

# Cryptocurrencies, Smart Contracts, and the Future of Economic Interaction

Steve Omohundro, Ph.D.  
PossibilityResearch.com  
SteveOmohundro.com  
SelfAwareSystems.com



70,000 BC: Population 5,000

Today: Population 7 billion



# New Mechanisms for Cooperation



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

[http://www.amazon.com/Before-Dawn-Recovering-History-Ancestors/dp/014303832X/ref=sr\\_1\\_1](http://www.amazon.com/Before-Dawn-Recovering-History-Ancestors/dp/014303832X/ref=sr_1_1)



# Hunter/Gatherer Prisoner's Dilemmas



Win - Win



Lose - Win



Win - Lose

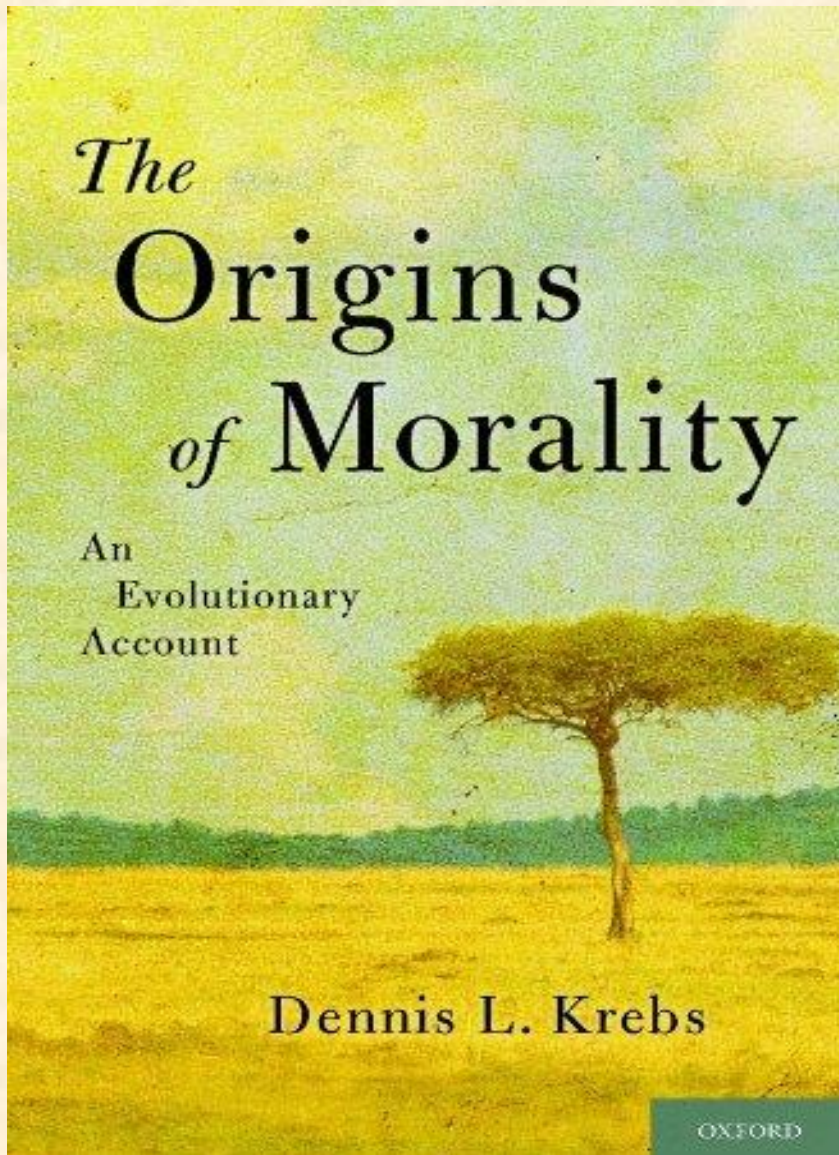


Lose - Lose





# Cooperation via Biology



- **Moral Emotions**  
(Compassion, Gratitude, Awe, Elevation, Anger, Contempt, Disgust, Embarrassment, Shame, Guilt)
- **Language**
- **Gossip**
- **Reputation**
- **Banishment**



# Cooperation via Contracts

*Agreements with incentive mechanisms.*

*“Society’s Programming Language”*

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



# Money

Contracts that transfer value across space and time.

