

SMART CONTRACTS

Steve Omohundro, Ph.D.

Possibility Research

SteveOmohundro.com

PossibilityResearch.com

SelfAwareSystems.com

<http://www.flickr.com/photos/klearchos/623501846/>



First Humans: 50,000 Years Ago

<http://www1.umn.edu/ships/evolutionofmorality/text/23b.htm>

- Nomadic
- Groups of 150
- Few possessions
- Exchange transactions



http://udtanzania2014.weebly.com/uploads/2/5/1/0/25106725/227878_orig.jpg

Roots



Honey



<http://ingervandyke.com/2012/10/africa-in-focus-day-15/>

http://commons.wikimedia.org/wiki/File:San_tribesman.jpg

Hunter/Gatherer Prisoner's Dilemma

http://commons.wikimedia.org/wiki/File:San_tribesman.jpg

http://udtanzania2014.weebly.com/uploads/2/5/1/0/25106725/227878_orig.jpg



Win - Win



Lose - Win



Win - Lose

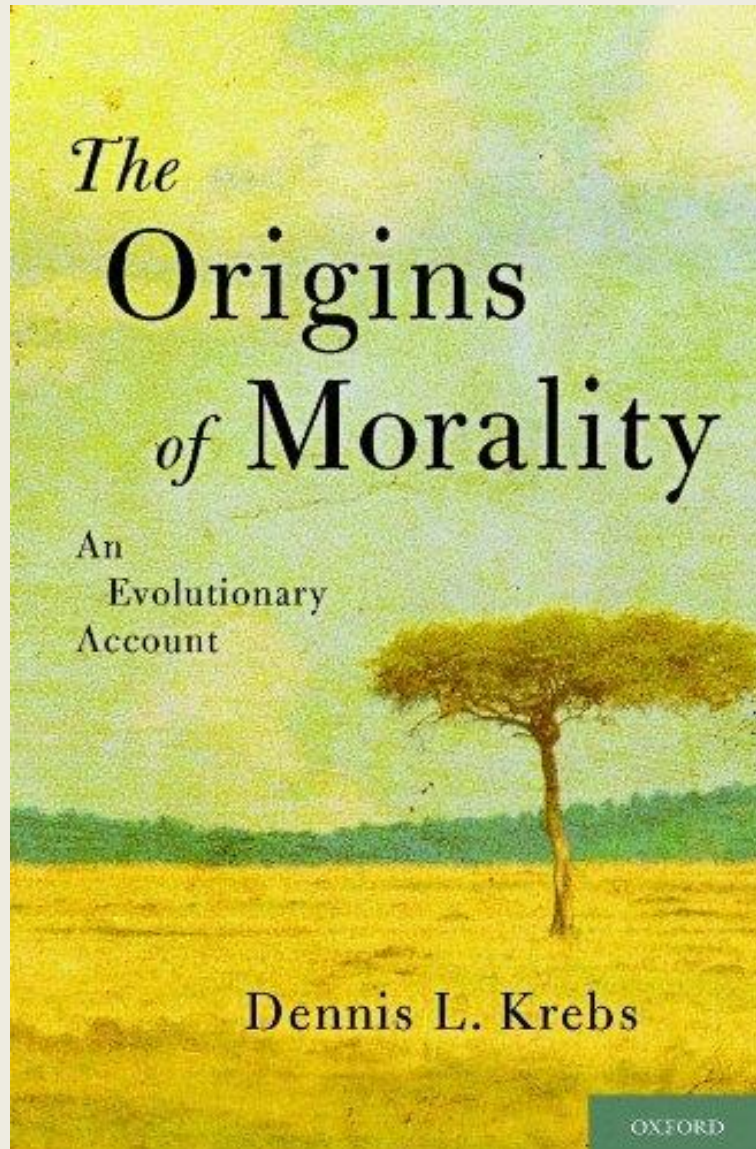


Lose - Lose



<http://ingervandyke.com/2012/10/africa-in-focus-day-15/>

Social and Moral Cooperation Mechanisms



- Language
- Gossip
- Reputation
- Moral Emotions
(Compassion, Gratitude, Awe, Elevation, Anger, Contempt, Disgust, Embarrassment, Shame, Guilt)
- Bare facial skin and color vision
- Altruistic Punishment
- Banishment

