21E6

How to mainstream Bitcoin
(...and mine it for less than $10/BTC)

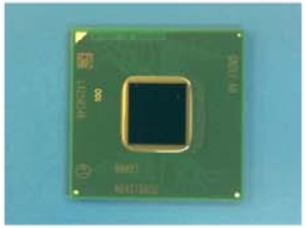
2013 Design the world’s best Bitcoin mining chip

2014 Prove it scales by mining millions in BTC

2015 A miner in every device and in every hand

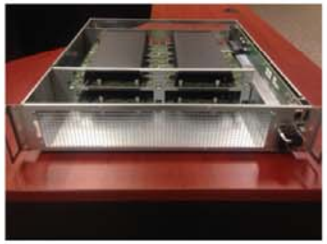
At A Glance

21E6 is one of the fastest growing startups of all time.



Chip

Intel 22nm



System

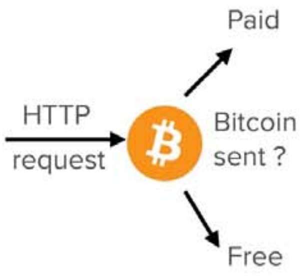
Custom mining server

Datacenter

20,000+ servers

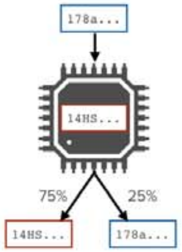
Datacenter OS

System management



402 Protocol

TCP/IP for transactions



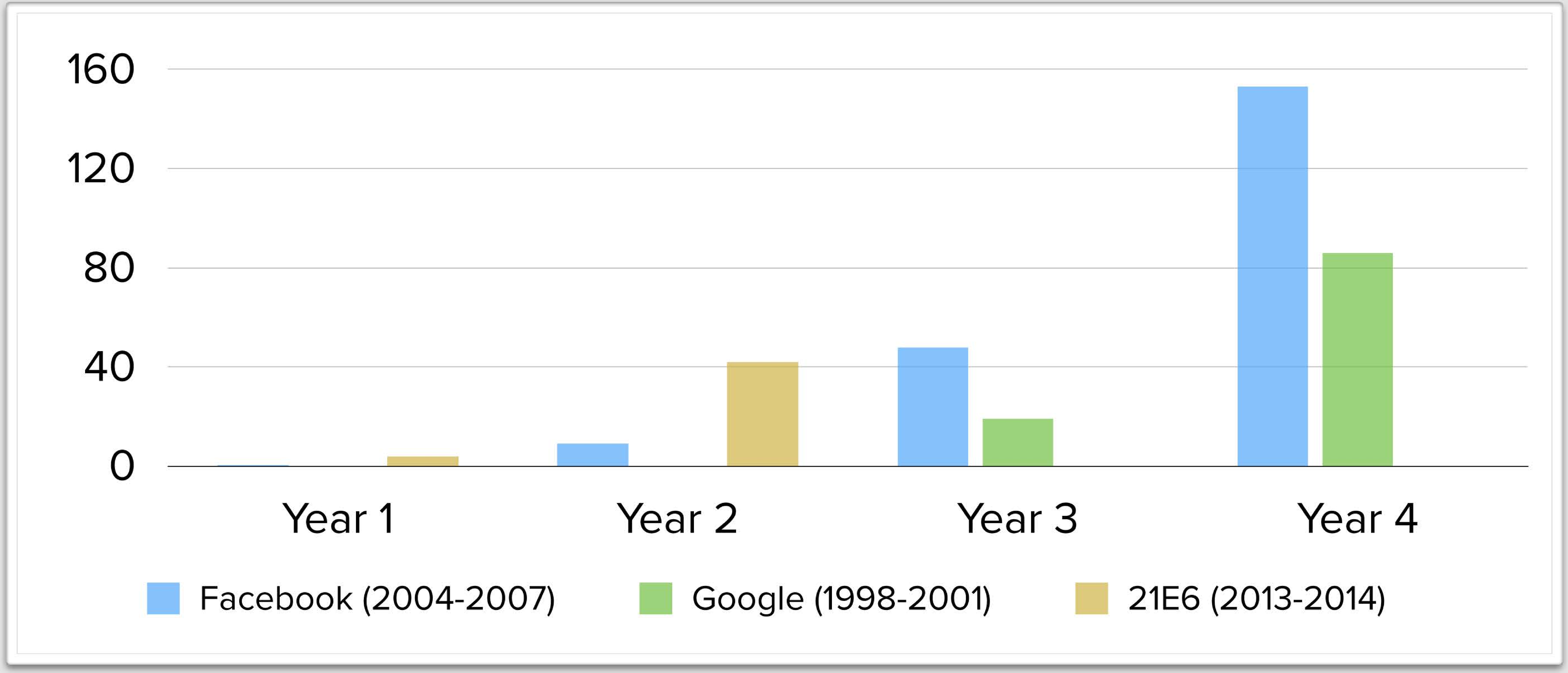
BitSplit

Charge Bitcoin from any power supply.

Founded	May 2013
Investors	a16z, Thiel, Levchin, Skoll, Pincus, ...
2013 Rev	$3.8M USD [5.7k BTC]
2014 Rev (YTD)	$37M USD [69k BTC]
2014 Rev (Proj)	$41M USD [82k BTC]
Chips	>725,000
Power	>25 MW
Employees	19
Customers	0

The Next Big Thing Never Looks Quite Like The Last

We're growing revenue faster than both Facebook and Google did in their first two years.



Team

Expertise at every level of the Bitcoin hardware stack, from cryptography through ASICs to datacenters.

Matt Pauker (CEO)

- Founder, Voltage Security (>$45m rev)
- Author of 15+ cryptography patents
- BS Computer Science, Stanford

Nigel Drego (Co-founder)

- PhD EE, MIT
- Thesis: semiconductor process variation to reduce energy consumption

Balaji Srinivasan (Chairman)

- General Partner at Andreessen Horowitz
- Founder/CTO, Counsyl ($1B+ val)
- BS/MS/PhD EE, MS ChemE Stanford

Veer Kheterpal (Co-founder)

- PhD EE, Carnegie Mellon
- Founded Fabbrix: semiconductor design startup ($19.6M acq., 10 employees)

Albert Esser (COO)

- Previously VP, Power & Infra. @ Dell
- VP Engineering, Eaton; CTO, Emerson
- MS/PhD EE, RWTH Aachen

Daniel Firu (Co-founder)

- MS EE, UF
- Supervised three years of monthly tapeouts at PDF Solutions

Executive Summary

We've figured out how to charge Bitcoin out of a wall socket - and finally enable web-scale micropayments.

bitcoin

Ben Bernanke
May hold "long-term promise"

Janet Yellen
No authority for Fed to regulate

Larry Summers
Critics "on wrong side of history"

