ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

Money-over-IP:

From Bitcoin to M2M Commerce

Professor George M. Giaglis
Vice Rector, AUEB
giaglis@aueb.gr; @giaglis

Questions

A. In a digital world, **why has money resisted digitization** so far?

B. How would **digital money** look like?

C. What **implications** would digital money have for commerce and society?

Agenda

1. The **nature and functions** of money

2. Digital Money and **Bitcoin**

3. Towards a **Digital Money World:** A new era for commerce?

1. The nature and functions of money

The nature of money

Money is the most widely used, yet misunderstood, ***technology*** *in the world*

C. Winklevoss & T. Winklevoss (2014)

The money around us, the money we grow up with, appears the only ***"real" money*** *to us*

M. Friedman (1994)

Why do we have money anyway?

We would hardly be able to trade with each other, unless we had a common **medium of exchange**

- **Bartering** is not an efficient economic mechanism
- The **Coincidence of Wants Dilemma**

*So, **money** was invented to facilitate **commerce***

The Functions of Money

Medium of exchange

Unit of account

Store of value

Functions are independent but mutually reinforcing

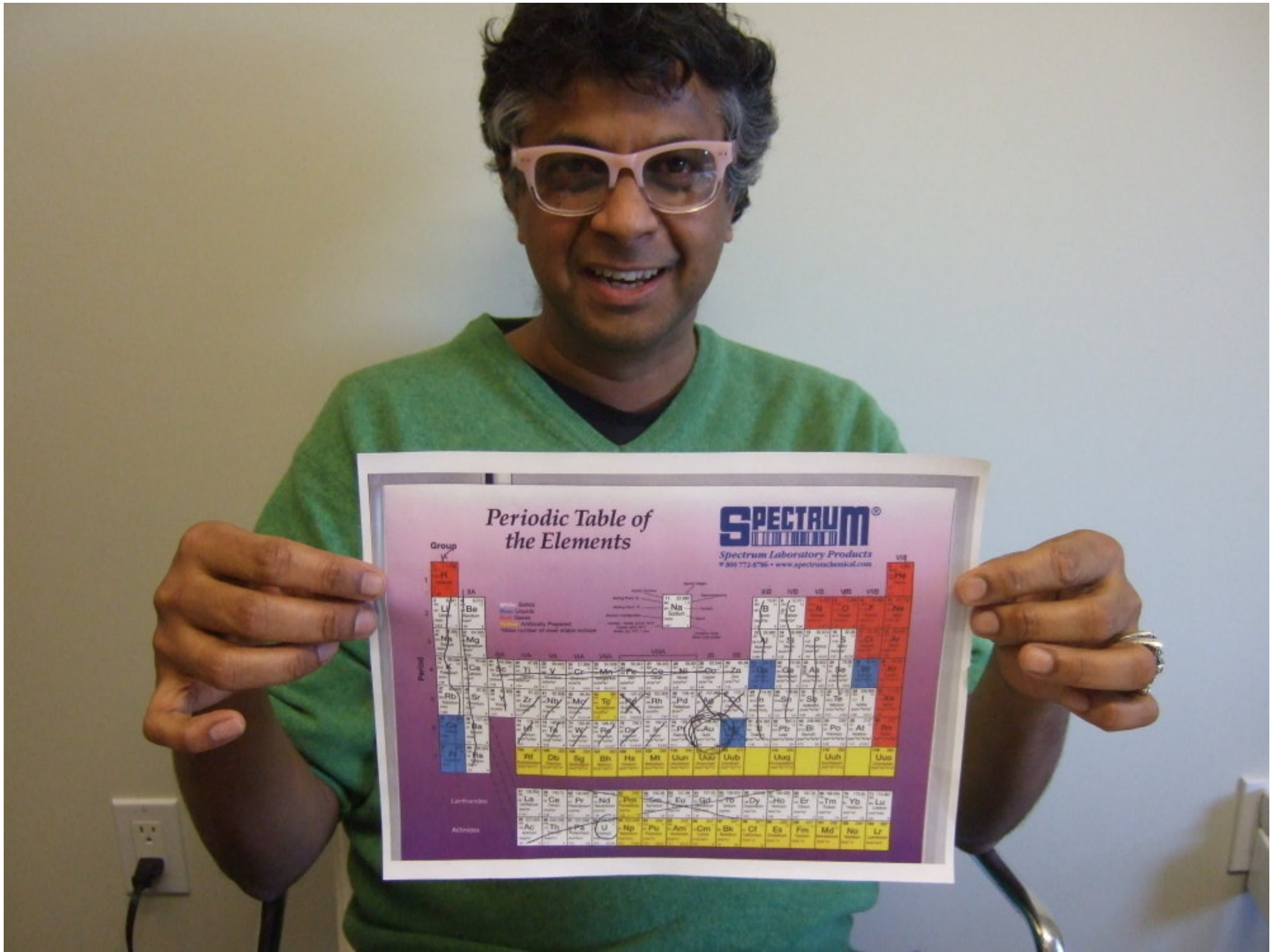
No currency is perfect on all these dimensions – all present trade-offs

What are the properties of ideal money?