First Large Societies: 11,000 Years Ago



- Money: 10,000 ya
- Writing: 5,000 ya
- Laws: 4,000 ya

200x Drop in Violence in 5000 Years

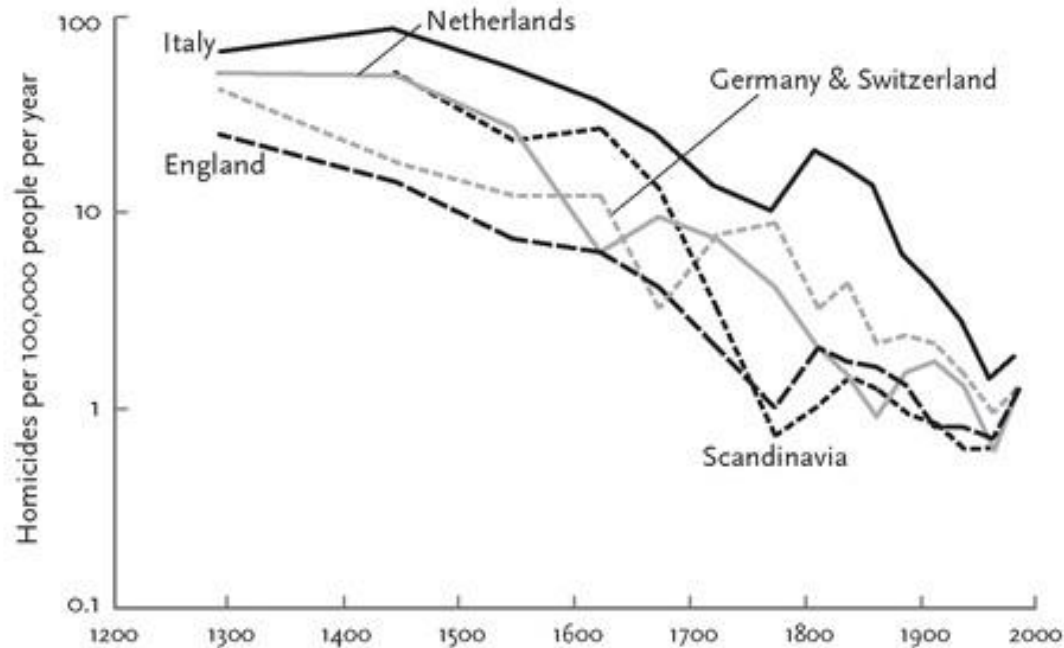
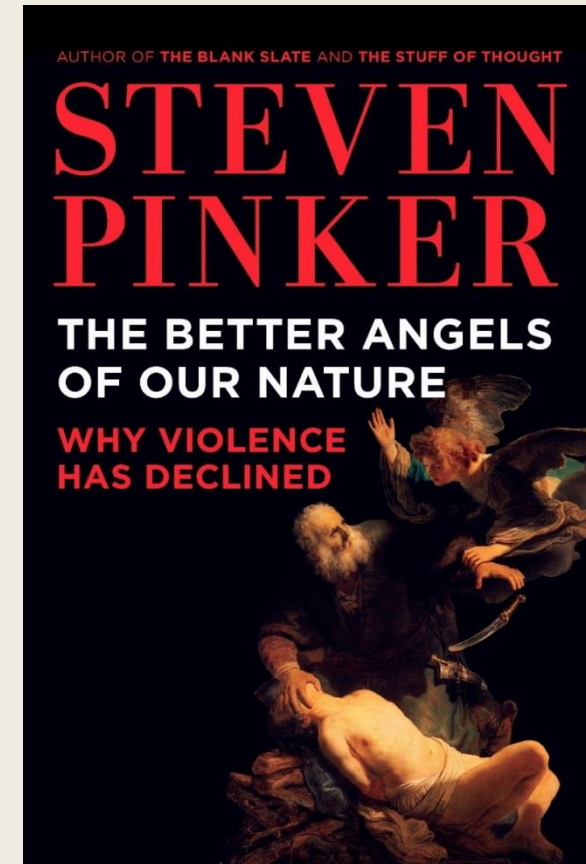


FIGURE 3-3. Homicide rates in five Western European regions, 1300–2000
Source: Data from Eisner, 2003, table 1.

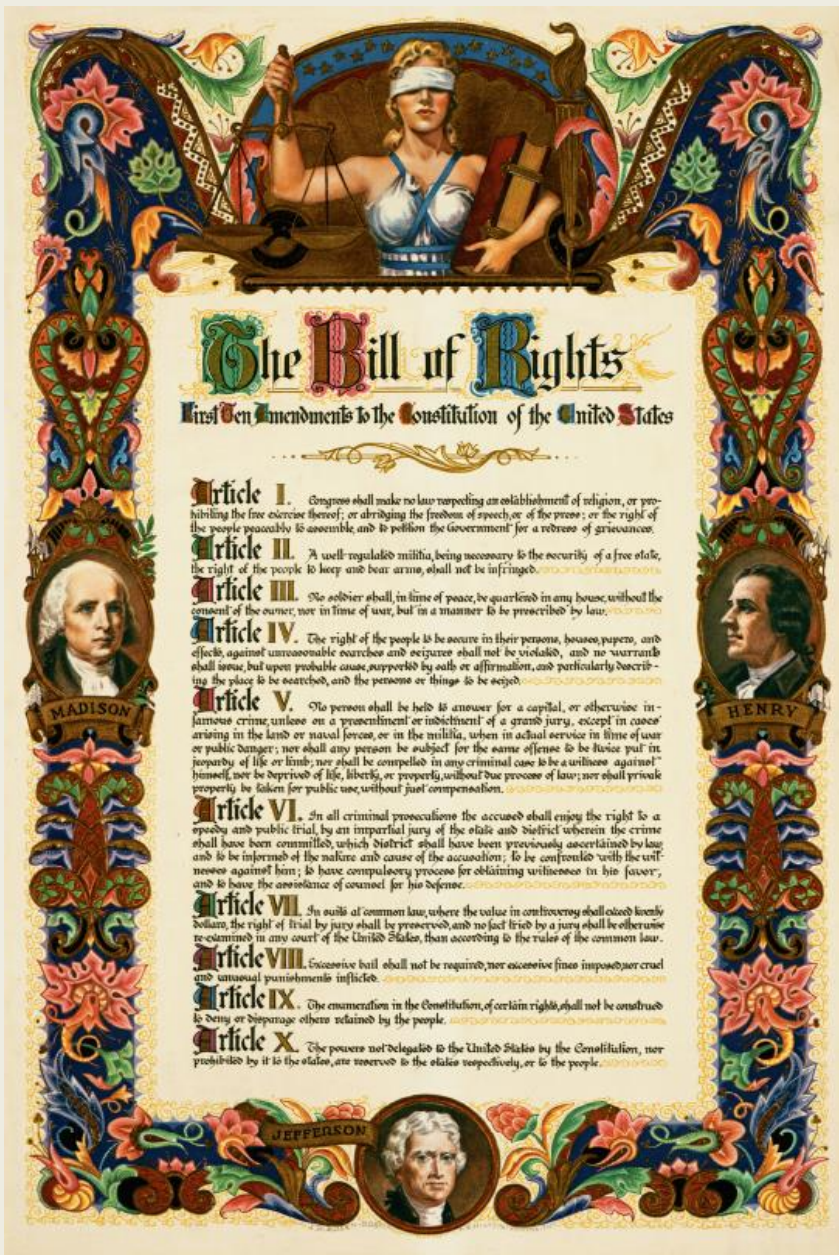
Pinker, "Better Angels of our Nature"



