

EOS



An Introduction

lang

Financial cryptographer

Inventor of Ricardian contracts

co-Inventor of triple entry accounting

Identity

ex-R3

“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/>

Disclaimer...

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.

But - *Cryptocurrencies are dangerous places.*

Not advocating an investment - Caveat Emptor



Where are we?

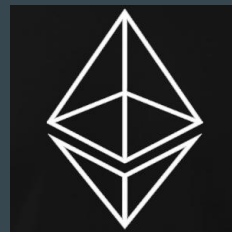
Bitcoin - great first effort?



BTC rules the cryptocurrency world, but wither smart contracts?

Ethereum - exciting potential for smart contracts

but progress is slow... ERC-20 crowdfunding is the success?



Corda - strips out blockchain - p2p workflow.

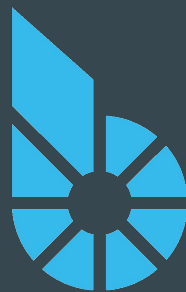
But for us?



Meanwhile, back in *userland*...

Bitshares is first successful business on a blockchain!

Issuance! Trading! Synthetics!



Steem is first successful *userland* DApp (hides blockchain)

blogging! Rewards!



Don't we need more of these?

STEEM

The state of the CryptoCurrency Nation

Consensus - client-server → PBFT → PoW → PoS → DPOS

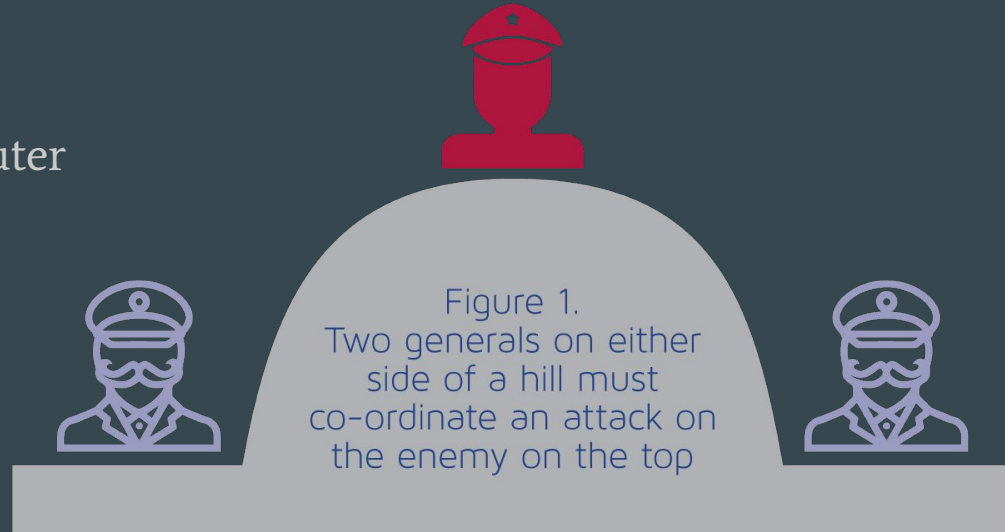
Value - card2card, blinding, triple entry, UTXO, ERC-20

Blockchain as engine of state - UTXO

Contracts - Bitcoin script, Turing computer

Performance - 3, 15 TPS

Governance - adhococracy



Vision - what does Alice want?

Talk to friends - know them, pay them, be paid

Contract - make small agreements, build big business

Retain and use value - safety, security

Find predictability in chaos

growing business, dev market, fix problems



*Alice in
Cryptoland*

Smart business for *ordinary* Alice!

EOS.IO software - the secret plan

Take Bitshares & Steem codebase ...

Scrape off the biz logic, throw it away

Add smart contracts.

Don't tell anyone!

with apologies to Elon Musk :-)

Architecture - The Medium is the Message

Uses messages not state

To recover, replay all the messages

Under determinism, state == messages

“State” is implied \Rightarrow Optimise



Architecture - Seeking Consensus

DPOS == Delegated Proof of Stake

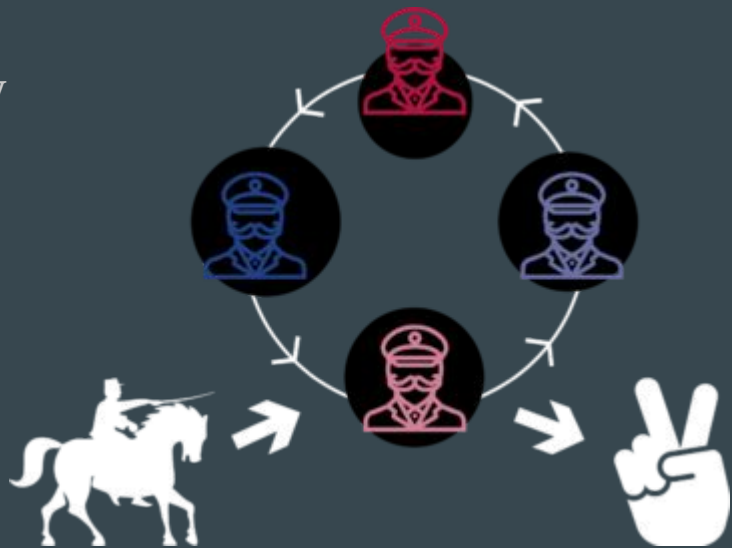
“Producers” selected into a round by Community

Each does 1 block, in random order

Every round, can be voted out

Separation of Stake from decision

eliminates “nothing at stake”



Architecture - The Contract

Accounts send *messages* to *handlers* on other accounts.

