Economics of CryptoCurrencies

Tymofiy Mylovanov

Kyiv School of Economics

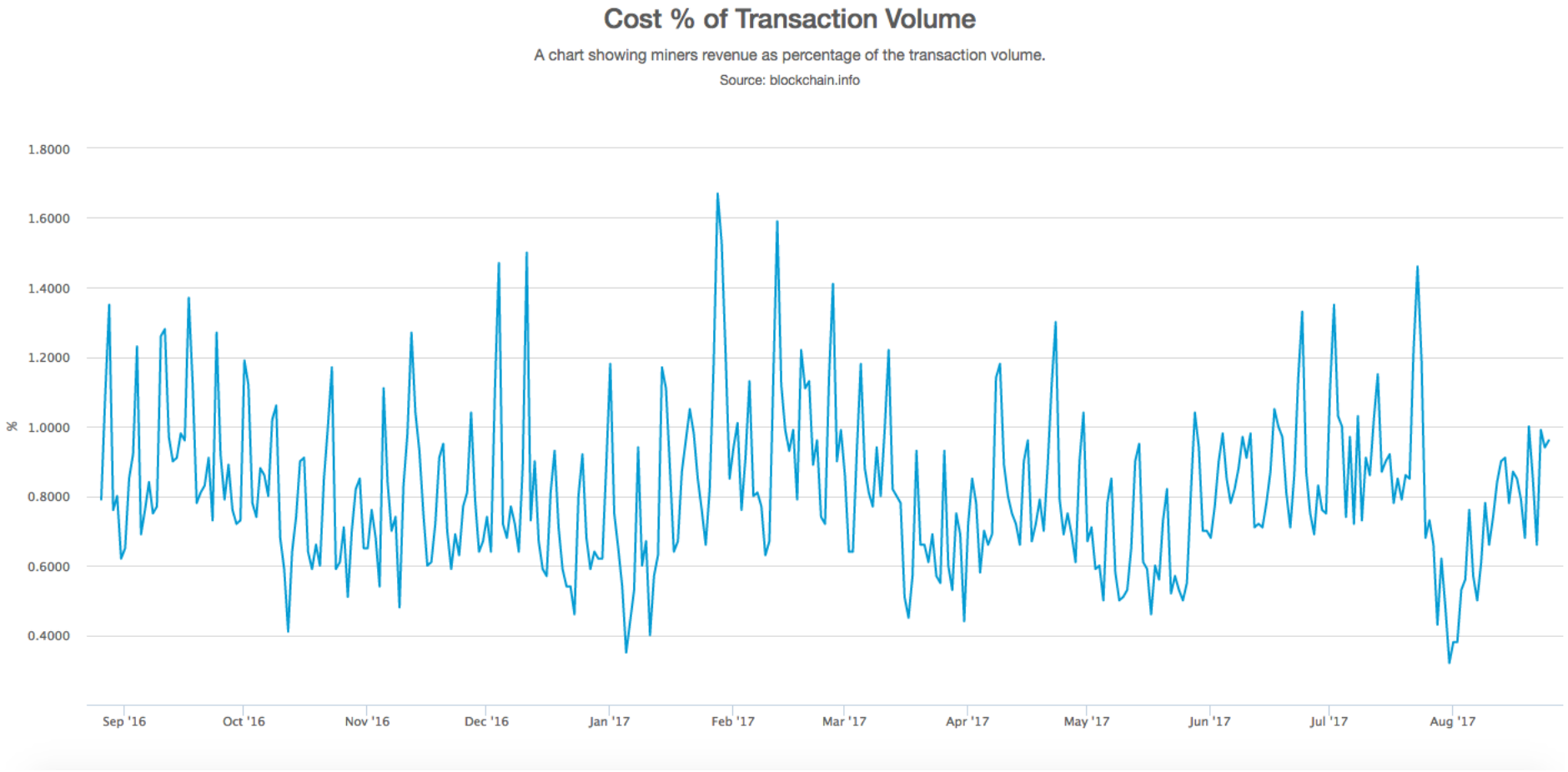
BEROC, August, 2017

1 Week High	1 Week Low	1 Week Change	Market Cap
$344.97	$286.43	$33.13 ▲	$31.00B


24h 1w 1m 3m 1y All Time
$416.17
$0.43
$328.69
$31.11B
ETH/USD
Exchange: Weighted Average
400
300
200
100
0
Sep '15 Nov '15 Jan '16 Mar '16 May '16 Jul '16 Sep '16 Nov '16 Jan '17 Mar '17 May '17 Jul '17
Sep '15 Jan '16 May '16 Sep '16 Jan '17 May '17
Highcharts.com