Contracts are Society's Programming Language

Network of agreements about:

- Investment
- Employment
- Purchases
- Supply
- Real Estate
- Construction
- Law
- Insurance
- Marriage
- ...



What is a contract?

“A contract is an agreement creating and defining obligations between the parties.” - Salmond

1. “Offer”: One party makes a proposal
2. “Acceptance”: Another party or parties accept it
3. “Intention to be legally bound”: E.g. competent
4. “Consideration”: Win-Win exchange of value



Economic Theory of Contract Law

“Remedies” for breach

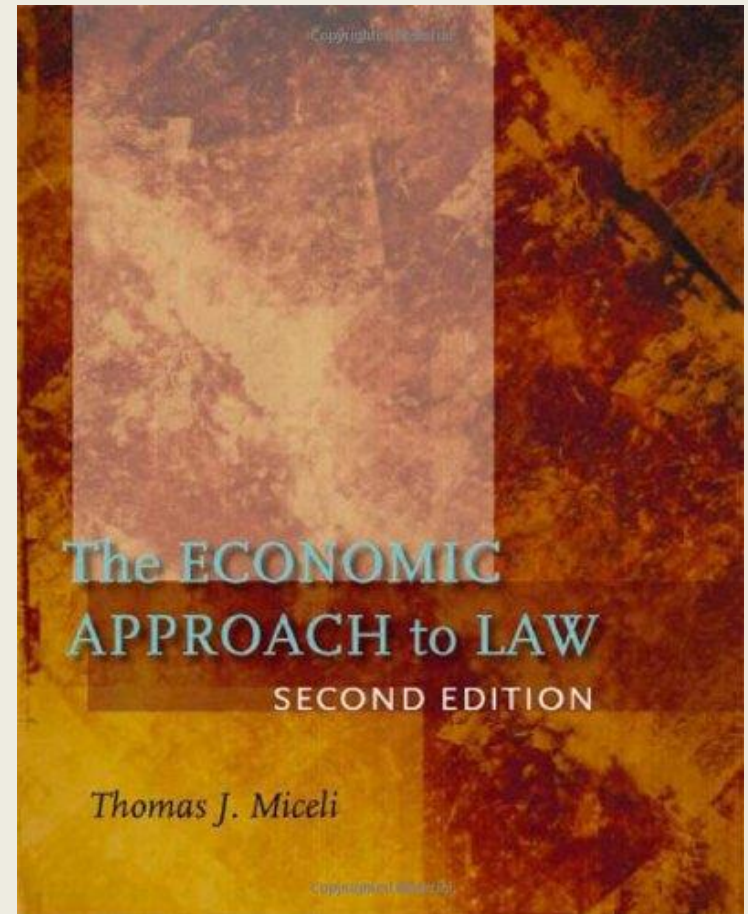
e.g. “Damages” or performance

Create prosocial incentives

“Economic efficiency”

Pareto, Kaldor-Hicks

- Incomplete contracts
- Adverse Selection
e.g. Illness -> health insurance
- Moral Hazard
e.g. Car insurance -> speeding



This is a very expensive mechanism!

Lawyer's fees, judge's costs, waiting time, uncertainty, etc.

Smart Contracts – Nick Szabo 1993

Home > Volume 2, Number 9 - 1 September 1997 > Szabo

f i ® s t m x ñ d @ ¥

PEER-REVIEWED JOURNAL ON THE INTERNET

Read related articles on [Internet economics](#) and [Security](#)

Formalizing and Securing Relationships on Public Networks by Nick Szabo

Abstract

Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols. Similarities and differences between smart contracts and traditional business procedures based on written contracts, controls, and static forms are discussed. By using cryptographic and other security mechanisms, we can secure many algorithmically specifiable relationships from breach by principals, and from eavesdropping or malicious interference by third parties, up to considerations of time, user interface, and completeness of the algorithmic specification. This article discusses protocols with application in important contracting areas, including credit, content rights management, payment systems, and contracts with bearer.

