Ethereum and Web 3.0

How we arrived and where we’re heading

Sumukh Shetty

co-founder, Automte Labs

sumukh@automte.com

The problem

Agreement necessary for collaboration.

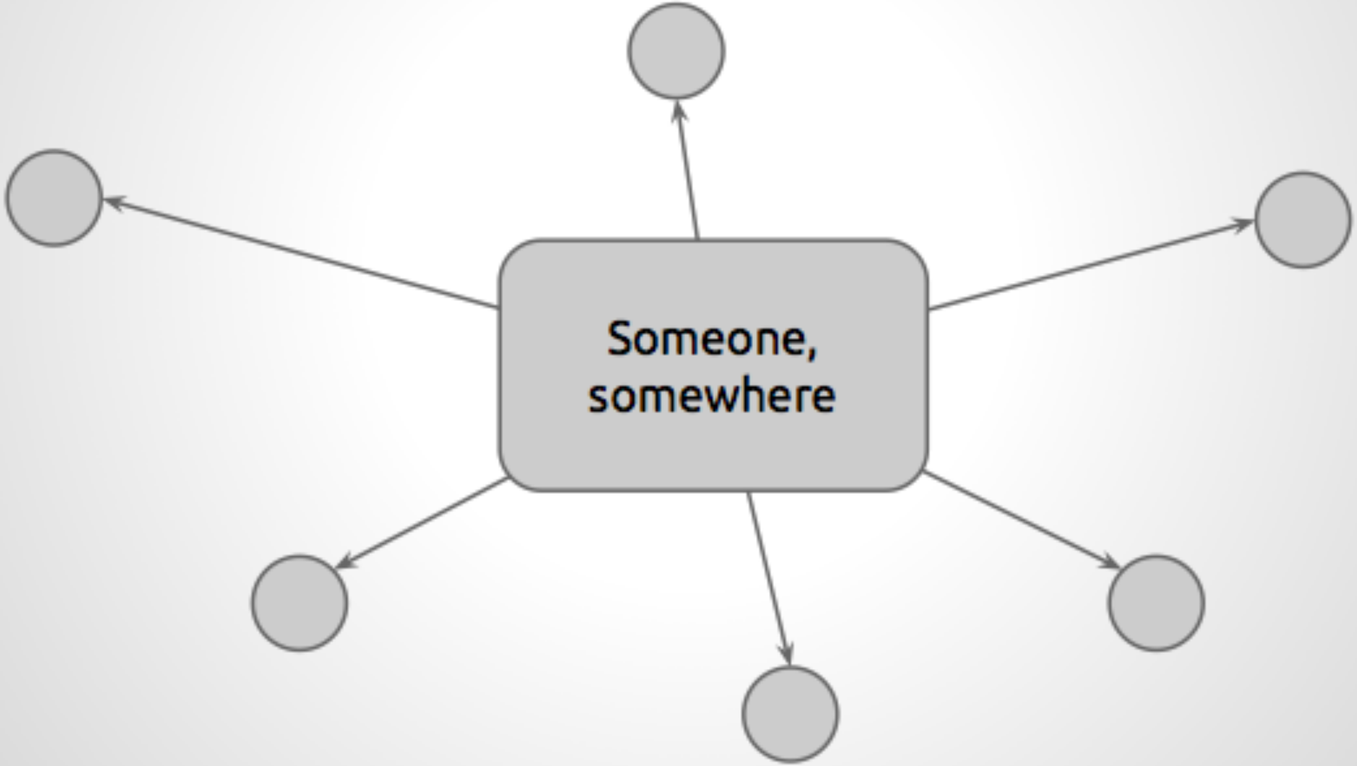
Internet is great for communications
but...

Too easy to lie.

The old solution

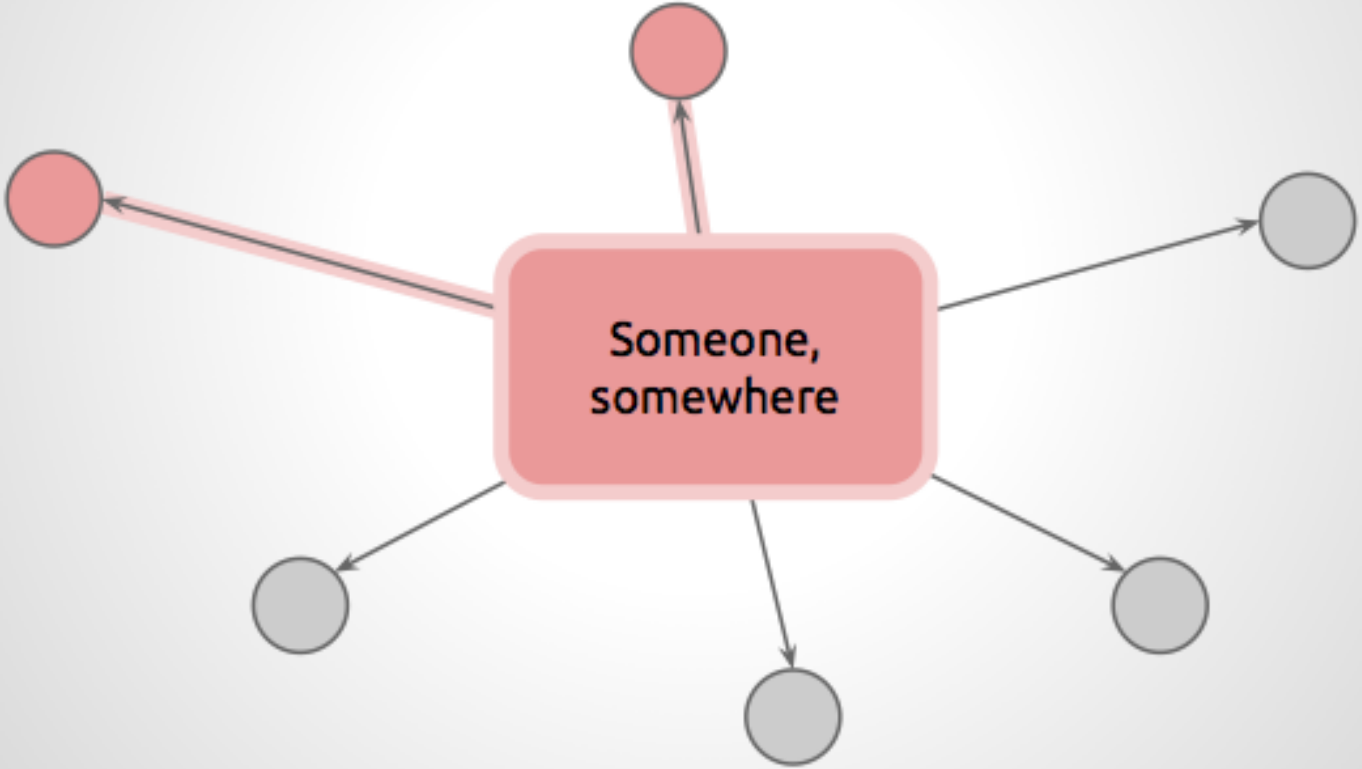
1. Identify authority
2. Allow authority to impose “truth”
3. Blindly trust authority

How things are :-(



Someone, somewhere

How things are :-(



Problems with Centralisation & Central Authorities

Single point of control

Single point of failure

Single bottleneck

Trust

Cost of Meddling: ~£0 (Marginal)

Cost of Attacking: ~£0

If you must trust, trust people, not orgs!

The limitation

Authority may be:

incompetent (Sony &c. vs thieves)

compromised (Google/Facebook &c. vs. NSA)

biased (Visa/Mastercard/Paypal vs. Wikileaks)

corrupt

unavailable

unknown

Technology!

Can’t we do better?

“YOU NEVER CHANGE THINGS BY FIGHTING THE EXISTING REALITY. TO CHANGE SOMETHING, BUILD A NEW MODEL THAT MAKES THE EXISTING MODEL OBSOLETE.”

