

Innovation of Bitcoin

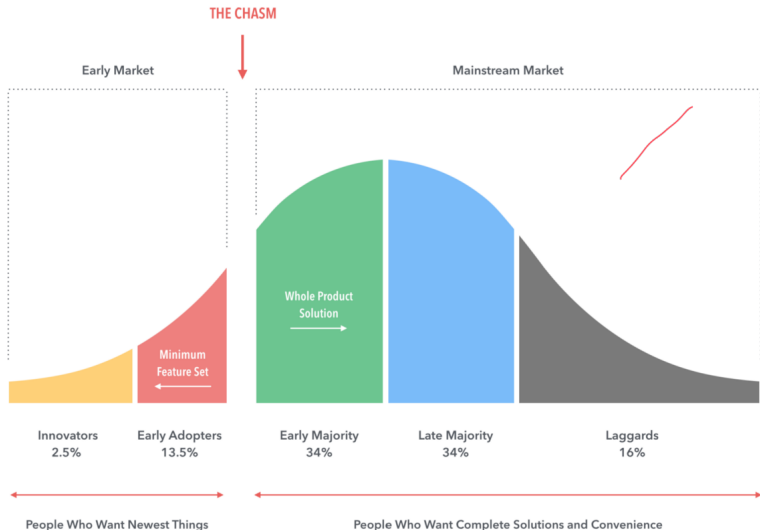
Sirvan Almasi

Imperial College London

October 2020

Observations and Questions

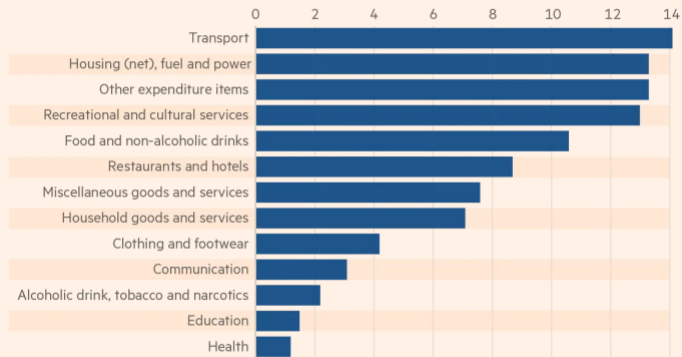
Has it crossed the chasm yet?



Quantifying 'mainstream'

UK household spending

2017-18 (%)



Source: ONS

© FT

A Prediction

Using the innovation estimate, we predict that Bitcoin has reached its intended market; for it to reach a broader and mainstream market then it has to fundamentally change its course.

Objectives

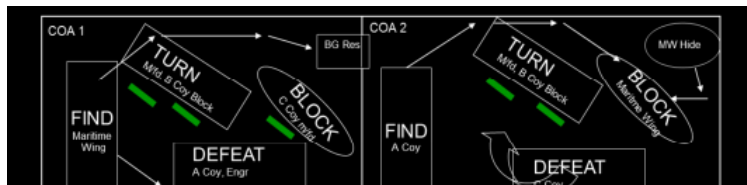
Primary objective is to understand the true product-nature of Bitcoin and its non-technical limitation in order to understand its potential path and re-assess the how and where we should conduct research.



What is the Innovation Estimate?

Combinatation of the following:

- ▶ Management Theories and Concepts
- ▶ The Combat Estimate [1]
- ▶ Intelligence Analytical Methods [7]



Question 1: What is it and value will it deliver?

What is it? 'A purely peer-to-peer version of electronic cash would allow *online payments* to be sent directly from one party to another *without going through a financial institution.*' [9]

What values will it deliver? Bypass financial institution in a financial transaction.

Motivation. 'it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads.'

Question 2: Who and where are my actors and why?

Thinking who would benefit from my product through the value it is delivering and who are my stakeholders.

- ▶ e-commerce users.
- ▶ Criminals and terrorists.
- ▶ Large transaction type users.
- ▶ Governments.
- ▶ Regulators.
- ▶ Existing financial institutions.

3 Column Format

Factors	Deduction	Action
<i>for each actor:</i> why? Pain points Pleasure points Resistance points Potential pleasure points Geography Scale Age group Incentives Income group Transaction		

Question 3: What are the defining characteristics of the class of my product?

- ▶ Transaction Cost
- ▶ Portability
- ▶ Privacy
- ▶ Settlement Speed
- ▶ Frequency of payments
- ▶ Circumvent financial system

Other Questions...

- ▶ Question 4: What is the current state of the environment?
- ▶ Question 5: What effects do I need to achieve and why?
- ▶ Question 6: What are my key assumptions and why?
- ▶ Question 7: What resources do I need to achieve my effects?
- ▶ Question 8: When and where do each effect take place?