<http://firstmonday.org/ojs/index.php/fm/article/view/548/469>

5 Contracting phases:

Search, Negotiation, Commitment, Performance, Adjudication

Simple Smart Contract: Vending Machine

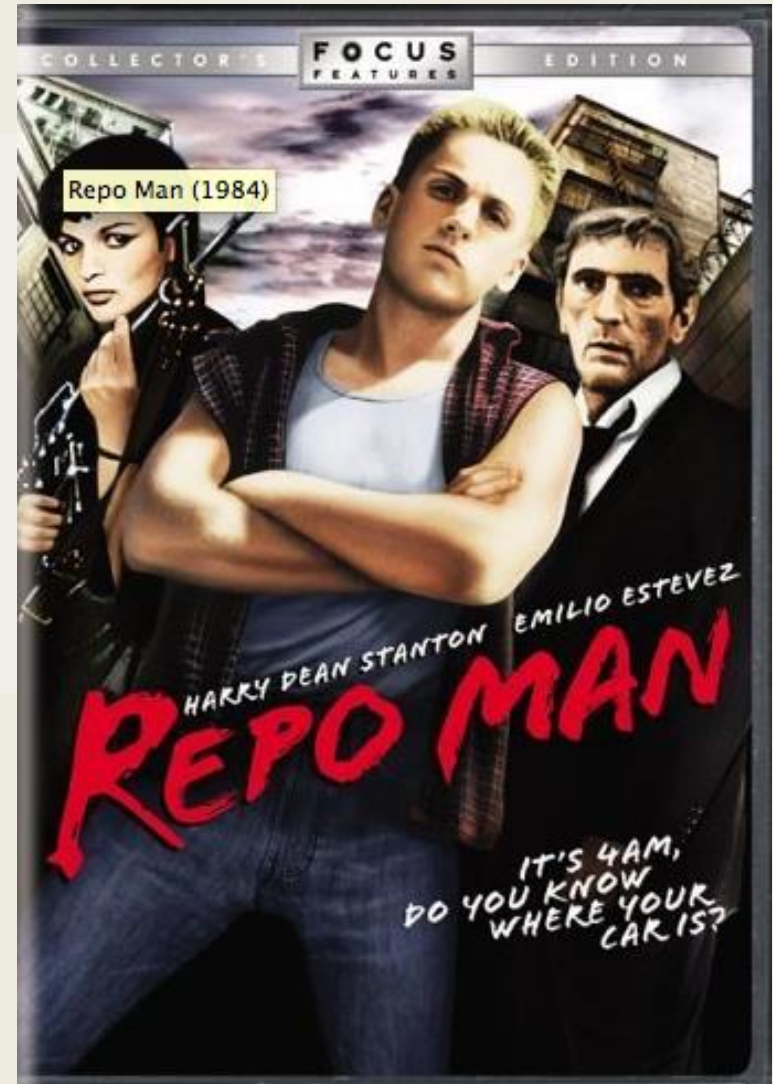
- Contract with bearer
- Takes coins
- Finite Automata
- Dispenses change and product
- Limited loss
- Cost of breaking lockbox is greater than gain



Automobile as Smart Property

- (1) A lock to selectively let in the owner and exclude third parties;
- (2) A back door to let in the creditor;
- (3a) Creditor back door switched on only upon nonpayment for a certain period of time; and
- (3b) The final electronic payment permanently switches off the back door.

<http://firstmonday.org/ojs/index.php/fm/article/view/548/469>



<http://alliancemediartshs.com/wp-content/uploads/2014/09/Repo-Man.png>

Ripped Instruments

- Al wants a cab ride
- Willing to pay \$100
- Doesn't trust cabby Bob
- Bob doesn't trust Al
- He rips \$100 bill in half
- Gives half to Bob
- Gives other half at destination
- Loses incentive to cheat



2008: Bitcoin - Satoshi Nakamoto

- Decentralized consensus
- “Blockchain” ledger prevents double spending
- “Bitcoin miners” get paid for adding blocks
- “Proof of work” prevents “Sybil” attacks
- Current market cap: \$5B



Bitcoin Price History

https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=



Bitcoin Mining Hardware


















<http://www.joeydevilla.com/wordpress/wp-content/uploads/2013/04/bitcoin-fpga-mining-rig.jpg-jpg>



<http://www.kotaku.com.au/2013/11/bitcoin-mining-is-getting-out-of-control/>

513 Altcoins on coinmarketcap.com

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$ 4,694,685,335	\$ 349.71	13,424,625 BTC	\$ 18,091,400	-2.46 %	
2	 Ripple	\$ 136,742,303	\$ 0.004717	28,989,252,282 XRP *	\$ 252,898	-7.33 %	
3	 Litecoin	\$ 122,579,529	\$ 3.69	33,223,706 LTC	\$ 2,547,880	-1.68 %	
4	 BitSharesX	\$ 45,509,349	\$ 0.022756	1,999,883,512 BTSX *	\$ 176,090	-2.50 %	
5	 Dogecoin	\$ 23,477,693	\$ 0.000248	94,670,788,777 DOGE	\$ 229,366	-1.88 %	
6	 Nxt	\$ 21,506,738	\$ 0.021507	999,997,096 NXT *	\$ 39,715	-2.54 %	
7	 Peercoin	\$ 18,698,869	\$ 0.856591	21,829,402 PPC	\$ 57,449	-1.73 %	
8	 Counterparty	\$ 9,375,161	\$ 3.54	2,647,341 XCP *	\$ 4,498	-1.67 %	
9	 Darkcoin	\$ 9,319,006	\$ 1.95	4,789,145 DRK	\$ 46,733	-4.51 %	
10	 Namecoin	\$ 9,209,337	\$ 0.909021	10,131,050 NMC	\$ 61,501	-2.42 %	



Bitcoin: \$4.7B

The rest: \$500M

Satoshi on Bitcoin Scripting 2010

“The design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multi-party signature, etc. If Bitcoin catches on in a big way, these are things we'll want to explore in the future, but they all had to be designed at the beginning to make sure they would be possible later.”

