SMART CONTRACTS IN THE CREATIVE INDUSTRIES

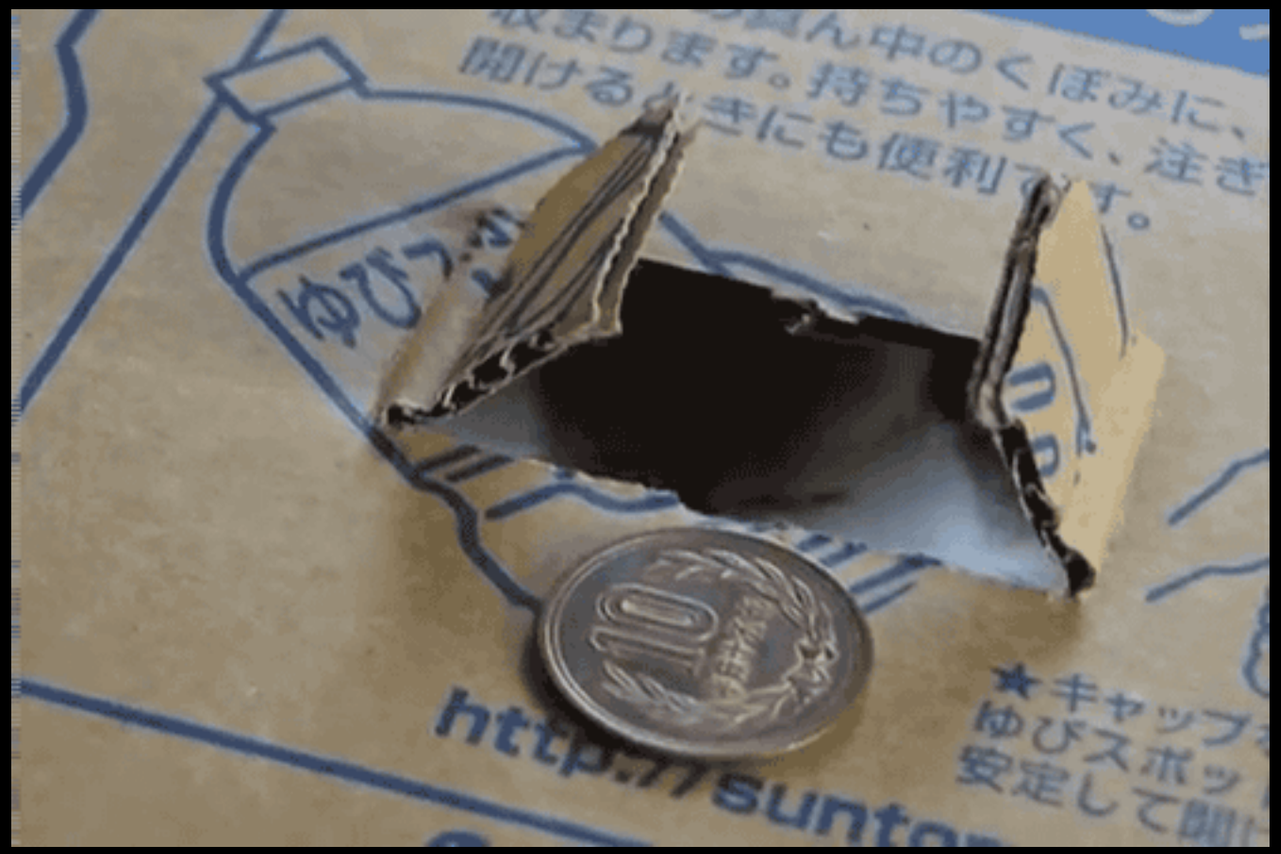
DR ANDRES GUADAMUZ, UNIVERSITY OF SUSSEX

LET’S GET ONE THING OUT OF THE WAY FIRST...

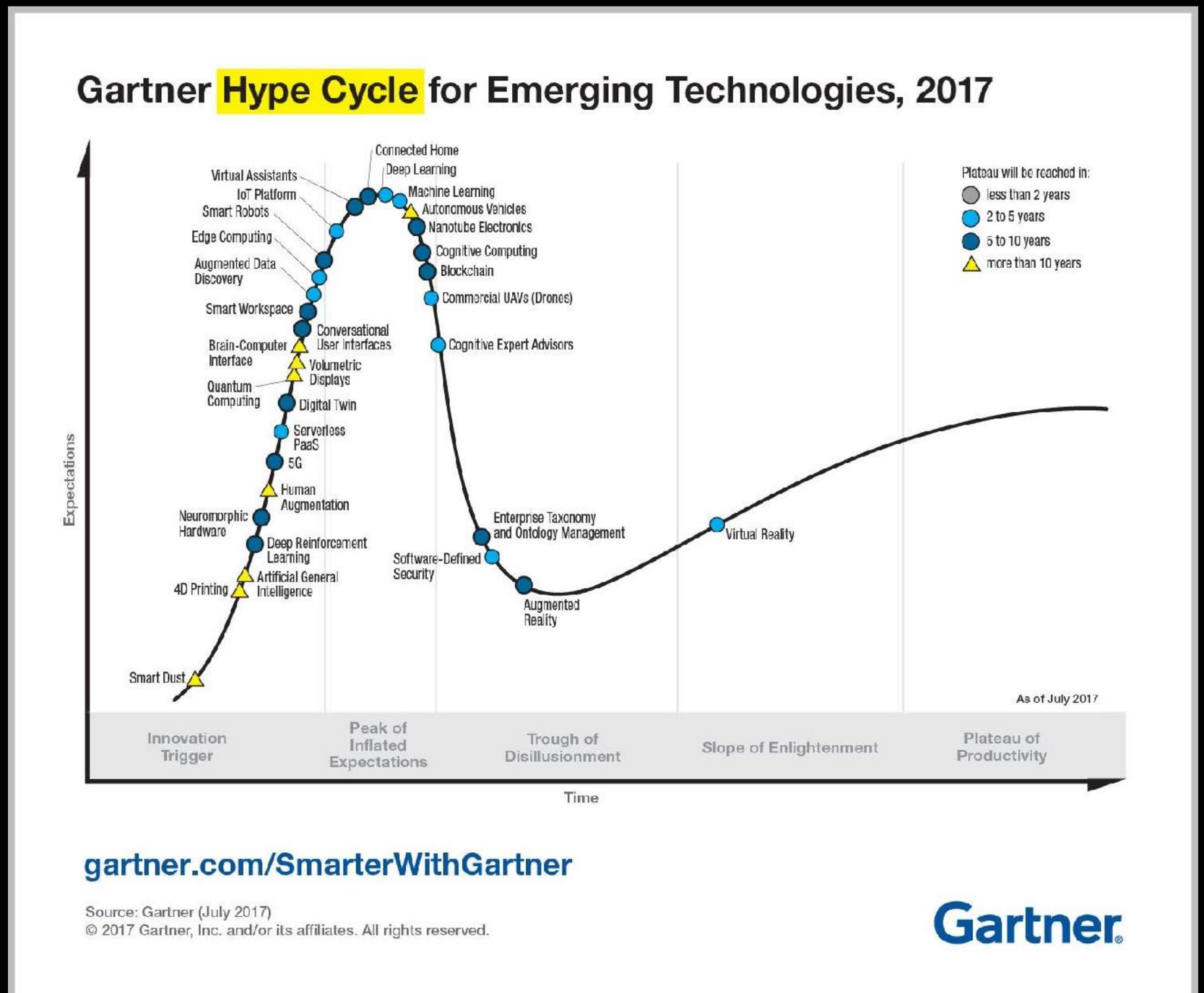
WHAT IS A SMART CONTRACT?

- Part of a larger topic dealing with autonomous agents and AI and the Law.
- Excellent scholarship on translating legal norms to machine-readable expressions.
- Traditional concept is just a self-executing contract written in code.
- Latest iteration includes the use of cryptographic tools, particularly the blockchain.