California
AB129: Bitcoin is legal money

NASDAQ
Endorses Bitcoin ETF

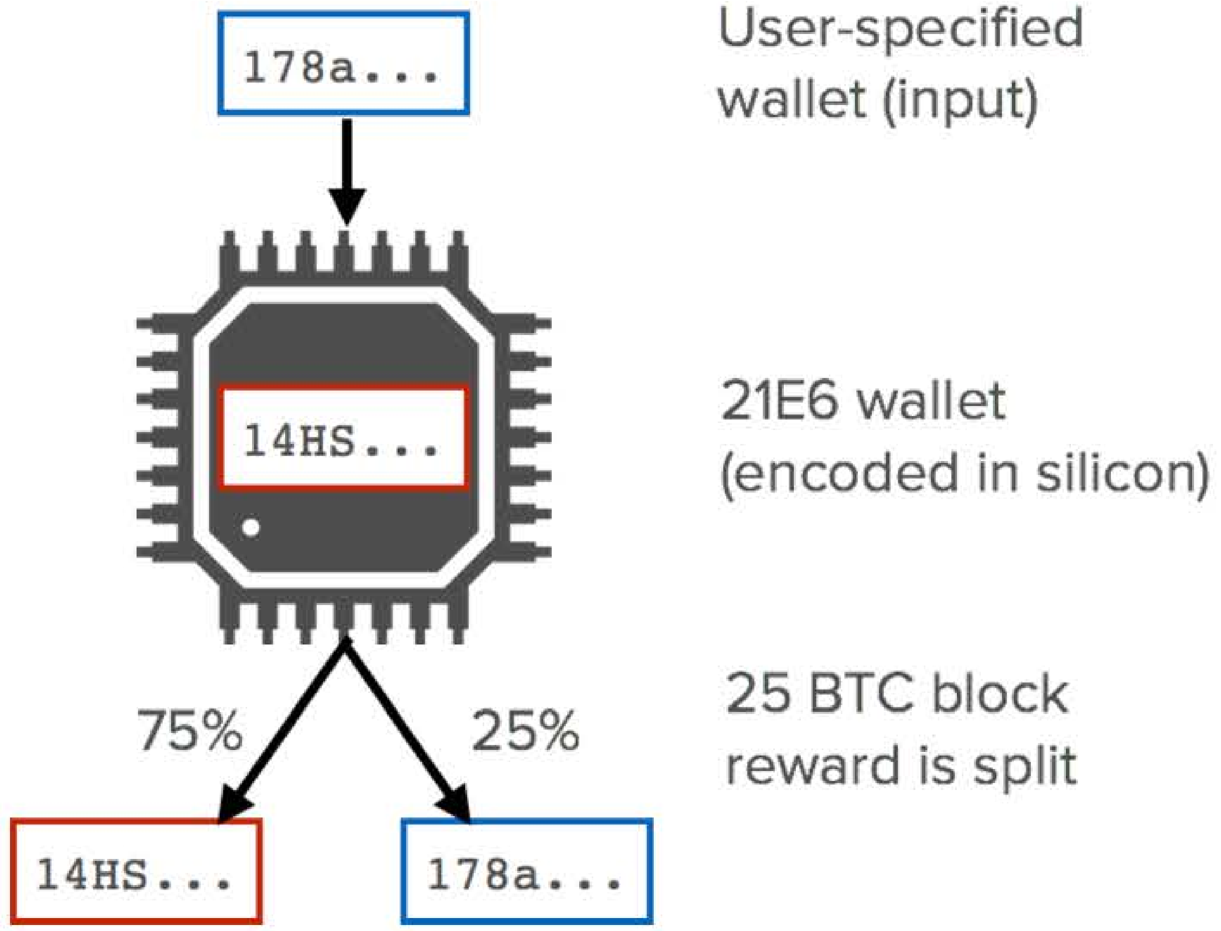
WSJ

BitBeat
Daily coverage of Bitcoin news

Bitcoin is here to stay. But what's the killer app?

Institutional acceptance & infrastructure network effect, but no consumer app.

21E6 Bitsplit: an embeddable Bitcoin "mining" chip

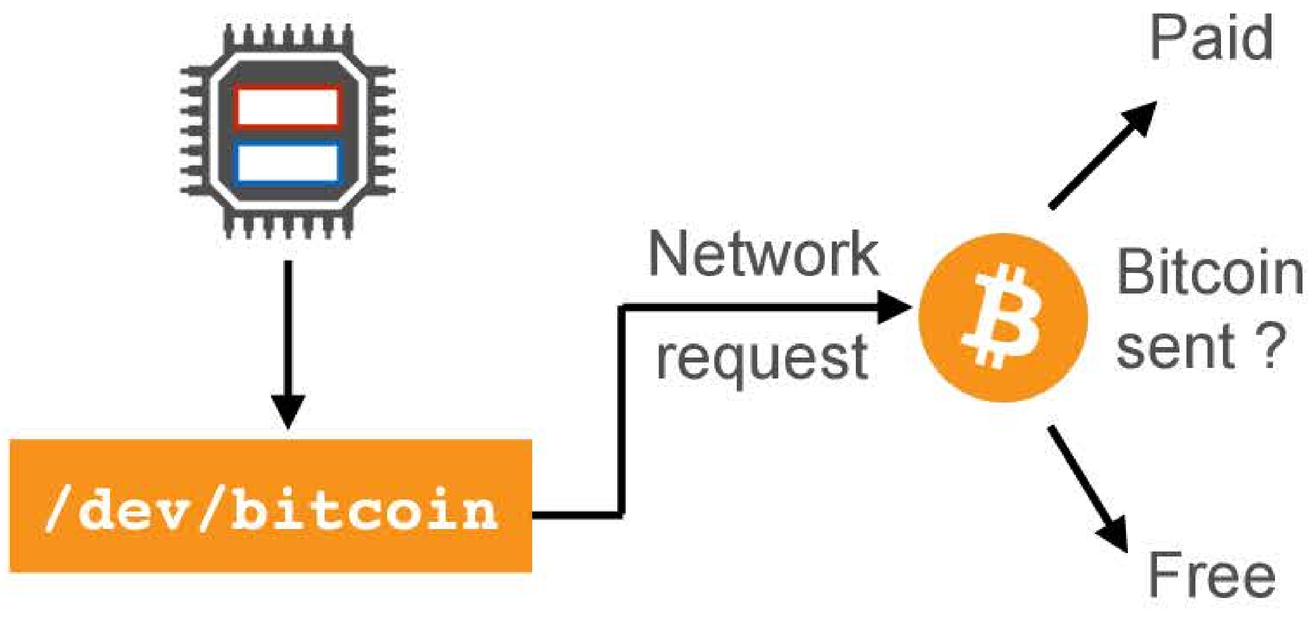

178a...
User-specified wallet (input)
14HS...
21E6 wallet (encoded in silicon)
75%
25%
14HS...
178a...
25 BTC block reward is split

Use "split" of BTC to give away chips or subsidize costs.

Idea: generate Bitcoin from on-chip mining

Turn power from wall socket into a universal digital currency.

Charge Bitcoin out of a wall socket, pay for online content or digital services of any kind.



Even low-power chip can mine millions of Satoshis annually.

Result: Micropayments are now finally feasible!

Not theory - we've actually built working chip & protocol demos.

Bitcoin is here to stay

Institutional acceptance now beyond tipping point

Bitcoin Timeline

Over last year, incredible mindshare growth in both government and institutional finance.

Government

Ben Bernanke
May hold "long-term promise"

Janet Yellen
No authority for Fed to regulate

Larry Summers
Critics "on wrong side of history"

California
AB129: Bitcoin is legal money

Finance

NASDAQ
Endorses Bitcoin ETF

WSJ

BitBeat
Daily coverage of Bitcoin news

Bloomberg

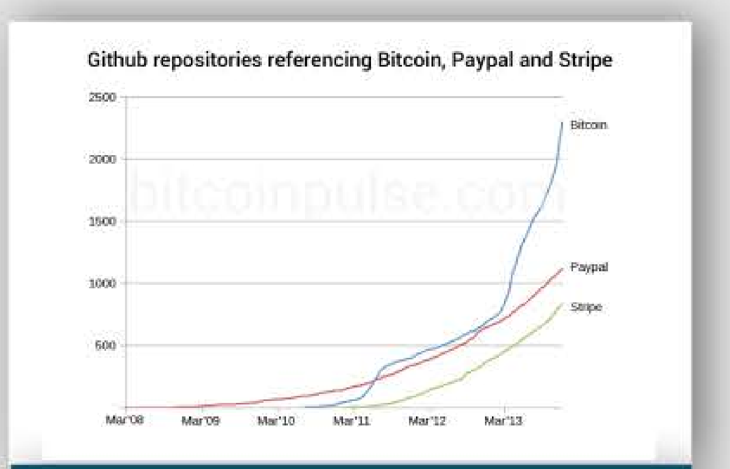
Bloomberg
BTC price on terminals

Wall Street
Reports from GS, MS, BofA, Citi

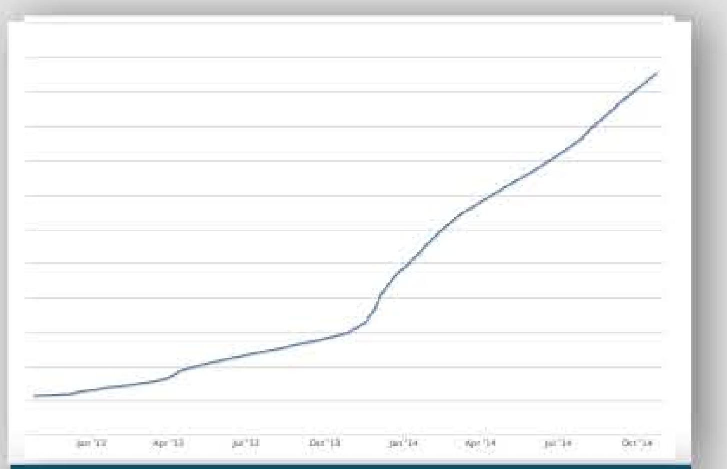
Bitcoin Timeline

...and not just in government/financial sector, but tech & market mindshare as well.

Tech



Developers
4000+ GitHub repos

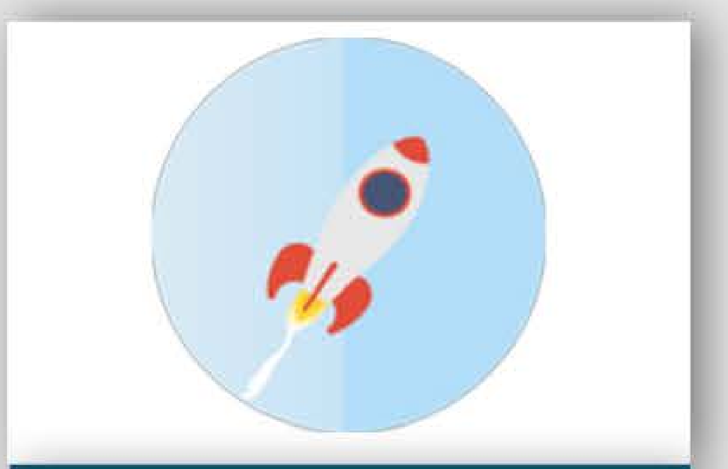


Wallets
8M+ wallets (BC + CB + Circle + ...)