10,000ya: Cattle

3,200ya: Cowrie Shells

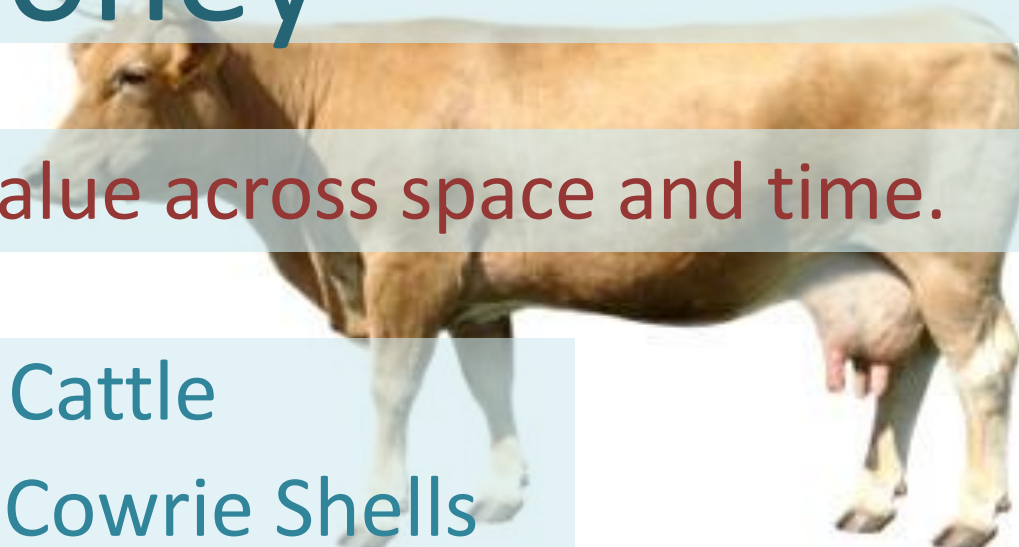
3,000ya: Metal money

2,500ya: Modern coins

1,200ya: Paper currency

200ya: Gold standard

40ya: Bits






# Money Failures

- Loss
- Theft
- Counterfeiting
- Value alteration
- Accidental Spend
- Double Spend
- Unstable Value
- Coin debasement
- Not Accepted

MEET THE NEW  
**\$100 BILL**

A NEW \$100 BILL GOES INTO CIRCULATION OCT. 8, 2013. IT STILL FEATURES THE FAMILIAR PORTRAIT OF BEN FRANKLIN, BUT COMES WITH A HOST OF NEW SECURITY FEATURES.



**RAISED PRINTING**  
RUN YOUR FINGER ALONG BEN FRANKLIN'S SHOULDER AND IT WILL FEEL BUMPY. THIS IS THE FIRST TIME A NEW TEXTURE HAS BEEN INTRODUCED TO AN AMERICAN BILL.

**3-D SECURITY RIBBON**  
A BLUE STRIP RUNNING DOWN THE BILL IS EMBEDDED WITH IMAGES THAT SHIFT FROM 100<sup>0</sup> TO BELLS AS YOU MOVE THE BILL SIDE TO SIDE. THE STRIP IS WOVEN INTO THE BILL, NOT PRINTED ON TOP OF IT.

**BELL AND INKWELL**  
A COLOR-SHIFTING BELL IS IMPOSED ON A COPPER INKWELL, REPRESENTING THE WELLS USED TO SIGN THE DECLARATION OF INDEPENDENCE. THE BELL SHIFTS COLORS AS THE BILL IS MOVED.

**THE "100" LABEL**  
A LARGE NUMERAL 100 CHANGES COLOR FROM COPPER TO GREEN WHEN THE BILL IS TILTED.

**FRANKLIN WATERMARK**  
WHEN THE BILL IS HELD UP TO THE LIGHT, A FAINT PORTRAIT OF BEN FRANKLIN BECOMES VISIBLE.

PHOTO CREDIT: BUREAU OF ENGRAVING AND PRINTING



# Yapese Rai stones: 1,000 AD





# Cryptographic Money

1500BC: Ciphers

1840: Cryptanalysis

1932: Enigma

1949: Shannon

1951: NSA

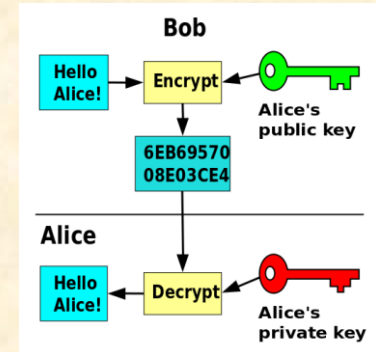
1975: DES

1976: Public Key

1983: Chaum

2001: SHA256

2008: Bitcoin



[http://upload.wikimedia.org/wikipedia/commons/a/a2/16th\\_century\\_French\\_cypher\\_machine\\_in\\_the\\_shape\\_of\\_a\\_book\\_with\\_arms\\_of\\_Henri\\_II.jpg](http://upload.wikimedia.org/wikipedia/commons/a/a2/16th_century_French_cypher_machine_in_the_shape_of_a_book_with_arms_of_Henri_II.jpg)

[http://en.wikipedia.org/wiki/File:Public\\_key\\_encryption.svg](http://en.wikipedia.org/wiki/File:Public_key_encryption.svg) <http://upload.wikimedia.org/wikipedia/commons/1/1c/Chaum.jpg>

<http://en.wikipedia.org/wiki/File:Enigma.jpg> <http://blog.newegg.com/blog/wp-content/uploads/bitcoin-logo-3d.jpg>