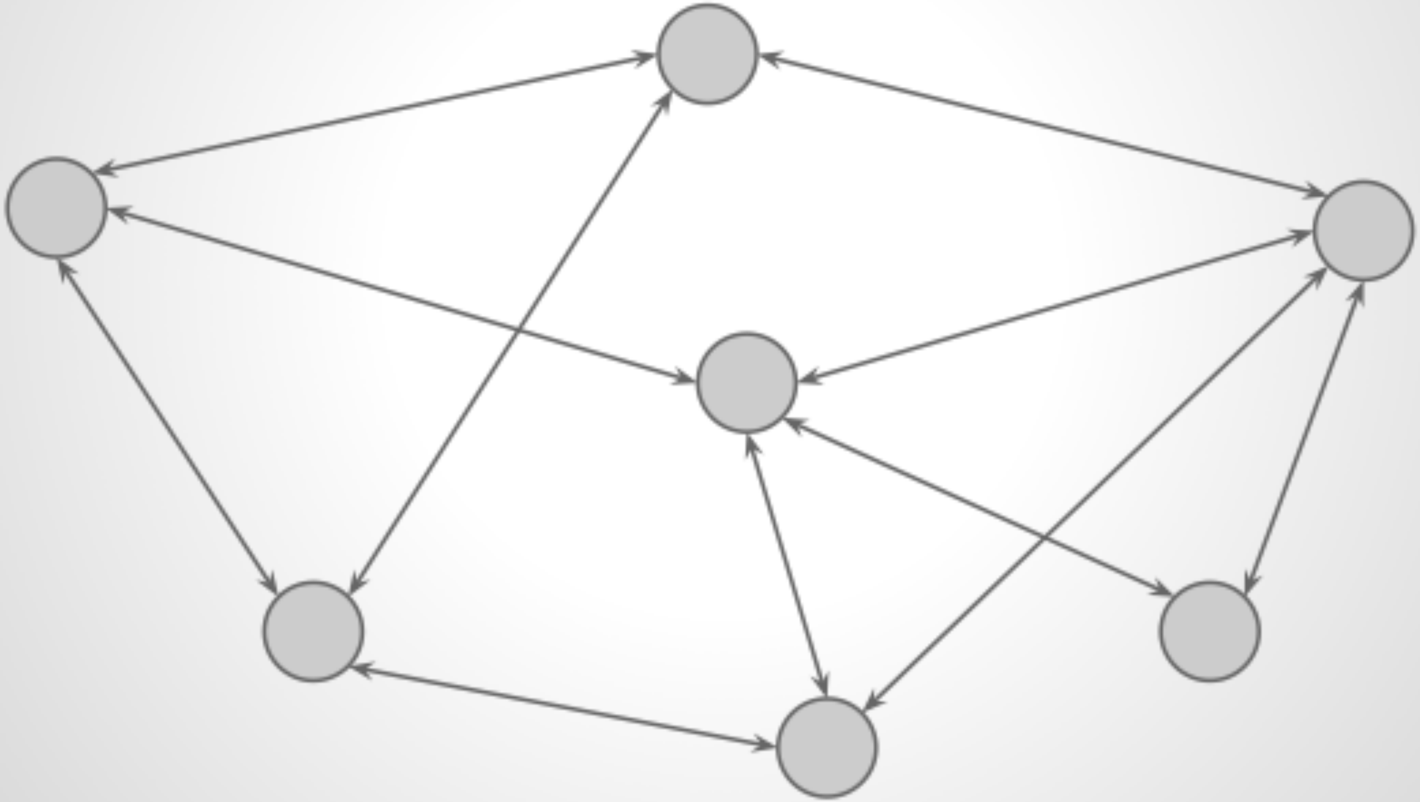
- BUCKMINSTER FULLER

The new solution

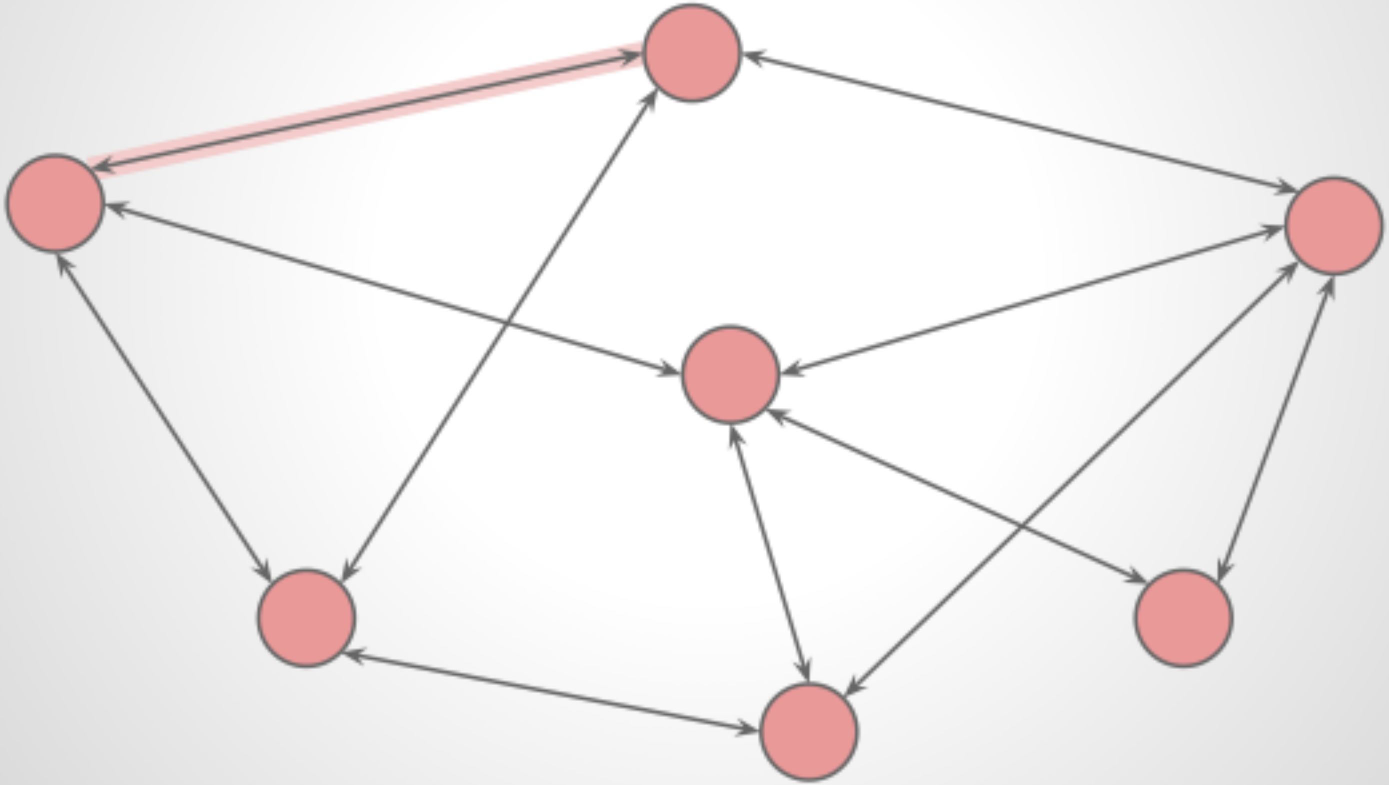
Avoid relying on authority.

Use consensus of peers.

How things should be :-)



How things should be :-)



Basic Premise

“The truth is more common than any one lie”

Liars can try but, ultimately, they’ll be ignored by all others.

Which makes…

A decentralised solution for any sort of **chronicling**.

Chronicling: Time-series of archivable data

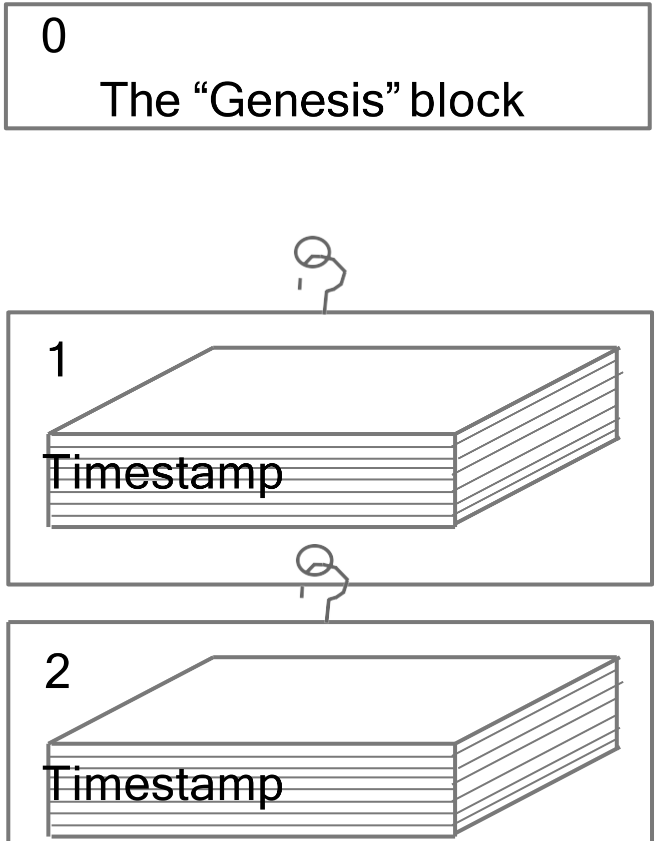
Block chain?

Digital messages (transactions) bundled into:

...Blocks.

Blocks linked in a chain to form chronicle.

The “Block Chain”



0

The “Genesis” block

1

Timestamp

Proof-of-Work

2

Timestamp

Proof-of-Work

The blockchain will be to banking, law and accountancy what the Internet was to media, commerce and advertising.

Joichi Ito, Director of the MIT Media Lab

Bitcoin

Transaction: the **transfer** of some **value** so it can only be transferred **onwards** by using (signing with) some **secret**.

Chronicle: The total **value accessible** by each **secret** key.

i.e. the account balances

Why form consensus?

Alice starts with **$100**

At the same time:

Alice transfers **$100** to **Bob**

Alice transfers **$100** to **Charlie**

What happens?

The "double-spend" solution

A **chronicle** that everyone agrees on forces a single **order**. This is required.

$100 goes to **either** Bob or Charlie, but never both.

Second transfer ignored as no funds left.

Everyone agrees upon the recipient

The Alts

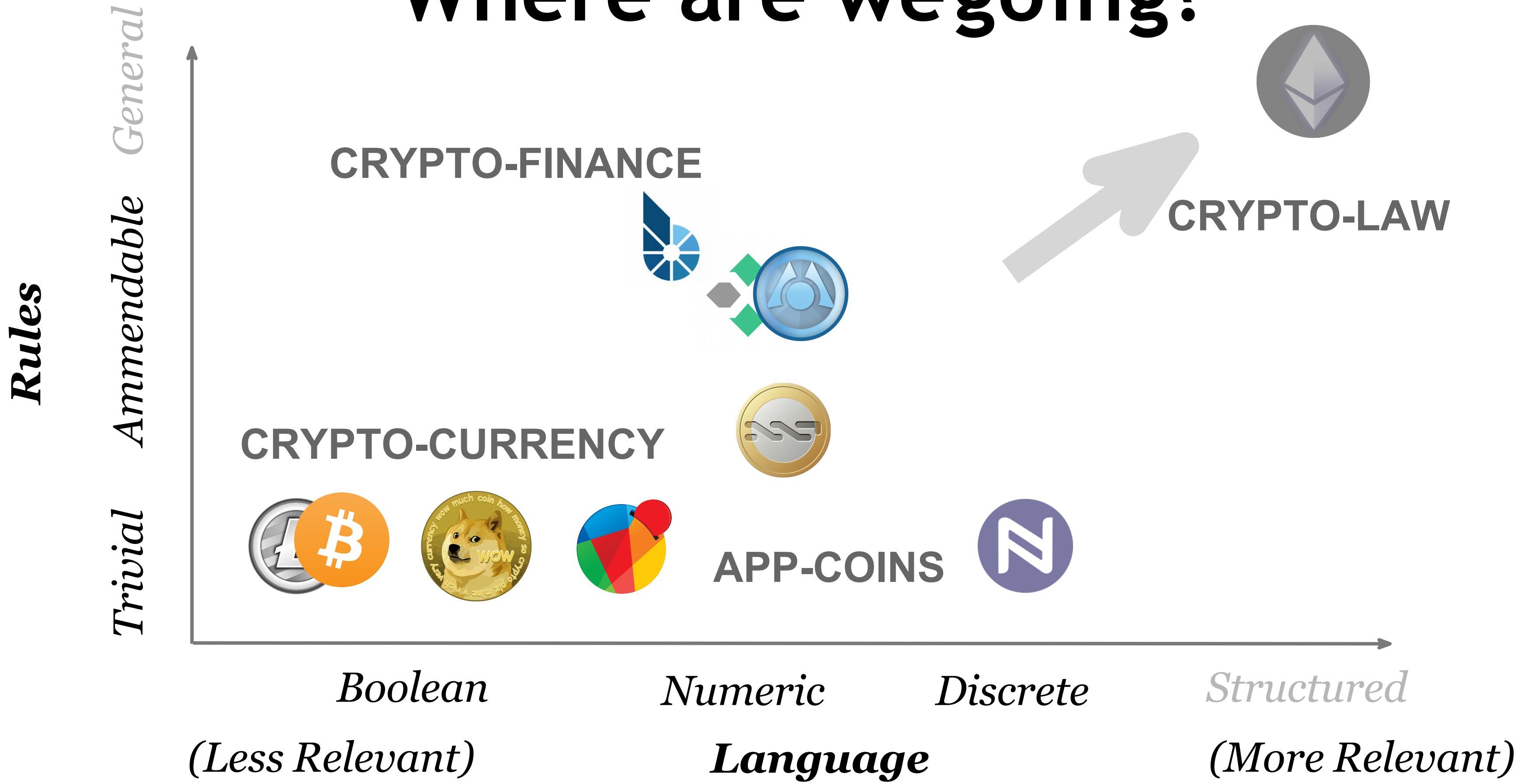
Attributes altered such as:

Proof-of-Stake: virtual “proof-of-work”

Supply: increase, reduce, fixed, random, select

Speed: Lower block-time

Where are wegoing?