Outcome of the Questions

- ▶ Design and build a pure p2p software that can handle private financial transactions.
- ▶ Circumvent Government and existing financial systems.
- ▶ Create an financial incentive model to maintain the system.

So... How are Bitcoins used already?

How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?

Dorit Ron and Adi Shamir

Department of Computer Science and Applied Mathematics,
The Weizmann Institute of Science, Israel
{dorit.ron, adi.shamir}@weizmann.ac.il

Abstract. The Bitcoin scheme is one of the most popular and talked about alternative payment schemes. It was conceived in 2008 by the mysterious Satoshi Nakamoto, whose real identity remains unknown even though his bitcoin holdings are believed to be worth several hundred million dollars. One of the most active parts of the Bitcoin ecosystem was the Silk Road marketplace, in which highly illegal substances and services were traded. It was run by another mysterious person who called himself Dread Pirate Roberts (DPR), whose bitcoin holdings were also estimated



Silk Road

anonymous marketplace

- ▶ 'We estimate that around \$76 billion of illegal activity per year involves bitcoin (46% of bitcoin transactions)...' [5]
- ▶ (Jan-April 2019) exchange-related transactions accounted for 89.7% of all Bitcoin activity.
The amount of Bitcoin used to pay for real world goods and services hit a peak of 1.5% in late 2017 but fell as low as 0.9% during 2018's bear market. It's currently at 1.3%. [4]
- ▶ '...the Dark Web and cryptocurrencies are misused for malicious operations.' [6]

Focused market positioning and highly speculative

- ▶ Bitcoin is tailored to circumvent the financial system
- ▶ Bitcoin's structure is fit for criminal activities but not mainstream users
- ▶ The mainstream market segment has different priorities (more on next slide)

Other Considerations

- ▶ Bitcoin emissions can alone push global temp above 2deg [8]
- ▶ Psychological and philosophical reasoning
 - ▶ 'Network Fetishism' and ideologies [2]
 - ▶ Endless accumulation of money becomes the sole goal of the capitalist, which Marx describes as a form of "fetishism" (Marx 1867, volume I)

How to go mainstream?

When there is adequate product performance, the mainstream customers start basing their purchasing decision (from functionality) to reliability, then to convenience and ultimately to price. Therefore, generally, disruptive products are simpler, cheaper and more reliable and more convenient than their established counterparts. [3]





Next steps...

- ▶ Verify transactions and find what are transactions used for.
- ▶ Why hasn't the likes of Monero overtaken Bitcoin?
 - ▶ Bitcoin is inflated by hype and most coins are sitting idle (explains the natural movement into DeFi?)
 - ▶ Is it harder to purchase Monero? Are there regulatory pressures in ensuring that KYC procedures do take place and thus it limits the freedom of the exchanges?
- ▶ Can we model the incentive model of Bitcoin?
 - ▶ It is interesting to note that alot of resources are voluntary being spent on an Open Source project whose core features are tailored for criminal activities and main beneficiaries are the early adopters. Does it therefore display pyramid scheme like incentives? [2]

References I

-  B. ARMY, *The british army tactical aid memoire 2020*, Jun 2020.
-  J. BALDWIN, *In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism*, Palgrave Communications, 4 (2018).
-  C. M. CHRISTENSEN, *The Innovators Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business Review Press, Boston, MA, USA, 2016.
-  A. FENTON, *Almost half of bitcoin payments are now made on the darknet - micky news*, Jul 2019.
-  S. FOLEY, J. R. KARLSEN, AND T. J. PUTNIII, *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?*, SSRN Electronic Journal, (2018).

References II

-  S. LEE, C. YOON, H. KANG, Y. KIM, Y. KIM, D. HAN, S. SON, AND S. SHIN, *Cybercriminal minds: An investigative study of cryptocurrency abuses in the dark web*, in NDSS, 2019.
-  D. T. MOORE AND C. FOR STRATEGIC INTELLIGENCE RESEARCH (U.S.), *Critical thinking and intelligence analysis*, Center for Strategic Intelligence Research, National Defense Intelligence College, 2007.
-  C. MORA, R. L. ROLLINS, K. TALADAY, M. B. KANTAR, M. K. CHOCK, M. SHIMADA, AND E. C. FRANKLIN, *Bitcoin emissions alone could push global warming above 2°C*, Nature Climate Change, 8 (2018), p. 931–933.
-  S. NAKAMOTO, *Bitcoin: A peer-to-peer electronic cash system*, Cryptography Mailing list at <https://metzdowd.com>, (2009).