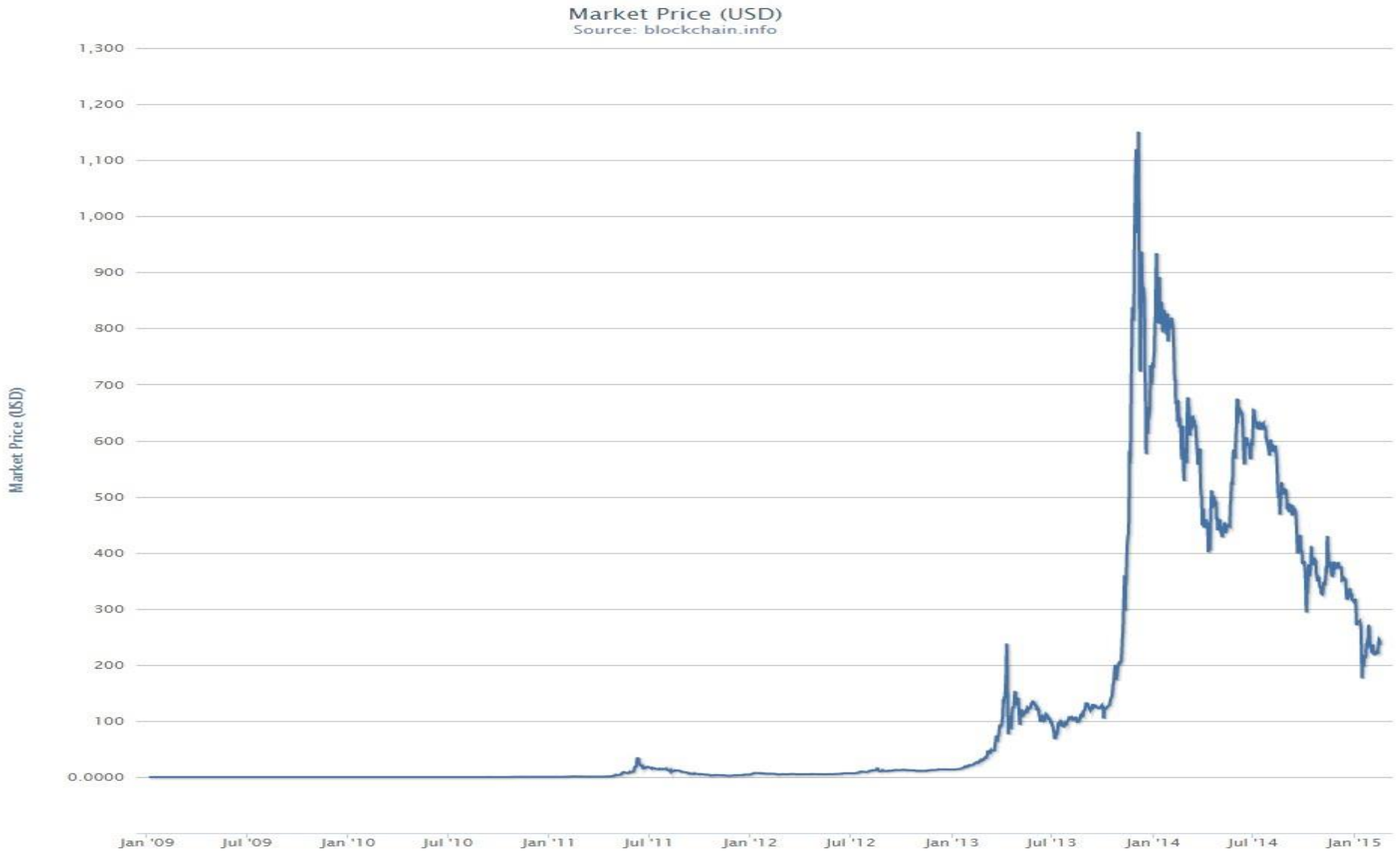
# 2008: Bitcoin - Satoshi Nakamoto

- Decentralized consensus
- “Blockchain” ledger prevents double spending
- “Bitcoin miners” get paid for adding blocks
- “Proof of work” prevents “Sybil” attacks
- Current market cap: \$3B




