#	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	$72,157,160,852	$4366.41
2	Ethereum	ETH	$31,217,839,432	$331.22
3	Bitcoin Cash	BCH	$10,496,487,259	$634.54
4	Ripple	XRP	$8,337,139,884	$0.217431
5	Litecoin	LTC	$2,684,655,421	$51.01

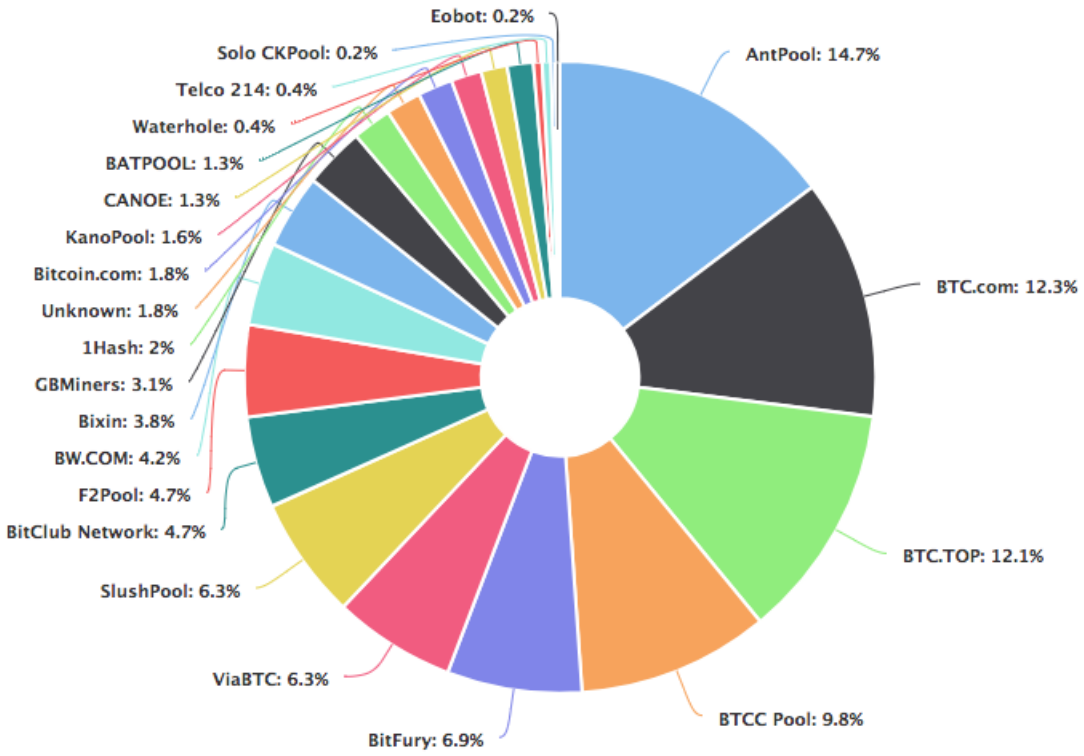

Bitcoin Charts
Zoom 1d 7d 1m 3m 1y YTD ALL
From Apr 28, 2013 To Aug 26, 2017
$60B
$40B
$20B
$0B
Market Cap
$6000.00
$4000.00
$2000.00
$0.0
Price (USD)
24h Vol
0B
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
2014
2015
2016
2017
Market Cap
Price (USD)
Price (BTC)
24h Vol
Highcharts.com