CRYPTO-FINANCE

CRYPTO-LAW

CRYPTO-CURRENCY

APP-COINS

Rules

General

Ammendable

Trivial

Boolean

Numeric

Discrete

Structured

(Less Relevant)

Language

(More Relevant)

What is Ethereum?

Chain to State

It’s one thing to have a single chronicle,
it’s another to know what it means

What is the language?

Transaction Semantics

...or the **meaning** of a transaction.

And thus the accumulated meaning of the chronicle.

Formally…

Collective of Non-Localised Singleton Programmable Data-Structures

no authority, no centre, no server

Simile

Internet is to communication

as

Ethereum is to agreements

Another Simile

Ethereum *is to Bitcoin*

as

a ***smart-phone*** *is to a calculator*

It’s a Computer, Silly!

Slow

Code runs 5-100x slower than natively compiled

Expensive to use

Basic computation, memory and storage costs are ~1950s levels

Not always immediately decisive

Actions of last 60s may be reorganised

Sounds. Awesome.

Actually, it is.

Truly Global Singleton

One computer for the entire planet now and forever

Cannot Fail, be Stopped, be Censored

No authority, government or corporation behind it, resistant to attack

Ubiquitous

Where ever there’s Internet, there’s Ethereum

Natively Multi-User

Has as many accounts as is needed

Natively Object-Oriented

Encapsulation enforced in “virtual silicon”

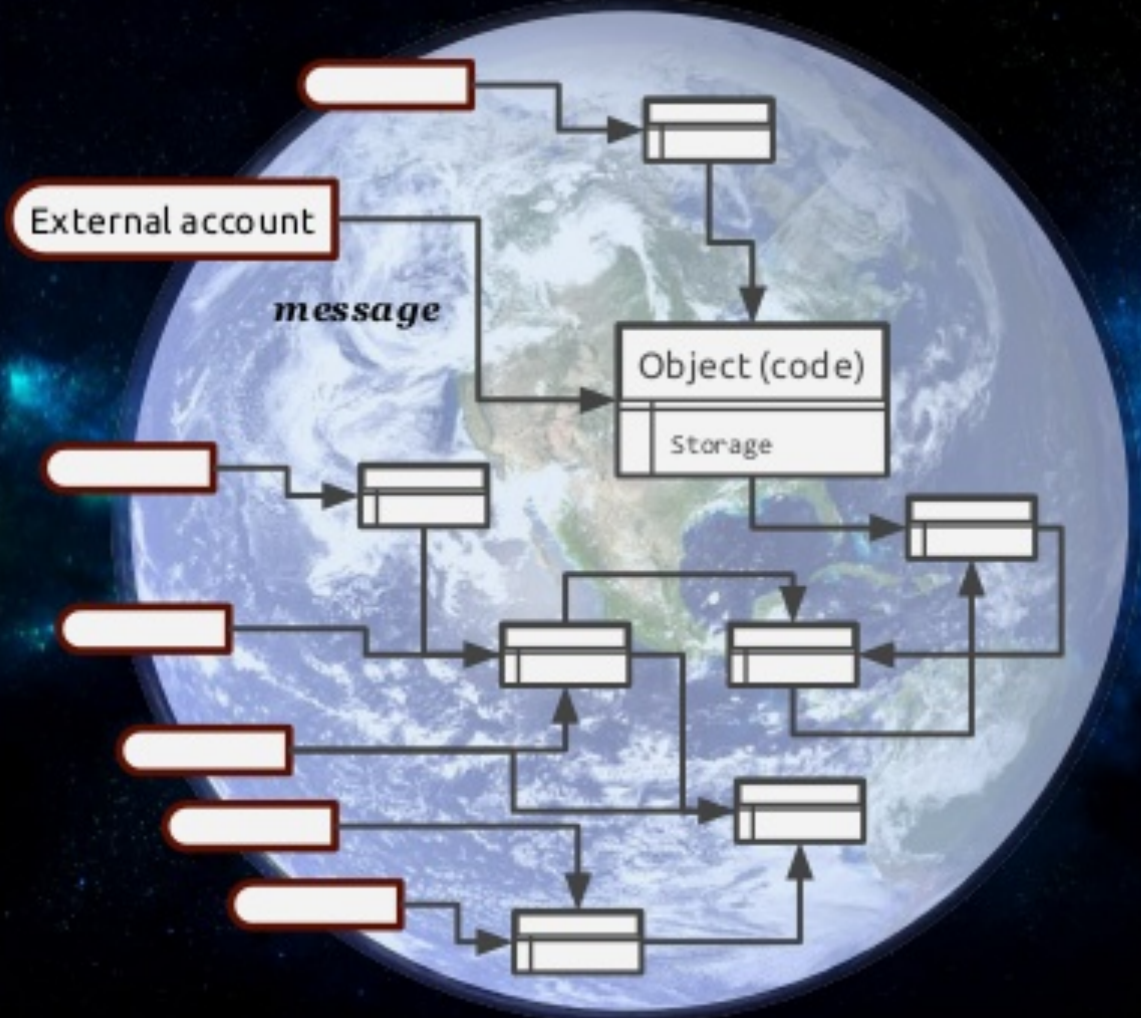
Accessible

Where ever there’s Javascript, there’s Ethereum

Verifyable & Auditable

All code honoured now and forever

The **World** Computer



Guarantees

Atomicity

Entire operation runs or nothing does

Synchrony

No two operations can interfere with each other

Provenance

All messages (method calls) can be inspected to determine caller address

Guarantees

Permanence

Object's data are **permanent**

Immortality

Object can **never** be externally deleted - can only voluntarily commit suicide

Immutability

Object's code can **never** be changed

Bitcoin & Crypto-currencies

Used **blockchain** to implement basic **clearing house contract** without a central server

Ethereum & Crypto-law

Uses **blockchain** to implement **arbitrary social contracts** without a central server

Take a step **back**

A Contract is...

A document which defines a **common understanding** intended to be **enforced** under **law**

Inefficiencies with status quo

Mostly paper

Slow and heavy

Errors creep in

Costly

Processes are stone age

Expensive lawyers required at every stage, often doing trivial “work”

Why? Certainty.

Certainty, provided by large institutions, is costly. Cost becomes endemic.

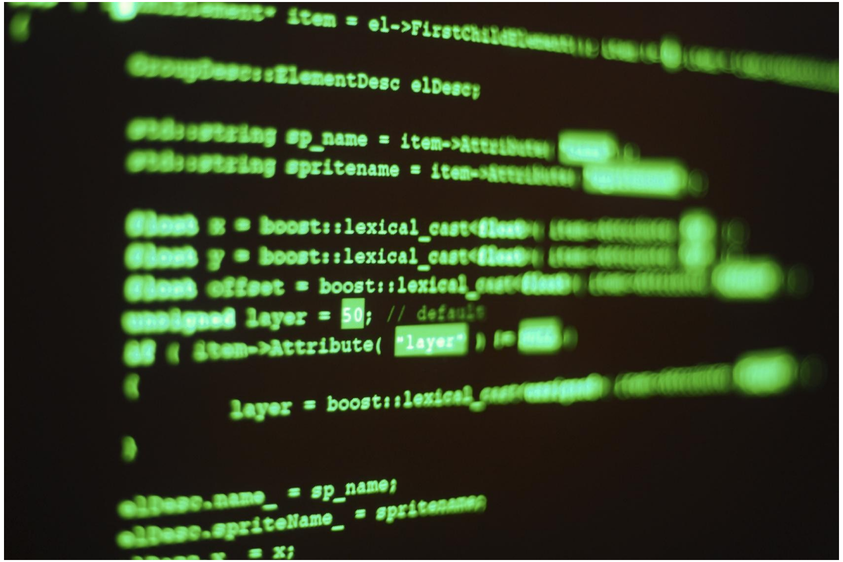
The system of law…

…is a bit like a system of computation

Lawyers are electrons,

institutions are silicon.

So... contracts?



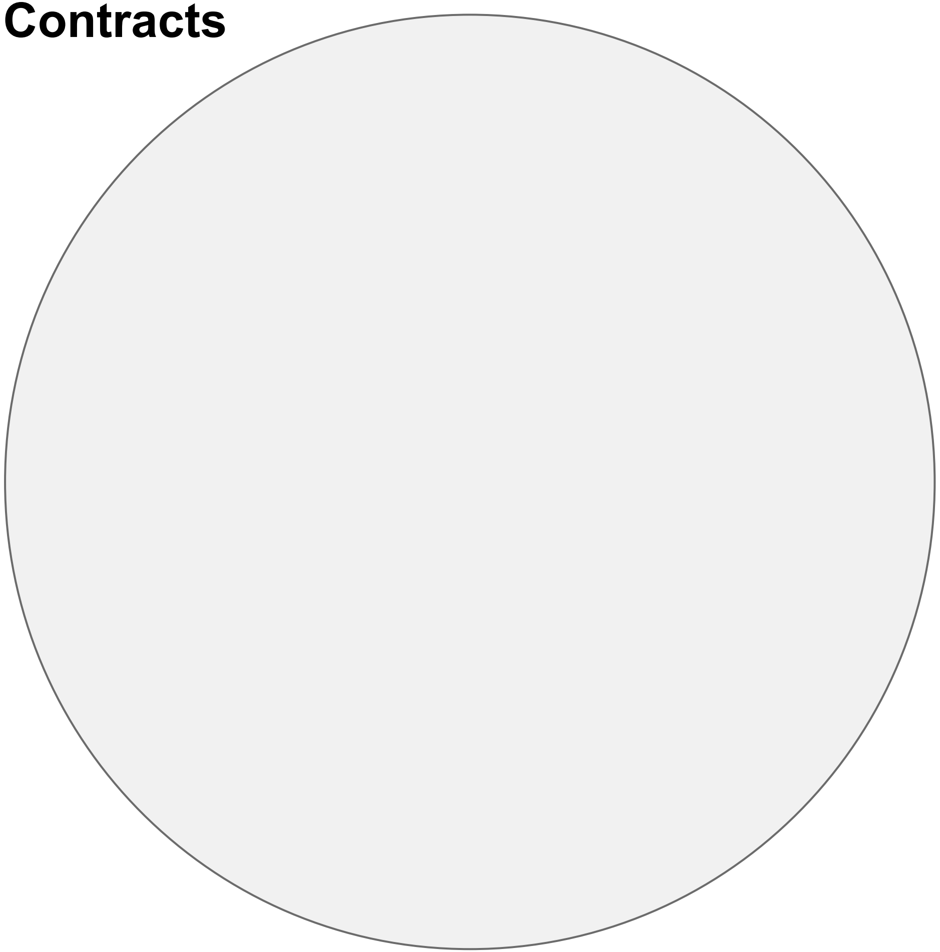
```
    [illegible] item = el->FirstChildElement[illegible]

    GroupDesc::ElementDesc elDesc;

    std::string sp_name = item->Attribute( [illegible]
    std::string spritename = item->Attribute( [illegible]

    float x = boost::lexical_cast<float>( [illegible]
    float y = boost::lexical_cast<float>( [illegible]
    float offset = boost::lexical_cast<float>( [illegible]
    unsigned layer = 50; // default
    if ( item->Attribute( "layer" ) [illegible]
    {
        layer = boost::lexical_cast<[illegible]
    }

    elDesc.name_ = sp_name;
    elDesc.spriteName_ = spritename[illegible]
    [illegible] = x;
```