# Bitcoin Price History





# 511 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: \$3.3B

The rest: \$650M



# Bitcoin Mining Hardware



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

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



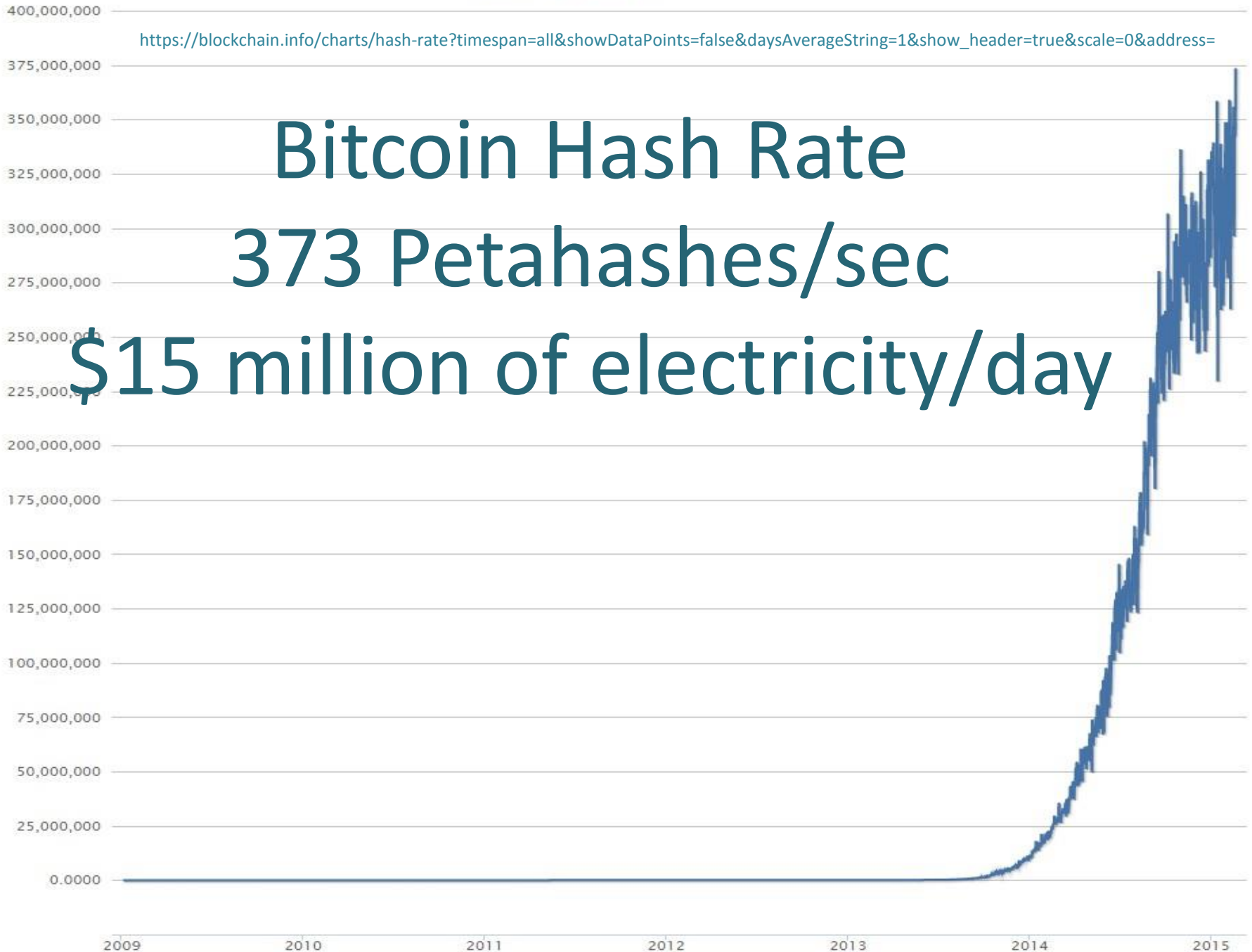
[https://blockchain.info/charts/hash-rate?timespan=all&showDataPoints=false&daysAverageString=1&show\\_header=true&scale=0&address=](https://blockchain.info/charts/hash-rate?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=)

# Bitcoin Hash Rate

373 Petahashes/sec

\$15 million of electricity/day

Hash Rate GH/s







**Reuven Cohen** Contributor

*I focus on disruptive trends in technology and cloud computing.*

Opinions expressed by Forbes Contributors are their own.

[FOLLOW](#)

TECH 11/28/2013 @ 6:00PM | 33,429 views

# Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!

[+ Comment Now](#) [+ Follow Comments](#)

I admit, like a lot of others, I've found myself with a bit of [a bitcoin obsession lately](#). I find the vast amount of effort it takes to create something that doesn't actually exist, completely fascinating. So I decided to find out how much computing power is exerted in the effort to mine and run the global bitcoin network.



*The bitcoin logo (Photo credit: Wikipedia)*

## 5 Investing Mistakes for Retirees to Avoid in 2015

If you have a portfolio worth \$500,000 or more, download the guide by *Wall Street Journal* featured financial advisor, Dash Investments. It's called **Retirement Planning Essentials** and it contains valuable information you need to know. Don't delay!

[Click here to download your free guide!](#)