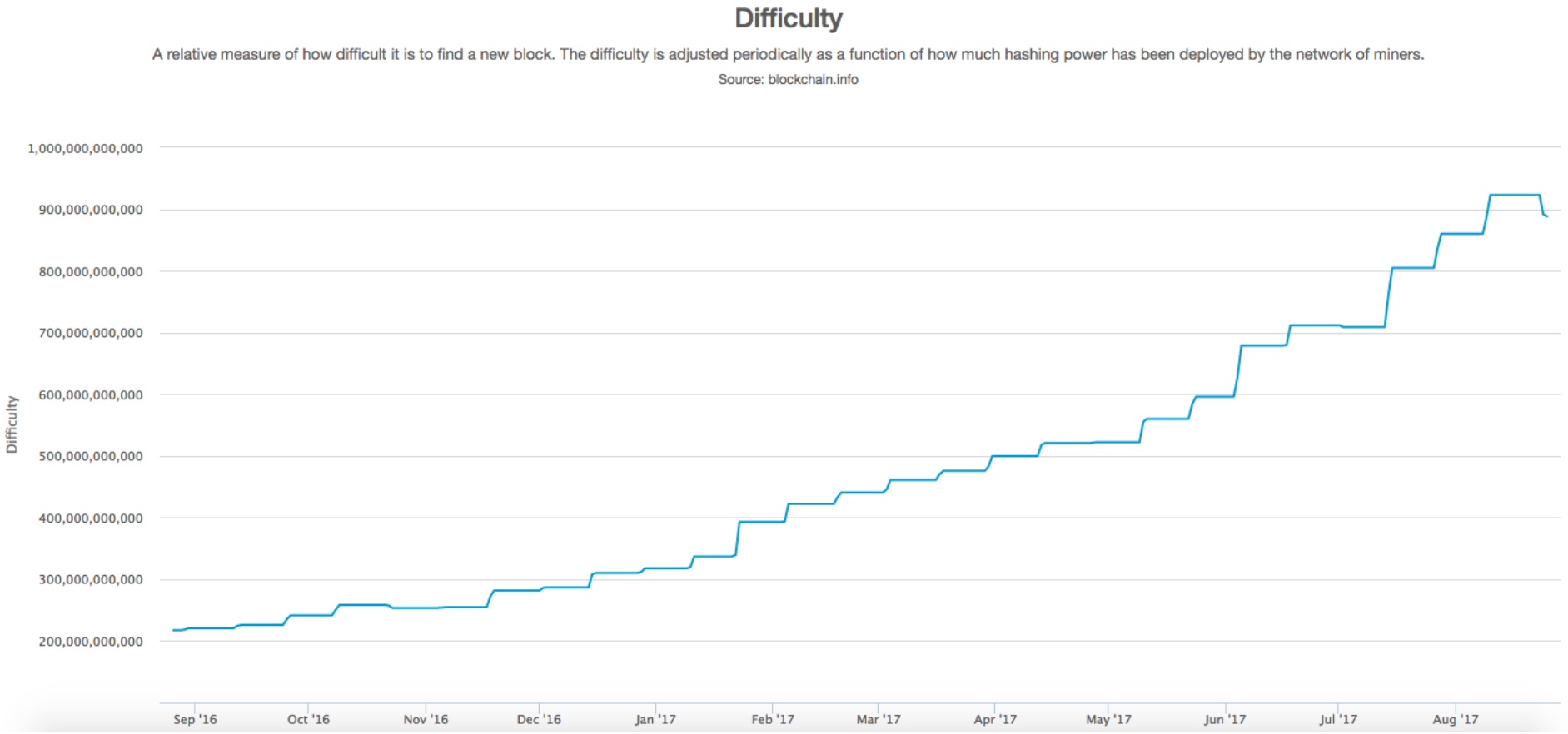

Cost % of Transaction Volume
A chart showing miners revenue as percentage of the transaction volume.
Source: blockchain.info
1.8000
1.6000
1.4000
1.2000
1.0000
0.8000
0.6000
0.4000
%
Sep '16
Oct '16
Nov '16
Dec '16
Jan '17
Feb '17
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17