Processes (understandings) are software

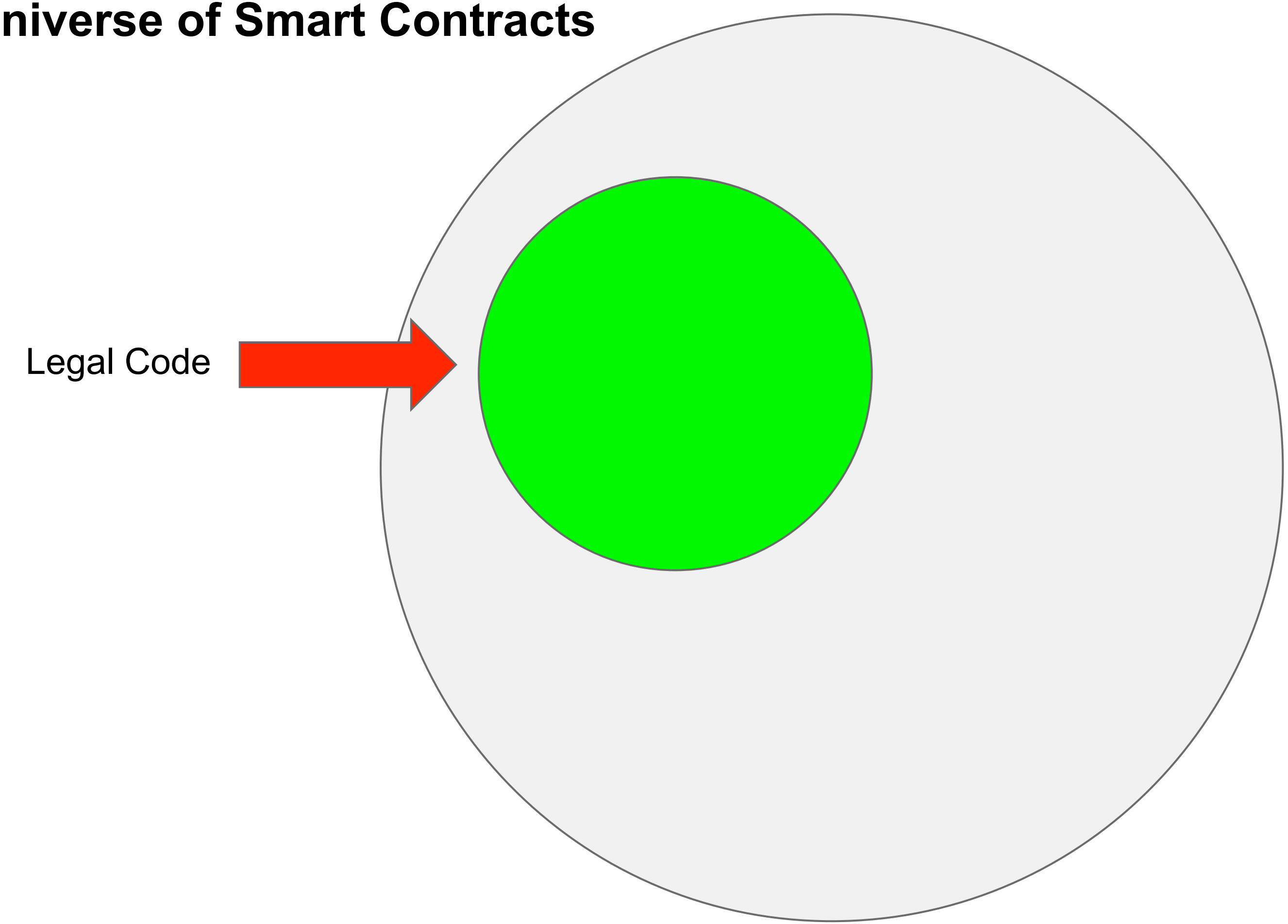
Smart contracts

Use of **code** and a **blockchain** to execute logic if certain conditions are met.