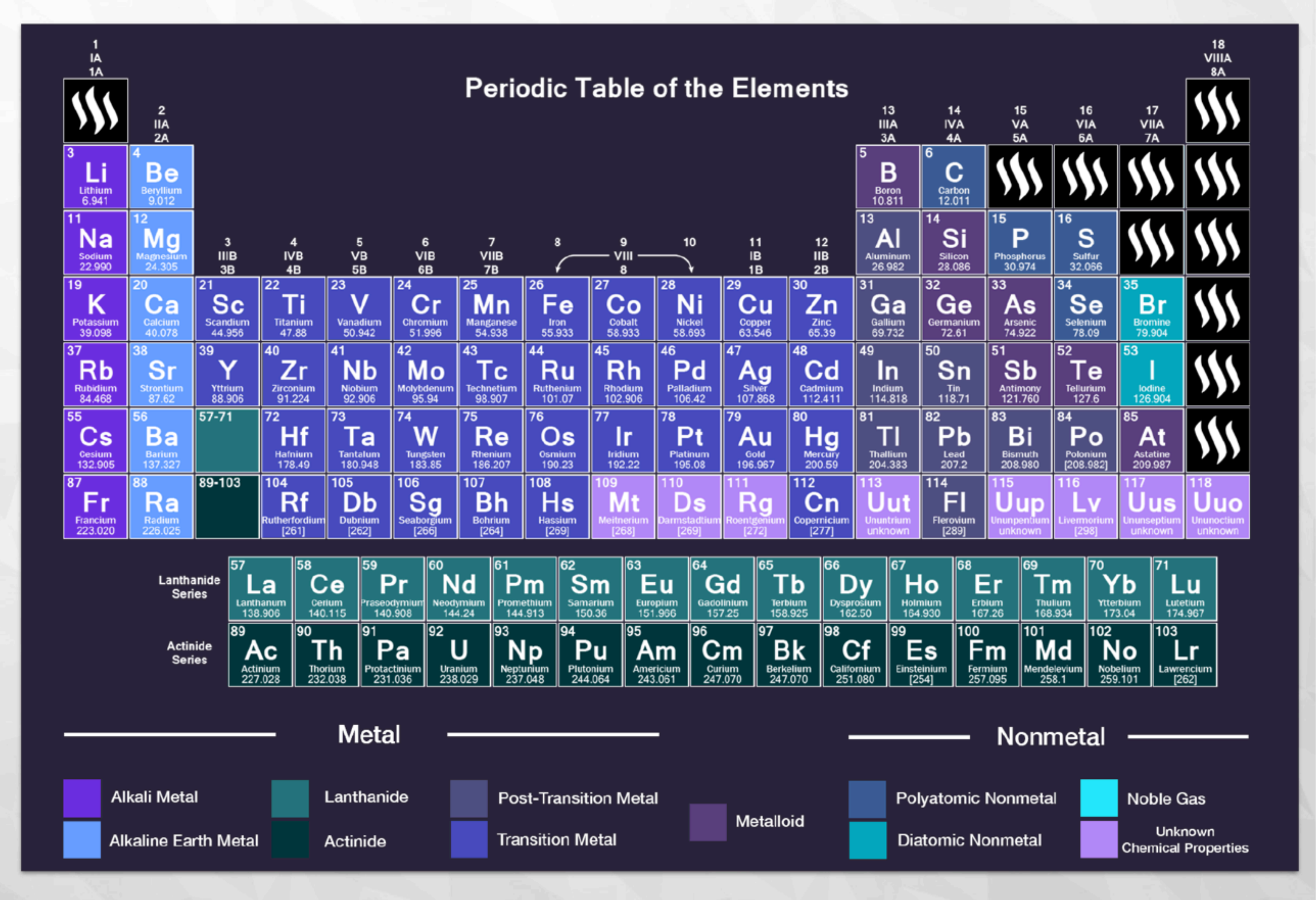
1. **Scarcity** (but, not too much!)
2. **Divisibility**
3. **Storability**
4. **Durability** (ideally, for ever)
5. **Fungibility** (equality of each unit)
6. **Portability**
7. **Verifiability** (incl. anti-counterfeiting)
8. **Acceptability** (perhaps the most important of all!)

So, which element would make ideal money?

Professor Sanat Kumar, chemical engineer at Columbia University, was asked this question



Money cannot be a *gas*



Periodic Table of the Elements

1 IA 1A	2 IIA 2A	3 IIIB 3B	4 IVB 4B	5 VB 5B	6 VIB 6B	7 VIIB 7B	8	9 VIII 8	10	11 IB 1B	12 IIB 2B	13 IIIA 3A	14 IVA 4A	15 VA 5A	16 VIA 6A	17 VIIA 7A	18 VIIIA 8A
3 Li Lithium 6.941	4 Be Beryllium 9.012											5 B Boron 10.811	6 C Carbon 12.011				
11 Na Sodium 22.990	12 Mg Magnesium 24.305											13 Al Aluminum 26.982	14 Si Silicon 28.086	15 P Phosphorus 30.974	16 S Sulfur 32.066		
19 K Potassium 39.098	20 Ca Calcium 40.078	21 Sc Scandium 44.956	22 Ti Titanium 47.88	23 V Vanadium 50.942	24 Cr Chromium 51.996	25 Mn Manganese 54.938	26 Fe Iron 55.933	27 Co Cobalt 58.933	28 Ni Nickel 58.693	29 Cu Copper 63.546	30 Zn Zinc 65.39	31 Ga Gallium 69.732	32 Ge Germanium 72.61	33 As Arsenic 74.922	34 Se Selenium 78.09	35 Br Bromine 79.904	
37 Rb Rubidium 84.468	38 Sr Strontium 87.62	39 Y Yttrium 88.906	40 Zr Zirconium 91.224	41 Nb Niobium 92.906	42 Mo Molybdenum 95.94	43 Tc Technetium 98.907	44 Ru Ruthenium 101.07	45 Rh Rhodium 102.906	46 Pd Palladium 106.42	47 Ag Silver 107.868	48 Cd Cadmium 112.411	49 In Indium 114.818	50 Sn Tin 118.71	51 Sb Antimony 121.760	52 Te Tellurium 127.6	53 I Iodine 126.904	
55 Cs Cesium 132.905	56 Ba Barium 137.327	57-71	72 Hf Hafnium 178.49	73 Ta Tantalum 180.948	74 W Tungsten 183.85	75 Re Rhenium 186.207	76 Os Osmium 190.23	77 Ir Iridium 192.22	78 Pt Platinum 195.08	79 Au Gold 196.967	80 Hg Mercury 200.59	81 Tl Thallium 204.383	82 Pb Lead 207.2	83 Bi Bismuth 208.980	84 Po Polonium [208.982]	85 At Astatine 209.987	
87 Fr Francium 223.020	88 Ra Radium 226.025	89-103	104 Rf Rutherfordium [261]	105 Db Dubnium [262]	106 Sg Seaborgium [266]	107 Bh Bohrium [264]	108 Hs Hassium [269]	109 Mt Meitnerium [268]	110 Ds Darmstadtium [269]	111 Rg Roentgenium [272]	112 Cn Copernicium [277]	113 Uut Ununtrium unknown	114 Fl Flerovium [289]	115 Uup Ununpentium unknown	116 Lv Livermorium [298]	117 Uus Ununseptium unknown	118 Uuo Ununoctium unknown

Lanthanide Series	57 La Lanthanum 138.906	58 Ce Cerium 140.115	59 Pr Praseodymium 140.908	60 Nd Neodymium 144.24	61 Pm Promethium 144.913	62 Sm Samarium 150.36	63 Eu Europium 151.966	64 Gd Gadolinium 157.25	65 Tb Terbium 158.925	66 Dy Dysprosium 162.50	67 Ho Holmium 164.930	68 Er Erbium 167.26	69 Tm Thulium 168.934	70 Yb Ytterbium 173.04	71 Lu Lutetium 174.967
Actinide Series	89 Ac Actinium 227.028	90 Th Thorium 232.038	91 Pa Protactinium 231.036	92 U Uranium 238.029	93 Np Neptunium 237.048	94 Pu Plutonium 244.064	95 Am Americium 243.061	96 Cm Curium 247.070	97 Bk Berkelium 247.070	98 Cf Californium 251.080	99 Es Einsteinium [254]	100 Fm Fermium 257.095	101 Md Mendelevium 258.1	102 No Nobelium 259.101	103 Lr Lawrencium [262]