Bitcoin Script

- List of instructions with transactions that limits access to bitcoins
- “Locking script” and “Unlocking script”
- Forth-like, stack-based, no loops
- 80 opcodes: 8 for constants, 7 flow control, 19 stack operations, 1 string, 2 bitwise compare, 20 arithmetic, 10 crypto
- P2SH “Pay-to-script-hash” allows transactions to be signed with a script (2012)

<https://en.bitcoin.it/wiki/Script>

http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#_script_construction_lock_unlock

MultiSig

- **m-of-n address** – associated with n private keys, sending bitcoins requires at least m sigs
- **2-of-2**: address to keep keys on 2 machines
- **2-of-3**: thief needs 2, and can lose 1
- **2-of-3**: buyer, seller, and escrow agent
- 2 factor authentication
- Use two different wallet services
- Use two different software implementations
- Service provider holds a key and is cosigner

Example Smart Contracts in Bitcoin

- Assurance Contracts: Like Kickstarter, only transfer payments if goal is reached
- Returnable Deposit: Demonstrate commitment by tying up funds
- Escrow and dispute mediation: Lock up coins so needs third party to spend
- Multi-party decentralized lotteries

2013: Ethereum – Vitalik Buterin

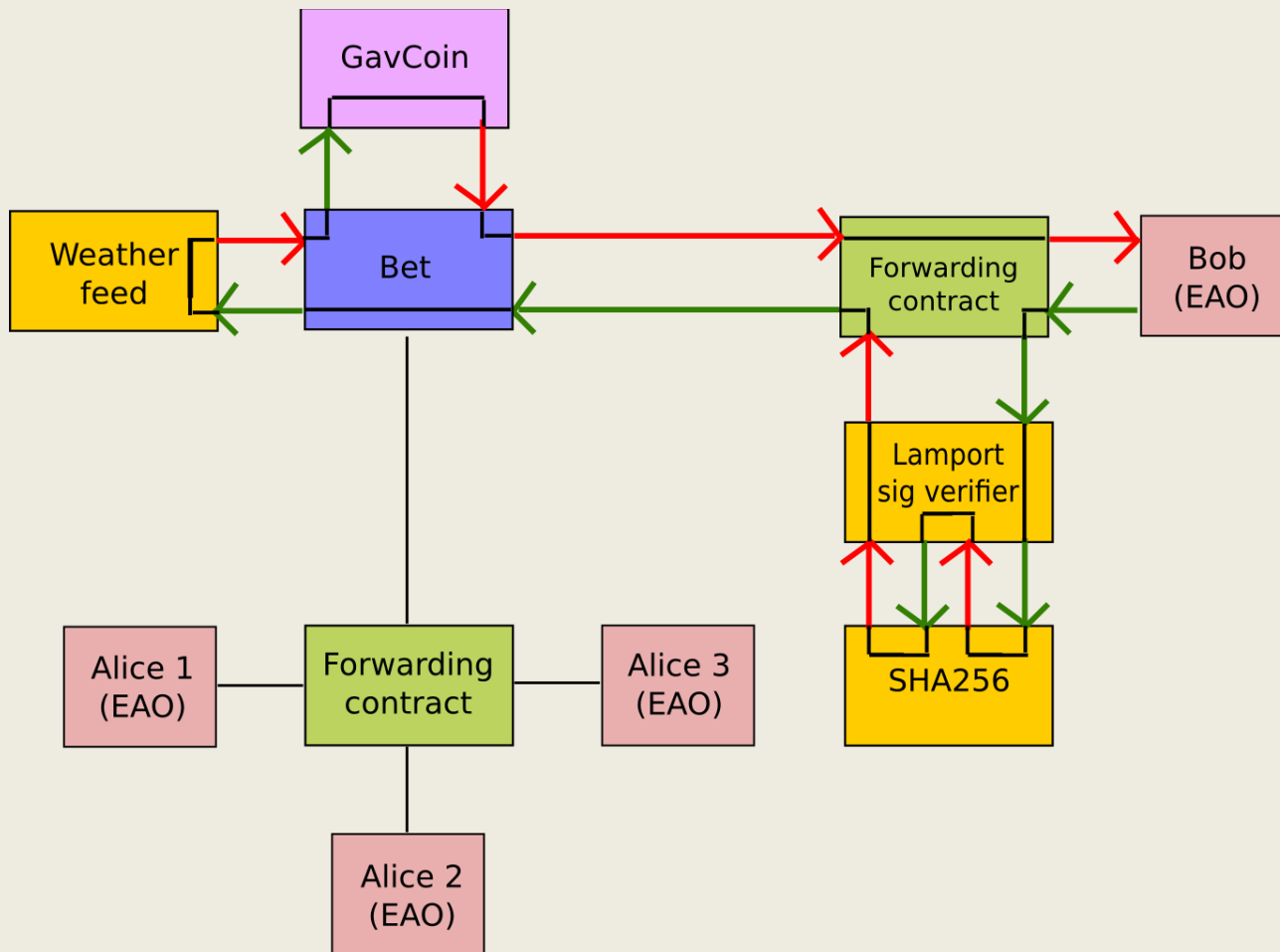
- “Blockchain with a built-in programming language”
- “Consensus-based globally executed virtual machine”
- Contracts in Turing complete programming language EVM
- Execution and storage use “gas”
- \$18.4M Ether Sale 7/2014



EVM: Ethereum Virtual Machine

- “Accounts” have key, code and storage
- Send each other “messages”
- “Externally Owned Accounts” EOA
- “Contracts” receive messages -> run code
- Stack-based language: 56 opcodes, arithmetic, Boolean, control flow, crypto
- New: loops, gas, create, suicide

Interacting Ethereum Contracts



Higher Level Ethereum Languages

- **LLL**: Low Level Lisp-like contract language
- **Serpent**: Python-like contract language
- **Mutan**: C-like contract language
- **Solidity**: JavaScript/C++-like contract language
 - object oriented, static typing