1 Bitcoin equals
521.01 US Dollar

1 Bitcoin
521.01 US Dollar

Google
Integration July 2014



Startups
500+ Bitcoin startups

Market

Merchants
5000+, including Dell & Expedia

PayPal
Integration September 2014

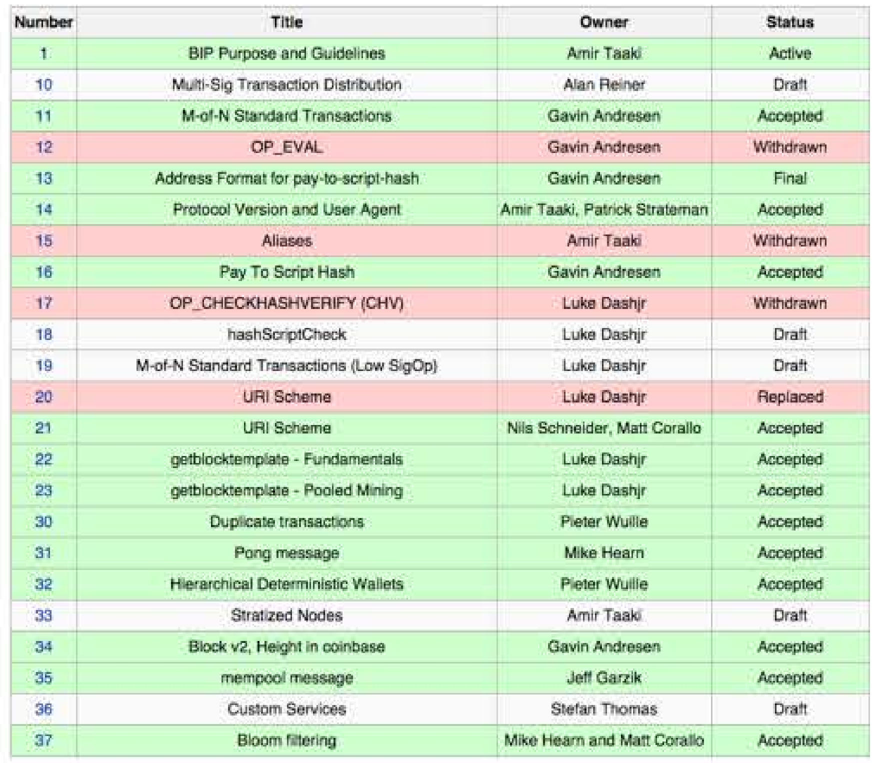
Pop Media
Newsweek cover story

VC Investing
2013: $100M
2014: $300M

Why is Bitcoin likely to be the winner?

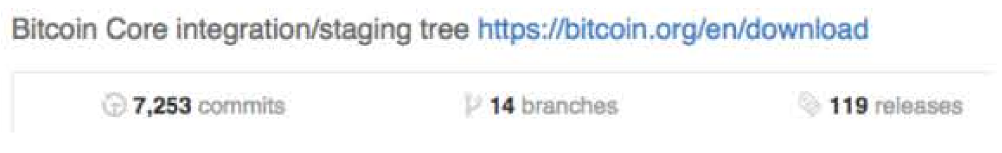
Let's talk through some of the most frequently raised questions.

Bitcoin Improvement Proposals



Number	Title	Owner	Status
1	BIP Purpose and Guidelines	Amir Taaki	Active
10	Multi-Sig Transaction Distribution	Alan Reiner	Draft
11	M-of-N Standard Transactions	Gavin Andresen	Accepted
12	OP_EVAL	Gavin Andresen	Withdrawn
13	Address Format for pay-to-script-hash	Gavin Andresen	Final
14	Protocol Version and User Agent	Amir Taaki, Patrick Strateman	Accepted
15	Aliases	Amir Taaki	Withdrawn
16	Pay To Script Hash	Gavin Andresen	Accepted
17	OP_CHECKHASHVERIFY (CHV)	Luke Dashjr	Withdrawn
18	hashScriptCheck	Luke Dashjr	Draft
19	M-of-N Standard Transactions (Low SigOp)	Luke Dashjr	Draft
20	URI Scheme	Luke Dashjr	Replaced
21	URI Scheme	Nils Schneider, Matt Corallo	Accepted
22	getblocktemplate - Fundamentals	Luke Dashjr	Accepted
23	getblocktemplate - Pooled Mining	Luke Dashjr	Accepted
30	Duplicate transactions	Pieter Wuille	Accepted
31	Pong message	Mike Hearn	Accepted
32	Hierarchical Deterministic Wallets	Pieter Wuille	Accepted
33	Stratized Nodes	Amir Taaki	Draft
34	Block v2, Height in coinbase	Gavin Andresen	Accepted
35	mempool message	Jeff Garzik	Accepted
36	Custom Services	Stefan Thomas	Draft
37	Bloom filtering	Mike Hearn and Matt Corallo	Accepted

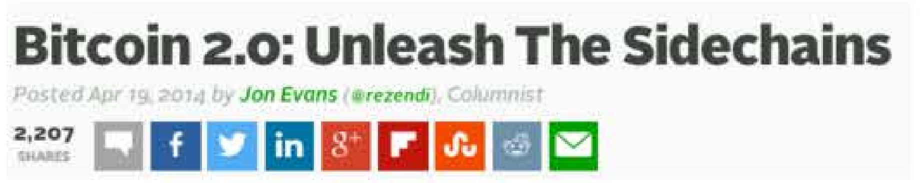
Rapid pace of open-source dev



Bitcoin Core integration/staging tree https://bitcoin.org/en/download

7,253 commits   14 branches   119 releases

Sidechains as a staging area



Bitcoin 2.0: Unleash The Sidechains

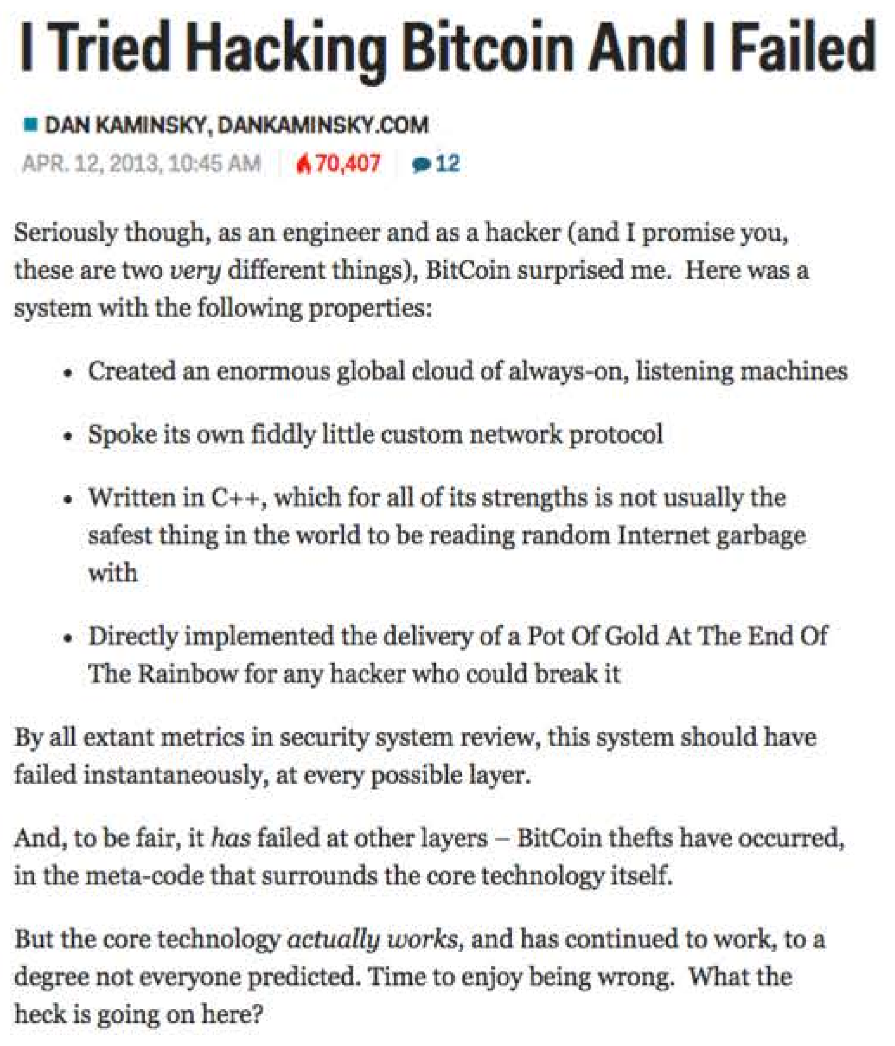
Posted Apr 19, 2014 by Jon Evans (@rezendi), Columnist

2,207 SHARES

Modifiable?