BLOCKCHAIN

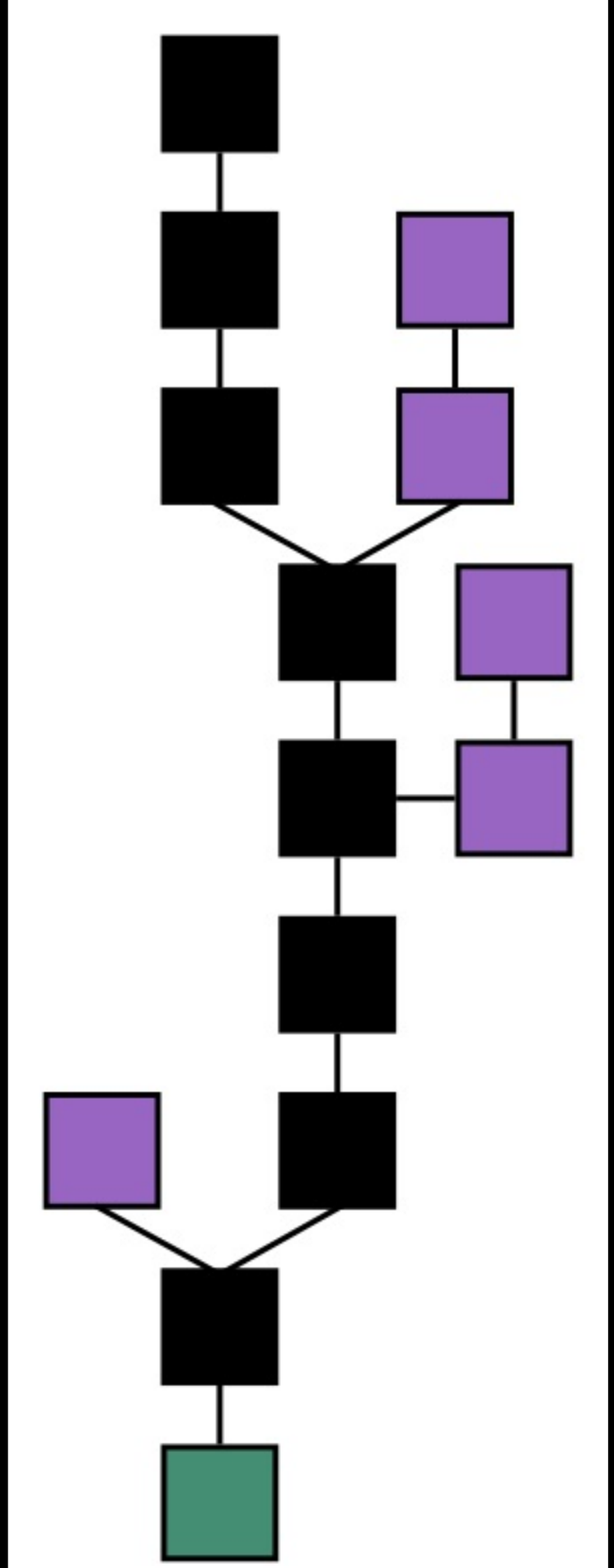


MIND THE HYPE



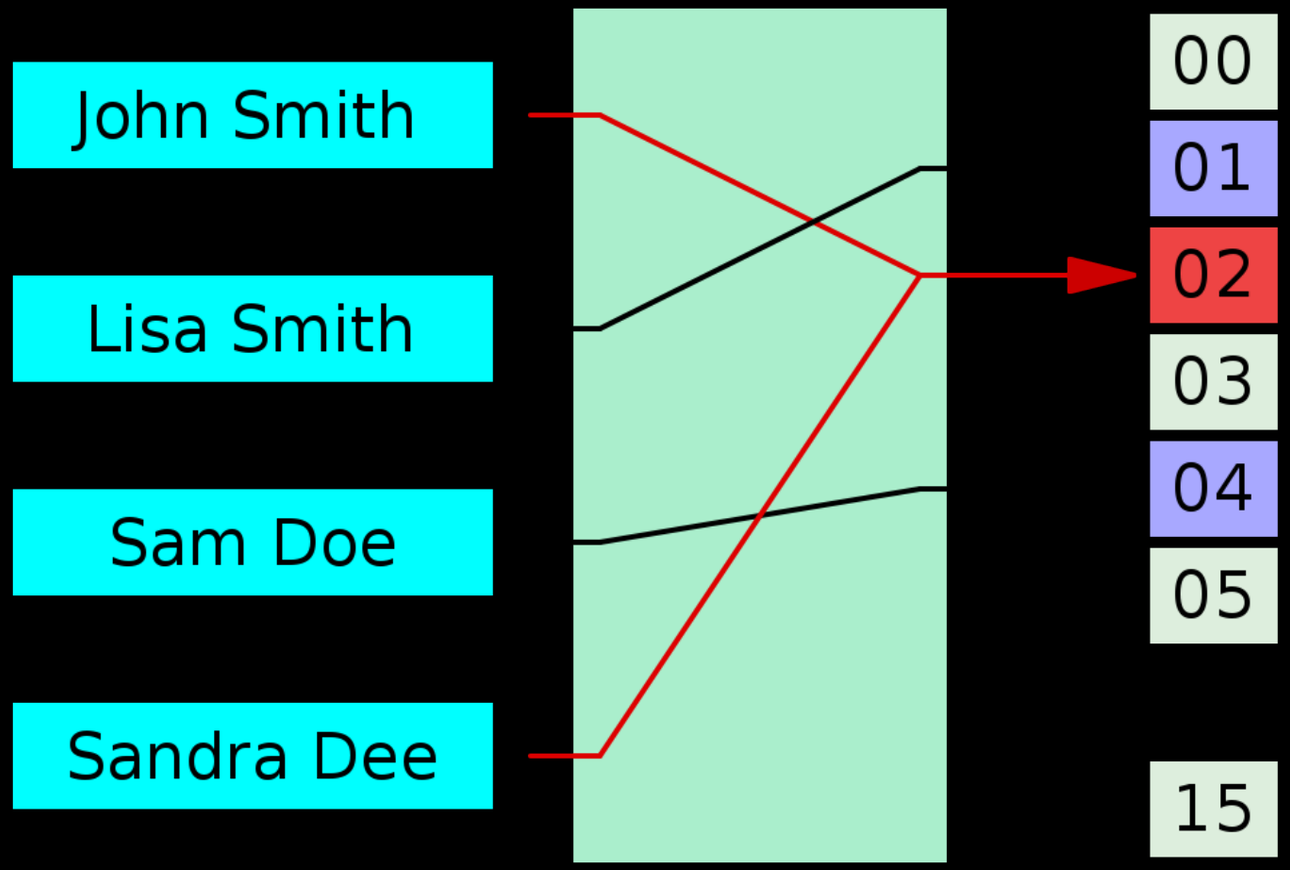
WHAT IS A BLOCKCHAIN?

- A blockchain is quite simply an open, permissionless, cryptographic, decentralised ledger.
- The ledger is public and decentralised, and since anyone can check past, present and proposed transactions, there is increased reliability in the system.



IMMUTABLE AND TAMPER-FREE

- A hash function: a mathematical operation that can produce a unique output depending on the input.
- Take some text, turn it into numbers, and then apply a formula (the hash function) that will produce a unique number (the hash value).
- Changing the original text, then the resulting number would not match the hash value.
- Blockchains consist of blocks of transactions that are chained together by appending the hash of the previous transaction, making it impossible to change, and therefore makes them tamper-free.



PROOF OF CONCEPT

16

1 3 5 7 8

24

CHARACTERISTICS

- Proof of Work. Reward for running the program to verify transactions.
- Proof of Stake: Chooses the allocation of the next block between those with a stake in the system without the need for large expenditure of resources.
- Authentication. This is the main function of a blockchain, the implementation must be designed to validate transactions securely and unequivocally.
- Decentralization. The blockchain must be decentralized, so copies of the entire ledger cannot be held centrally. This presents a few technical problems, such as the increasingly unmanageable size of the blockchain as more transactions accumulate.