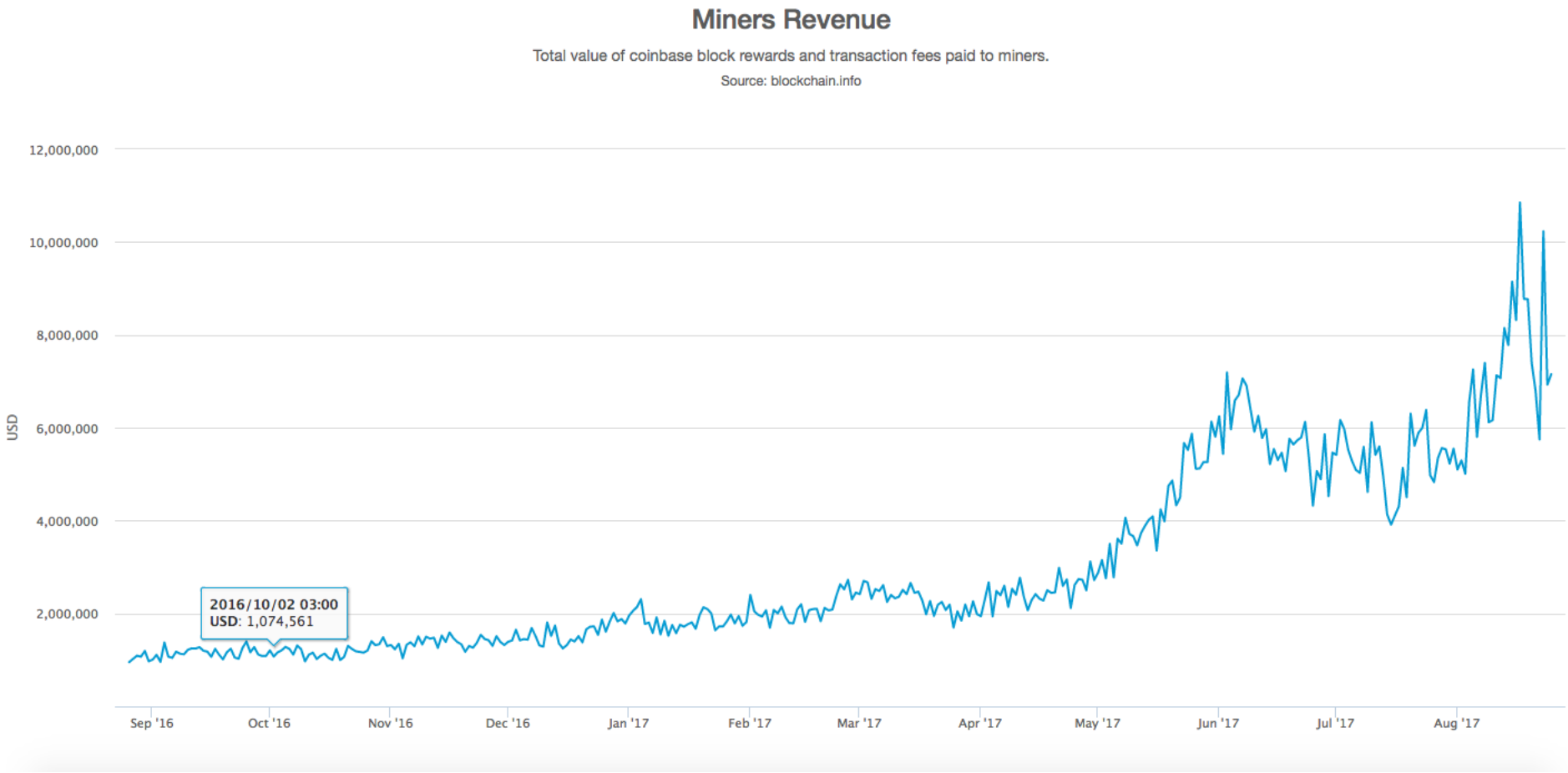
Hashrate Distribution An estimation of hashrate distribution amongst the largest mining pools

The graph below shows the market share of the most popular bitcoin mining pools. It should only be used as a rough estimate and for various reasons will not be 100% accurate. A large portion of Unknown blocks does not mean an attack on the network, it simply means we have been unable to determine the origin.

24 hours - 48 hours - 4 Days




Difficulty
A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.
Source: blockchain.info
Difficulty
1,000,000,000,000
900,000,000,000
800,000,000,000
700,000,000,000
600,000,000,000
500,000,000,000
400,000,000,000
300,000,000,000
200,000,000,000
Sep '16
Oct '16
Nov '16
Dec '16
Jan '17
Feb '17
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17