Yes. Like Linux, BIPs/patches regularly incorporated.

Important: Bitcoin protocol itself has not been hacked.



I Tried Hacking Bitcoin And I Failed

DAN KAMINSKY, DANKAMINSKY.COM

APR. 12, 2013, 10:45 AM | 70,407 | 12

Seriously though, as an engineer and as a hacker (and I promise you, these are two *very* different things), BitCoin surprised me. Here was a system with the following properties:

- Created an enormous global cloud of always-on, listening machines
- Spoke its own fiddly little custom network protocol
- Written in C++, which for all of its strengths is not usually the safest thing in the world to be reading random Internet garbage with
- Directly implemented the delivery of a Pot Of Gold At The End Of The Rainbow for any hacker who could break it

By all extant metrics in security system review, this system should have failed instantaneously, at every possible layer.

And, to be fair, it *has* failed at other layers – BitCoin thefts have occurred, in the meta-code that surrounds the core technology itself.

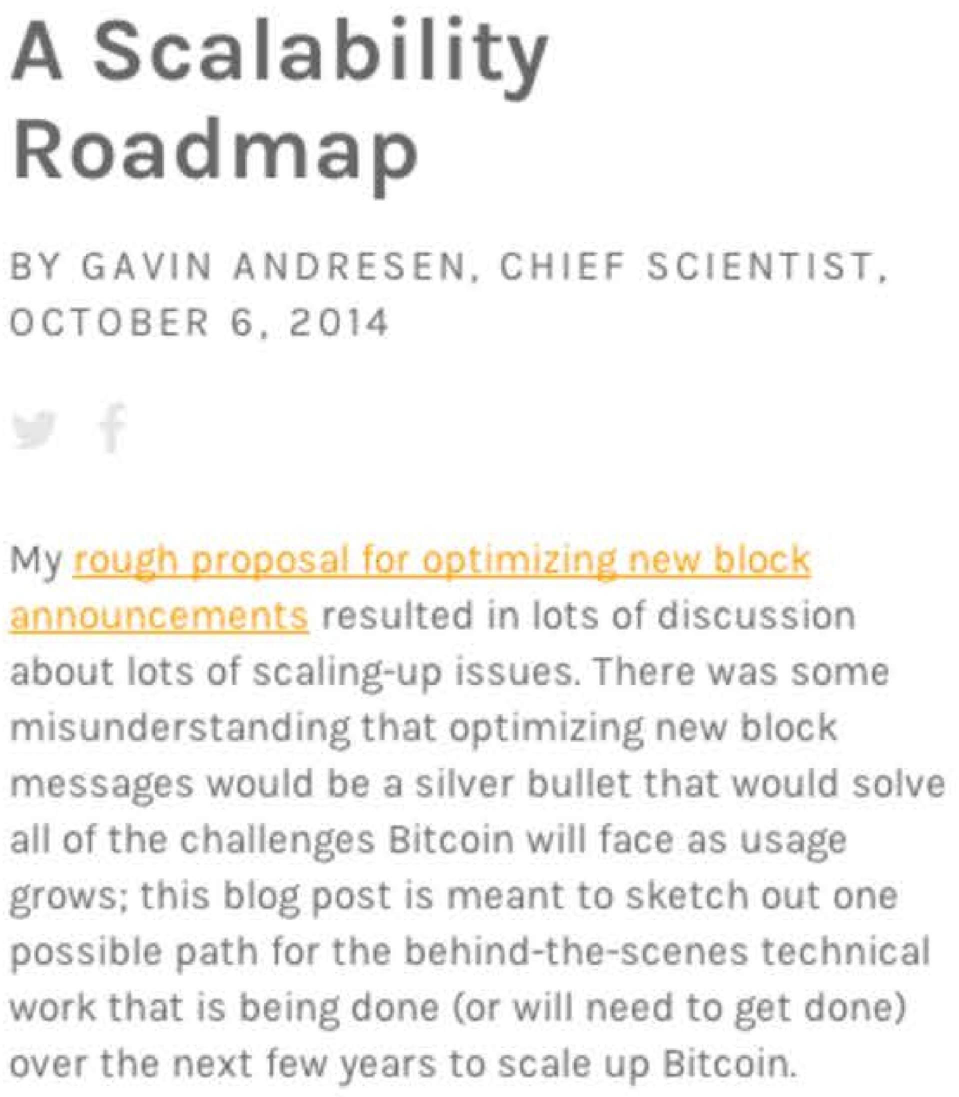
But the core technology *actually works*, and has continued to work, to a degree not everyone predicted. Time to enjoy being wrong. What the heck is going on here?

Analogy: a bank robbery is not a counterfeit dollar. Similarly, Mt. Gox hack did not mean a double spend of Bitcoins.

Secure?

Appears so. Protocol itself has not been hacked.

Like early Internet, demand is pushing scalability innovation.



A Scalability Roadmap

BY GAVIN ANDRESEN, CHIEF SCIENTIST, OCTOBER 6, 2014

My rough proposal for optimizing new block announcements resulted in lots of discussion about lots of scaling-up issues. There was some misunderstanding that optimizing new block messages would be a silver bullet that would solve all of the challenges Bitcoin will face as usage grows; this blog post is meant to sketch out one possible path for the behind-the-scenes technical work that is being done (or will need to get done) over the next few years to scale up Bitcoin.

Scaling will be nontrivial, but Internet pushed communications up to 10000/day. Bitcoin will do same for transactions.

Scalable?

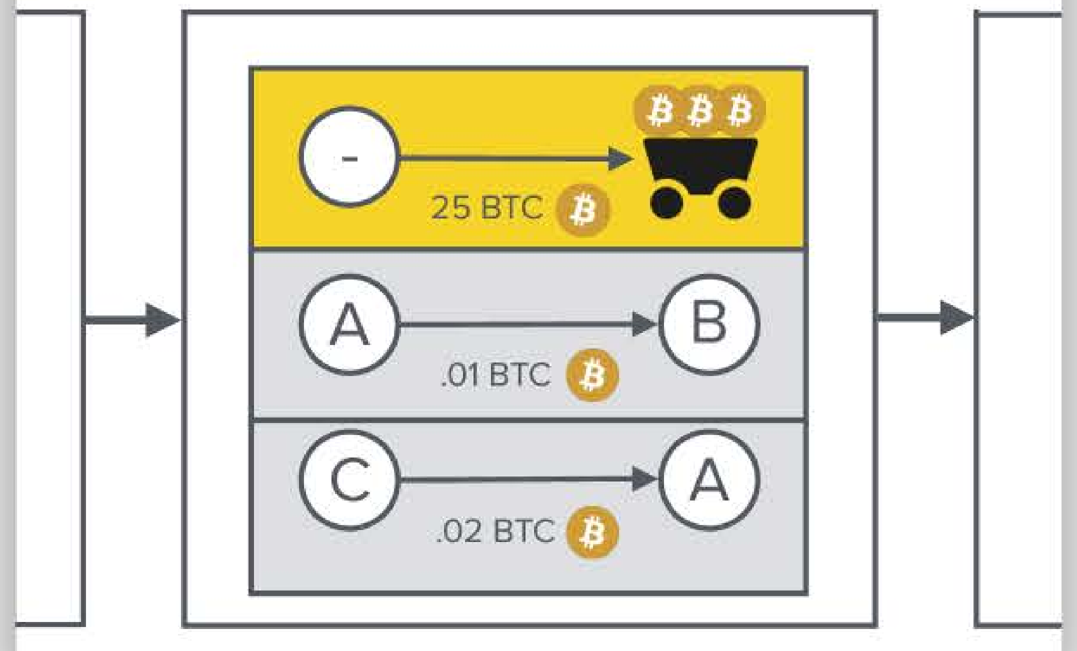
Yes. Core devs have published billion tx roadmap.

There will be blockchain-based apps besides Bitcoin itself...

namecoin

Filecoin

...but blockchain tokens must have value (like Bitcoin) to incentivize mining process.



Blockchain, not Bitcoin?

Not really separable; token is incentive for distributed mining

Bitcoin has a four-sided network effect

Four groups: miners, developers, users, and merchants.

Miners

Verify transactions, receive BTC.