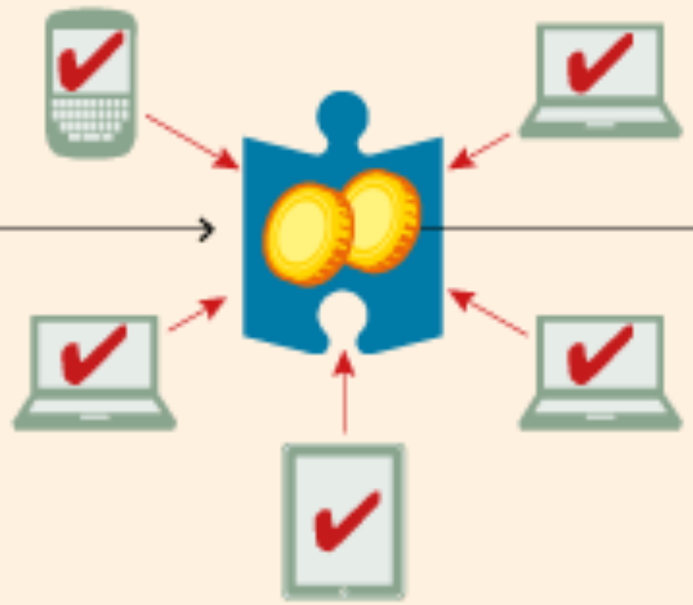
How a blockchain works

1. A wants to send money to B

2. The transaction is represented online as a 'block'

3. The block is broadcast to every party in the network

4. Those in the network approve the transaction is valid

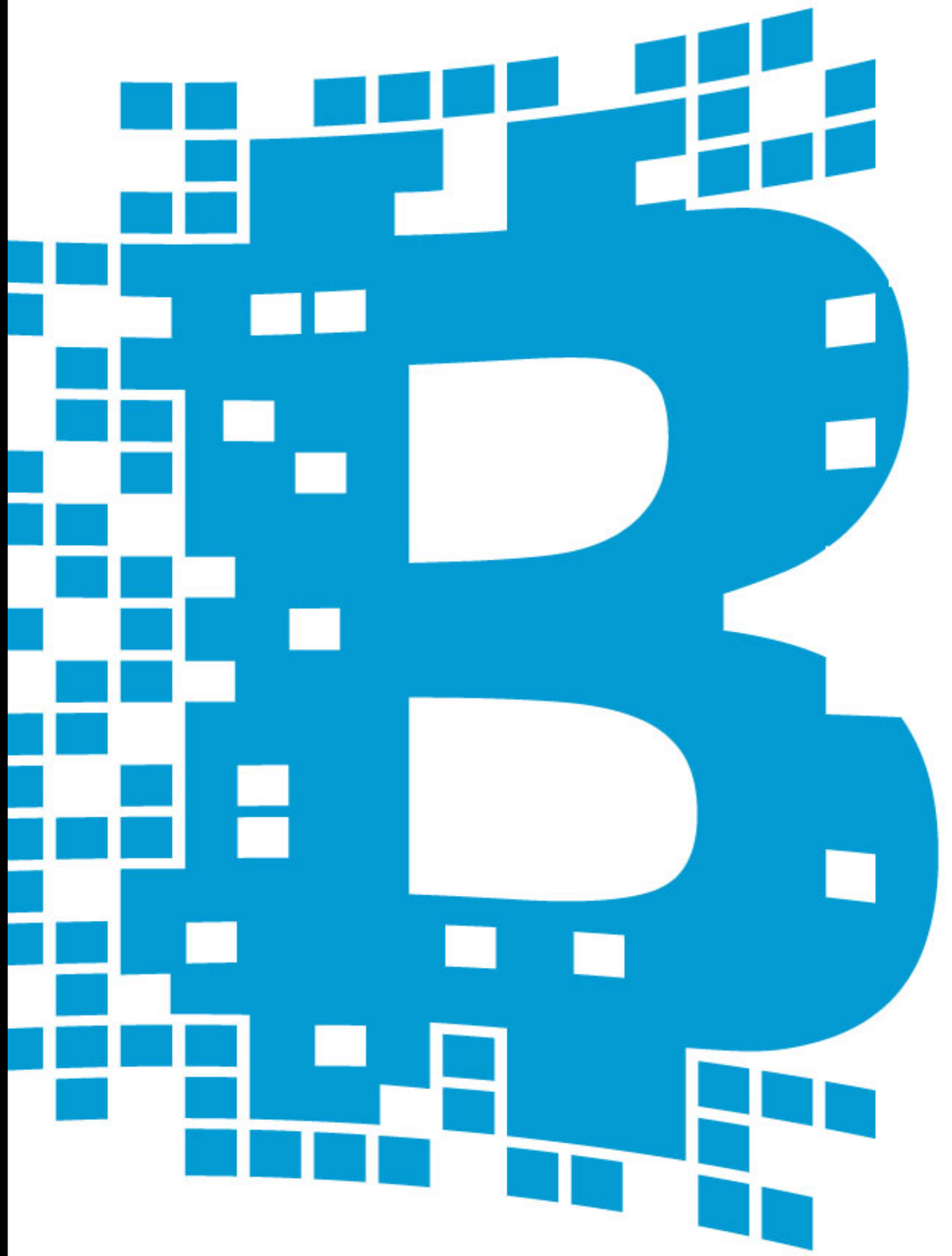


5. The block then can be added to the chain, which provides an indelible and transparent record of transactions

6. The money moves from A to B

BLOCKCHAIN POTENTIAL

- Verify banking transactions.
- Verify bets.
- Verify music uses to give royalties to artists real time.
- Identify a work owner.
- Verify contracts.
- Verify provenance.



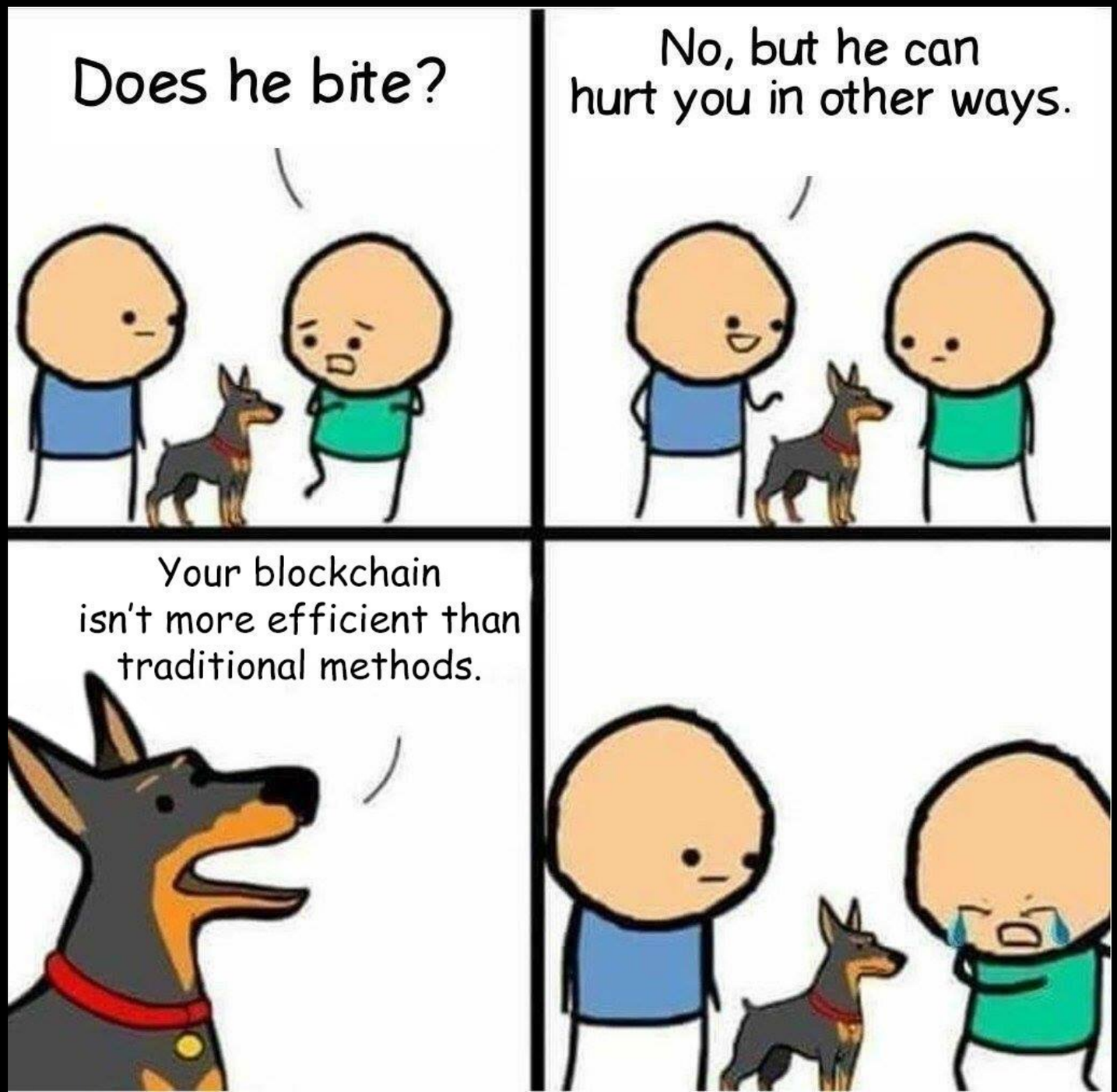
BLOCKCHAIN LAWS

- Several US states have amended their legislation to allow smart contracts, or have implemented sui generis laws.
- Arizona, Delaware, Illinois, Nevada, Tennessee, Vermont, and Wyoming.
- Usually they define blokchain and smart contracts in one way or another.
- Pretty poor definitions, not technology neutral.

ARIZONA LAW 2017 (HB2417)

- “Blockchain technology" means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.

HOWEVER...

