Money-over-IP: From Bitcoin to M2M Commerce

Professor George M. Giaglis
Vice Rector, AUEB

giaglis@auceb.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?
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
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
Money cannot be reactive or corrosive
Money cannot be radioactive
Money cannot be abundant or too rare.
So, what’s left?

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Money 1.0</th>
<th>Money 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scarcity</td>
<td>✓</td>
<td>✓✓</td>
</tr>
<tr>
<td>Divisibility</td>
<td>✓</td>
<td>✓✓</td>
</tr>
<tr>
<td>Storability</td>
<td>So and so</td>
<td>✓</td>
</tr>
<tr>
<td>Durability</td>
<td>So and so</td>
<td>✓✓</td>
</tr>
<tr>
<td>Fungibility</td>
<td>✓✓</td>
<td>✓✓</td>
</tr>
<tr>
<td>Portability</td>
<td>So and so</td>
<td>✓✓</td>
</tr>
<tr>
<td>Verifiability</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Acceptability</td>
<td>✓✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
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 is a public record of all bitcoin transactions in history.
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

6663 nodes
24-hour charts »
Top 10 countries with their respective number of reachable nodes are as follows.

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

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 years 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!