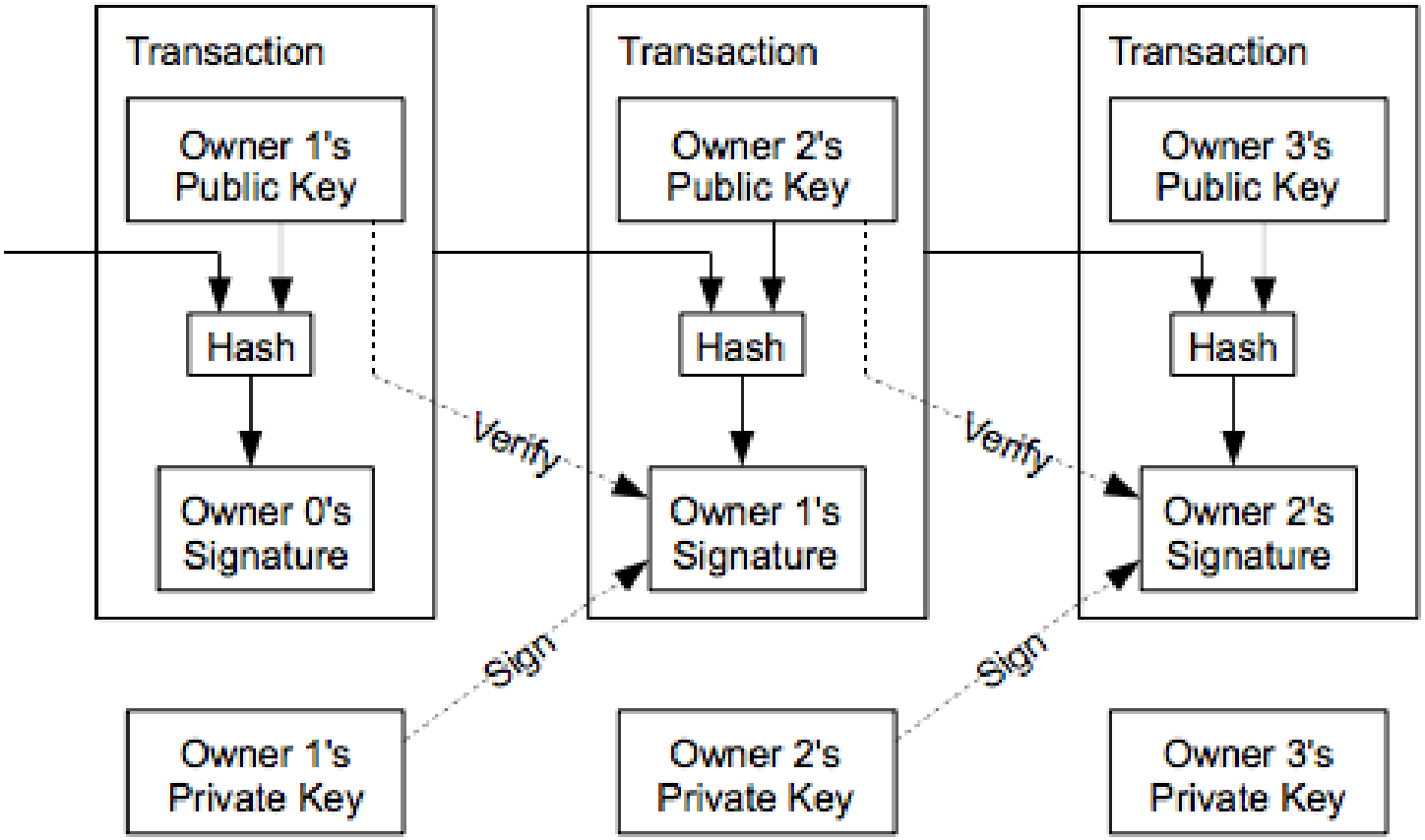

Miners Revenue
Total value of coinbase block rewards and transaction fees paid to miners.
Source: blockchain.info
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
USD
2016/10/02 03:00
USD: 1,074,561
Sep '16
Oct '16
Nov '16
Dec '16
Jan '17
Feb '17
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17