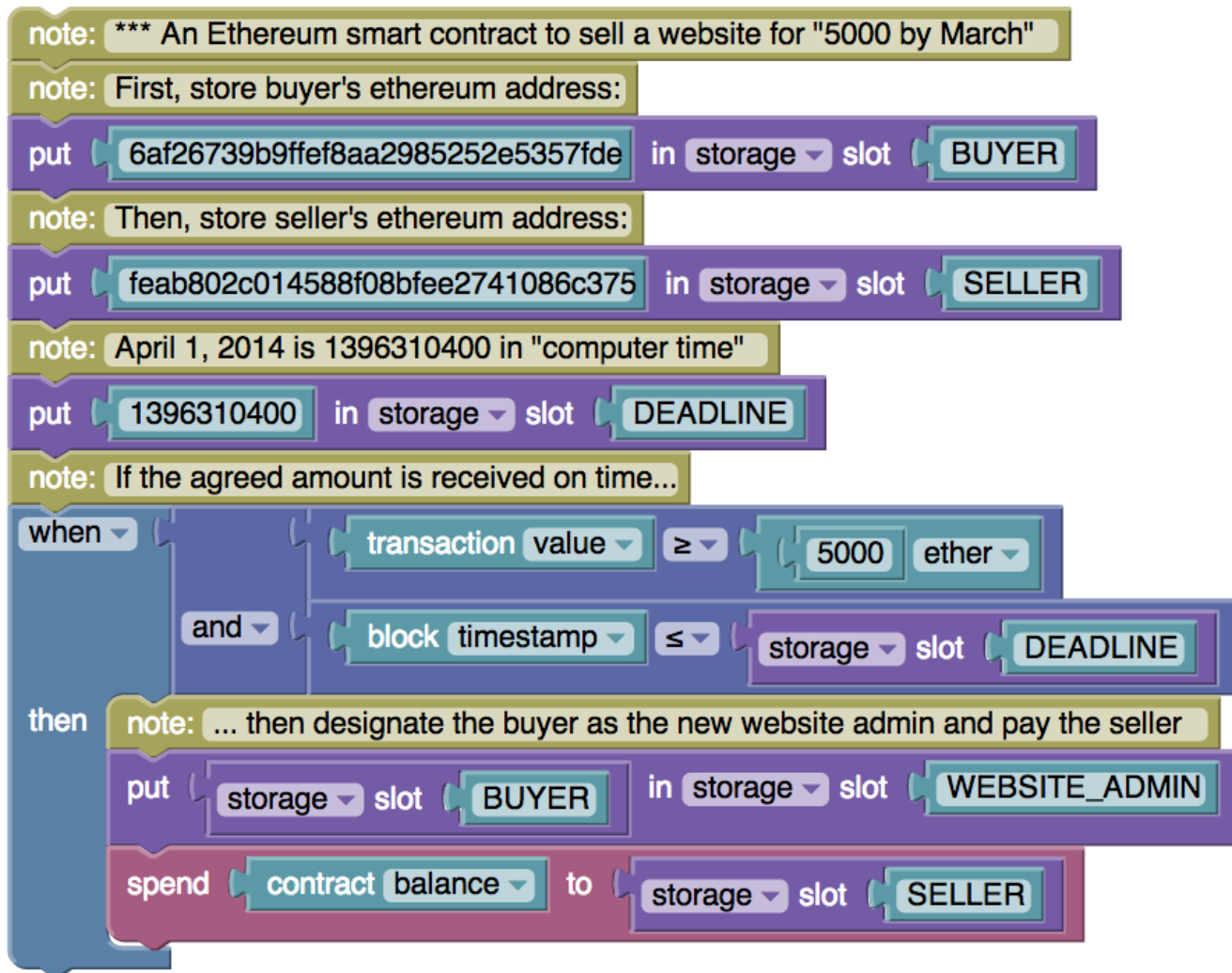
<https://github.com/ethereum/cpp-ethereum/wiki/LLL>