Devs

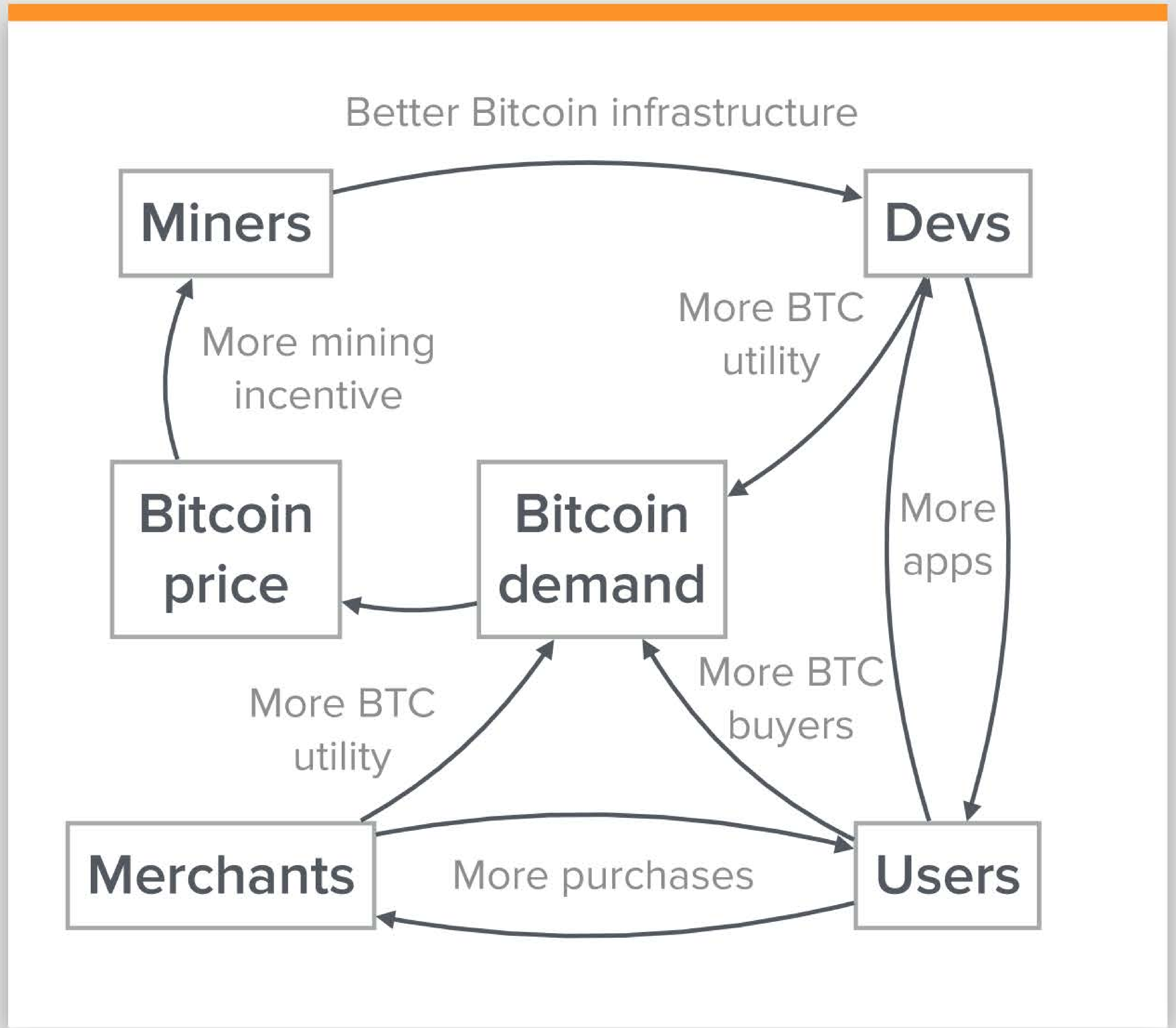
Write Bitcoin apps.

Merchants

Accept Bitcoin for goods.

Users

Use Bitcoin for goods & apps.

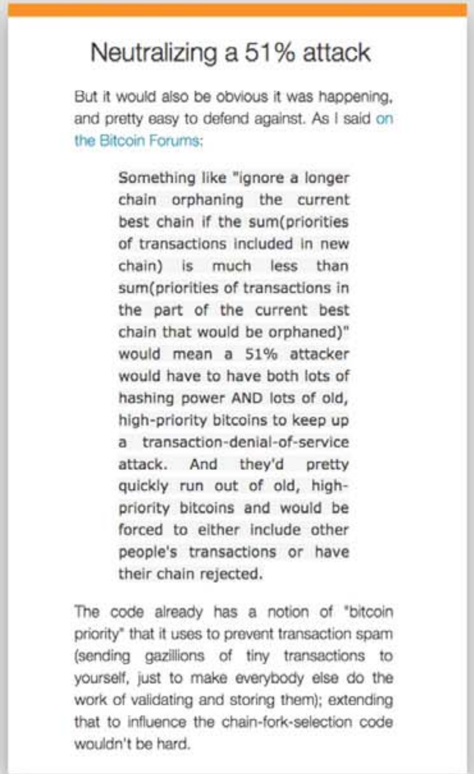


The 4-Sided Network Effect

Every node increases value for other nodes.

Why is Bitcoin likely to be the winner?

Let's talk through some of the most frequently raised questions.



Neutralizing a 51% attack

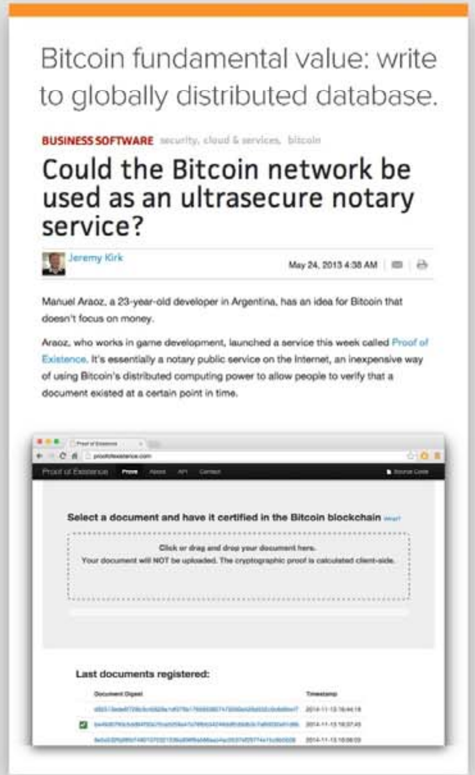
But it would also be obvious it was happening, and pretty easy to defend against. As I said on the Bitcoin Forums:

> Something like "ignore a longer chain orphaning the current best chain if the sum(priorities of transactions included in new chain) is much less than sum(priorities of transactions in the part of the current best chain that would be orphaned)" would mean a 51% attacker would have to have both lots of hashing power AND lots of old, high-priority bitcoins to keep up a transaction-denial-of-service attack. And they'd pretty quickly run out of old, high-priority bitcoins and would be forced to either include other people's transactions or have their chain rejected.

The code already has a notion of "bitcoin priority" that it uses to prevent transaction spam (sending gazillions of tiny transactions to yourself, just to make everybody else do the work of validating and storing them); extending that to influence the chain-fork-selection code wouldn't be hard.

51% attack?

Oversold. Technical countermeasures available.



Bitcoin fundamental value: write to globally distributed database.

BUSINESS SOFTWARE security, cloud & services, bitcoin

Could the Bitcoin network be used as an ultrasecure notary service?

Jeremy Kirk May 24, 2013 4:38 AM

Manuel Araoz, a 23-year-old developer in Argentina, has an idea for Bitcoin that doesn't focus on money.

Araoz, who works in game development, launched a service this week called Proof of Existence. It's essentially a notary public service on the Internet, an inexpensive way of using Bitcoin's distributed computing power to allow people to verify that a document existed at a certain point in time.

Select a document and have it certified in the Bitcoin blockchain what?

Click or drag and drop your document here.
Your document will NOT be uploaded. The cryptographic proof is calculated client-side.

Last documents registered:

	Document Digest	Timestamp
	[illegible]	2014-11-13 16:44:18
☑	[illegible]	2014-11-13 16:37:45
	[illegible]	2014-11-13 16:06:03

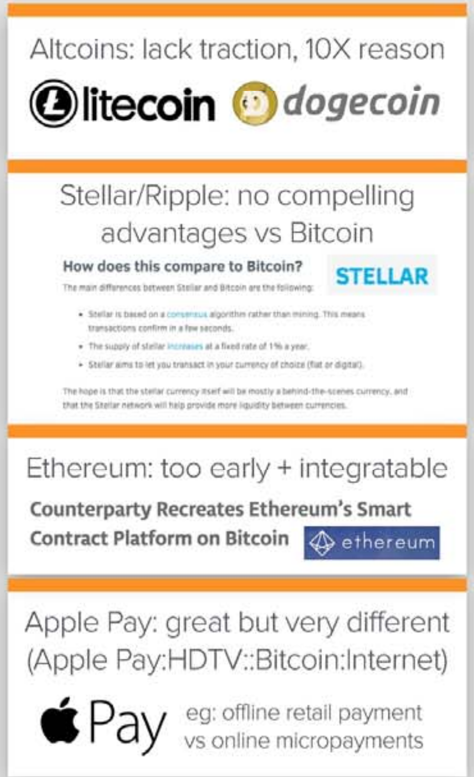
Fundamental value?