Universe of Smart Contracts

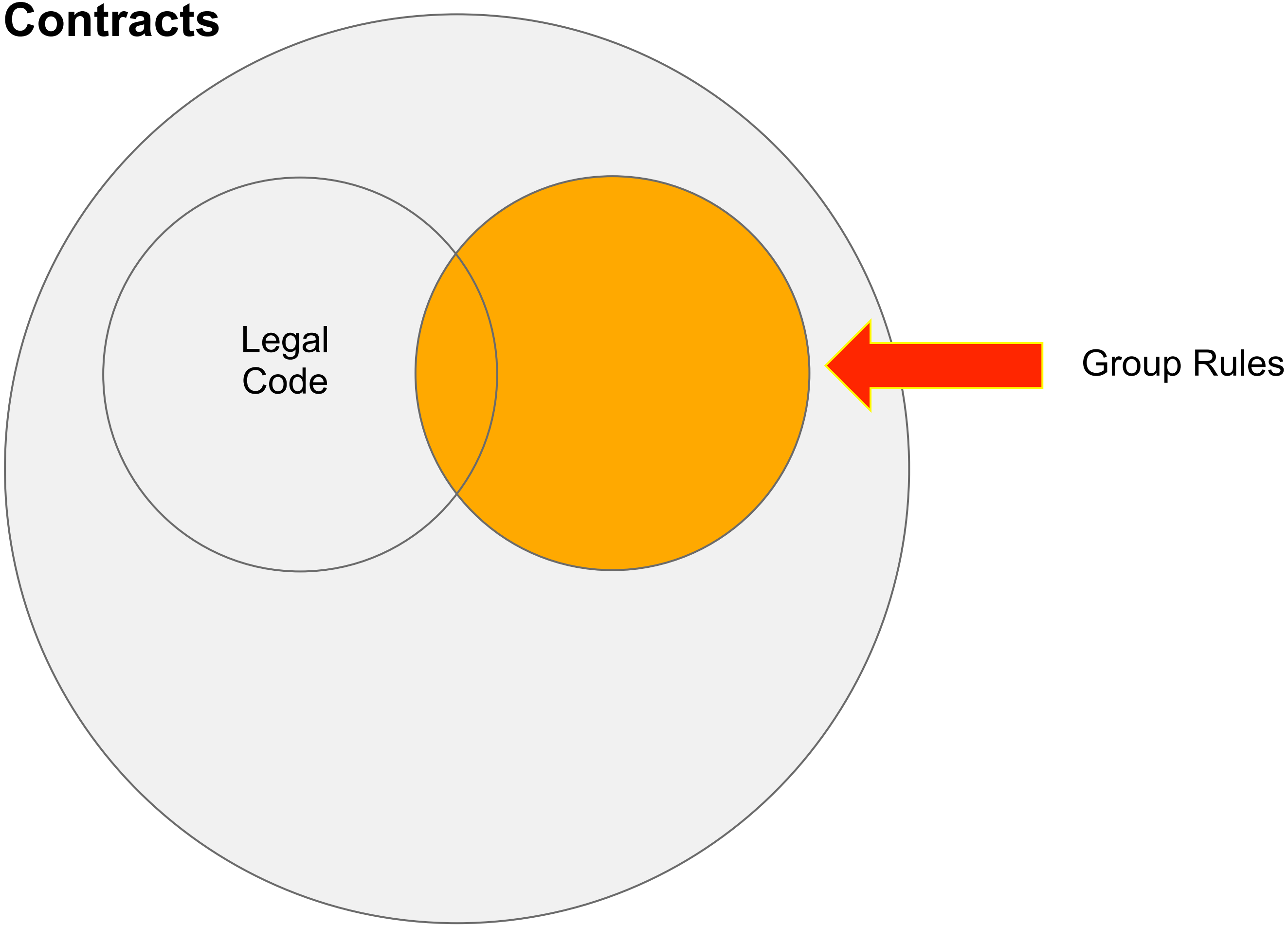


Universe of Smart Contracts



Legal Code

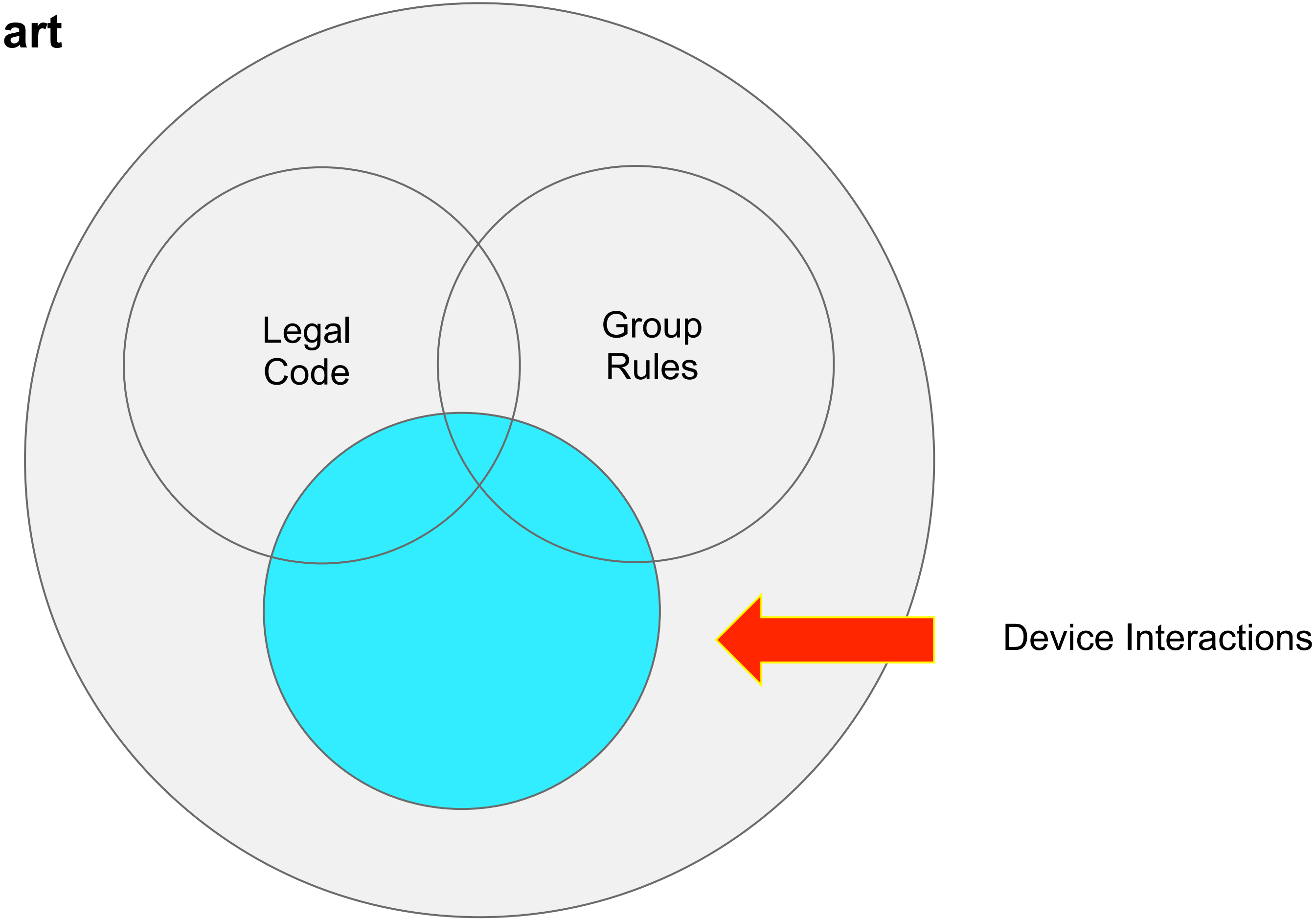
Universe of Smart Contracts



Legal Code

Group Rules

Universe of Smart Contracts

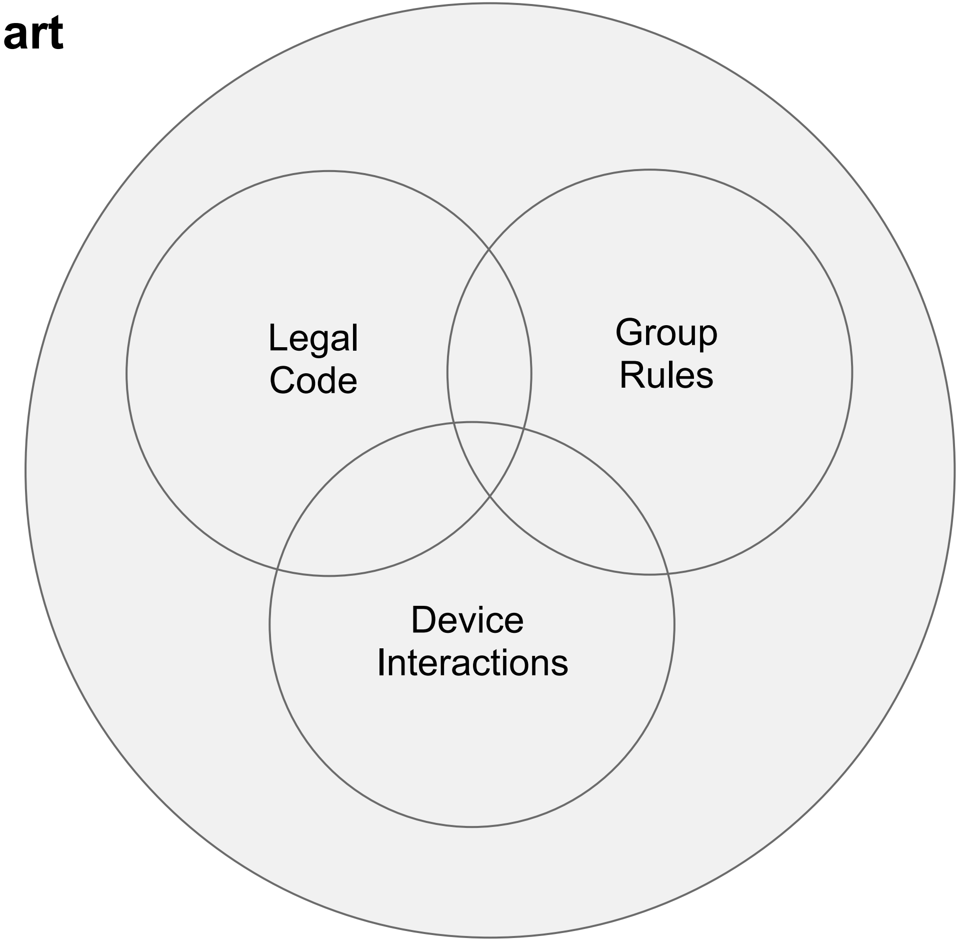


Legal Code

Group Rules

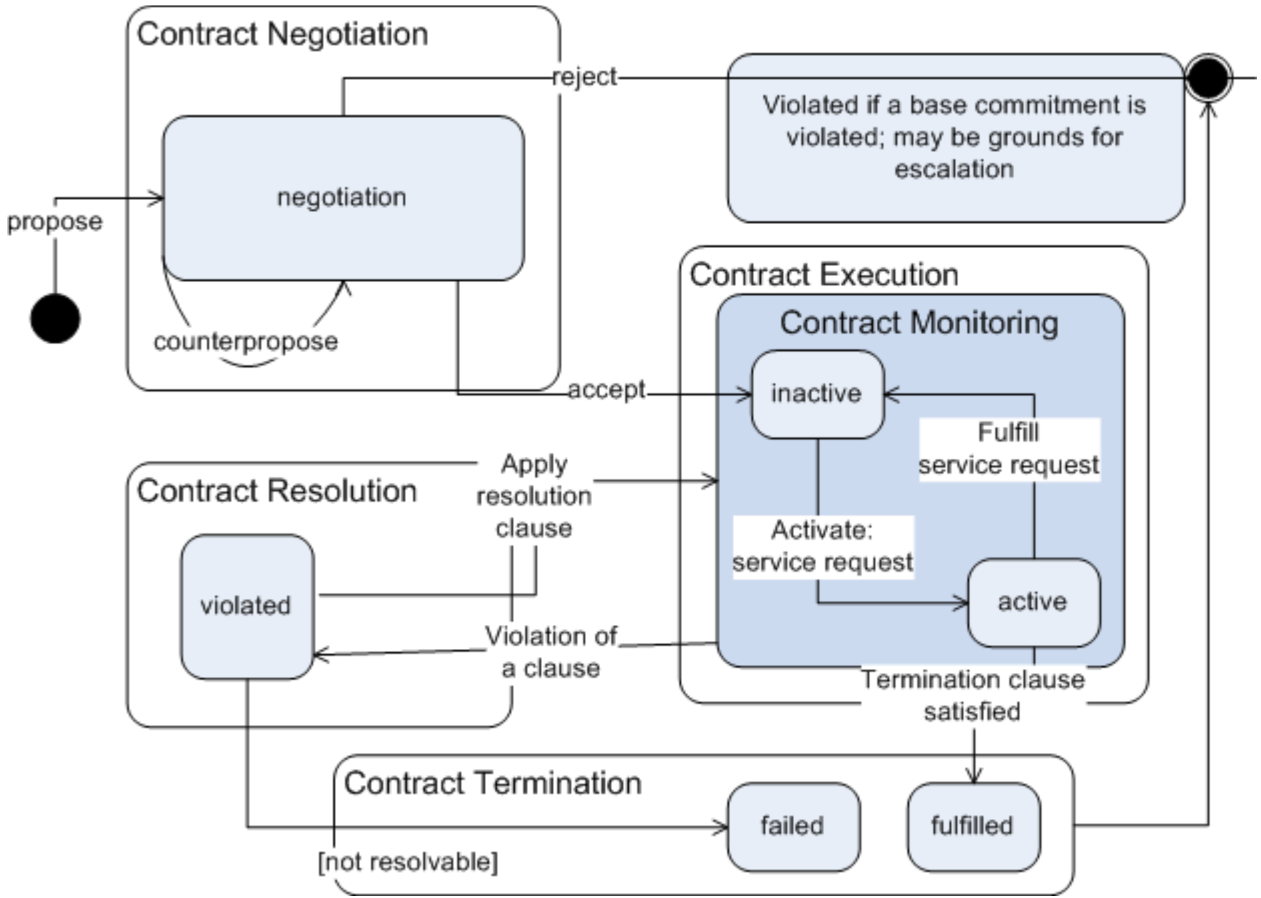
Device Interactions

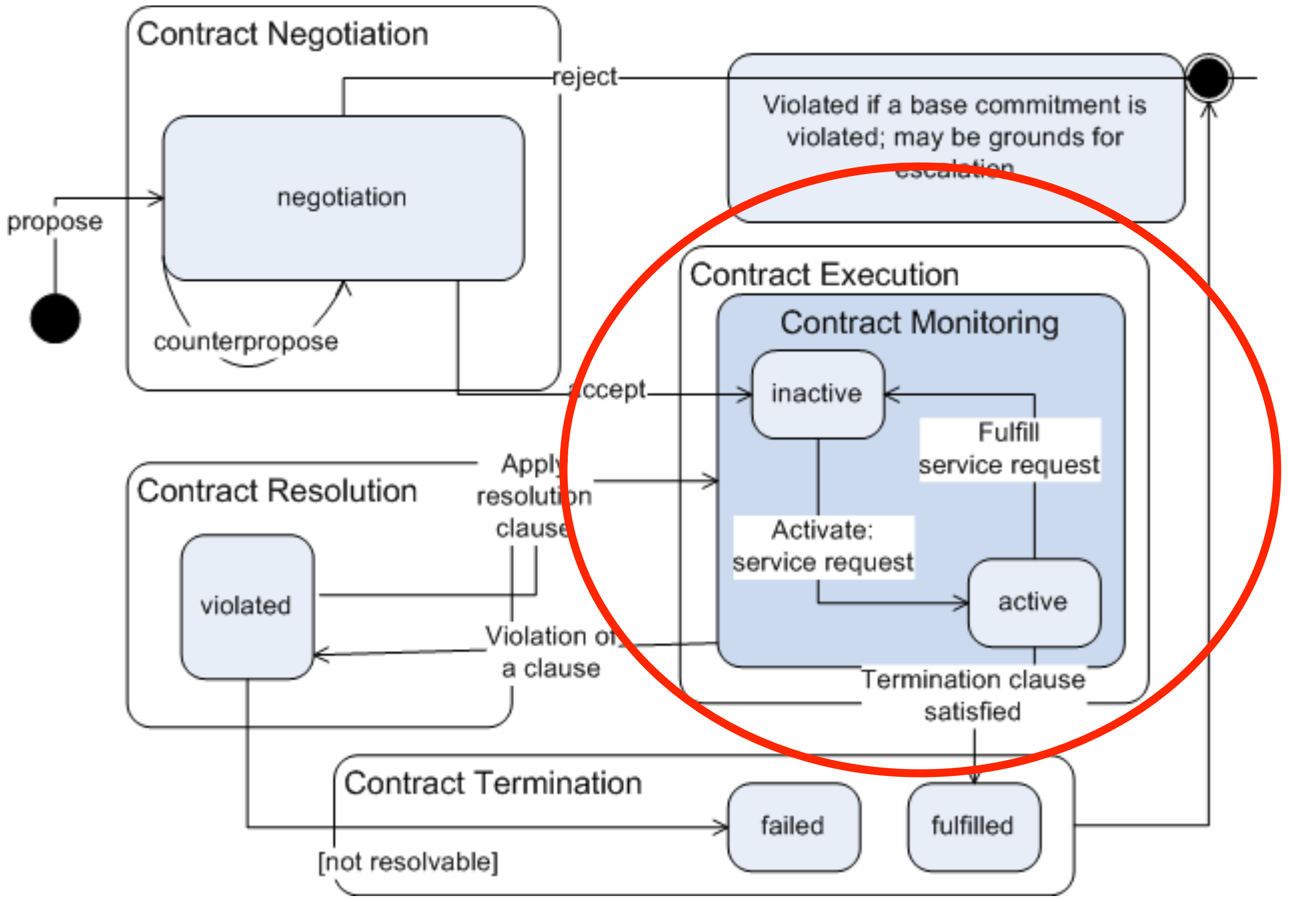
Universe of Smart Contracts



Code → **less ambiguous** than words

Self-executing → harder to breach


Contract Negotiation
reject
Violated if a base commitment is violated; may be grounds for escalation
propose
negotiation
counterpropose
Contract Execution
Contract Monitoring
accept
inactive
Fulfill service request
Apply resolution clause
Contract Resolution
Activate: service request
violated
active
Violation of a clause
Termination clause satisfied
Contract Termination
failed
fulfilled
[not resolvable]