<https://github.com/ethereum/wiki/wiki/Serpent>

<https://github.com/obscuren/mutan>

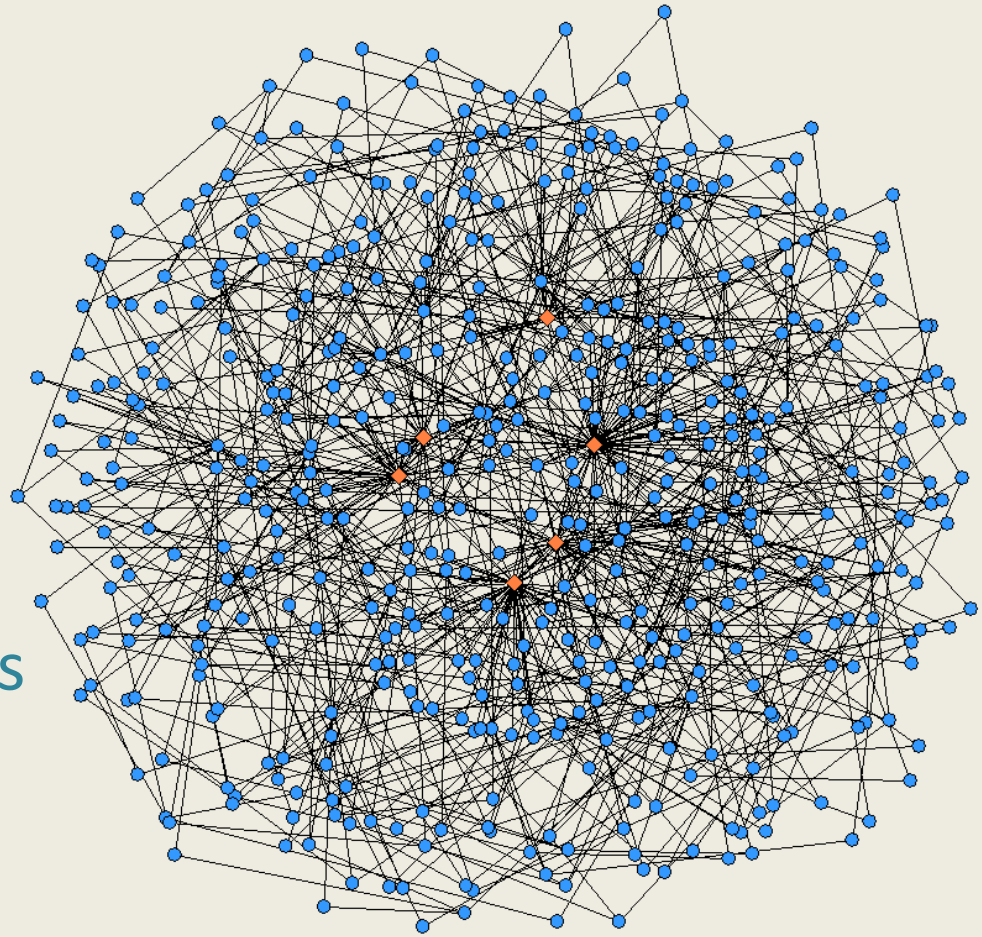
<https://github.com/ethereum/cpp-ethereum/wiki/Solidity,-Docs-and-ABI>

EtherScripter



Smart Contract Applications

- Voting systems
- Domain registries
- Financial exchanges
- Derivatives
- Savings accounts
- Prediction markets
- Crowdfunding platforms
- Intellectual property
- Other Cryptocurrencies
- Smart Property

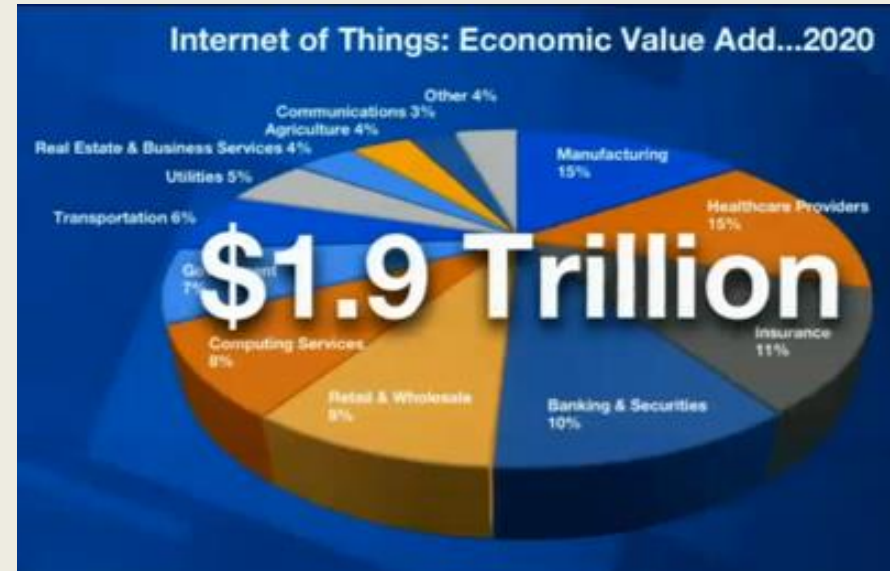


<http://www.ricardoaraujo.net/img/graph.png>

Internet of Things

Gartner: By 2020:

- From 2.5 billion ->
30 billion devices
- Economic value add:
\$1.9 Trillion
- Need:
“Internet of Money”
- Cryptocurrencies and
Smart Contracts!



Obfuscated Contracts – Buterin 2014

- “Indistinguishability Obfuscation”
– Amit Sahai 2013
- Obscure programs or circuits so keys remain hidden
- Contracts can have private keys to external bank or other cryptocurrencies
- But how to agree on obfuscated contracts?