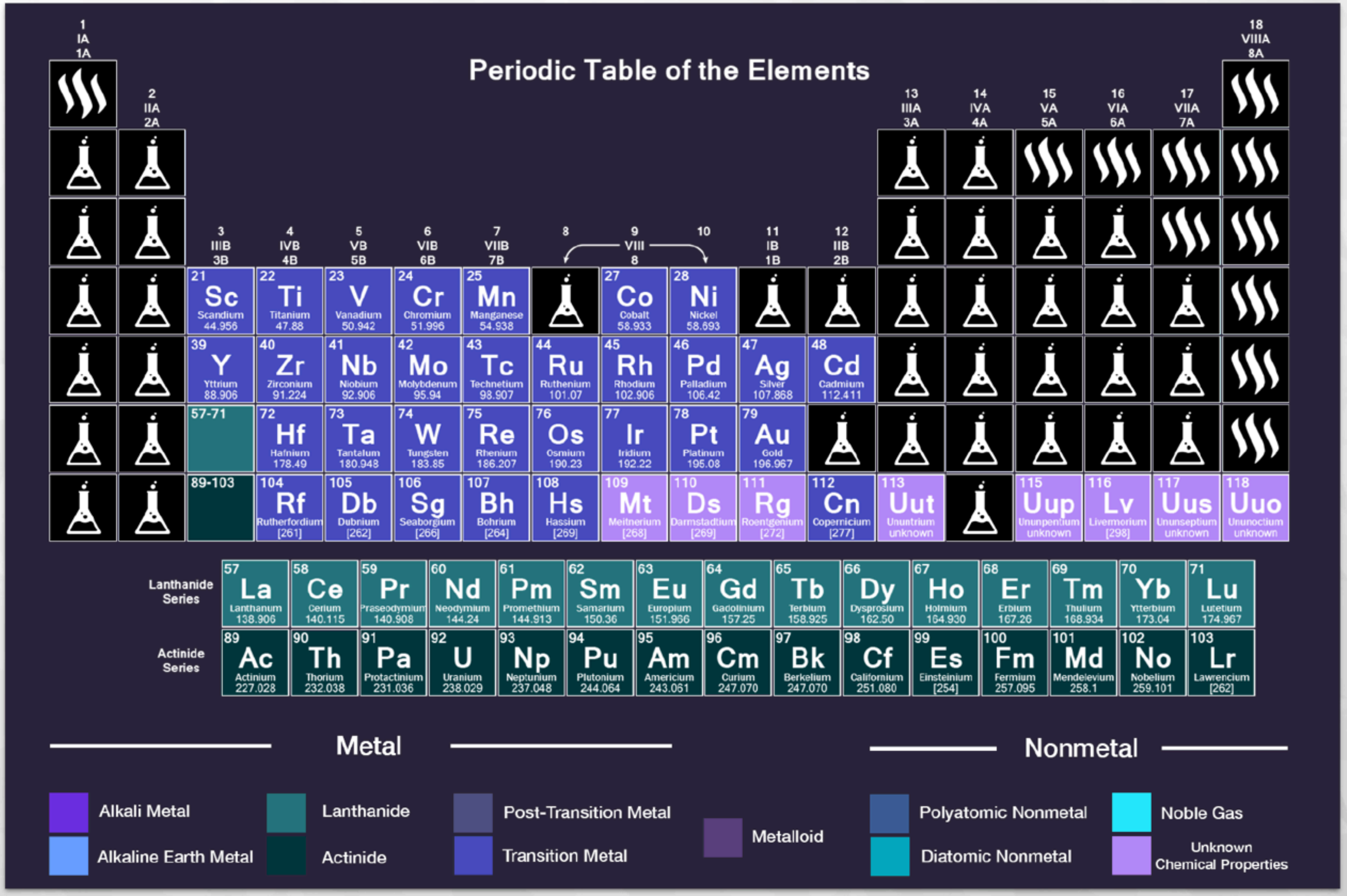
Metal

- ■ Alkali Metal
- ■ Alkaline Earth Metal
- ■ Lanthanide
- ■ Actinide
- ■ Post-Transition Metal
- ■ Transition Metal
- ■ Metalloid

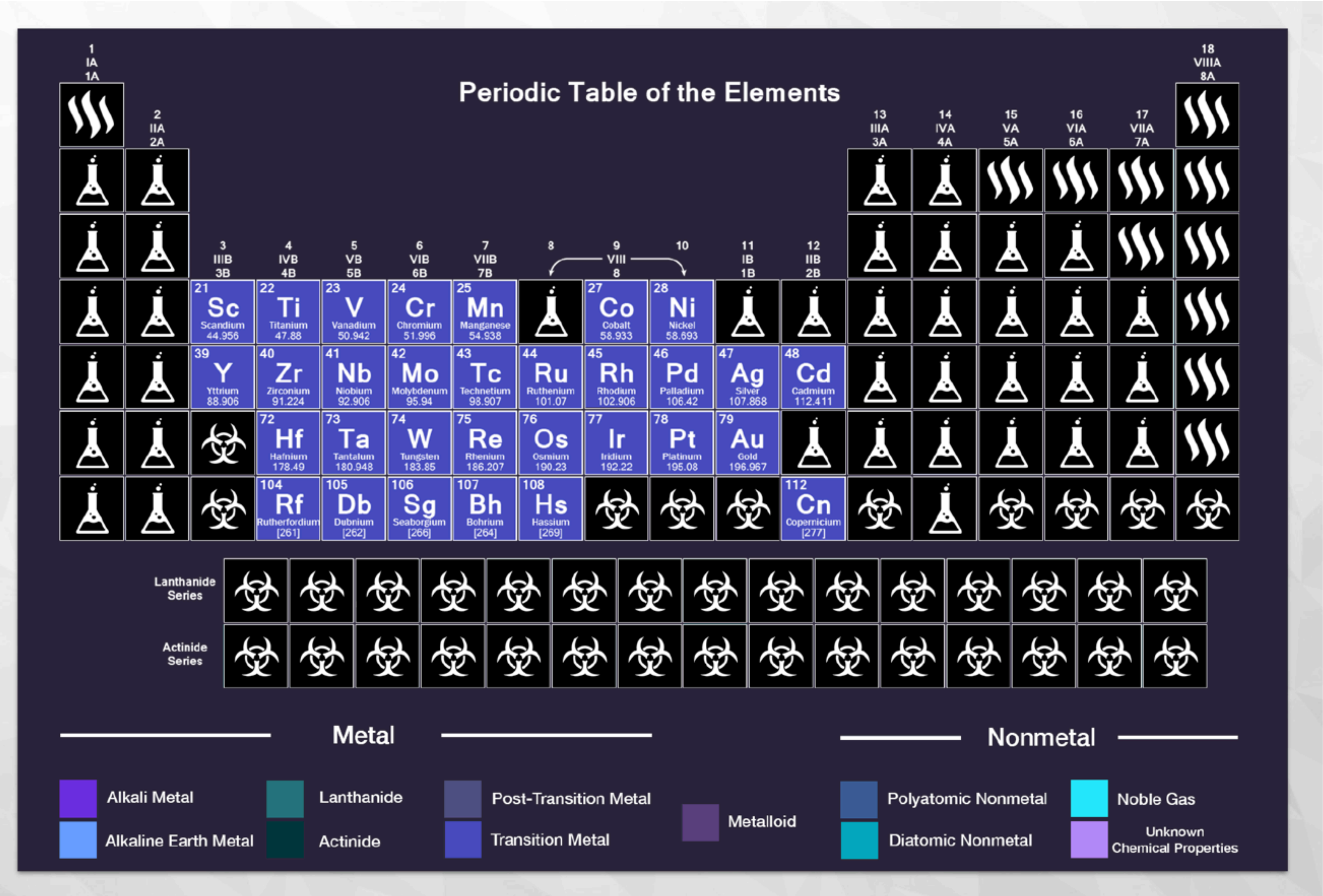
Nonmetal

- ■ Polyatomic Nonmetal
- ■ Diatomic Nonmetal
- ■ Noble Gas
- ■ Unknown Chemical Properties