Contract Negotiation
reject
negotiation
propose
counterpropose
accept
Violated if a base commitment is violated; may be grounds for escalation
Contract Execution
Contract Monitoring
inactive
Fulfill service request
Activate: service request
active
Contract Resolution
Apply resolution clause
violated
Violation of a clause
Termination clause satisfied
Contract Termination
failed
fulfilled
[not resolvable]

And the legal system?

crypto law

Necessarily means **unpermissioned**

Backed by **nature**, not by **force**

Differences

Contracts machine-accessible

Readable and **executable** by machines

Completely unambiguous

Though flexibility can be definitely introduced if required

Autonomous

Agreement and enactment are merged; (unarranged) **disputes impossible**

Repercussions

Lower barriers

Can be sliced, diced, remixed. Think mail -> e-mail -> facebook progression

Smaller, nimbler, more agile

Micro-agreements become possible (μInsurance, μFinance, μLoans)

Near zero costs

Few lawyers, increased certainty, better tools, more reuse; many now non-viable uses become feasible

Repercussions

Agreements accessible, fast and cheap

Similar to the “like” button on Facebook or buying a Mars bar

Zero-cost proofs

Proof-of-Identity, Proof-of-Ownership, Proof-of-Provenance, …

Difference of “internal” & “public” muddied

Uber’s “employee-like” private service agreements is a portent

Possible uses?

Virtual currencies (Bitcoin)

Digital proxy currencies (CFD, ‘Goldcoin’)

Financial instruments (Derivatives, Futures)

Insurance & gaming

Registrars (ICANN, Namecoin, land)

Reputation systems (Facebook, eBay)

And eventually…

Trust systems (Verisign)

Deeds & ownership

Document revision control

Voting systems

DAOs

Your imagination!

And Web 3.0?

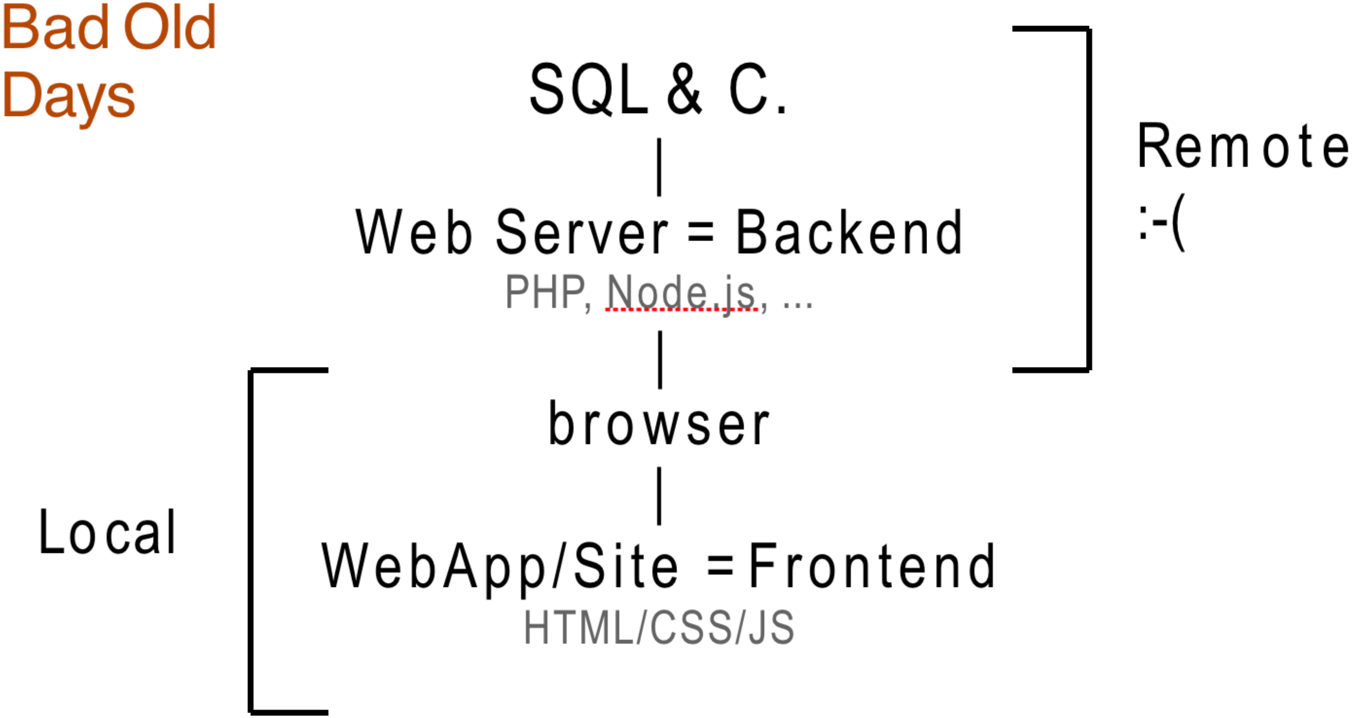
The decentralised Web

- or -

The Web without any web servers

Status Quo

Bad Old Days



SQL & C.

Web Server = Backend

PHP, Node.js, ...

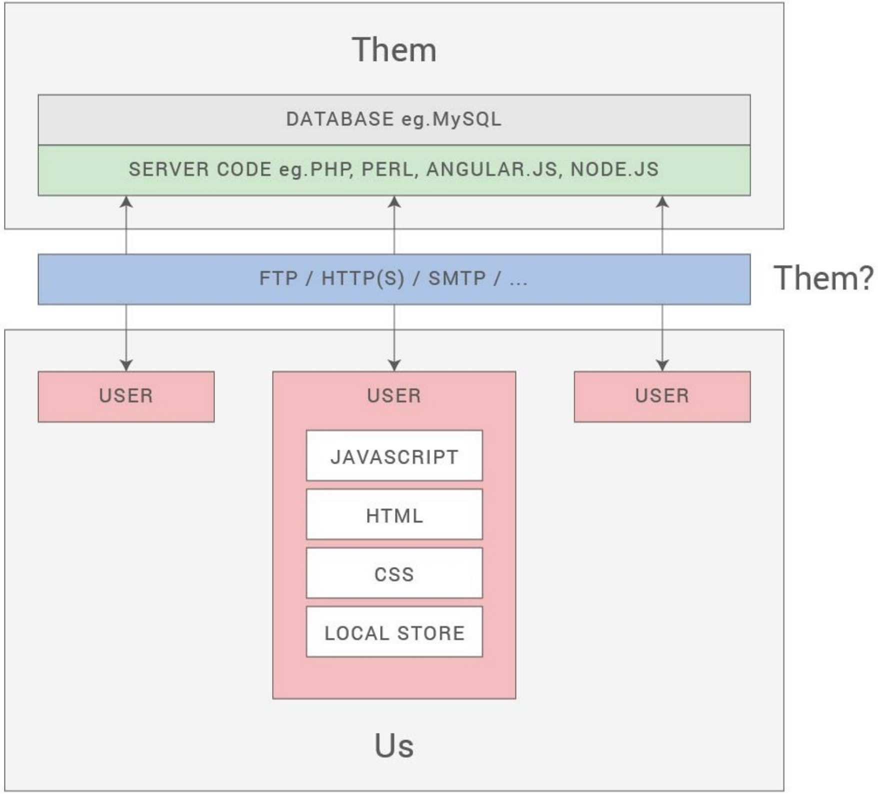
browser

WebApp/Site = Frontend

HTML/CSS/JS

Remote :-(

Local


Them
DATABASE eg.MySQL
SERVER CODE eg.PHP, PERL, ANGULAR.JS, NODE.JS
FTP / HTTP(S) / SMTP / ...
Them?
USER
USER
USER
JAVASCRIPT
HTML
CSS
LOCAL STORE
Us

Web 2.0, How it is

The Ethereum Experience with Dr. Gavin Wood, CTO

Trust

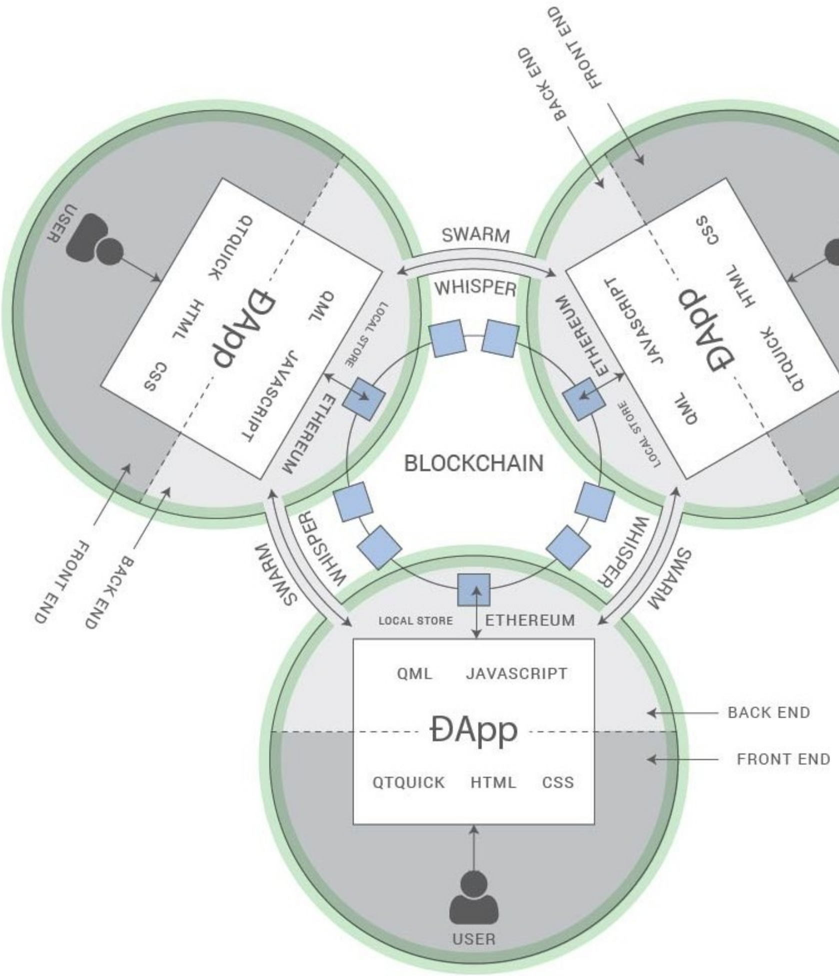
Cost of Meddling: ~£0 (Marginal)