Actually, yes. 1 Satoshi: write to a global notary public.

Ben Bernanke
May hold "long-term promise"
Janet Yellen
No authority for Fed to regulate
California
AB129: Bitcoin is legal money
Larry Summers
Critics "on wrong side of history"
NASDAQ
NASDAQ
Endorses Bitcoin ETF
WSJ
BitBeat
Daily coverage of Bitcoin news

Legal issues?

As of 2014, major govt & financial acceptance.



Altcoins: lack traction, 10X reason

Stellar/Ripple: no compelling advantages vs Bitcoin

How does this compare to Bitcoin?

The main differences between Stellar and Bitcoin are the following:

- Stellar is based on a consensus algorithm rather than mining. This means transactions confirm in a few seconds.
- The supply of stellar increases at a fixed rate of 1% a year.
- Stellar aims to let you transact in your currency of choice (fiat or digital).

The hope is that the stellar currency itself will be mostly a behind-the-scenes currency, and that the Stellar network will help provide more liquidity between currencies.

Ethereum: too early + integratable

Counterparty Recreates Ethereum's Smart Contract Platform on Bitcoin

Apple Pay: great but very different (Apple Pay:HDTV::Bitcoin:Internet)

eg: offline retail payment vs online micropayments

Alternatives?

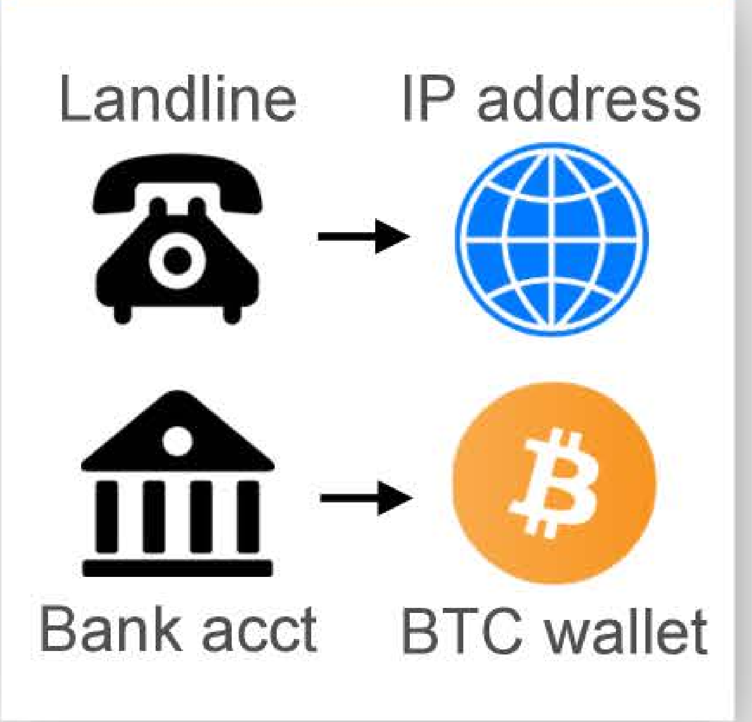
Prob not. BIPs + Sidechains: Bitcoin adaptable like x86

Bitcoin is to Paypal as Linux is to Windows

We've already seen what happens when an open-source, decentralized, programmable version arises.

EVERY ENTITY

Banking for anything

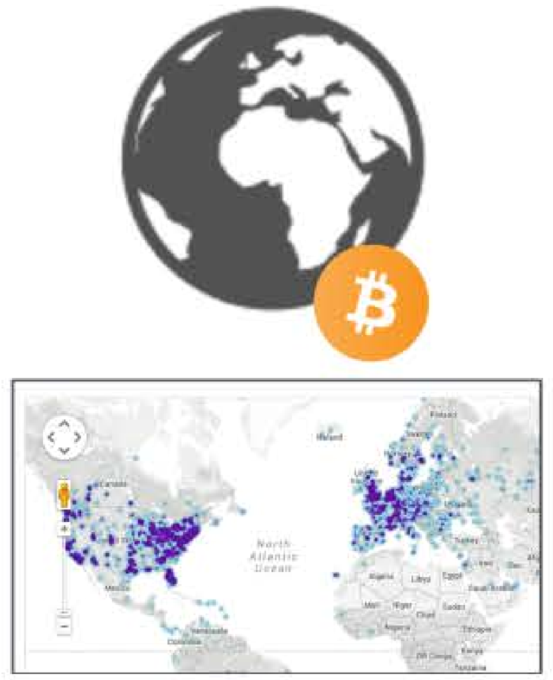


EVERY DEVICE

Connected? Send/receive.

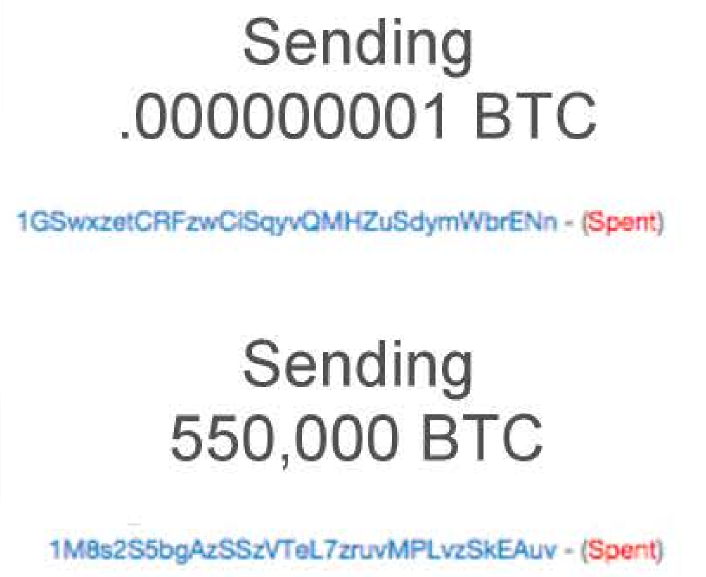
EVERY COUNTRY

Available worldwide



EVERY AMOUNT

From micro to macro



Sending
.000000001 BTC

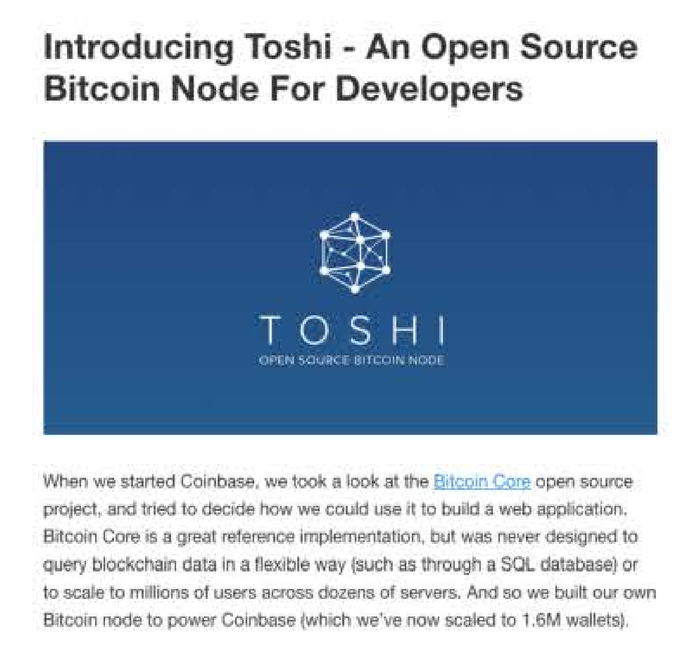
1GSwxzetCRFzwCiSqyvQMHZuSdymWbrENn - (Spent)

Sending
550,000 BTC

1M8s2S5bgAzSSzVTeL7zruvMPLvzSkEAuv - (Spent)

EXTENSIBLE

Modify code, add features

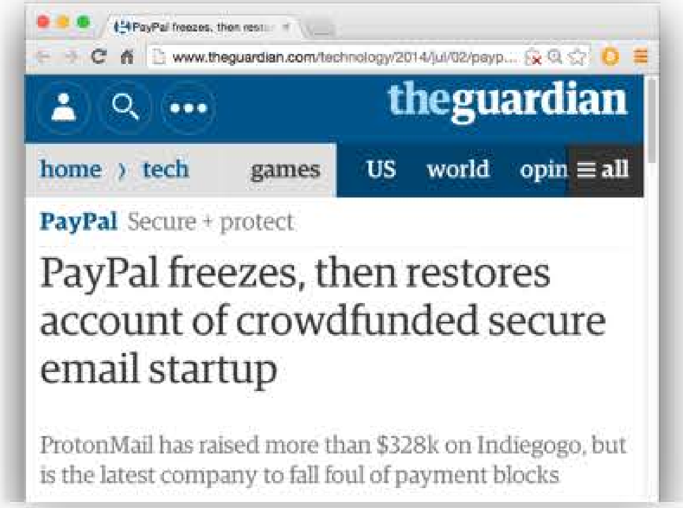


Introducing Toshi - An Open Source Bitcoin Node For Developers

When we started Coinbase, we took a look at the Bitcoin Core open source project, and tried to decide how we could use it to build a web application. Bitcoin Core is a great reference implementation, but was never designed to query blockchain data in a flexible way (such as through a SQL database) or to scale to millions of users across dozens of servers. And so we built our own Bitcoin node to power Coinbase (which we've now scaled to 1.6M wallets).