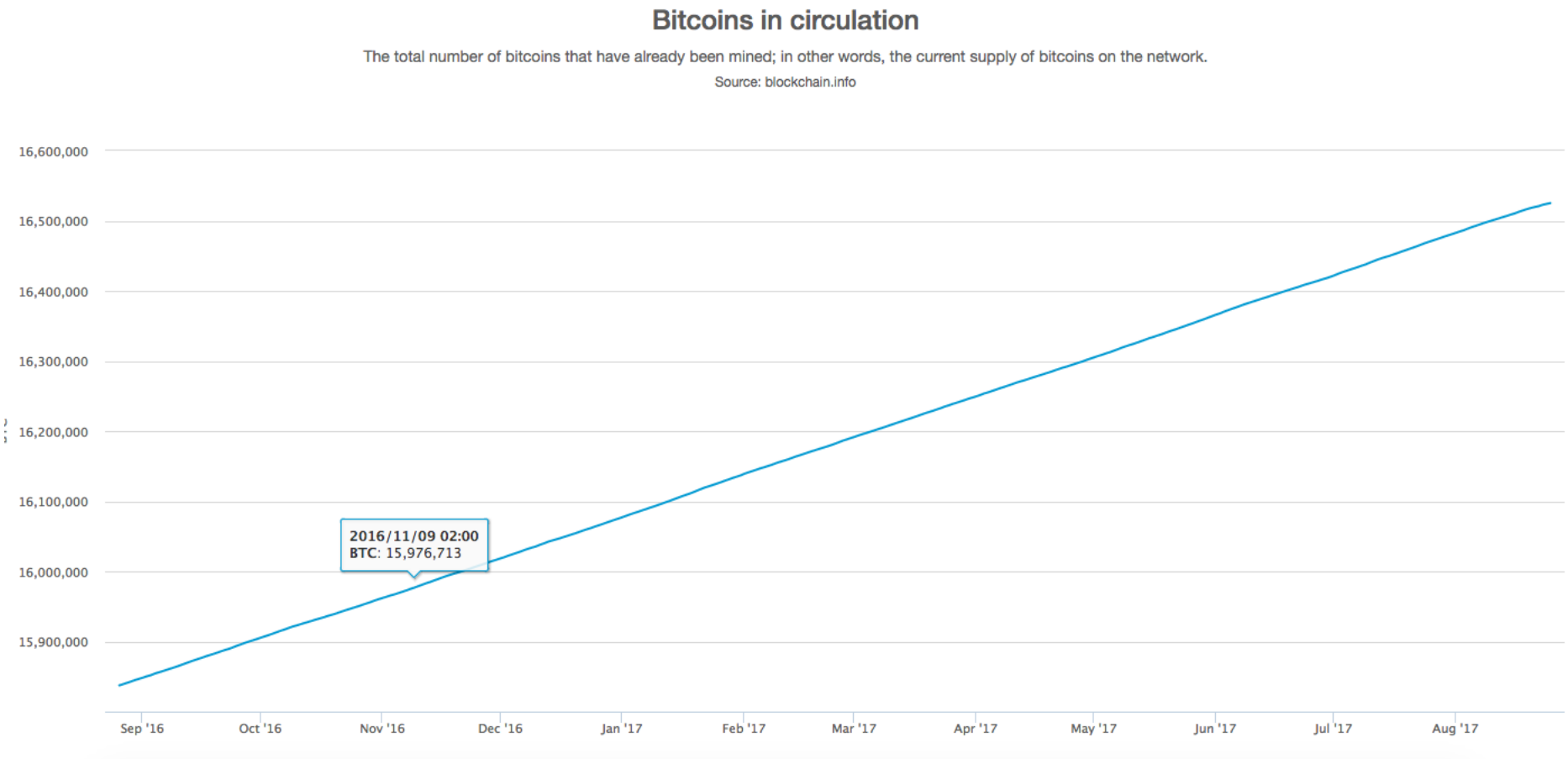
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

2. Transactions

We define an electronic coin as a chain of digital signatures.