DASH INVESTMENTS

# An enormous bitcoin mine went up in flames, affecting the entire network

SHARE



WRITTEN BY

Kabir Chibber

@quinto\_quarto

OBSESSION

Digital Money

November 9, 2014



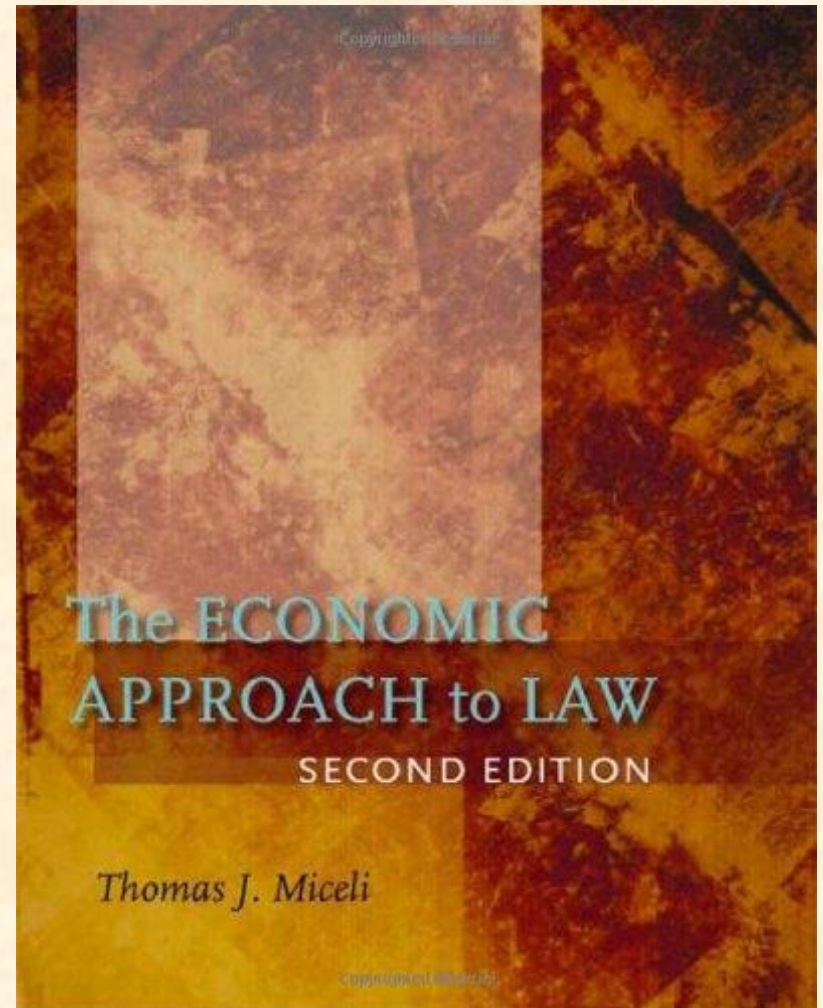
 (Flickr/Coindesk)

<http://qz.com/293418/an-enormous-bitcoin-mine-went-up-in-flames-affecting-the-entire-network/>



# Contracts

- Created by expensive lawyers
- Ambiguous and hard to read
- Remedy is to sue
- Lawsuits expensive, uncertain
- Judge's expensive, very busy
- Laws designed for economic efficiency (*Pareto, Kaldor-Hicks*)



*This is a very expensive mechanism!*

# 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*



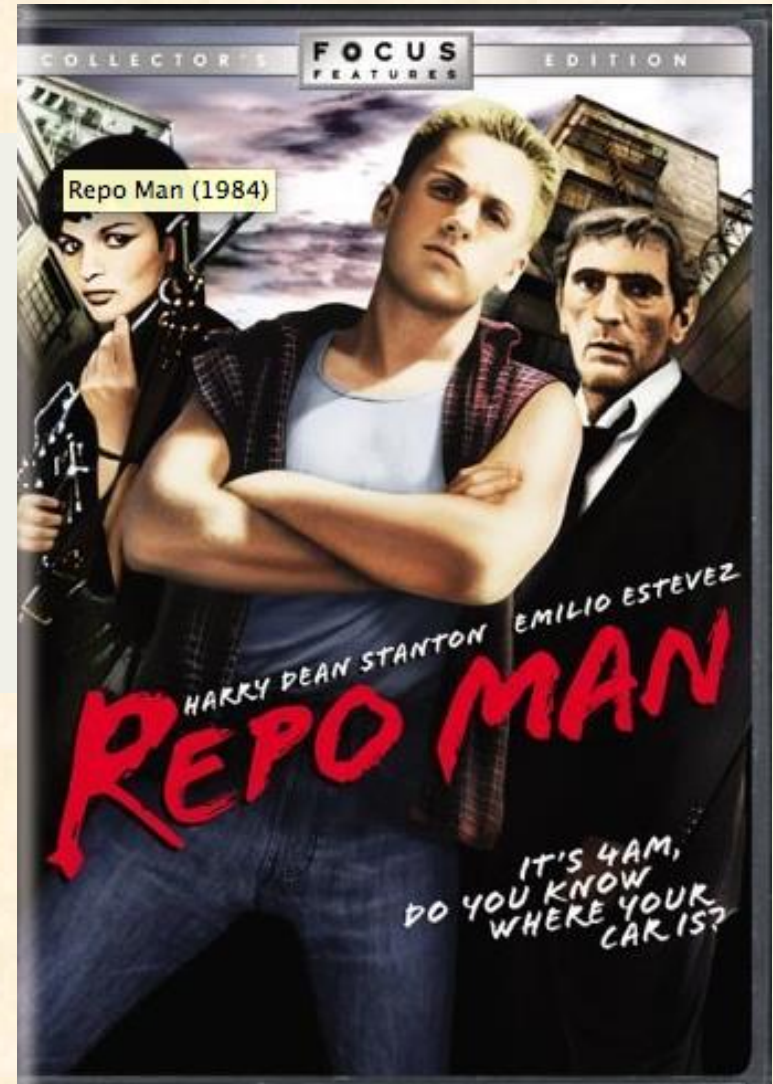
# Simple Smart Contract: Vending Machine

- 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.