Money cannot be *reactive* or *corrosive*



Money cannot be *radioactive*



Periodic Table of the Elements

1 IA 1A	2 IIA 2A	3 IIIB 3B	4 IVB 4B	5 VB 5B	6 VIB 6B	7 VIIB 7B	8	9 VIII 8	10	11 IB 1B	12 IIB 2B	13 IIIA 3A	14 IVA 4A	15 VA 5A	16 VIA 6A	17 VIIA 7A	18 VIIIA 8A
♨																	♨
⚗	⚗											⚗	⚗	♨	♨	♨	♨
⚗	⚗											⚗	⚗	⚗	⚗	♨	♨
⚗	⚗	21 Sc Scandium 44.956	22 Ti Titanium 47.88	23 V Vanadium 50.942	24 Cr Chromium 51.996	25 Mn Manganese 54.938	⚗	27 Co Cobalt 58.933	28 Ni Nickel 58.693	⚗	⚗	⚗	⚗	⚗	⚗	⚗	♨
⚗	⚗	39 Y Yttrium 88.906	40 Zr Zirconium 91.224	41 Nb Niobium 92.906	42 Mo Molybdenum 95.94	43 Tc Technetium 98.907	44 Ru Ruthenium 101.07	45 Rh Rhodium 102.906	46 Pd Palladium 106.42	47 Ag Silver 107.868	48 Cd Cadmium 112.411	⚗	⚗	⚗	⚗	⚗	♨
⚗	⚗	☣	72 Hf Hafnium 178.49	73 Ta Tantalum 180.948	74 W Tungsten 183.85	75 Re Rhenium 186.207	76 Os Osmium 190.23	77 Ir Iridium 192.22	78 Pt Platinum 195.08	79 Au Gold 196.967	⚗	⚗	⚗	⚗	⚗	⚗	♨
⚗	⚗	☣	104 Rf Rutherfordium [261]	105 Db Dubnium [262]	106 Sg Seaborgium [266]	107 Bh Bohrium [264]	108 Hs Hassium [269]	☣	☣	☣	112 Cn Copernicium [277]	☣	⚗	☣	☣	☣	☣

Lanthanide Series	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣
Actinide Series	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣	☣

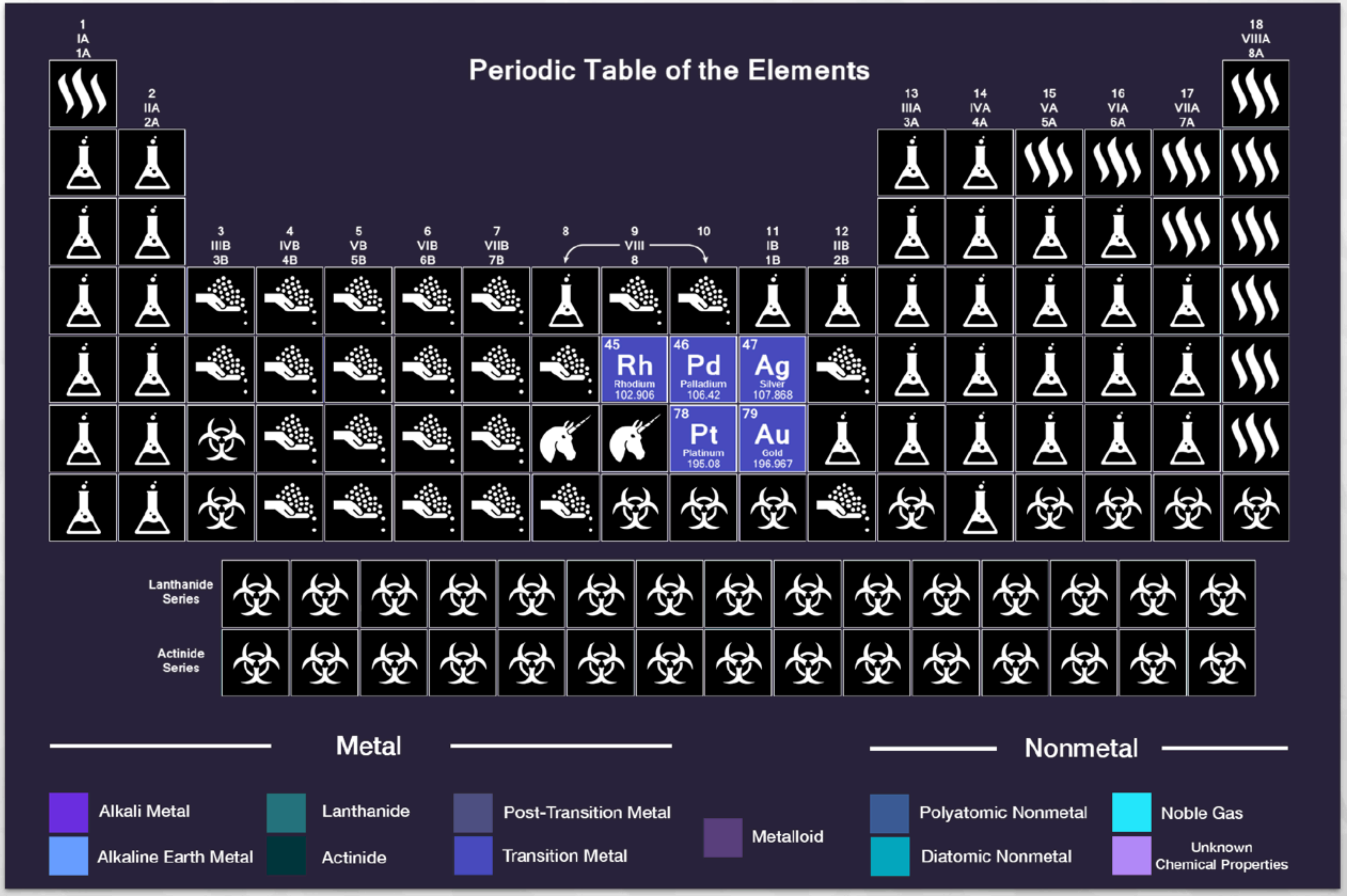
Metal

- ■ Alkali Metal
- ■ Alkaline Earth Metal
- ■ Lanthanide
- ■ Actinide
- ■ Post-Transition Metal
- ■ Transition Metal
- ■ Metalloid