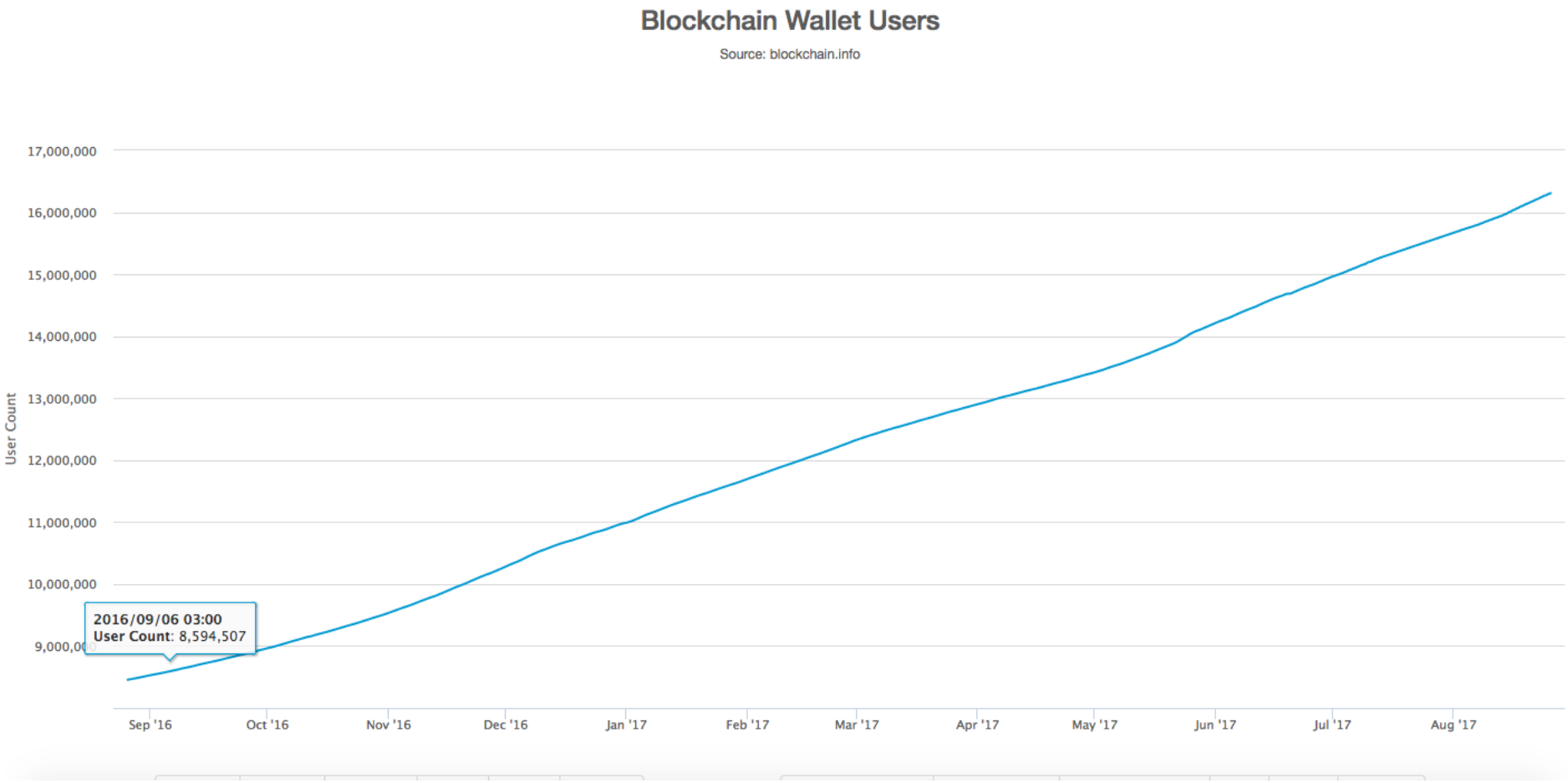

Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Verify
Verify
Sign
Sign
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key


Bitcoins in circulation
The total number of bitcoins that have already been mined; in other words, the current supply of bitcoins on the network.
Source: blockchain.info
16,600,000
16,500,000
16,400,000
16,300,000
16,200,000
16,100,000
16,000,000
15,900,000
2016/11/09 02:00
BTC: 15,976,713
Sep '16
Oct '16
Nov '16
Dec '16
Jan '17
Feb '17
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17

Feature	Bitcoin	USD (home currency)	Euro (foreign currency)
Economic demand factors			
Intrinsic value	None	None	None
Claim to issuers?	No	Yes	Yes
Legal tender	No	Yes	No (in the U.S.)
Used as a medium of exchange	Small, but rising especially in online retail	Yes	Limited (in the U.S.) possibly more for cross-border trade
Used as unit of account	No	Yes	No (in the U.S.)
Used as store of value	Yes, subject to very high exchange rate risk and sudden confidence shock	Yes, subject to inflation risk	Yes, subject to foreign exchange risk

Supply structures			
Monopoly/decentralized	Decentralized	Monopoly	Monopoly
Supply source	Private	Public	Foreign public
Supply quantity	Inflexible	Flexible	Flexible
Supply rule	Computer program	Rule-based (inflation target)	Rule-based (inflation target)
Supply rule change (by issuers) possible?	Yes with agreement of majority miners	Yes	Yes
Cost of production	High (electricity consumption for computation)	Low	Low