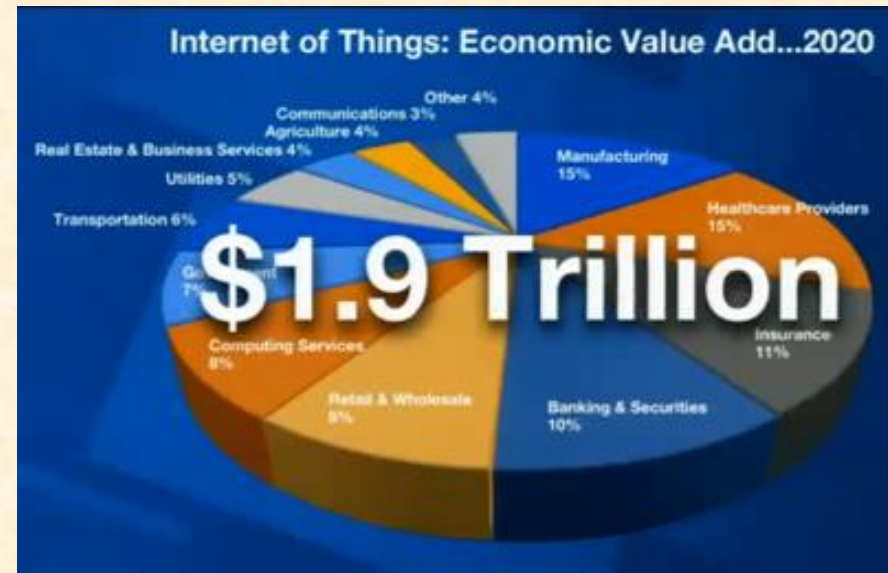




# Internet of Things

Gartner: By 2020:

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



# 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.”



# 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

# 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”
- Summer 2014 presold more than \$15 million Ether

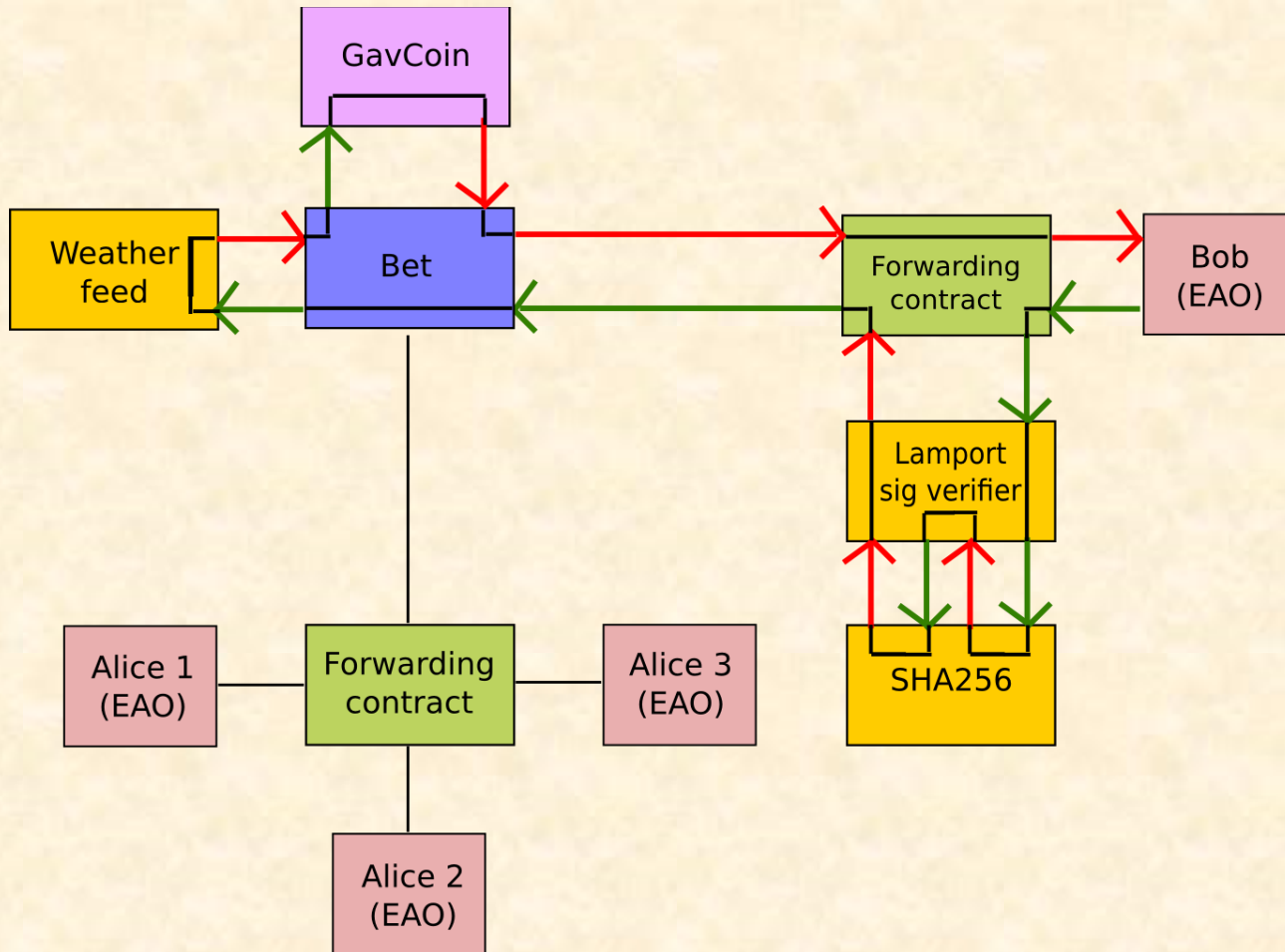




# EVM: Ethereum Virtual Machine

- “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: 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

# EtherScripter

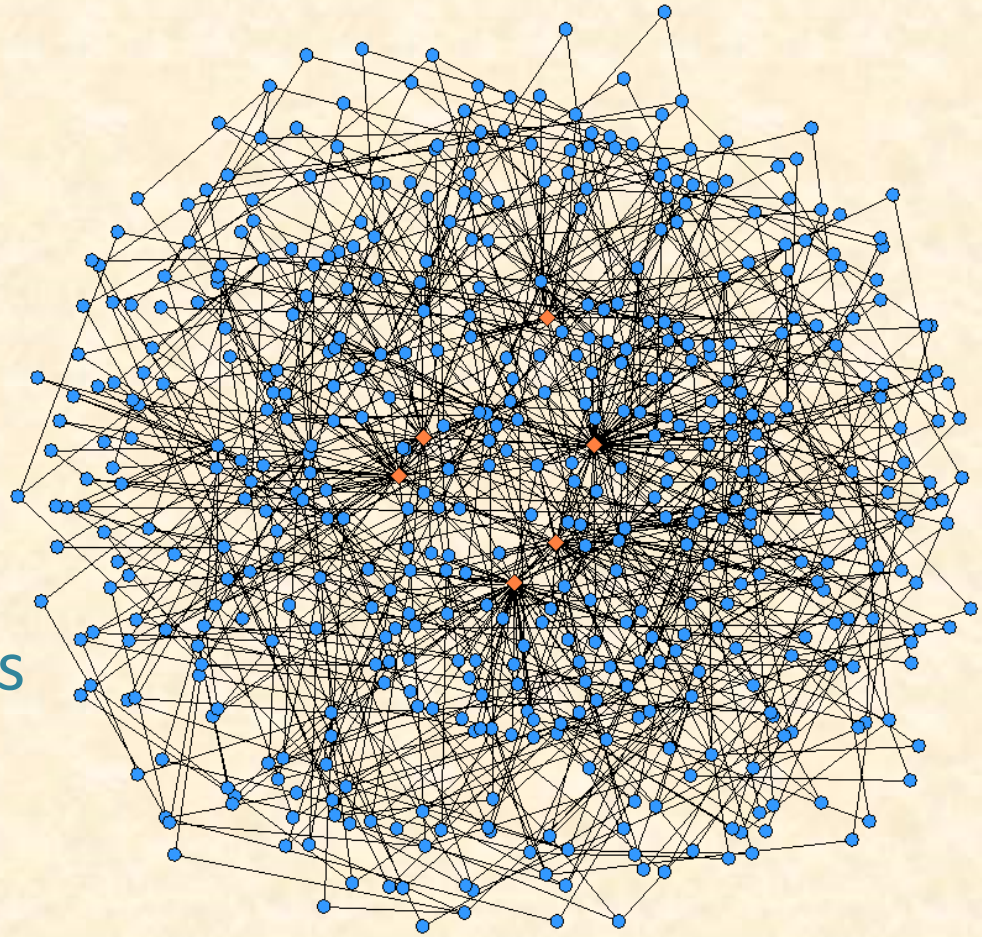
The image shows a sequence of code blocks in EtherScripter, a visual programming language for Ethereum smart contracts. The blocks are as follows:

- note:** `*** An Ethereum smart contract to sell a website for "5000 by March"`
- note:** `First, store buyer's ethereum address:`
- put:** `6af26739b9ffef8aa2985252e5357fde` in storage slot `BUYER`
- note:** `Then, store seller's ethereum address:`
- put:** `feab802c014588f08bfee2741086c375` in storage slot `SELLER`
- note:** `April 1, 2014 is 1396310400 in "computer time"`
- put:** `1396310400` in storage slot `DEADLINE`
- note:** `If the agreed amount is received on time...`
- when:** `transaction value`  $\geq$  `5000 ether` and `block timestamp`  $\leq$  `storage slot DEADLINE`
- then:** `note: ... then designate the buyer as the new website admin and pay the seller`
- put:** `storage slot BUYER` in `storage slot WEBSITE_ADMIN`
- spend:** `contract balance` to `storage slot SELLER`