Cost of Attacking: ~£0

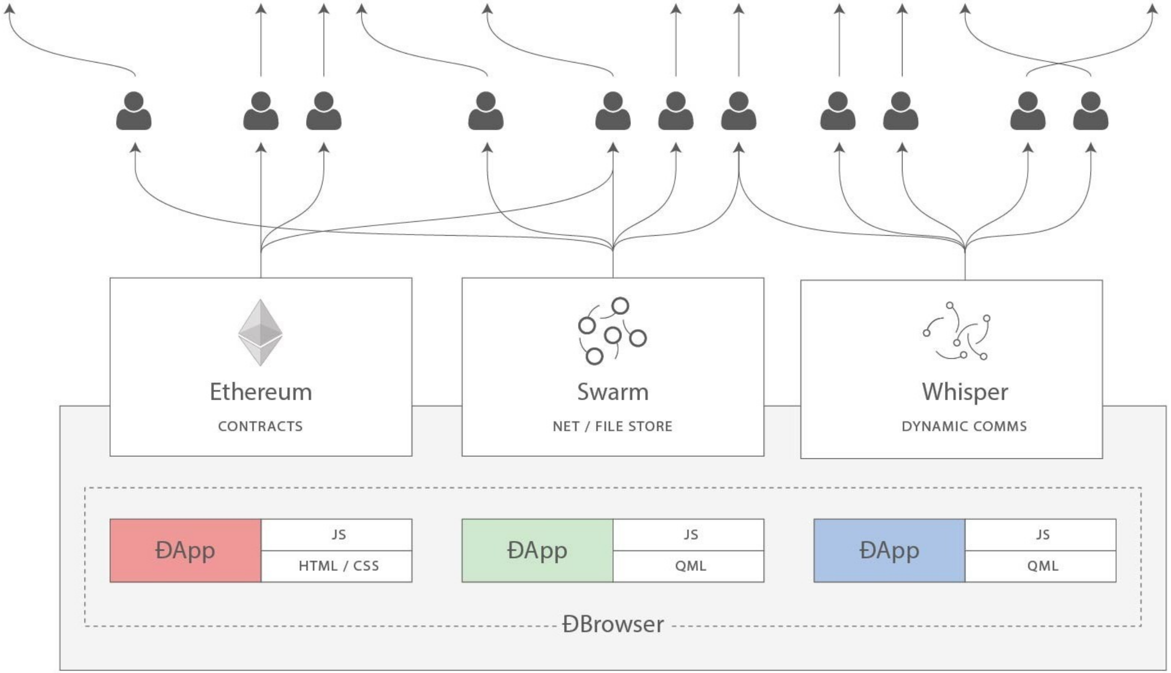
If you must trust, trust people, not orgs!

Solution?

Web 3.0



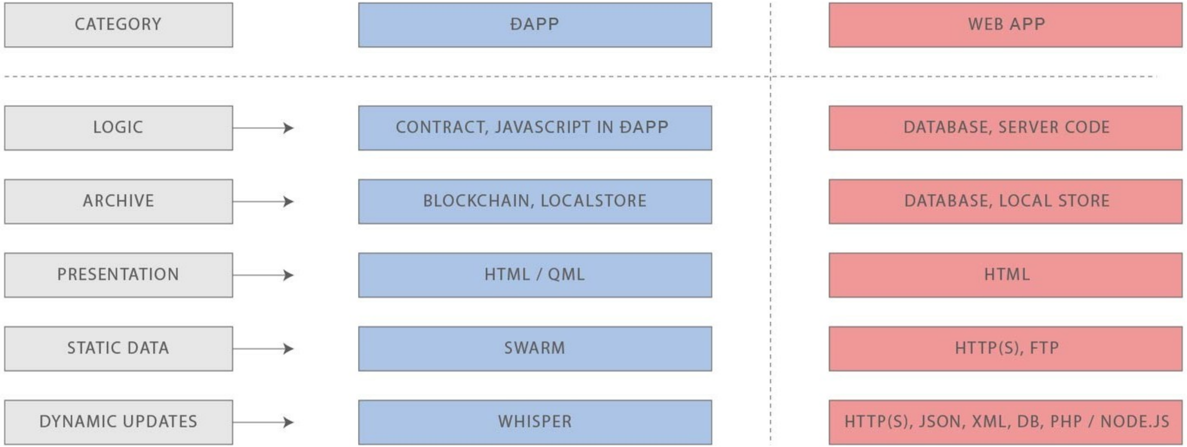
BLOCKCHAIN
SWARM
WHISPER
SWARM
WHISPER
SWARM
WHISPER
USER
ĐApp
QTQUICK
HTML
CSS
QML
JAVASCRIPT
LOCAL STORE
ETHEREUM
FRONT END
BACK END
USER
ĐApp
QTQUICK
HTML
CSS
QML
JAVASCRIPT
LOCAL STORE
ETHEREUM
FRONT END
BACK END
LOCAL STORE
ETHEREUM
QML
JAVASCRIPT
ĐApp
QTQUICK
HTML
CSS
BACK END
FRONT END
USER



ĐBrowser

The Ethereum Experience with Dr. Gavin Wood, CTO

Compared to what you know…



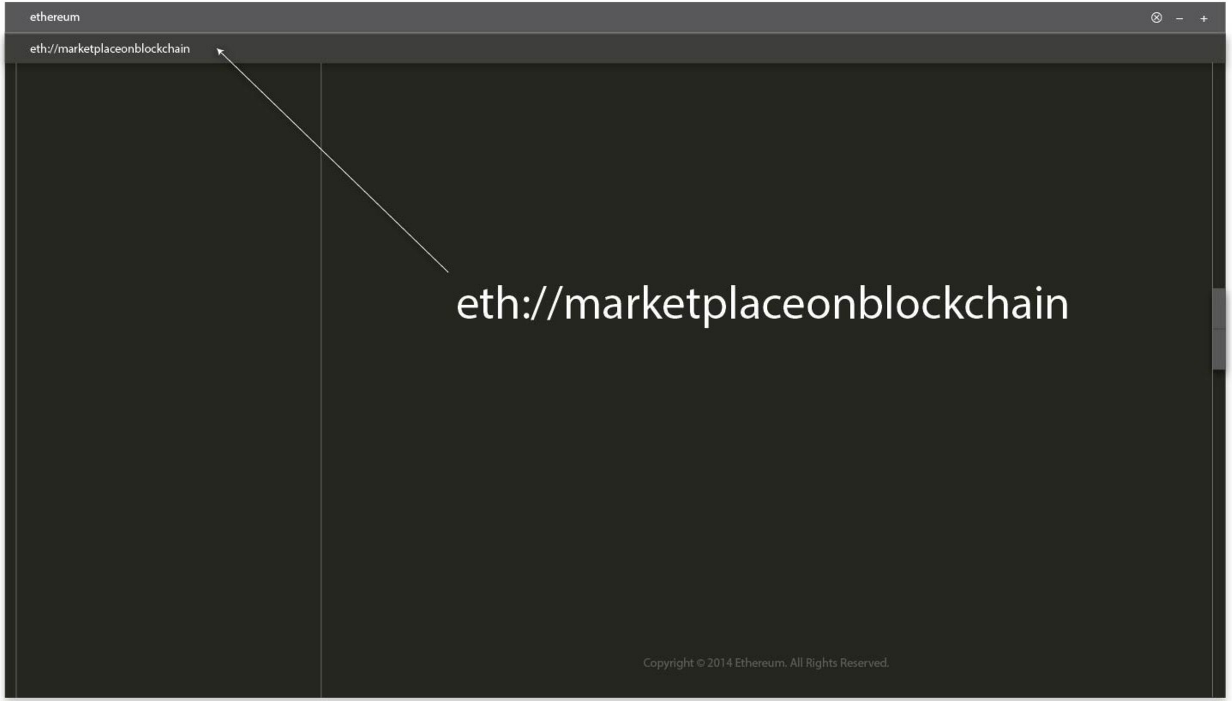
CATEGORY	ĐAPP	WEB APP
LOGIC	CONTRACT, JAVASCRIPT IN ĐAPP	DATABASE, SERVER CODE
ARCHIVE	BLOCKCHAIN, LOCALSTORE	DATABASE, LOCAL STORE
PRESENTATION	HTML / QML	HTML
STATIC DATA	SWARM	HTTP(S), FTP
DYNAMIC UPDATES	WHISPER	HTTP(S), JSON, XML, DB, PHP / NODE.JS

ĐApp / WebApp Comparison

The Ethereum Experience with Dr. Gavin Wood, CTO

An example

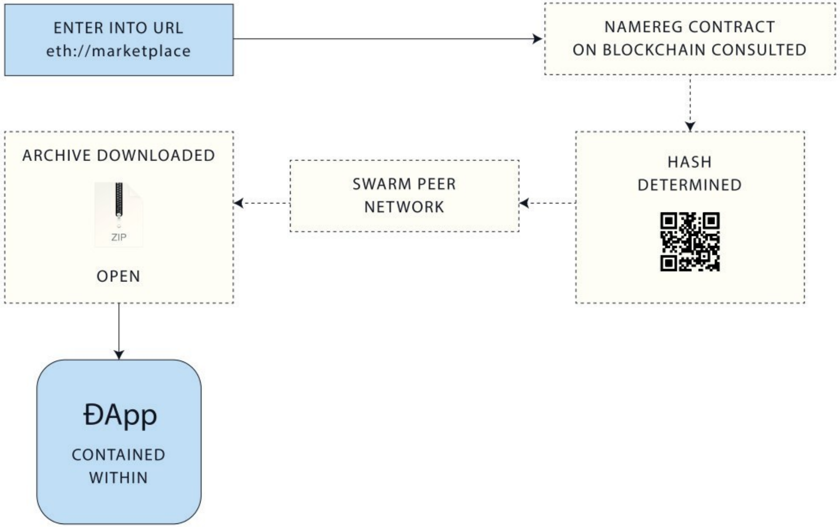
A Marketplace



eth://marketplaceonblockchain

Getting the ĐApp (Static Content / URL)