Nonmetal

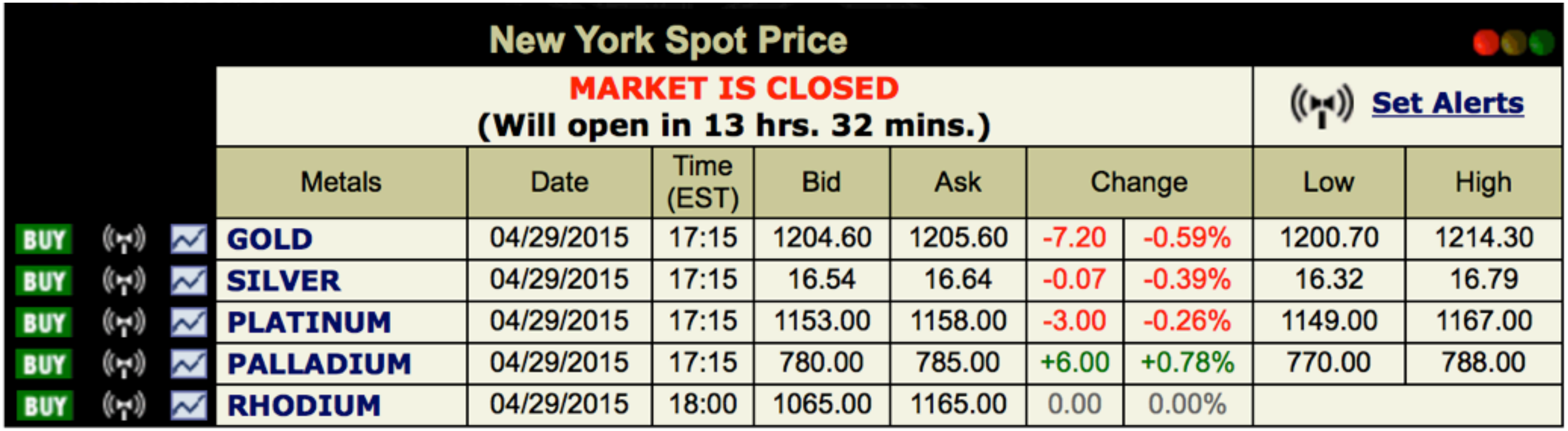
- ■ Polyatomic Nonmetal
- ■ Diatomic Nonmetal
- ■ Noble Gas
- ■ Unknown Chemical Properties

Money cannot be *abundant* or *too rare*



So, what's left?

- Five **precious** metals:
  - Rhodium
  - Palladium
  - Platinum
  - Silver
  - Gold



New York Spot Price

MARKET IS CLOSED
(Will open in 13 hrs. 32 mins.)

Set Alerts

	Metals	Date	Time (EST)	Bid	Ask	Change		Low	High
BUY	GOLD	04/29/2015	17:15	1204.60	1205.60	-7.20	-0.59%	1200.70	1214.30
BUY	SILVER	04/29/2015	17:15	16.54	16.64	-0.07	-0.39%	16.32	16.79
BUY	PLATINUM	04/29/2015	17:15	1153.00	1158.00	-3.00	-0.26%	1149.00	1167.00
BUY	PALLADIUM	04/29/2015	17:15	780.00	785.00	+6.00	+0.78%	770.00	788.00
BUY	RHODIUM	04/29/2015	18:00	1065.00	1165.00	0.00	0.00%		

So, what's left?

- Five precious metals:
  - ~~Rhodium~~ *Not discovered until 1880*
  - ~~Palladium~~ *Not discovered until 1880*
  - Platinum
  - Silver
  - Gold

So, what's left?

- Five precious metals:
  - ~~Rhodium~~ *Not discovered until 1880*
  - ~~Palladium~~ *Not discovered until 1880*
  - ~~Platinum~~ *Melts at 3,000 degrees Fahrenheit*
  - Silver
  - Gold

So, what's left?

- Five precious metals:
  - ~~Rhodium~~ *Not discovered until 1880*
  - ~~Palladium~~ *Not discovered until 1880*
  - ~~Platinum~~ *Melts at 3,000 degrees Fahrenheit*
  - ~~Silver~~ *Tarnishes easily and has industrial applications*
  - Gold

So, what's left?

- Five precious metals:
  - ~~Rhodium~~ *Not discovered until 1880*
  - ~~Palladium~~ *Not discovered until 1880*
  - ~~Platinum~~ *Melts at 3,000 degrees Fahrenheit*
  - ~~Silver~~ *Tarnishes easily and has industrial applications*
  - **Gold is ideal: rare (but not too rare), durable, and useless**

So, what's left?

- Five precious metals:
  - ~~Rhodium~~ *Not discovered until 1880*
  - ~~Palladium~~ *Not discovered until 1880*
  - ~~Platinum~~ *Melts at 3,000 degrees Fahrenheit*
  - ~~Silver~~ *Tarnishes easily and has industrial applications*
  - **Gold is ideal: rare (but not too rare), durable, and useless**

So, even if history was repeated, gold would probably emerge as the money of historic times again!

But, what about money in the digital age?

From money 1.0 to money 2.0

Money 1.0: Hardware-based

Antiquity to 1200-1700 AD: **Commodities** (e.g. gold)

Until c. 1973: **Commodity-backed fiat money**

Until now: **Government-backed fiat money**

- *"Real" money?*
- *Intrinsic value?*
- *Value as a commerce-facilitating medium?*

From money 1.0 to money 2.0

Money 1.0: Hardware-based

Antiquity to 1200-1700 AD: **Commodities** (e.g. gold)

Until c. 1973: **Commodity-backed fiat money**

Until now: **Government-backed fiat money**

Money 2.0: Software-based

- *A digital medium for the digital age*
- *Challenges: ownership, control, policy, etc.*

2. Digital money and Bitcoin

What is Bitcoin?

Bitcoin is a private, decentralized, digital cryptocurrency

- **Private**: Not issued by a sovereign
- **Decentralized**: No central issuing party / counter-party; units are issued algorithmically
- **Digital**: Fully electronic currency, with no underlying peg to assets or commodities and no necessary physical manifestation
- **Cryptocurrency**: Anti-counterfeiting is conducted through cryptography