Feature	Bitcoin	USD (home currency)	Euro (foreign currency)
Macro-financial stability risks			
Risk of hyperinflation due to over-supply?	No for individual VCs	Possible (with policy mismanagement)	…
Risk of long-term hyperdeflation	High	Low	…
Base money quantity changes to temporary shocks?	No (limited even with rule changes)	Yes	No (to US money demand shocks)
Can the issuer be lender of last resort with outside money?	No	Yes	Yes


Blockchain Wallet Users
Source: blockchain.info
User Count
17,000,000
16,000,000
15,000,000
14,000,000
13,000,000
12,000,000
11,000,000
10,000,000
9,000,000
2016/09/06 03:00
User Count: 8,594,507
Sep '16
Oct '16
Nov '16
Dec '16
Jan '17
Feb '17
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17

Questions: focused on cryptocurrency

- What is it? A currency? An asset? A fad?

- What is its (fundamental?) value? Economic function?

- What are the risks? How to regulate it?

B. What are Virtual Currencies?

8. VCs are digital representations of value, issued by private developers and denominated in their own unit of account.[2] VCs can be obtained, stored, accessed, and transacted electronically, and can be used for a variety of purposes, as long as the transacting parties agree to use them. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (such as Internet or mobile coupons and airline miles), VCs backed by assets such as gold,[3] and "cryptocurrencies" such as Bitcoin.

9. As digital representations of value, VCs fall within the broader category of digital currencies (Figure 1). However, they differ from other digital currencies, such as e-money, which is a digital payment mechanism for (and denominated in) fiat currency. VCs, on the other hand, are not denominated in fiat currency and have their own unit of account.

Risks and Transaction Costs of Distributed-Ledger Fintech: Boundary Effects and Consequences

Kim Kaivanto*‡ and Daniel Prince§
‡Department of Economics, Lancaster University, Lancaster LA1 4YX, UK
§Security Lancaster, Lancaster University, Lancaster LA1 4WA, UK

this version: March 1, 2017

Abstract

Fintech business models based on distributed ledgers – and their smart-contract variants in particular – offer the prospect of democratizing access to faster, anywhere-accessible, lower cost, reliable-and-secure high-quality financial services. In addition to holding great, economically transformative promise, these business models pose new, little-studied risks and transaction costs. However, these risks and transaction costs are not evident during the demonstration and testing phases of development, when adopters and users are drawn from the community of developers themselves, as well as from among non-programmer fintech evangelists. Hence, when the new risks and transaction costs become manifest – as the fintech business models are rolled out across the wider economy – the consequences may also

Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System*

Gur Huberman Jacob D. Leshno Ciamac Moallemi
Columbia Business School

August 24, 2017

Abstract

Many crypto-currencies, Bitcoin being the most prominent, are reliable electronic payment systems that operate without a central, trusted authority. They are enabled by blockchain technology, which deploys cryptographic tools and game theoretic incentives to create a two-sided platform. Profit maximizing computer servers called miners provide the infrastructure of the system. Its users can send payments anonymously and securely. Absent a central authority to control the system, the

Perspective here

- innovation: (decentralized) commitment

- commitment is used to provide (equity) incentives for adoption

Simple example

- two individuals, two periods
- in period one, only one individual is aware of a new technology (blockchain)
- in period two, the second individual becomes aware of the new technology with probability λ

Simple example

- outside option is normalized to 0
- there is a cost of adoption $c > 0$
- the period utility from adopting is a sum of private value u and an externality v.

Simple example

- We assume that $0 < 2u + \lambda v < c$, $u = \overline{u}$ if both individuals use the technology and $u = 0$ otherwise, and $u + v > c$

  This implies (a) that both individuals are happy to adopt in the second period if they expect the other one to adopt and (b) that the first individual is not willing to adopt in the first period

Simple example

- There are multiple equilibria with or without adoption in the second period

- In all equilibria, no adoption in the first period

Example with cryptocurrency

- We now introduce an asset and commit to limit its total emission at 1.

- The value of the asset is provided by the technologies "legal tender": the asset is required as a means of payment to use the technology.

- We exogenously fix that the asset pays δ units of utility in the last period by taxing the economy using the technology.

Example with cryptocurrency

- We now can allow the technology to determine the amount of asset $M_1 \leq 1$ to be allocated to the early adopter in the first period.

- If M_1 is sufficiently high ($> 1/2$), then there exists an equilibrium in which the technology is adopted in the first period. This equilibrium can be made unique if v is sufficiently large.

What's new?

- commitment to the supply and taxation rule (at a low cost)