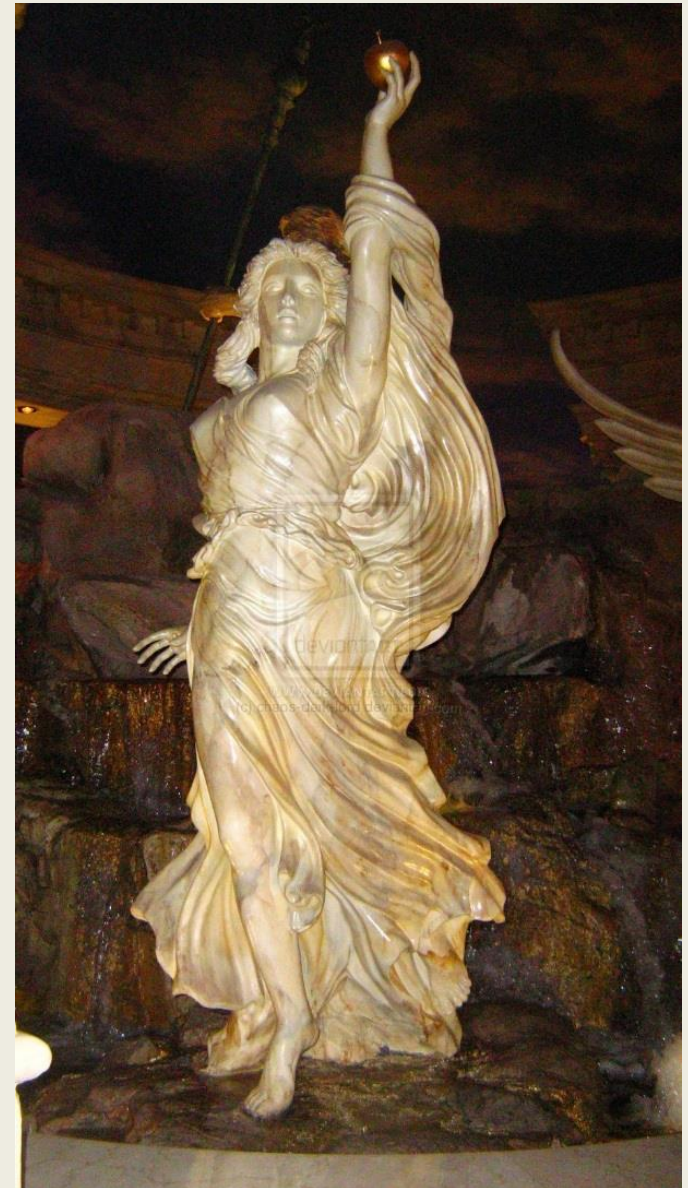
<http://bitcoinmagazine.com/10055/cryptographic-code-obfuscation-decentralized-autonomous-organizations-huge-leap-forward/>

<http://www.cs.ucla.edu/news/news-archive/2013/professor-amit-sahai-has-record-success-at-crypto-2013>

Decentralized Autonomous Organizations (DAO)

Eris: *Ethereum DAO platform inspired by Stack Exchange*

- **Bylaws** on the Blockchain
- Decentralized **Forums**
- Decentralized **Crowdfunding**
- Decentralized **Voting**
- Decentralized **Reputation**
(*Citizenship, Development, Moderation*)
- Standardized “**Contract Factories**”



Self-Bootstrapping DAOs – Adam Levine

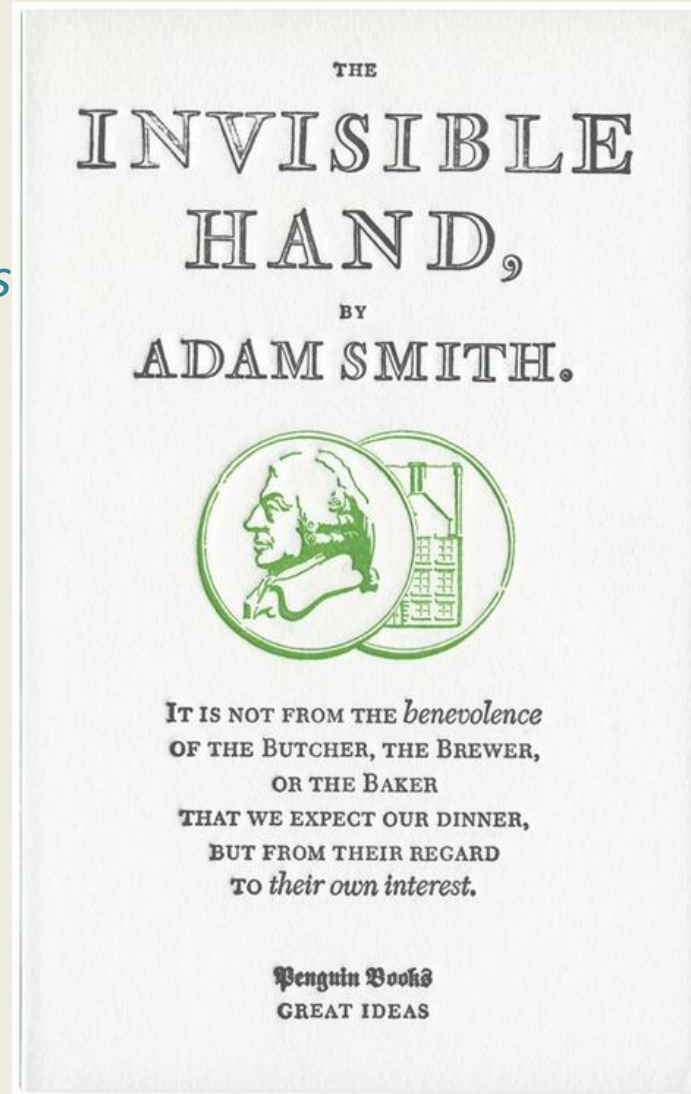
- Propose a project
- Kickstarter-like funding
- Issue “shares”
- Stake-based voting
- Vote on contractors
- Vote as developed
- Distribute profits



Externalities and DAS

(Decentralized Autonomous Societies)

- Adam Smith's "Invisible Hand"
- Inefficiency from "Externalities"
- **Negative:** *Pollution, Climate change, Arms races, Noise, Fraud, Scams, Antibiotics, Overfishing, Overlogging, Speeding, DUI, Status competition*
- **Positive:** *Vaccination, Bees, Education, Network effects*
- **Internalize:** *Regulation, Taxes, Fines*
- Coase Theorem (1960)
- Information and Transaction Costs



Smart Contracts and AI

Als enable smart contract:

- Perception
- Action
- Dispute resolution
- Design
- Constraints

Smart contracts constrain
Robots and Als:

- AI legal framework
- Self-enforcing structures



<http://www.trbimg.com/img-50fe0287/turbine/ct-biz-0122-baxter1.jpg-20130121/600>