A brief history of Bitcoin

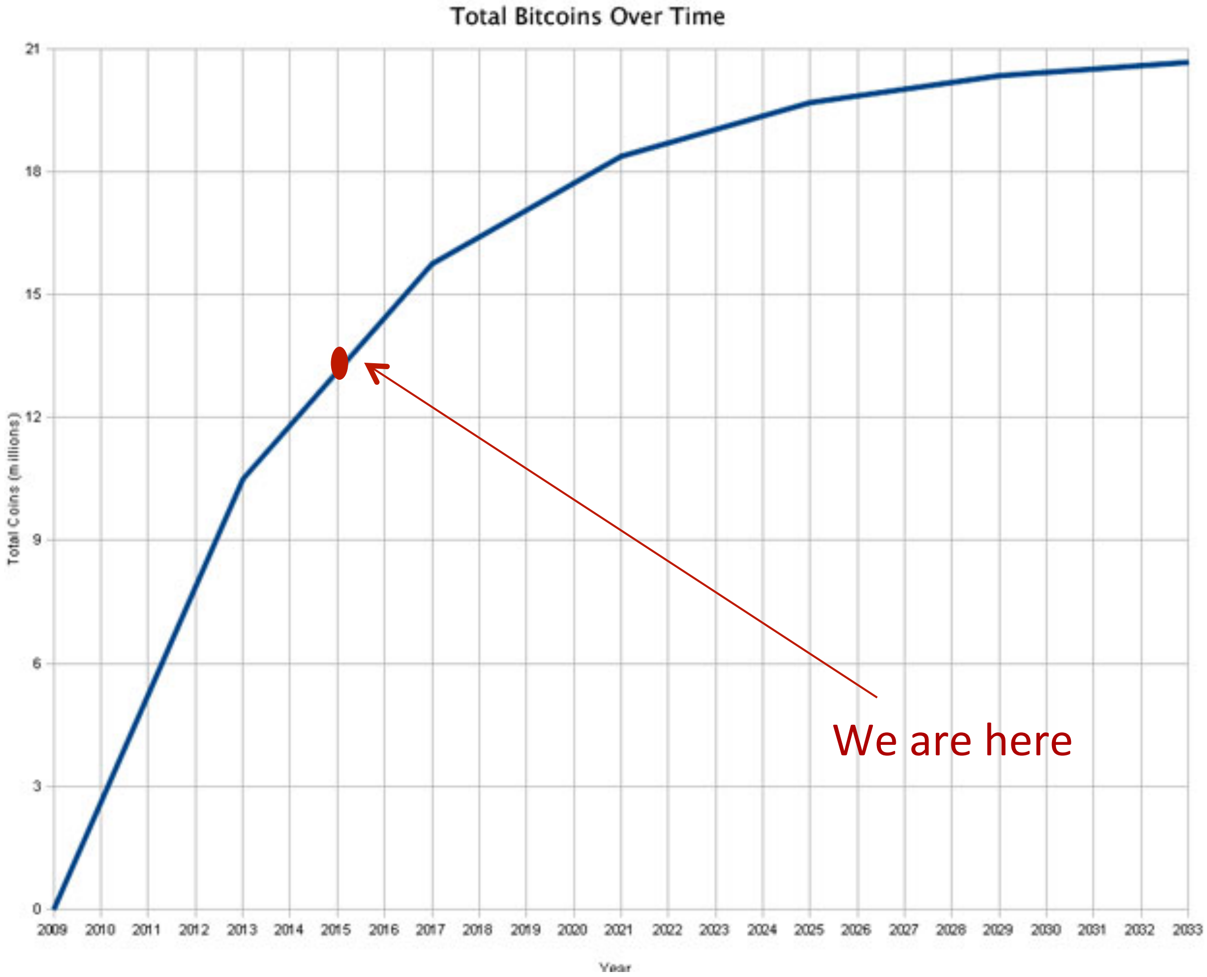
October 2008:	Satoshi Nakamoto’s **Bitcoin design paper** published
January 2009:	**Genesis block** established
October 2009:	BTC to USD exchange rate first published (1$ = 1,309.03 BTC)
November 2010:	Bitcoin market capitalization exceeds **$1 million**
February 2011:	Bitcoin reaches **parity** with the US dollar
March 2013:	Bitcoin market capitalization exceeds **$1 billion**
April 2013:	BTC exceeds **$100**
December 2013:	BTC exceeds **$1,000**
April 29, 2015:	**BTC market cap at $3.18 bn, price at $225.67**

Bitcoin as a currency

- Bitcoin has a number of interesting monetary features:
  - **Fixed Supply**: The money supply is regulated from the protocol itself and only 21,000,000 bitcoins (BTC) will ever exist.
  - **Transparent monetary policy**: Available to everyone to examine and verify, as the protocol is based on open source code.
  - **Driven by consensus**: Key characteristics can't change unless a majority of participants in the system agree to change them.

Bitcoin production over time

Bitcoin production curve



We are here

Bitcoin – A Familiar Story

‘A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers.

Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it.

On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it.

Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn’t more obvious from the start.

What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014.’

M. Andreesen, Why Bitcoin Matters (2014)

From money 1.0 (H/W) to money 2.0 (S/W)

Property	Money 1.0	Money 2.0
Scarcity	✓	✓✓
Divisibility	✓	✓✓
Storability	So and so	✓
Durability	So and so	✓✓
Fungibility	✓✓	✓✓
Portability	So and so	✓✓
Verifiability	✓	✓
Acceptability	✓✓	✗

Bitcoin – Not just currency

- Most people regard Bitcoin as a digital currency. But, in reality, **Bitcoin is much more than that**!

- At its foundation, it is **a collection of concepts and technologies** that form **the basis of a digital money ecosystem**. These technologies include:

  - A de-centralized peer-to-peer network (**the bitcoin protocol**);
  - A public transaction ledger (**the blockchain**);
  - A de-centralized mathematical and deterministic currency issuance and transaction verification mechanism (**proof-of-work and mining**)

The Blockchain

- Bitcoin's most prevalent innovation is the concept of the "**blockchain**", a publically reviewable ledger, where every transaction is written in and verified.

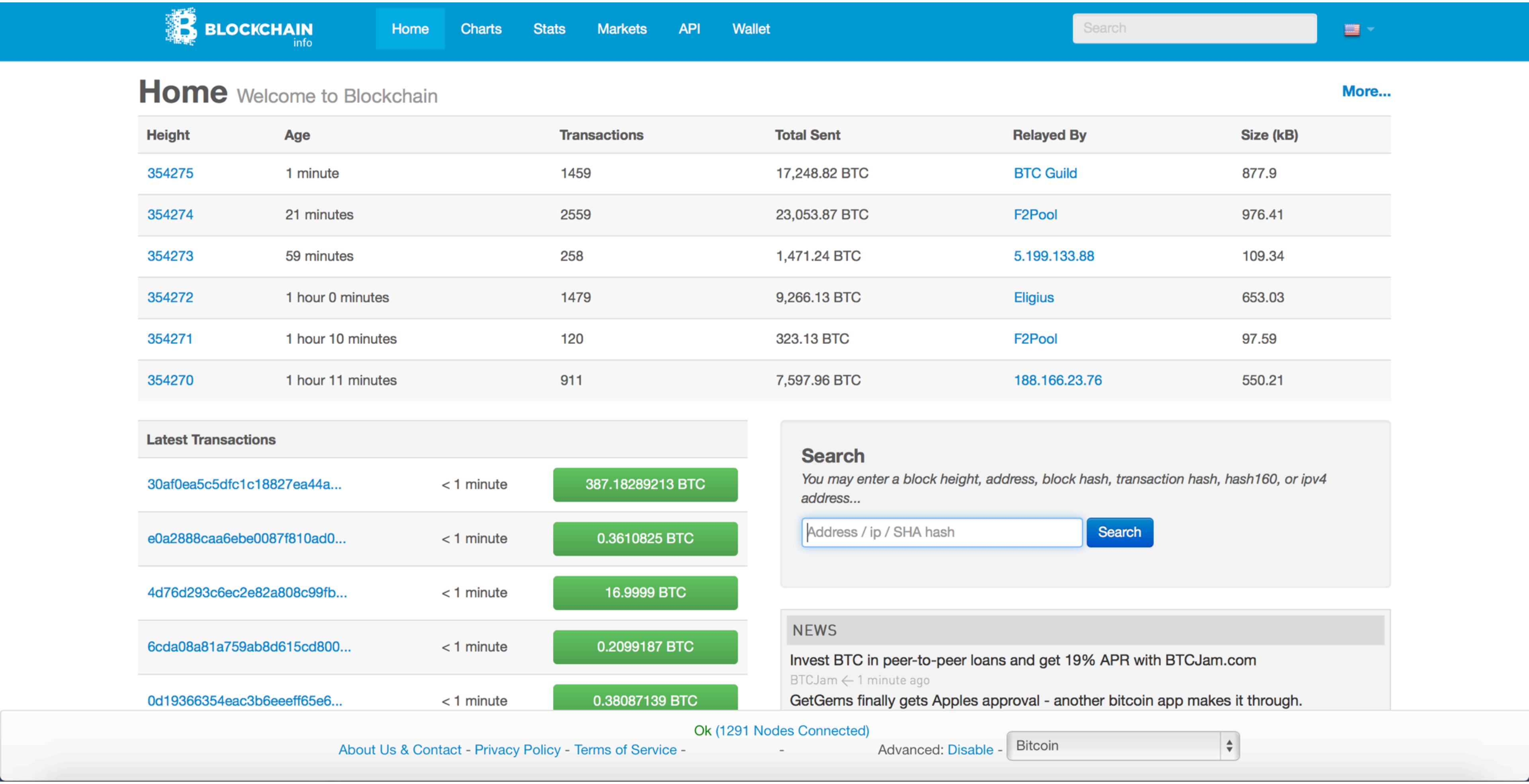
- The blockchain is a major breakthrough in **economics and finance**
  - It creates the world's first purely decentralized, dis-intermediated, trusted monetary system