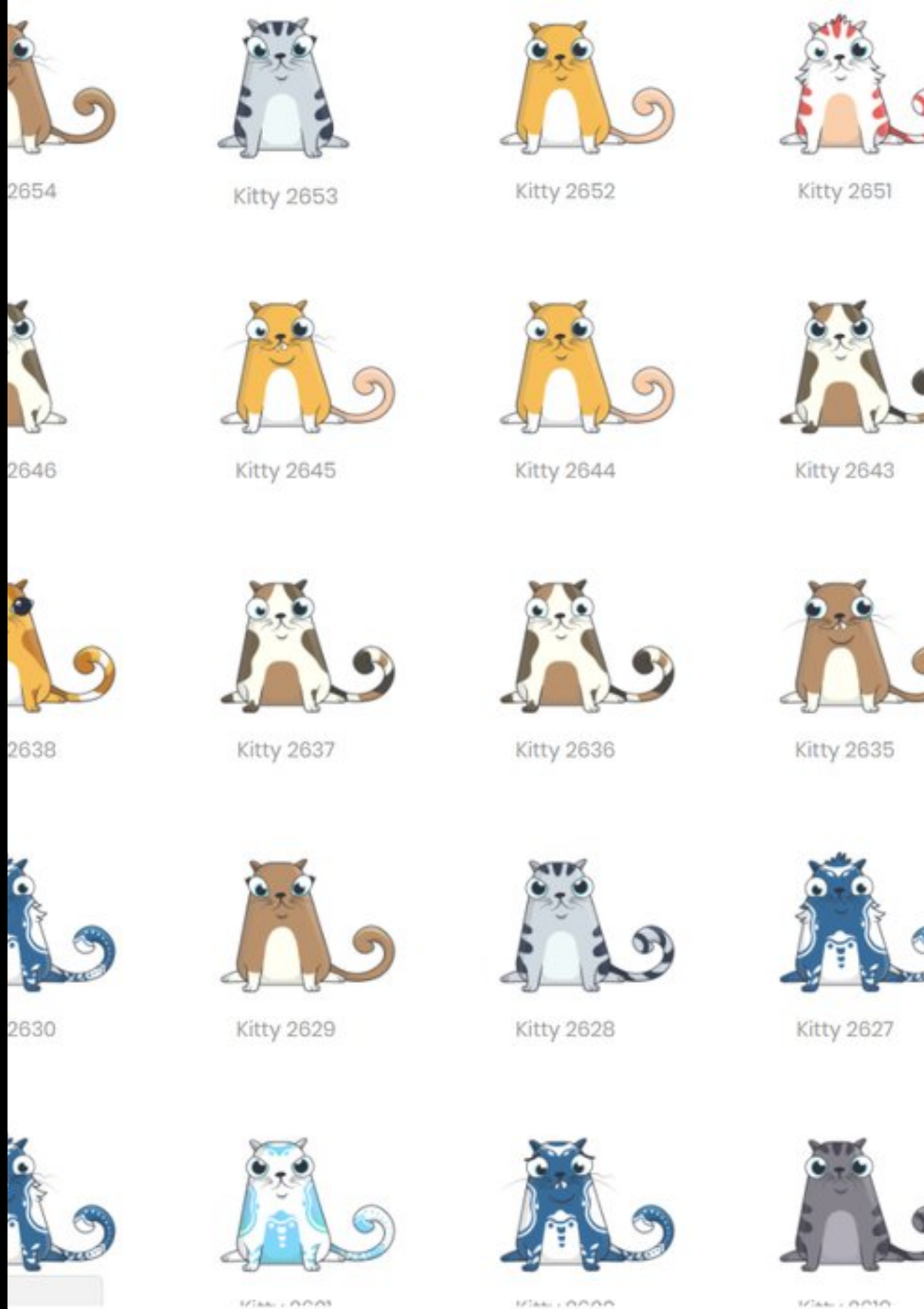

Does he bite?
No, but he can hurt you in other ways.
Your blockchain isn't more efficient than traditional methods.

HTTPS://MEDIUM.COM/MOBGEN/PLANTS-LEARN-TO-SPEAK-BECAUSE-MONEY-TALKS-291DB4B116DF

AND GOOD THINGS

HOWEVER...

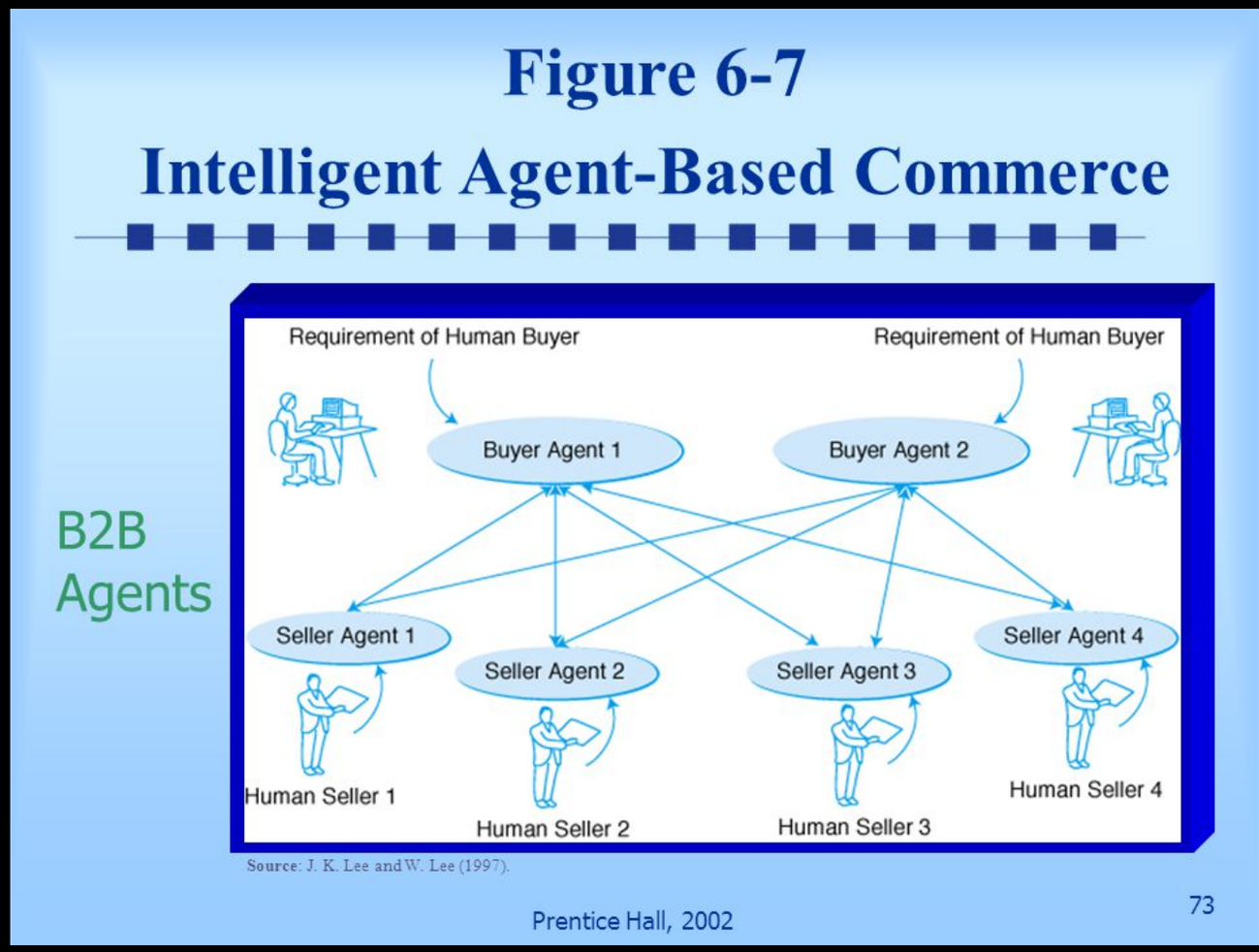
- Clunky, heavy, expensive, environmentally unfriendly.
- Do not scale well, particularly PoW blockchains.
- Lots of projects that start out as blockchain have been abandoned, or became non-blockchain.
- Immutable nature presents several problems.
- Whoever writes the blockchain writes history forever.



