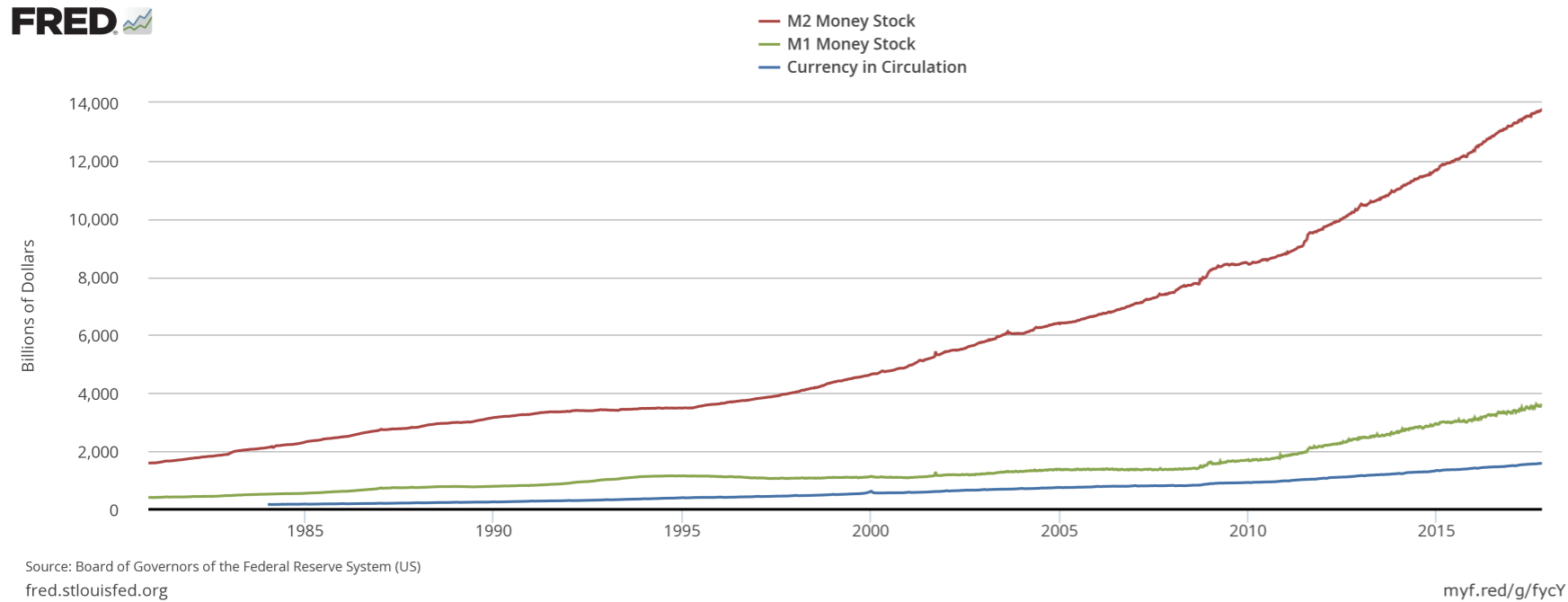


Introduction to the Blockchain, Bitcoin, Ethereum, and Smart Contracts

Valuable assets are becoming digital

Digital assets are becoming valuable



List of most expensive domain names

From Wikipedia, the free encyclopedia

This is a list of some of the highest prices paid for [domain names](#). The list is limited to domains that sold for \$3 million or more.

Domain	Price	Sale Date	Ref
Insurance.com	\$35.6 million	2010	[1]
VacationRentals.com	\$35 million	2007	[2]
PrivateJet.com	\$30.18 million	2012	[1]
Internet.com	\$18 million	2009	[1]
360.com	\$17 million	2015	[3]
Insure.com	\$16 million	2009	[4]
Fund.com	£9.99 million	2008	[4]
Sex.com	\$13 million	2010 November 17	[5]
Hotels.com	\$11 million	2001	[1]
Porn.com	\$9.5 million	2007	[4]
Porno.com	\$8,888,888	2015 February	[1]
Fb.com	\$8.5 million	2010 November	[6]
Business.com	\$7.5 million	1999 December	[4]
Diamond.com	\$7.5 million	2006	[4]
Beer.com	\$7 million	2004	[4]

Forbes



NOV 13, 2010 @ 07:20 PM 82,454

Meet The Man Who Just Made A Half Million From The Sale Of Virtual Property



Oliver Chiang, FORBES STAFF

Gaming The System [FULL BIO](#)

Opinions expressed by Forbes Contributors are their own.