- It also is a major breakthrough in **computer science**
  - It solves (under assumptions) the Byzantine Generals' Problem: how to establish trust between untrusted entities in a distributed P2P system

The Blockchain

The blockchain is a

public record of all bitcoin transactions in history



Home Welcome to Blockchain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
354275	1 minute	1459	17,248.82 BTC	BTC Guild	877.9
354274	21 minutes	2559	23,053.87 BTC	F2Pool	976.41
354273	59 minutes	258	1,471.24 BTC	5.199.133.88	109.34
354272	1 hour 0 minutes	1479	9,266.13 BTC	Eligius	653.03
354271	1 hour 10 minutes	120	323.13 BTC	F2Pool	97.59
354270	1 hour 11 minutes	911	7,597.96 BTC	188.166.23.76	550.21

Latest Transactions		
30af0ea5c5dfc1c18827ea44a...	< 1 minute	387.18289213 BTC
e0a2888caa6ebe0087f810ad0...	< 1 minute	0.3610825 BTC
4d76d293c6ec2e82a808c99fb...	< 1 minute	16.9999 BTC
6cda08a81a759ab8d615cd800...	< 1 minute	0.2099187 BTC
0d19366354eac3b6eeeff65e6...	< 1 minute	0.38087139 BTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Address / ip / SHA hash

NEWS

Invest BTC in peer-to-peer loans and get 19% APR with BTCJam.com

BTCJam ← 1 minute ago

GetGems finally gets Apples approval - another bitcoin app makes it through.

Ok (1291 Nodes Connected)

About Us & Contact - Privacy Policy - Terms of Service - - Advanced: Disable - Bitcoin

How does the blockchain work?

- When a Bitcoin client executes a transaction, it broadcasts the transaction to the Bitcoin network.
  - Within a few seconds, almost every Bitcoin client in the world receives the transaction.

- At this point, however, the transaction is considered **unconfirmed**
  - what if a rogue Bitcoin client sent out two transactions moving the same bitcoin to two different addresses? Which one should the clients accept? (the Byzantine Generals' Problem!)

- The mechanism that Bitcoin uses to confirm transactions and resolve the Byzantine Generals' Problem is a process called **mining.**

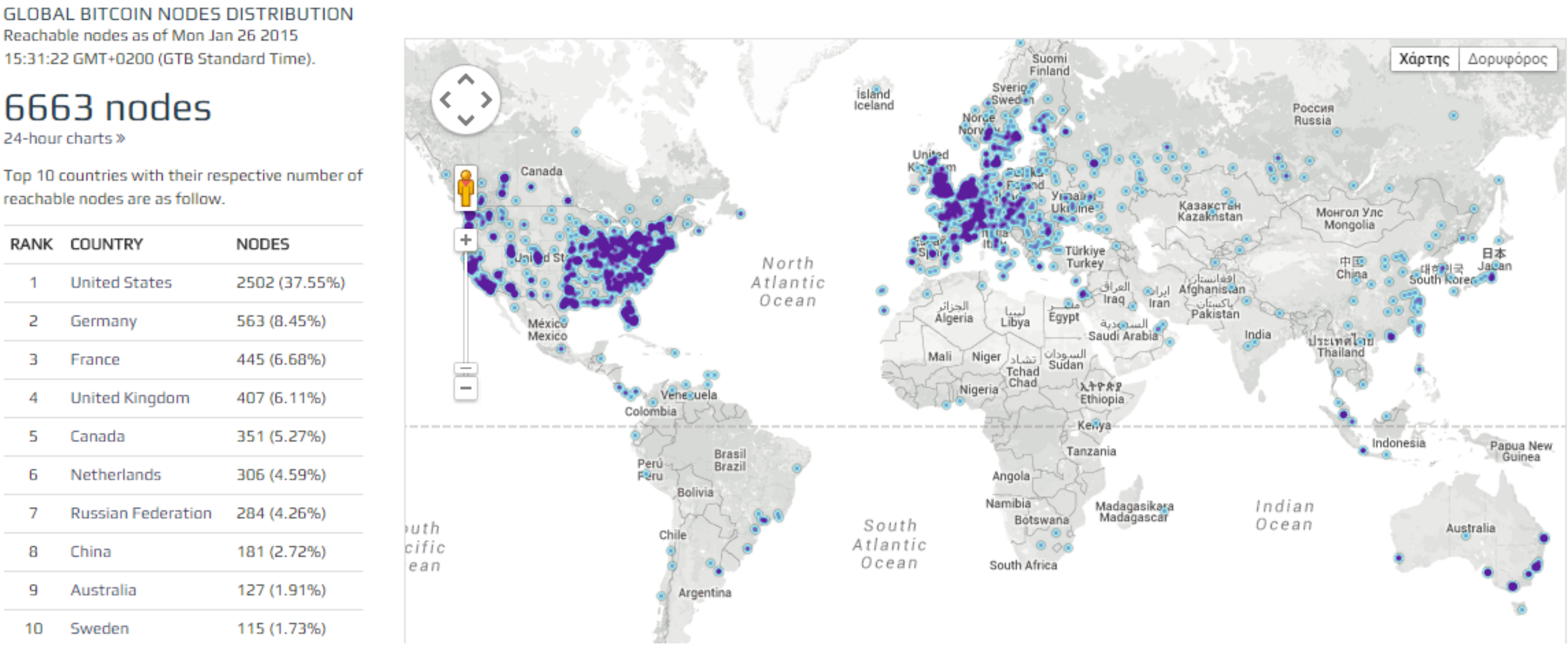
Mining

- Mining serves two purposes:
  - It **creates new bitcoins** in each block, almost like a central bank printing new money.
  - It **creates trust** by ensuring that transactions are confirmed only when enough computational power was devoted to the block that contains them. More blocks mean more computation, which means more trust.