SMART CONTRACTS

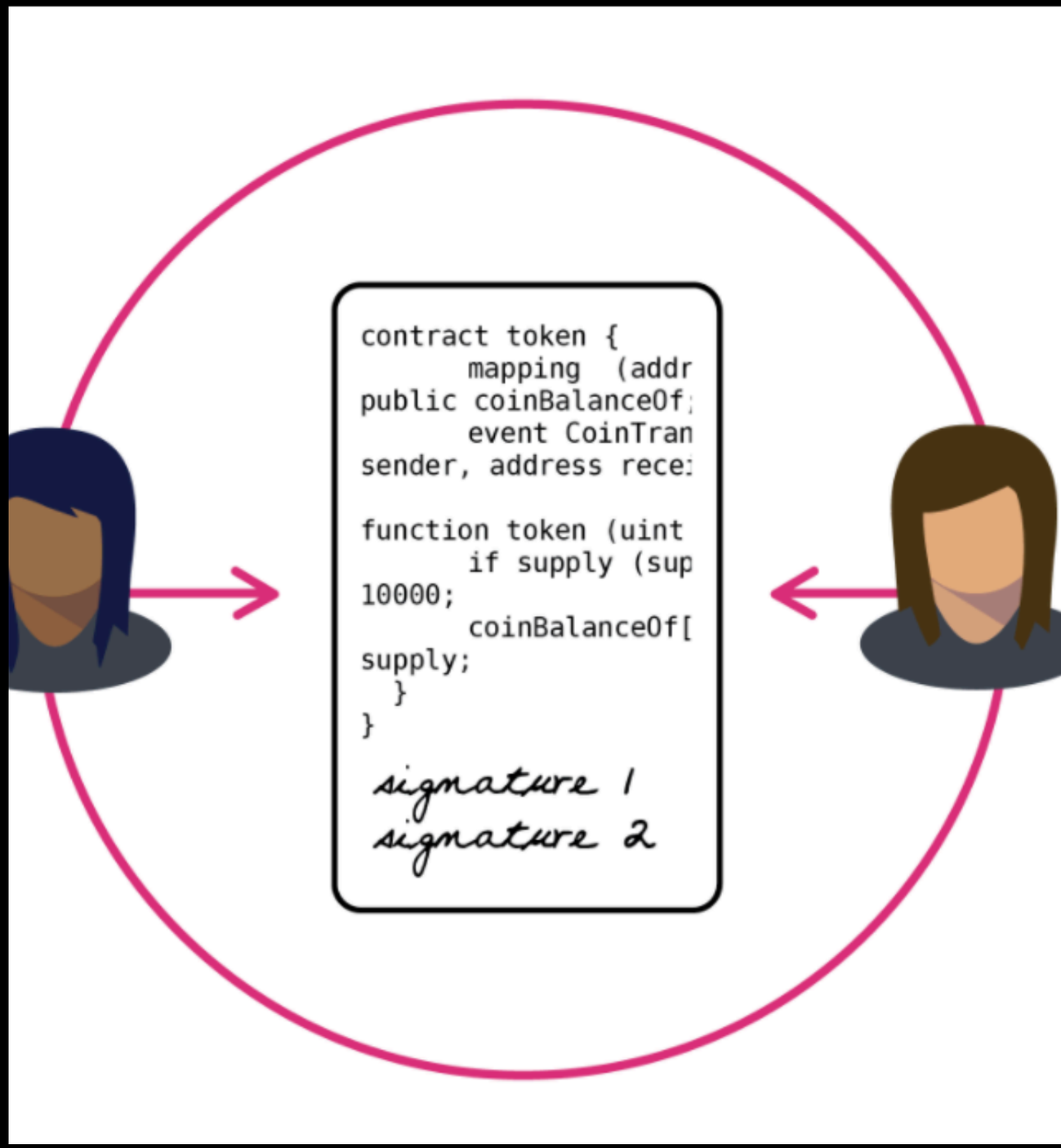
WHAT IS A SMART CONTRACT?

- There was a time before the blockchain!
- Traditionally smart contracts meant any code implementation of a contract where the parties were automated.
- It's been in use in B2B contracts for decades.



"STRONG" SMART CONTRACTS

- Implemented in code using a common language (eg Solidity).
- Pegged to a cryptocurrency for automated payments and transactions.
- Transaction and contract get written into the blockchain.
- Immutable code, openly verifiable transactions.



Smart Contracts are Awesome!

Autonomy

1

You're the one making the agreement; there's no need to rely on a broker or lawyer

Trust

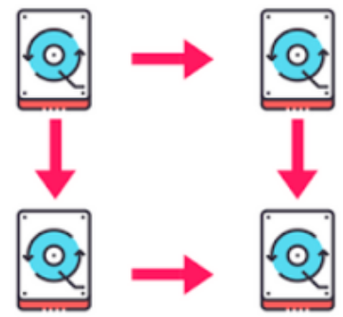
2

Your documents are encrypted on a shared ledger

Backup

3

On the blockchain,Your documents are duplicated many times over



Savings

4

Smart contracts save you money since they knock out the presence of an intermediary

Accuracy

5

Smart contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.

ARIZONA LAW 2017 (HB2417)

- "Smart contract" means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger.

TYPES OF SMART CONTRACTS

- Machine-to-machine transactions
- Cryptocurrencies
- Crowdfunding (ICO)
- Governance (DAO)
- Decentralised apps (ĐApps)
- Rights management
- Registries
- Dispute resolution

```
tract Puzzle{
ddress public owner;
ool public locked;
nt public reward;
ytes32 public diff;
ytes public solution;

unction Puzzle() //constructor{
 owner = msg.sender;
 reward = msg.value;
 locked = false;
 diff = bytes32(11111); //pre-defined diffi


unction(){ //main code, runs at every invoc
 if (msg.sender == owner){ //update reward
   if (locked)
     throw;
   owner.send(reward);
   reward = msg.value;
}
else
   if (msg.data.length > 0){ //submit a sol
     if (locked) throw;
     if (sha256(msg.data) < diff){
       msg.sender.send(reward); //send rewa
       solution = msg.data;
       locked = true;
     }}}}
```

e 3: A contract that rewards users who solve a co
puzzle.

USEFUL CONCEPTS

- Contract Source Code
- Wallet: Where your coins are stored.
- Token: represents any fungible tradable good: coins, loyalty points, gold certificates, IOUs, in-game items, etc.
- Keys: Used to digitally sign the contract, usually pegged to your token, need the key to access your coins.

IT'S ALL CODE

Modular-Network / **ethereum-contracts**

Watch 8 | Star 33 | Fork 2

Code | Issues 0 | Pull requests 0 | Projects 0 | Wiki | Insights

Smart contracts for Ethereum https://Majoolr.io

23 commits | 1 branch | 0 releases | 1 contributor | MIT

Branch: master | New pull request | Create new file | Upload files | Find File | Clone or download

Hackdom finish-fix — Latest commit 9b213f4 on 9 Sep 2017

MintedTokenAuction	Update README.md	2 years ago
StandardICOAuction	Update README.md	2 years ago
TokenContract	finish-fix	2 years ago
WalletContract	Update README.md	2 years ago
.gitignore	Add travis	2 years ago
.travis.yml	Fix params for update	2 years ago
LICENSE	Fix README	2 years ago
README.md	Update README.md	2 years ago

IT'S ALL CODE

```
pragma solidity >=0.4.22 <0.6.0;

contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    constructor(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
        return true;
    }
}
```

INSURANCE

Pre-defined contract

- Terms of the policy are agreed by all counterparties
- These are hard coded into the smart contract and cannot be chan-ged without all parties knowing

Events

- Event triggers insurance policy execution

Execute & Value transfer

- The smart contract policy is automatically executed based on the pre-agreed terms

Settlement

- Payout / other settlement completed instantly and efficiently

INTERNET OF THINGS

CAN A BLOCKCHAIN BE USED TO CONDUCT A CONTRACT?

- Yes, if the parties can express properly offer and acceptance (and consideration), and other formalities according to national law.
- Art 9 E-commerce Directive 2000/31/EC: "Member States shall ensure that their legal system allows contracts to be concluded by electronic means."

USE CASES

- “Let’s say that we want to organize a small conference. We need 100 people to sign up and pay/deposit money, so we can rent a hotel and such. But if not enough people sign up by a certain date, then the deposits need to be refunded. With Ethereum, we can write in a JavaScript-like language to code up this contract. It’ll guarantee that everyone will get a ticket to the conference, or everyone will get their money refunded, depending on how many sign up.”

FORMALITIES

- Yes, if the parties can express properly offer and acceptance (and consideration), and other formalities according to national law.
- Art 9 E-commerce Directive 2000/31/EC: "Member States shall ensure that their legal system allows contracts to be concluded by electronic means."
- US blockchain legislation allows contract formation using smart contracts.

HOWEVER...

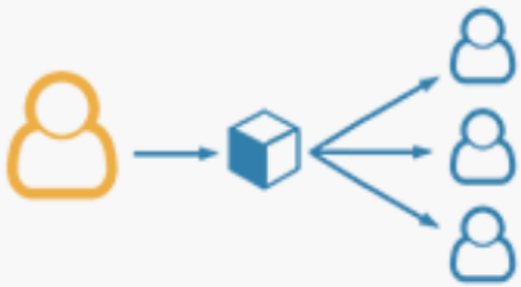
- Not all “smart contracts” are contracts.
- Smart contracts can be anonymous, so legitimacy and capacity could be an issue.
- Electronic Identification and Trust Services Regulation: advanced electronic signatures need to identify the person.