UNFREEZABLE

Full personal control


PayPal freezes, then resto
www.theguardian.com/technology/2014/jul/02/payp...
theguardian
home
tech
games
US
world
opin
≡ all

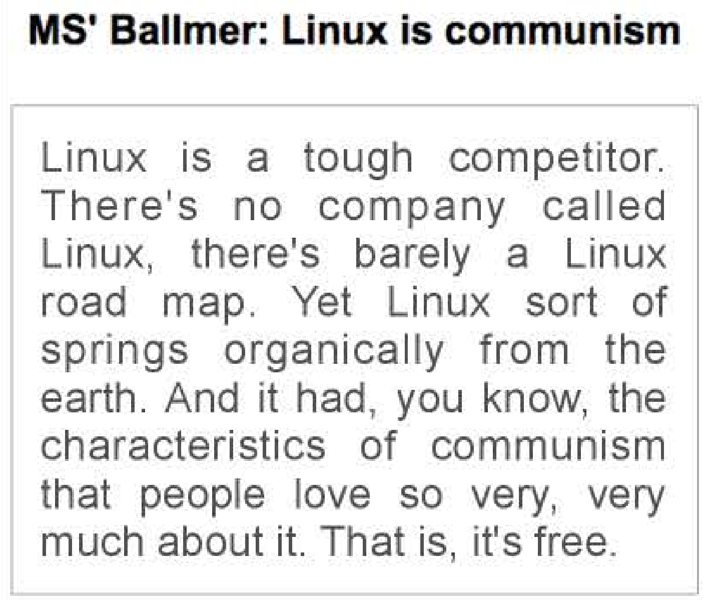
PayPal Secure + protect

PayPal freezes, then restores account of crowdfunded secure email startup

ProtonMail has raised more than $328k on Indiegogo, but is the latest company to fall foul of payment blocks

FREE & OPEN SOURCE

No toll from .com



MS' Ballmer: Linux is communism

Linux is a tough competitor. There's no company called Linux, there's barely a Linux road map. Yet Linux sort of springs organically from the earth. And it had, you know, the characteristics of communism that people love so very, very much about it. That is, it's free.

MUCH MORE

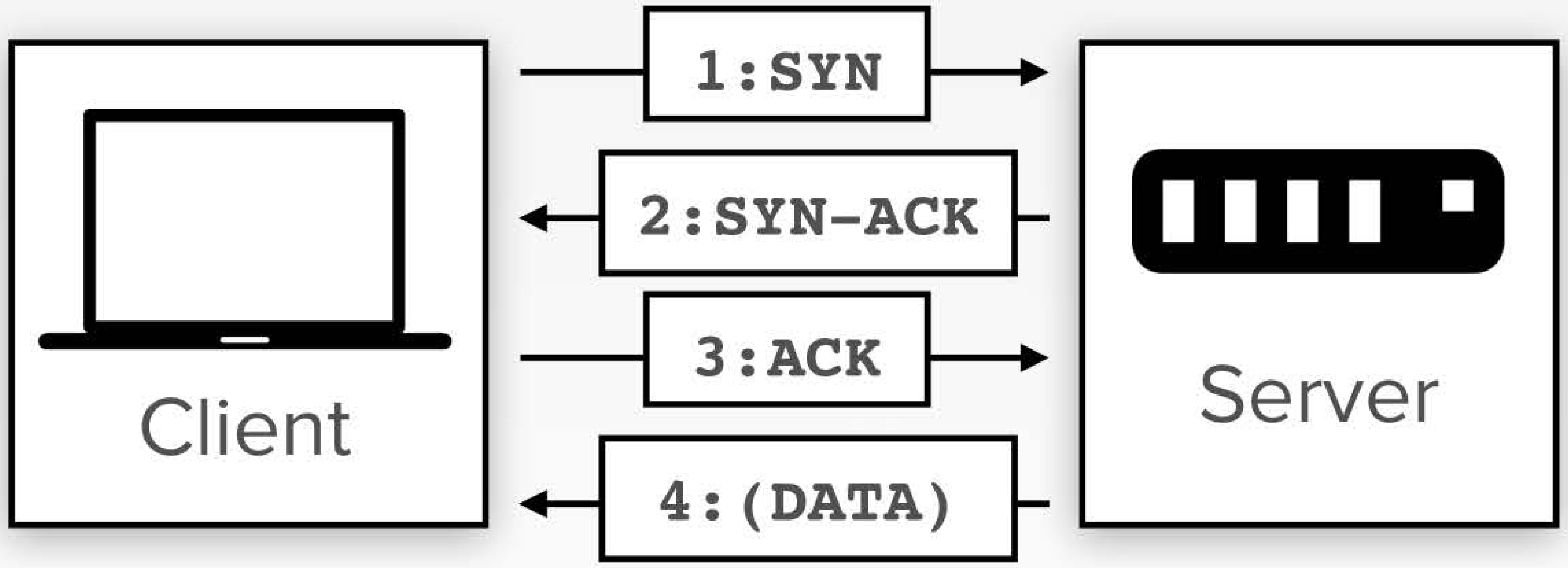
Multisig, Blockchain, Contracts!

Bitcoin enables TCP/IP for transactions

Recall the TCP/IP handshake. It's possible to implement a payments handshake like this using Bitcoin.

TCP/IP IS FOR DATA

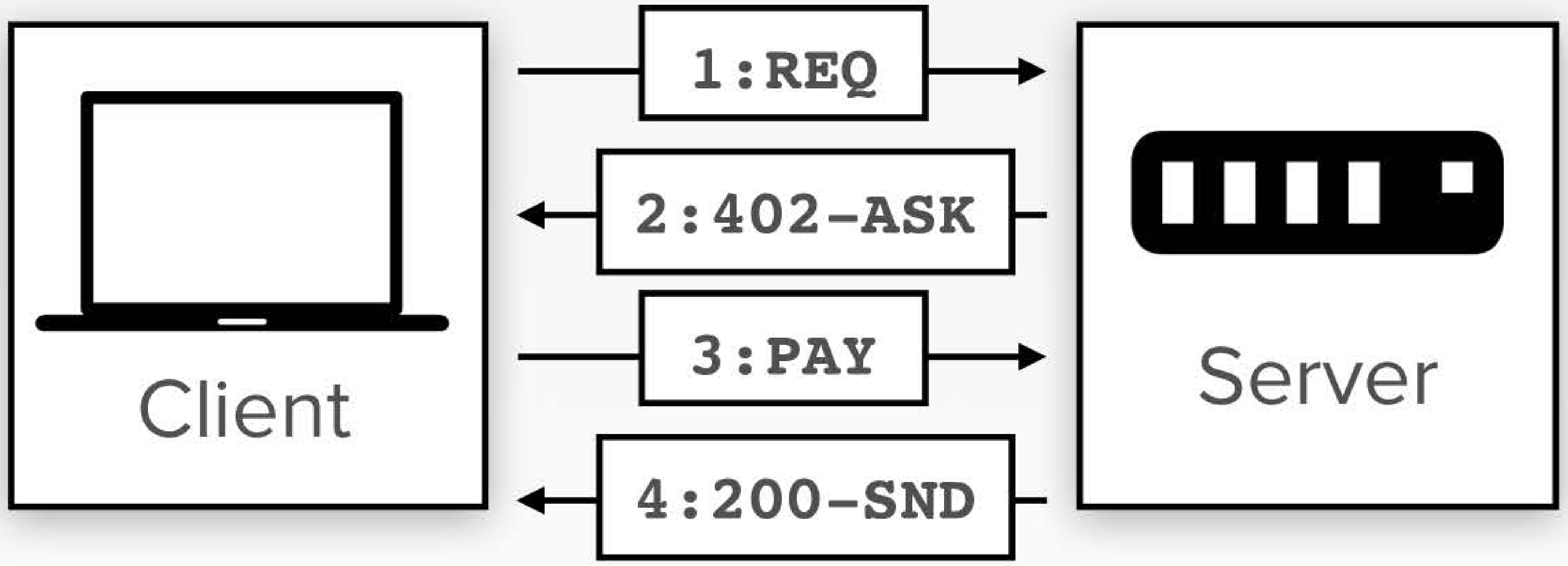
The TCP/IP handshake



Client asks to open connection.
Server acks, then client acknowledges.
TCP socket open. Server sends data.