Problem

Existing systems for managing these assets are insecure, incompatible, jurisdictionally dependent, and old

Risk Factor | Telecom | Security

DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands

By Robert Charette
Posted 9 Sep 2011 | 20:45 GMT

NEWS

Technology

Equifax to be investigated by FCA over data breach

🕒 24 October 2017 | Technology

[f](#) [t](#) [v](#) [e](#) [Share](#)

#BUSINESS NEWS

OCTOBER 3, 2017 / 1:57 PM / 21 DAYS AGO

Yahoo says all three billion accounts hacked in 2013 data theft

Jonathan Stempel, Jim Finkle

[t](#) [f](#)

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

Target ignored its own alarms—and turned its customers into victims

By Michael Riley, Benjamin Elgin, Dune Lawrence, and Carol Matlack
March 17, 2014, 7:31 AM PDT



Bitcoin



Downtown Josh Brown 

@ReformedBroker



“We don’t like Bitcoin we love blockchain” is the new “I read Playboy for the articles.”

1:07 PM · Oct 13, 2017



In-person

Online



{BTC txn walkthrough}

Ethereum & Smart Contracts

What is Ethereum?

- It's a **general purpose** blockchain
- Turing-complete programming language
- Account types:
 - Standard user accounts
 - Contracts
- Allows anyone to create an application whose behavior depends **only** on the contract's code

What are smart contracts?

- Computer programs that control digital assets
- Nick Szabo's analogy: **vending machines**
- Except...
 - In the real world, scaling defense is difficult
 - In the digital world, scaling defense is easy

Smart contract creation

- Write code
- Compile code
- Send code-containing transaction to the blockchain
- Code-containing transaction is assigned a contract address
- Any future transactions sent to that contract address execute the code contained by that address

Blockchains

What is a blockchain?

A blockchain is a decentralized network **with a memory**

The Trust Protocol

- Blockchains allow for running applications on a fully trusted foundation
- Strong guarantee the application won't:
 - Charge rents
 - Arbitrarily change
 - Shut down
- Disintermediation ('app XYZ' without XYZ, Inc.)

Game Theory / Coordination

Scenario: you and another prisoner are locked in separate rooms and given the following list of numbers:

[564735] - [100328] - [048752] - [203947]

[100000] - [970934] - [457224] - [161051]

If you both choose the same number, you both go free, otherwise you're both killed

Game Theory / Coordination

Properties of blockchains create naturally good coordination points

- Reliable
- Neutral
- Independent of any single corporate and/or political pressure

Pillars of Cryptoeconomics

- Cryptography provides guarantees about the past
 - Transaction validity, historical integrity
- Economic incentives provide guarantees about the future
 - Finality, immutability
- Decentralization provides guarantees about the blockchain's neutrality and availability
 - Fault tolerance, redundancy

Incentives

Behavior	Penalty/Reward
Do not participate	\$0
Create block on main chain	$(\text{Block reward} + \text{Tx fees}) - \text{Operating costs}$
Create block not on main chain	Operating costs

Why use a blockchain?

- “Zero infrastructure”
 - Users are the infrastructure
- Lower social cost to bootstrapping
- High security and reliability
 - Fault tolerant
- Global
- Open
- Developers don’t need to think about:
 - What computers/servers their programs are running on
 - Who controls them
 - What jurisdiction their software is running in
- **Democratize the ability to make agreements**

Applications

- Identity (uPort, Civic)
- Decentralized cloud computing (Golem, iExec)
- Decentralized cloud storage (IPFS/Filecoin, Storj, Swarm)
- Asset management (Melonport, Iconomi)
- Prediction markets (Augur, Gnosis)
- Other digital assets (reward/merchant points, domain names, in-game currencies, etc.)
- Many, many more...

Problems with blockchains

- Scalability
- Privacy
- Speed
- Ease of development
- Price volatility

Solutions

- State channels
- Sharding
- Ring signatures
- Zero-knowledge proofs
- Faster consensus algorithms
- Formal code verification

Questions?