The Ethereum Experience with Dr. Gavin Wood, CTO



ENTER INTO URL
eth://marketplace

NAMEREG CONTRACT
ON BLOCKCHAIN CONSULTED

HASH
DETERMINED

SWARM PEER
NETWORK

ARCHIVE DOWNLOADED

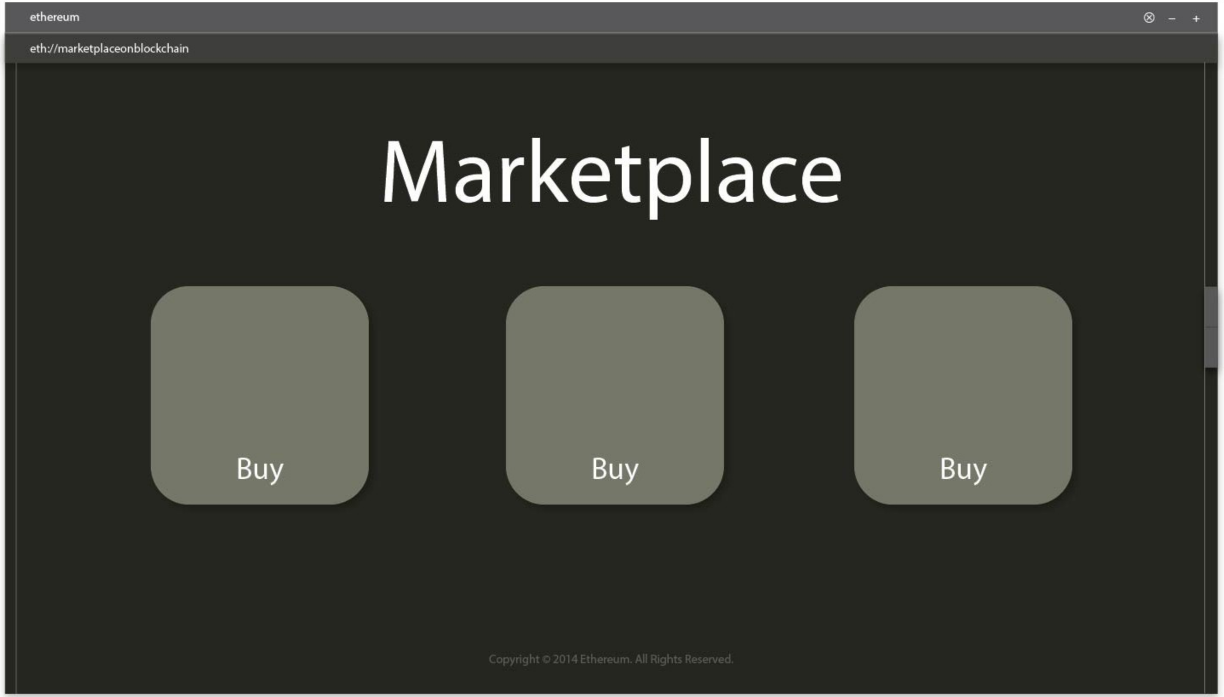
OPEN

ĐApp

CONTAINED
WITHIN

Getting the ĐApp (Static Content / URL)

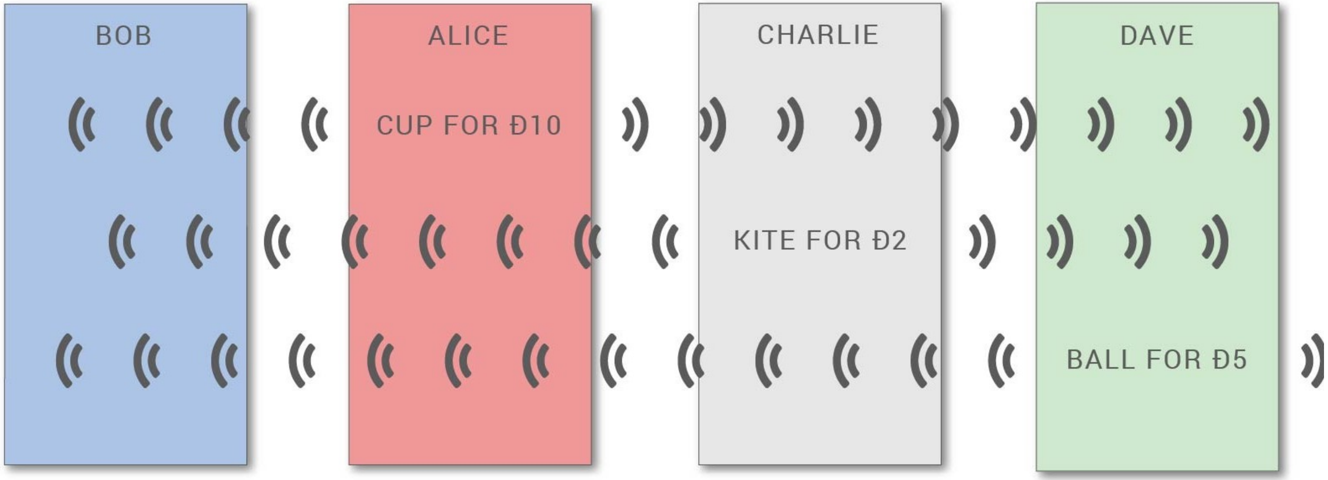
The Ethereum Experience with Dr. Gavin Wood, CTO



Copyright © 2014 Ethereum. All Rights Reserved.

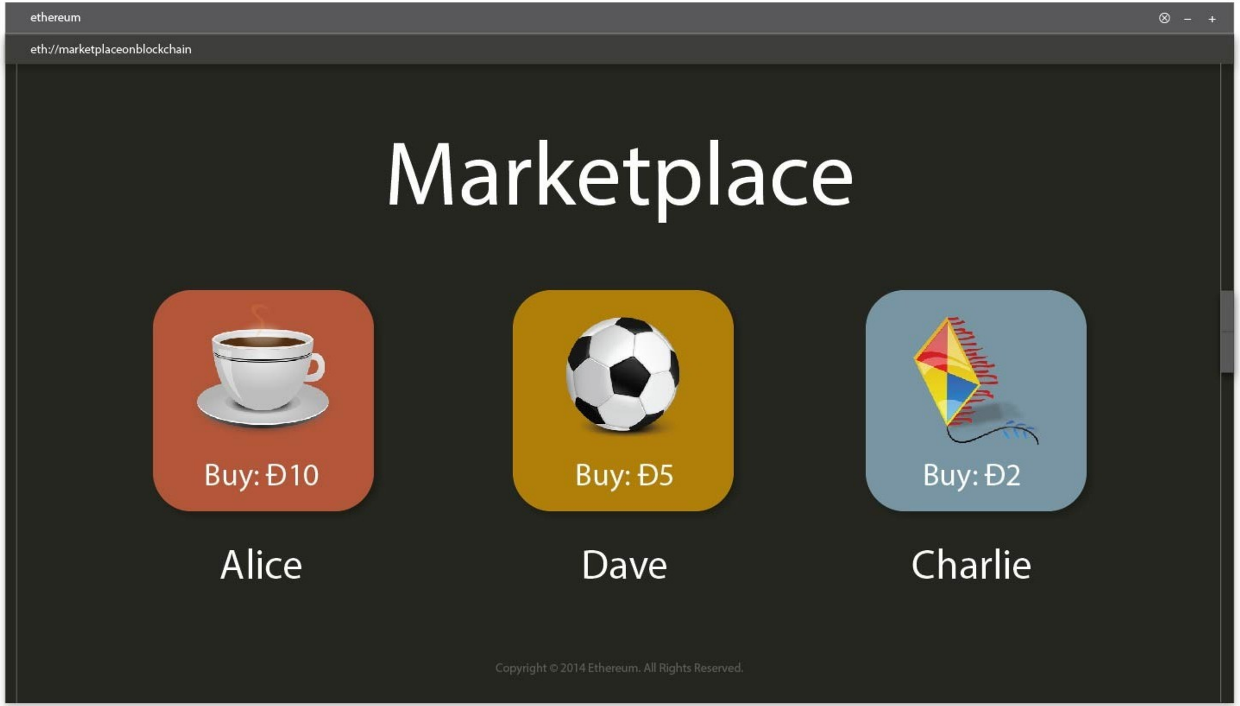
Dynamic Content

The Ethereum Experience with Dr. Gavin Wood, CTO



Getting the ĐApp

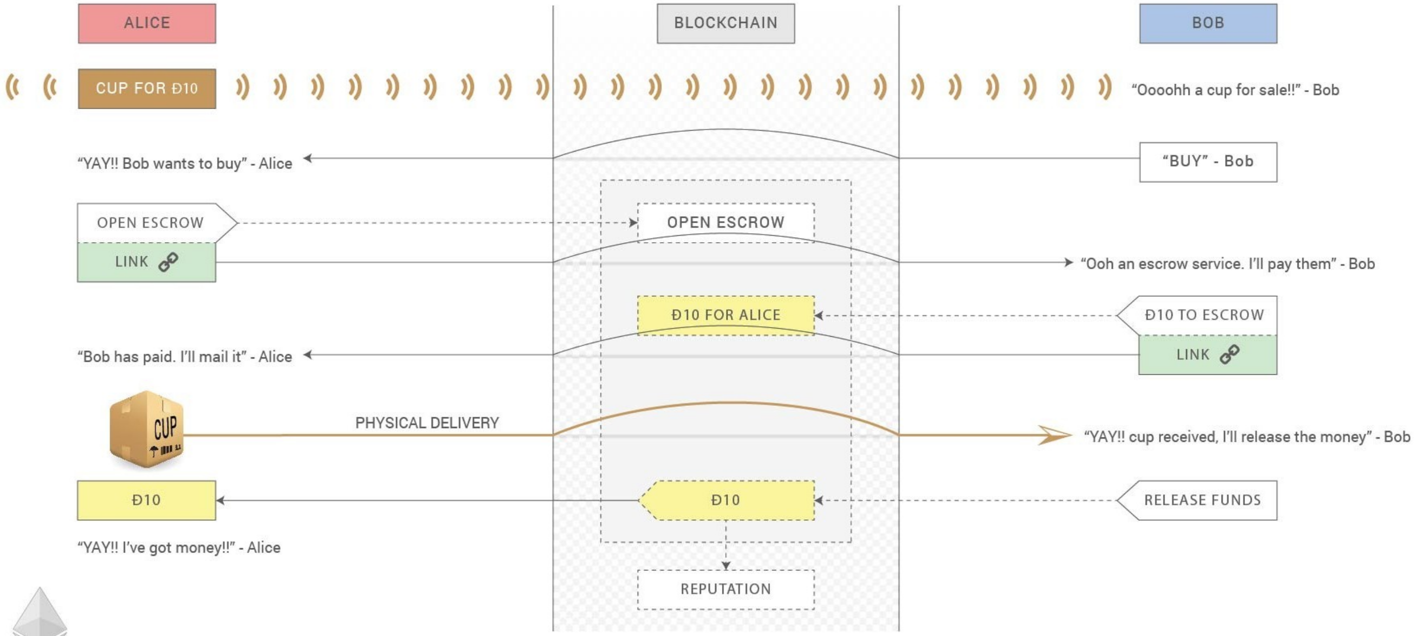
The Ethereum Experience with Dr. Gavin Wood, CTO



Copyright © 2014 Ethereum. All Rights Reserved.

ĐApp (Dynamic Content)

The Ethereum Experience with Dr. Gavin Wood, CTO


ALICE
BLOCKCHAIN
BOB
CUP FOR Đ10
“Oooohh a cup for sale!!” - Bob
“YAY!! Bob wants to buy” - Alice
“BUY” - Bob
OPEN ESCROW
OPEN ESCROW
LINK
“Ooh an escrow service. I’ll pay them” - Bob
Đ10 FOR ALICE
Đ10 TO ESCROW
“Bob has paid. I’ll mail it” - Alice
LINK
CUP
PHYSICAL DELIVERY
“YAY!! cup received, I’ll release the money” - Bob
Đ10
Đ10
RELEASE FUNDS
“YAY!! I’ve got money!!” - Alice
REPUTATION

Purchasing the cup

The Ethereum Experience with Dr. Gavin Wood, CTO

No “authorities” to trust.

No centralisation to fail.

Just individuals cooperating under agreement for mutual benefit.

Questions?

Feel free to connect with me at
sumukh@automte.com
or
@sumshetty