SMART CONTRACTS IN IP

LICENSING

1. Rights holder publish ownership information on the blockchain

2. Use policies for registered works are written into smart contracts that automatically transfer usage rights



3. Royalities and fees are delivered instantly, transparently and automatically based on the stakeholder information contained in the blockchain database

4. An open platform faciliitates infinite potential roles, applications and business models

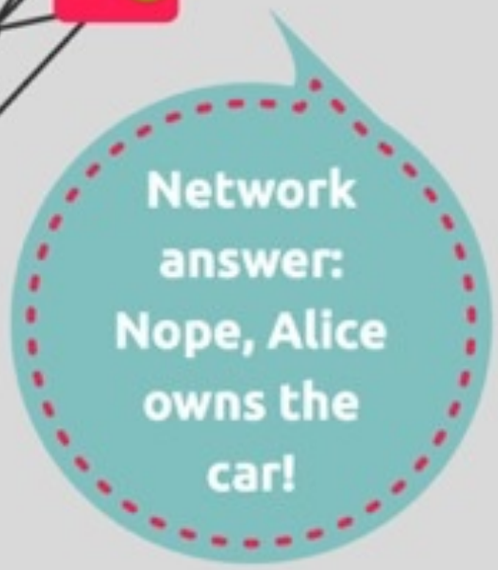
REGISTRIES

MICROPAYMENTS

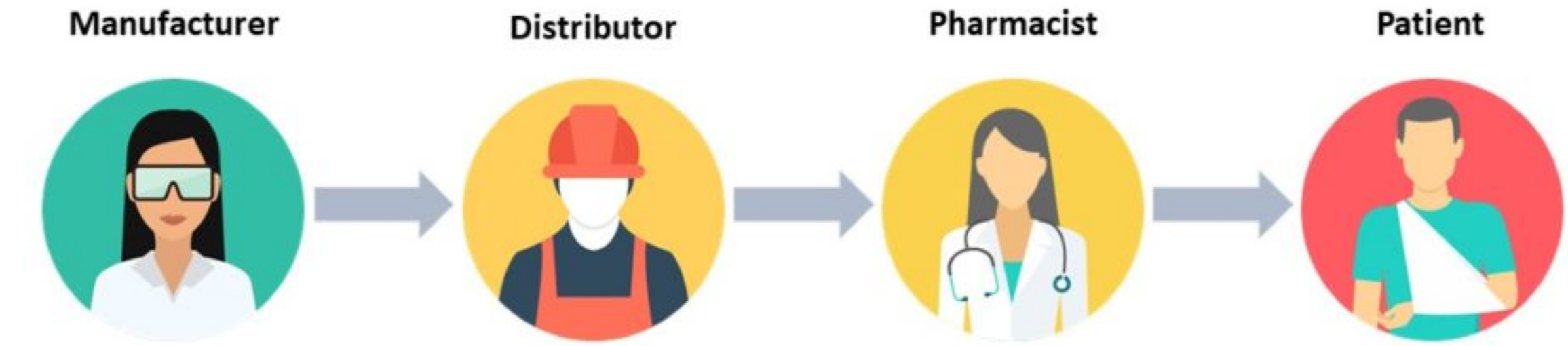
ENFORCEMENT

Why can I trust Code?

C steals the car and claims ownership of Alice's car.
Since every transaction is stored on the public blockchain, everyone can inspect it and see that the owner of the unique car ID with the Blockchain address 13849Z is Alice, not C



PROVENANCE



- The manufacturer produces the drug and marks it with a unique code
- The information is stored on the blockchain
- The wholesaler verifies the origin of the product
- The transaction is added to the blockchain
- The pharmacist verifies the origin of the product
- The transaction is added to the blockchain
- The patient verifies the origin of the product
- The transaction is added to the blockchain

THE LLAMA SOCK PROBLEM

PROBLEMS WITH SMART CONTRACTS

LOTS OF PROBLEMS

Address 0.01 BTC

Address 1F9arzFyYFXTEd2FEjiRxHuyTSGNxehwEt

Summary confirmed

Total Received	0.01 BTC
Total Sent	0 BTC
Final Balance	0.01 BTC
No. Transactions	1

Transactions

2163a13a742bf63dd287e6e8590e0f3543de1983b2fad030da692b8599f3efc1 mined Jun 21, 2011 7:57:05 AM

1PZCkWavRa87LZysMo5pssyKSVWrzhhqz8	0.01 BTC	1F9arzFyYFXTEd2FEjiRxHuyTSGNxehwEt	0.01 BTC (U)

FEE: 0 BTC

340441 CONFIRMATIONS 0.01 BTC

MEMEFEST

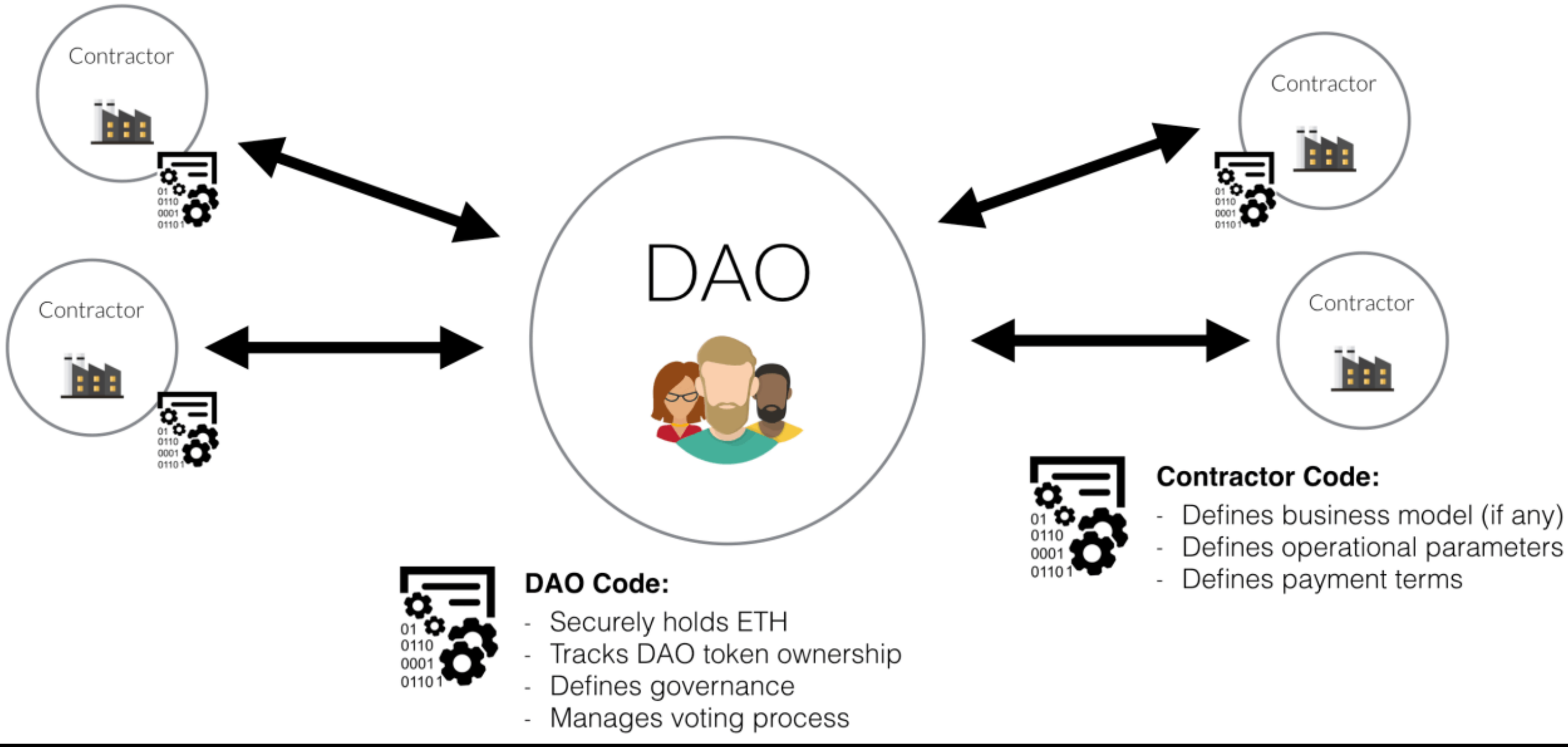
REMEDIES AND ERRORS

- Immutability could be a problem.
- Once written, the contract tends to stay that way forever.
- Bugs can lead to huge losses. See the Parity Wallet, and Ethereum smart contract that locked out between $100 and $300 million USD due to a bug.
- Other bugs have allowed fraudsters to take advantage.