- Mining is a **distributed consensus system** that is used to confirm waiting transactions by including them in the blockchain.
  - It enforces a chronological order in the block chain, protects the **neutrality** of the network, and allows different computers to agree on the state of the system.
  - To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks.
  - Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

The Bitcoin network

Number of Bitcoin nodes (clients) by country



GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Mon Jan 26 2015
15:31:22 GMT+0200 (GTB Standard Time).

6663 nodes

24-hour charts »

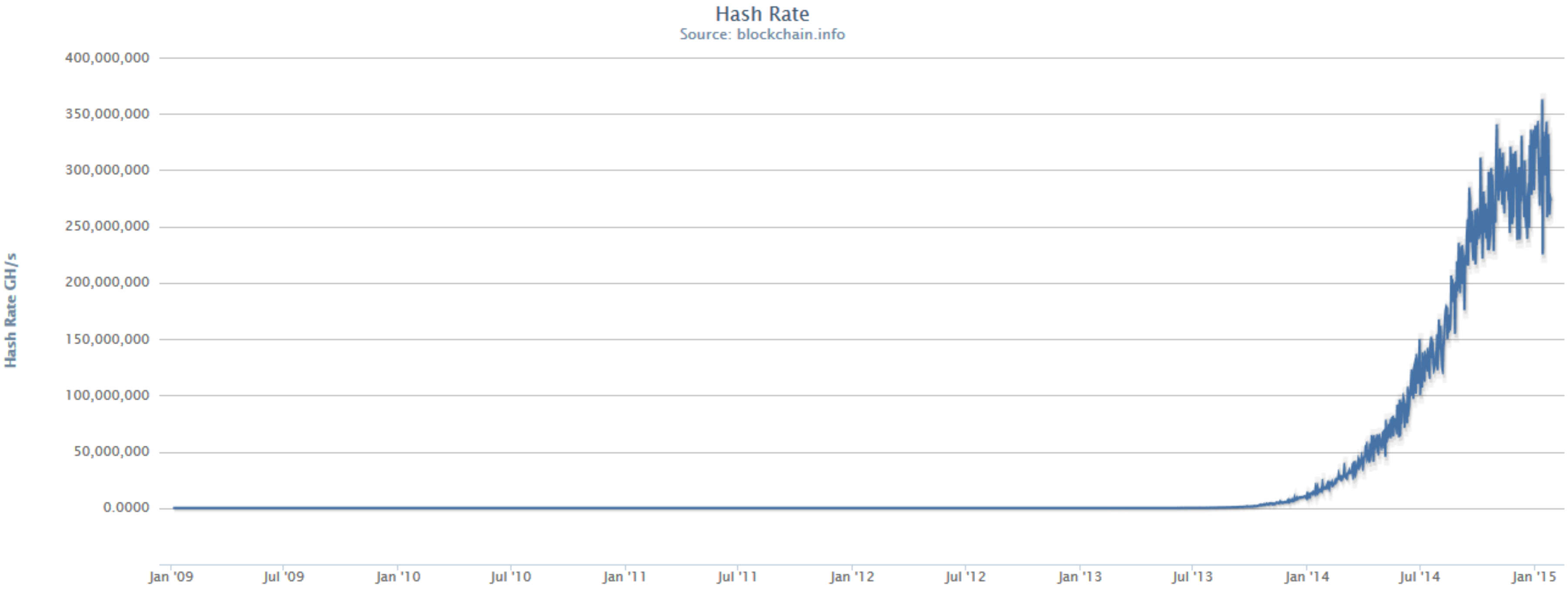
Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2502 (37.55%)
2	Germany	563 (8.45%)
3	France	445 (6.68%)
4	United Kingdom	407 (6.11%)
5	Canada	351 (5.27%)
6	Netherlands	306 (4.59%)
7	Russian Federation	284 (4.26%)
8	China	181 (2.72%)
9	Australia	127 (1.91%)
10	Sweden	115 (1.73%)

Source : getaddr.bitnodes.io

Computational power of the Bitcoin network

Total Mining Power (Network Hashing Power over time)



Why is this important?

- Think of Bitcoin as **an Internet-wide distributed ledger:**
  - Anyone can buy into or sell out of this ledger
  - Anywhere
  - Without anyone's permission or intervention
  - Without needing to trust the counterparty
  - Without chargebacks
  - At virtually no cost

- Practically, this gives us, for the first time, **a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that:**
  - the transfer is guaranteed to be safe and secure
  - everyone knows that the transfer has taken place
  - nobody can challenge the legitimacy of the transfer

- **The consequences of this breakthrough and the application implications are hard to overstate.**

3. Towards a Digital Money World

Key takeaways so far

- **Money 1.0**
  - While money is a 10,000 years old technology, government-backed fiat money exists for the last 40 year only.
  - Yet, it appears the only "real" money to us; simply because we grew up with it!
  - Money was invented to facilitate commerce; it may have reached the limits of its capacity to do so.

- **Money 2.0**
  - An Internet-wide distributed ledger
  - Programmable money!
  - Open to examination
  - Open to innovation

Money-over-IP

- Almost every component of commerce has been digitized
  - But money!

- We desperately need **Money-over-IP**
  - A disruptive innovation that will drive the next generation of commerce

- Bitcoin may be a **beta version** of Money-over-IP
  - Its real potential may lie in backing (security-wise and infrastructure-wise) other **protocols for value transfer over the Internet**
  - These could be **application-specific coins**, **autonomous economic agents**, and even **autonomous digital corporations**

Some examples

- **Application-specific coins**
  - A value token needed to send (or prioritize) an e-mail
  - A nano-payment for content monetization
  - A nano-reward for community service

- **Autonomous economic agents**
  - A driverless car bidding for your ride
  - An independent certification agent (e.g. academic degrees, national IDs)

- **Autonomous digital corporations**
  - A digital land registry office or notary
  - An independent, trust election management office
  - A car sharing collective

M2M and H2M Commerce

- The existence of such digital money will unleash **a new era of commerce**

- Combining **Programmable Money** with **Cryptographically-Proven Transactions (Block chains)** would allow **programmable agents** to enter the global commerce arena and become rational economic actors.

- **Machine-to-machine (M2M)** and **human-to-machine (H2M)** economic transactions.
  - More efficient allocation of resources
  - Better balance of supply and demand
  - Perfect market competition

Conclusion: A new Networked Economy

- For the first time in history, we have access to Internet-based **programmable money**.

- For the first time in history, we have access to **open, distributed, trusted networks**, verifying and storing financial transactions without requiring any sort of trusted intermediary.

- For the first time in history, we can conceive the notion of **human-less corporations**, which exist only in the cloud.

- Taken together, these developments will unleash a new **Networked Economy**, with profound consequences to the fabric of how societies and economies operate.

Research and business opportunities (and challenges) abound!