The *handler* is code that can also send messages.

Compose code + messages + semantics (prose) == smart.

Messages are *committed as intent* by the blockchain, both in and out

Smart contracts is not settled science



Architecture - Usability

Usability means: how to build a DApp?

like Steemit, like Bitshares

Web based toolkit - DApps are 90% in common

WASM - fast, standard, will get all the main languages

Wren - easy to understand, reason about, learn

Experiments continue...

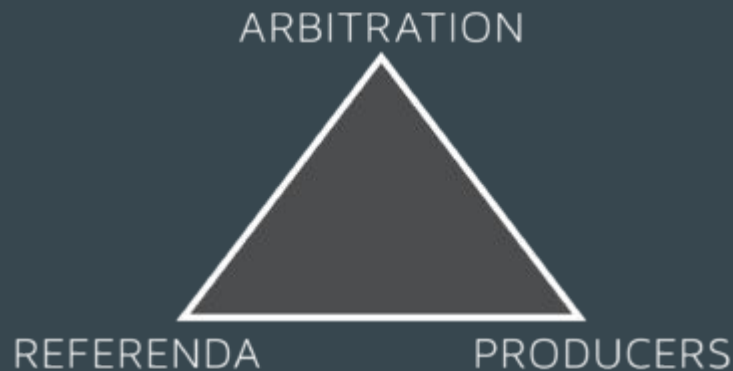


Architecture - Governance

DPOS - delegation establishes/requires community

Community \Leftarrow Members + Constitution

Every transaction signs the Constitution



All usage under Constitution

\Rightarrow problems? Add arbitration

The Community is in driver's seat

Comparison

Bitcoin - low TPS, unused contracts, poor issuance, adhococracy

Ethereum - Turing machine is good, but contracts are uncertain, adhococracy, low TTP

Corda - not a blockchain \Rightarrow great TTP. Marketplace uncertain - big corp.

The point is SMART business

users on DApp \Rightarrow devs onto a toolkit

High throughput - 50k TPS

Contracts as mesh of handlers

Community \Rightarrow appoint governors

Community! Are the base \Rightarrow

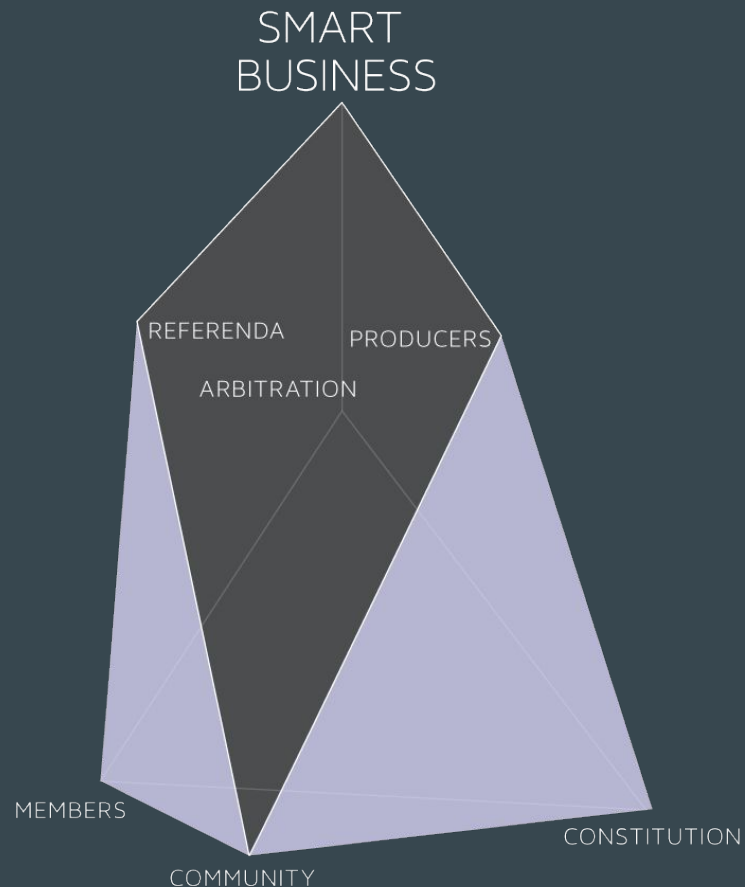


Fig. 7. The point is Smart Business



block.one is ...

Block.one is: Brendan, Abby, Dan, Guo, Josh, Aaron, Christian, Nathan, Wendy,
Andrew, Michael, Brock, Winnie, Phil, Gerlof, Bo Shen, Li Xiao Lai, Sanjay, Brian,
Tama & Iang

Busy!