# 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>

# 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?





# 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”**



<http://hplusmagazine.com/2014/06/17/eris-the-dawn-of-distributed-autonomous-organizations-and-the-future-of-governance/>

<https://eris.projectdouglas.org/>

[http://fc01.deviantart.net/fs70/i/2010/073/8/a/godess\\_eris\\_statue\\_by\\_chaos\\_dark\\_lord.jpg](http://fc01.deviantart.net/fs70/i/2010/073/8/a/godess_eris_statue_by_chaos_dark_lord.jpg)

# Self-Bootstrapping DAOs – Adam Levine

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





# Some Blockchain Issues

- Blockchain size: 29G, growing 1G/mo
- Miner concentration – 10 big pools
- Vitalik: Bitcoin is paying \$600 million/year for a 5-of-10 multisig
- Wallet security: multisig wallets
- Anonymity brings out the worst
- Irreversibility – Assassination markets
- Non-economic attack incentives

# Crypto-Tech Platforms, Programs and Protocols

## Non-Bitcoin Blockchain Bitcoin Currency

**Blockstream**  
**Truthcoin**

## Non-Bitcoin Blockchain Non-Bitcoin Currency

**Ethereum: *Ether***  
**BitShares: *BTS***  
**Truthcoin: *CashCoin***  
**Litecoin: *LTC***  
**PayCoin: *XPY***

## Non-Blockchain Consensus

**Ripple: *XRP***  
**Stellar: *STR***  
**NXT: *NXT***  
**Hyperledger**  
**Tendermint**  
**Pebble**  
**Open Transactions**

## Bitcoin Blockchain Bitcoin Currency

**Bitcoin: *BTC***

## Bitcoin Blockchain Non-Bitcoin Currency

**Factom: *Factoids***  
**Mastercoin: *MSC***  
**Counterparty: *XCP***  
**Namecoin: *NMC***

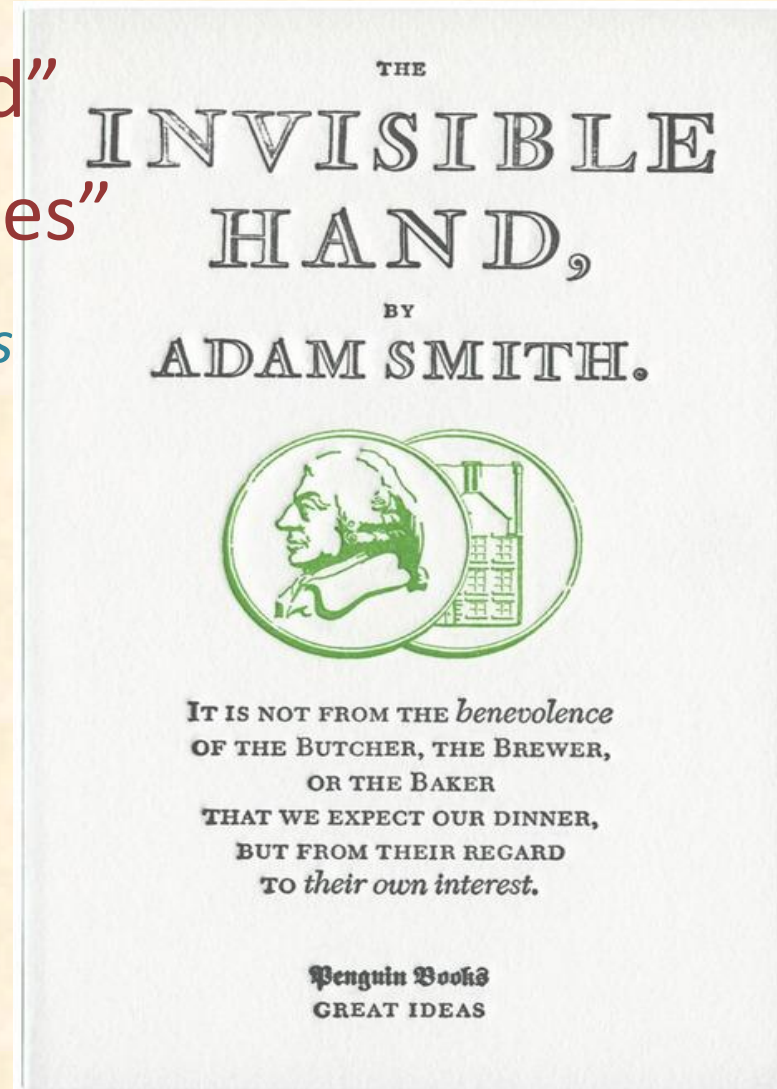
## Blockchain Neutral Smart Services

**Eris Industries**  
**PeerNova**  
**Codium**  
**SmartContract**  
**SAE**  
**Tezos**  
**Tillit**



# Externalities and DAS (Decentralized Autonomous Societies)

- Adam Smith's "Invisible Hand"
- Inefficiency from "Externalities"
- 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>