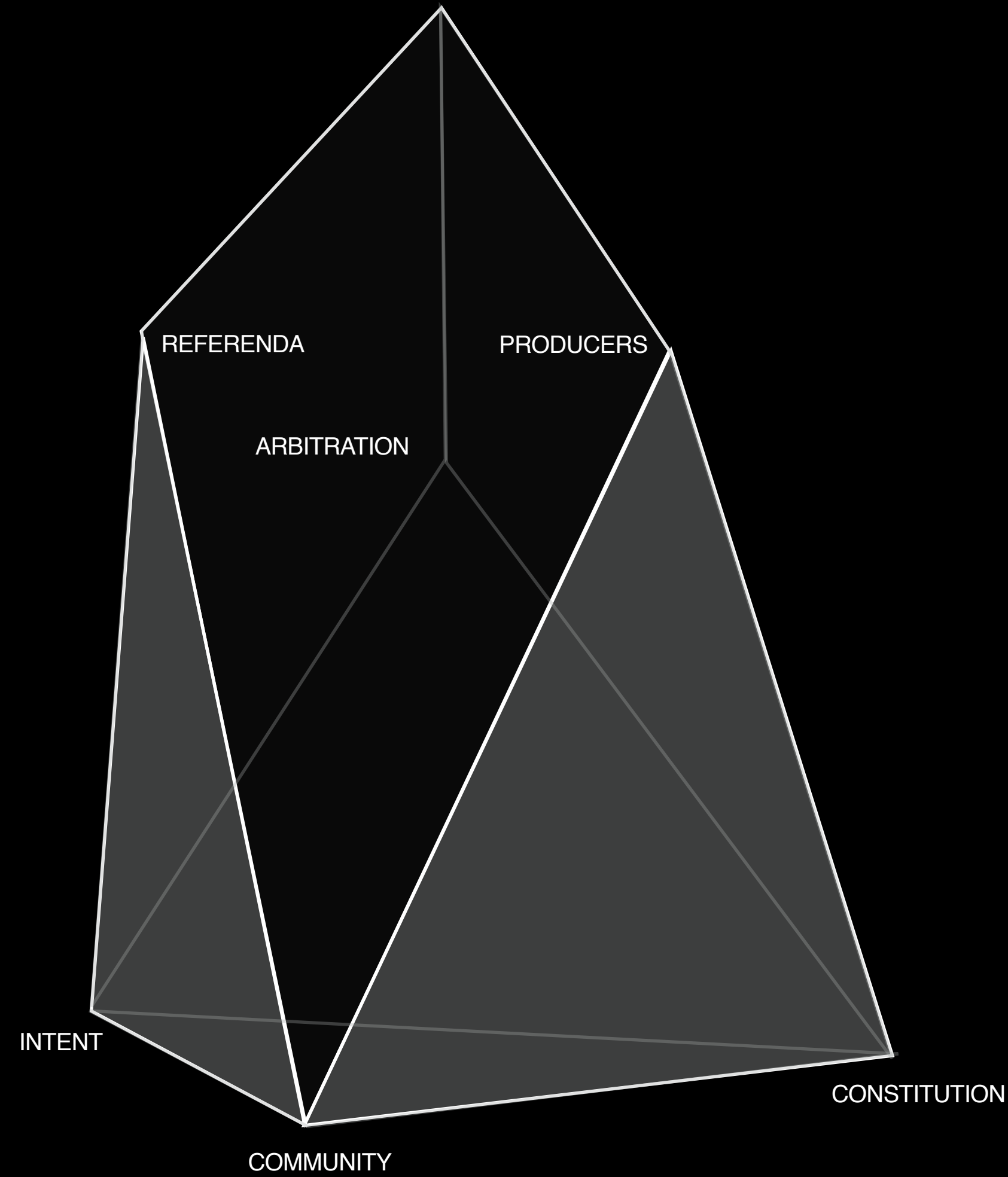
Members + Constitution == Community

---

**Sets rules**

EOS is...

# THE GOVERNED BLOCKCHAIN



**Thank you!**