LORD HODGE

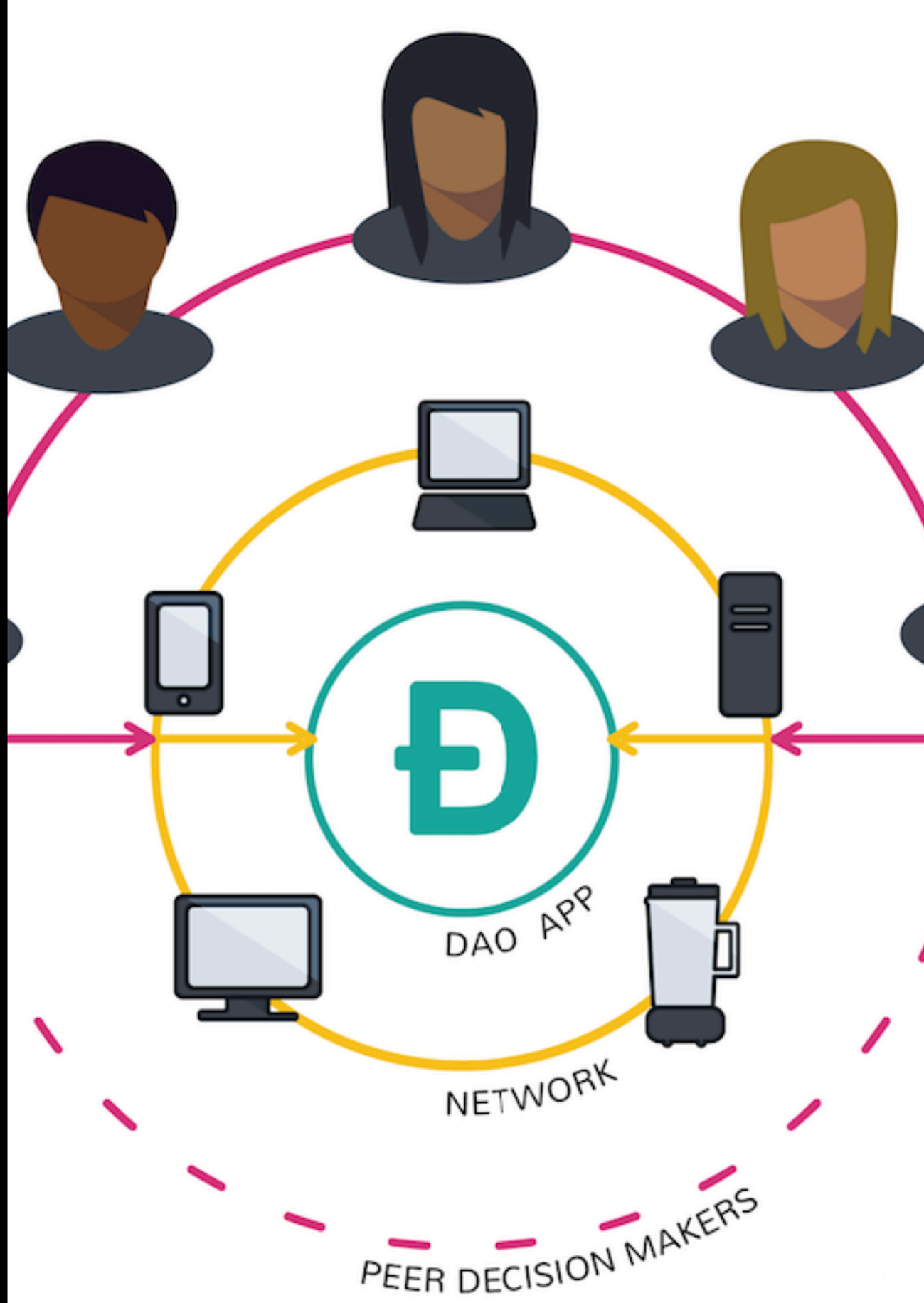
- “Smart contracts” are contracts which can be partially or fully executed or enforced without human intervention […] Courts will not be able to cancel the performance of the contract. But a remedy may lie in the law of unjust enrichment... to compel the parties to re-transfer the property or money".

DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)



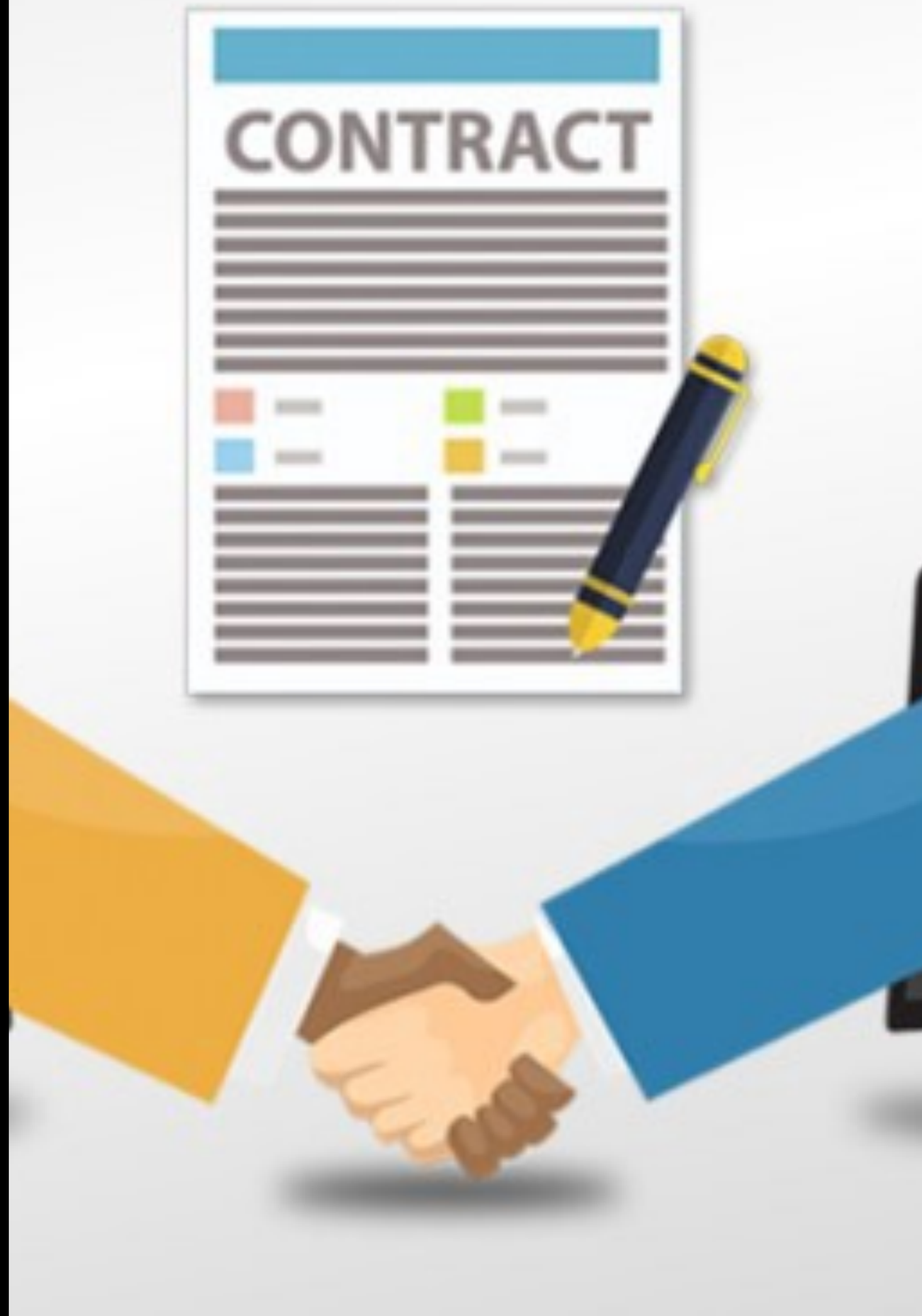
DAO "THEFT"

- DAO operates a pool of millions of USD worth in Ether (ETH).
- Only those participating in contract verification can withdraw funds according to terms of participation.
- On June 17 2016, a bug in the code allowed malicious party to syphon funds from common pool (estimated 3.6m ETH, about $50 million USD at the time).
- Hard fork from developers "turned back time".



REMEDIES

- Here's where the few articles dealing with smart contracts talk about remedies.
- No reason to forego existing principles of contract law. Error, contracting under mistake, frustration, unjustified enrichment, etc.
- Assumption is that under normal circumstances, smart contracts should be treated as any other contract.



ATTACK OF THE BLOCKCHAIN

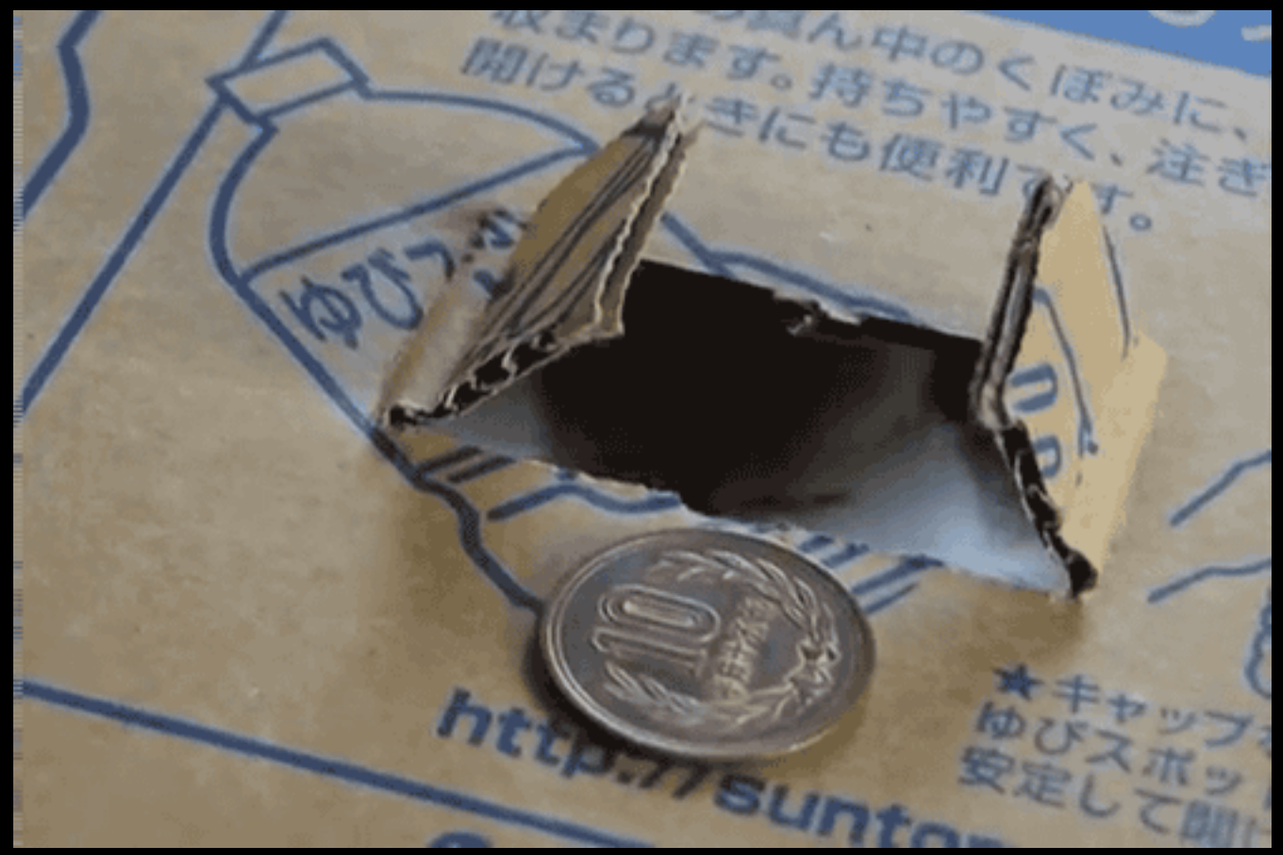
- The problem is that blockchains have specific features that may make enforcement difficult.
- Anonymity
- Reliance on a network
- 51% attack
- Forking

SCENARIOS

- Error in code cannot be changed, funds are frozen, who is liable? Who can you sue?
- Contract contains purposeful error by fraudster.
- Coin used for payment that loses all value.
- Developers fork code, making two copies of contract, perhaps diluting value.
- Miners decide to attack a contract, changing history in the ledger.
- “Garbage in, garbage out”.

DISCUSSION

CRYPTOCURRENCIES



CRYPTOCURRENCIES

- A cryptocurrency is a digital or virtual currency that uses cryptography for security.
- A cryptocurrency is difficult to counterfeit because of this security feature.
- A defining feature of a cryptocurrency is that it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation.

BITCOIN

- Satoshi Nakamoto (an alias) wrote a paper and sent it to cryptography mailing list in 2008.
- The paper was a concept, it’s not sure who he or she is, and it’s not sure if they intended it to go anywhere.
- A conglomerate of developers turned the paper into an open source client, and made it available in 2009.
- First Bitcoins were mined that year, it didn’t take off until 2011.

BITCOIN BASICS

- Method for exchanging value electronically.
- Bitcoins are mined by a computer program which verifies all other transactions.
- “value” arises from computational power.
- Only 21 million Bitcoins will exist.

GETTING A BITCOIN

- Mine it (no longer viable unless you have server farm).
- Buy it from someone
- You have to install an app on your phone or program on your computer. This is a wallet.
- The wallet has a unique address, and the BTC owner transfers the value to your wallet.
- You can now spend it (transfer it to other addresses).

RESOURCES

- All transactions require resources, this is what gives value to cryptocurrencies.
- Some coins are built with transaction fees, so each transaction will cost x amount.
- In Bitcoin, the more transactions there are, the more difficult it is for the next transaction to take place. With high volumes, this means slow network and higher transaction fees.
- In Ethereum, each transaction costs “gas”, the more complex the transaction, more gas is needed to run it.

PRICE INSTABILITY

- Price when I first read about Bitcoin: $7 USD
- Price in June 2011 (first blog post): $14 USD
- Price April 2015: (first class) $230 USD.
- Price November 2015 (first LLM class): $365.
- Price November 2017: $7000
- Price December 2017: $19,500
- Price yesterday: around $5400


wow
such doge
much meme
very internet
so currency
many popular

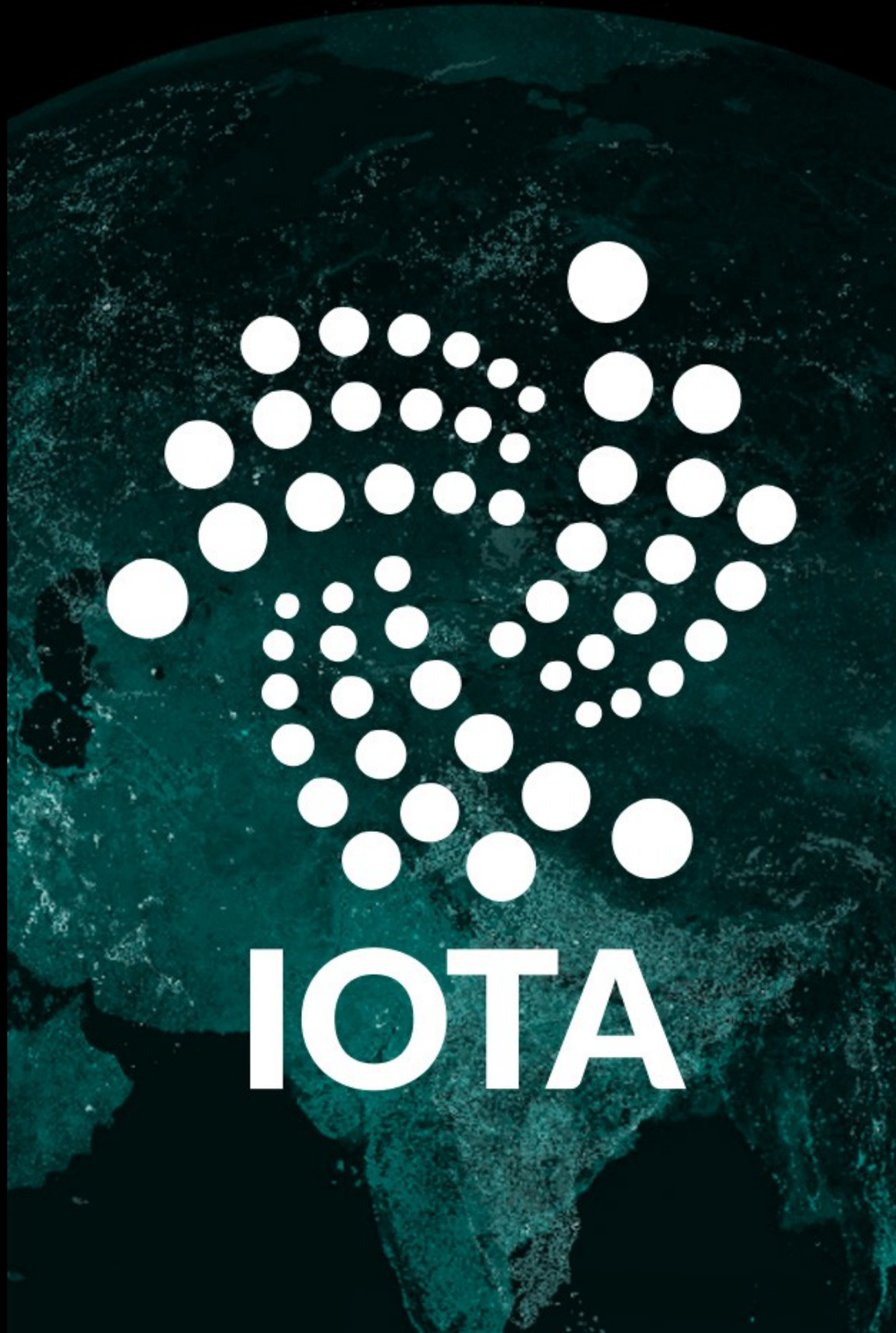
INITIAL COIN OFFERINGS (ICO)

WHAT IS AN ICO?

- Crowdfunding using a cryptocurrency.
- Can be pegged to existing cryptocurrency, or can use its own coin, created specifically for this purpose.
- Designed to bypass regulation.

BUMPY HISTORY

- 2017 saw huge rise in ICOs.
- Everything from porn sites to bananas have been the subject of an ICO.
- IOTA, an IOT-based coin offering, boasts a Market Cap of over $5 billion USD.



LEGAL ISSUES

- Unregulated means unregulated.
- Filled with scams and dodgy characters out to cash in on the hype.
- Possible malpractice claims against attorneys involved in some ICOs.
- Over 75 of all ICOs have folded.

SEC WARNING

- “A number of concerns have been raised regarding the cryptocurrency and ICO markets, including that, as they are currently operating, there is substantially less investor protection than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation. Investors should understand that to date no initial coin offerings have been registered with the SEC.”

CONLCUDING