BITCOIN IS FOR TRANSACTIONS

The Bitcoin 402 handshake



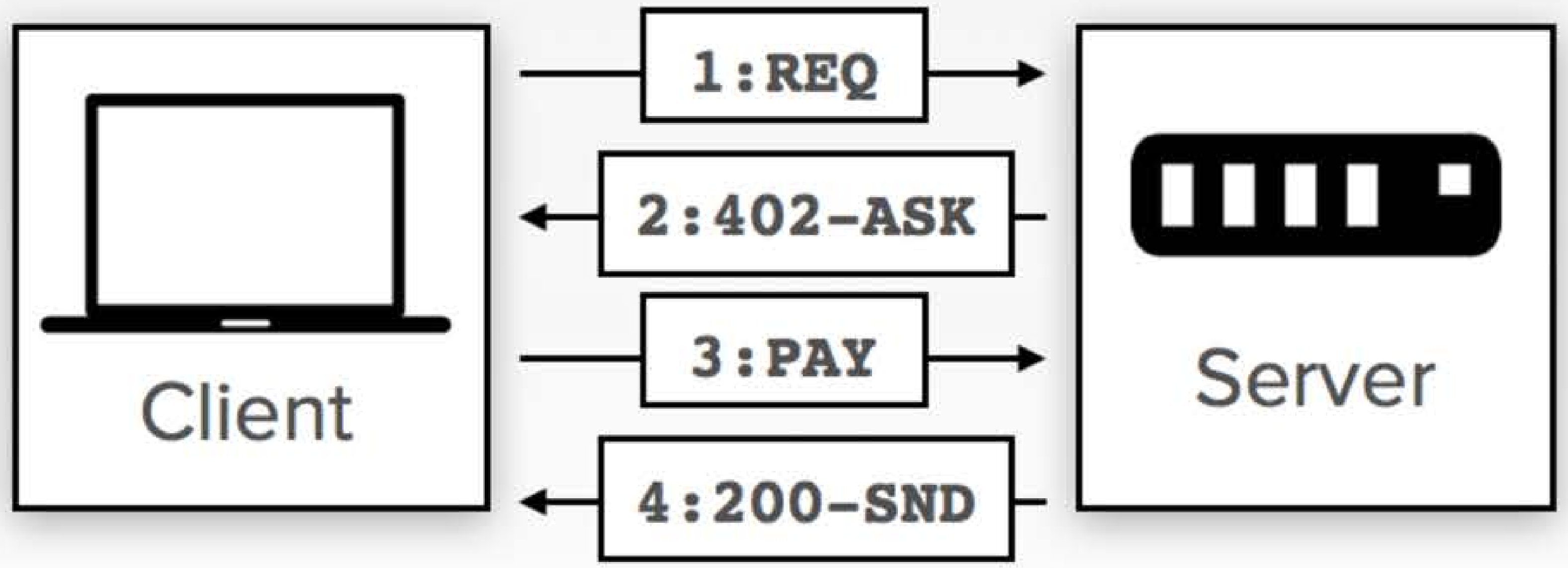
Client requests resource.
Server initially refuses but quotes price.
Client pays BTC. Server sends resource.

Bitcoin enables TCP/IP for transactions

We know this is possible because we implemented it.

BITCOIN IS FOR TRANSACTIONS

The Bitcoin 402 handshake



Client requests resource.
Server initially refuses but quotes price.
Client pays BTC. Server sends resource.

CLIENT INITIATES HTTP REQUEST

SERVER DENIES, ASKS FOR .001 BTC

CLIENT REREQUESTS AND ATTACHES BTC

SERVER RETURNS RESOURCE FOR BTC

```
demo@402demo:~$ bitcurl -X POST -d '{"to":
6502071548,"msg":"hello world via bitcurl"}'
http://api.demo.21e6.com/api/twilio -v
Requesting http://api.demo.21e6.com/api/twilio
Status 402
Bitcoin address: 1Gy4AvTeA2LftFdMm2TfBojV1LfcT22KRr
Price in BTC: 0.001
Transaction id:
6428b54af4e2f03bf5d806472d2081d4a0dac7f53d156906f9c8aeec6
01cb34b
Retrying request with txid..
Status 200
{"status":"ok","message_id":"SM04d5c769e8a847098c16da328b
658037"}
demo@402demo:~$
```

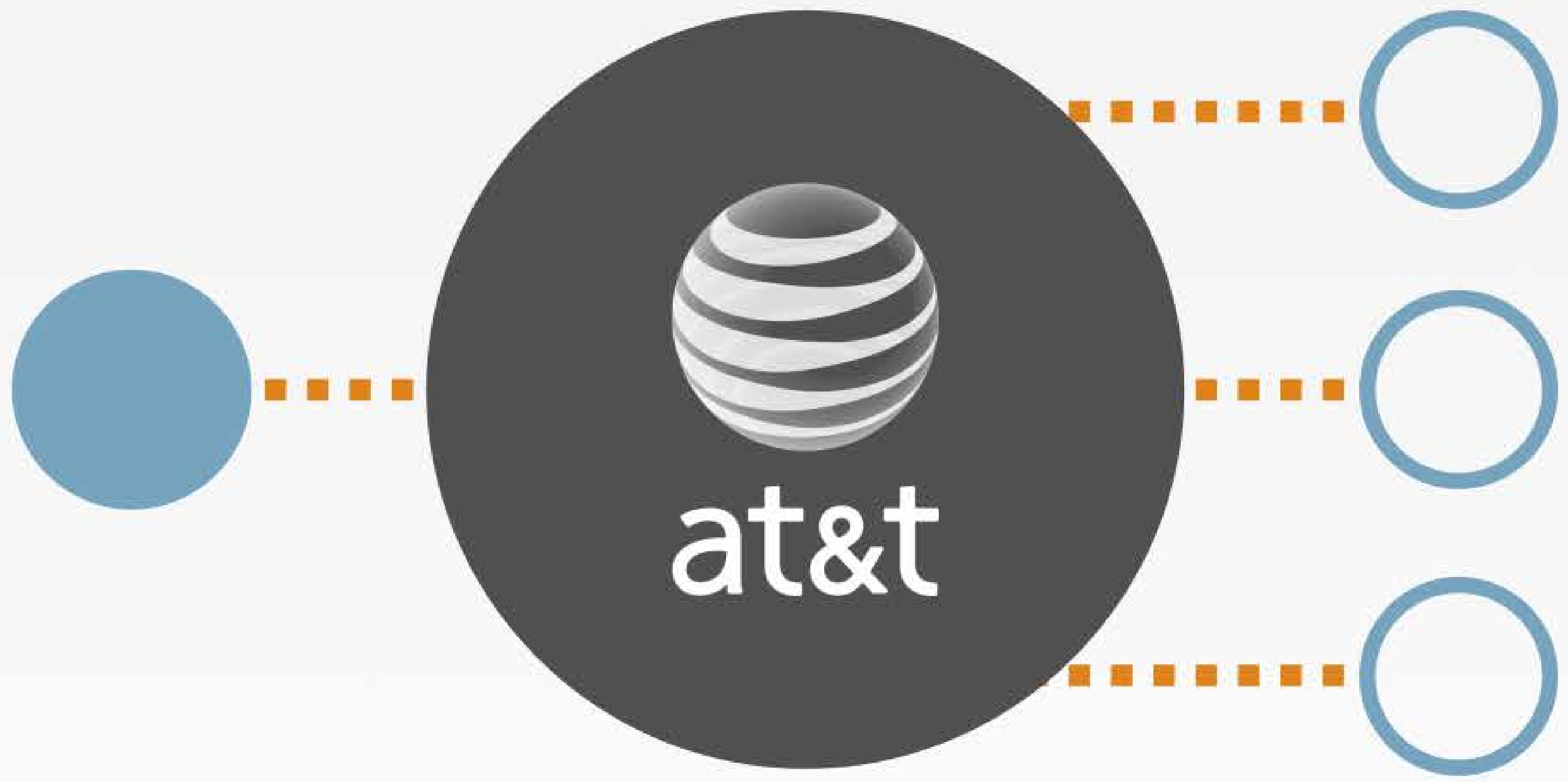
```
demo@402demo:~$ bitcurl -X POST -d '{"to":6502071548,"msg":"hello world via bitcurl"}' http://api.demo.21e6.com/api/twilio -v
Requesting http://api.demo.21e6.com/api/twilio
Status 402
Bitcoin address: 1Gy4AvTeA2LftFdMm2TfBojV1LfcT22KRr
Price in BTC: 0.001
Transaction id: 6428b54af4e2f03bf5d806472d2081d4a0dac7f53d156906f9c8aeec601cb34b
Retrying request with txid..
Status 200
{"status":"ok","message_id":"SM04d5c769e8a847098c16da328b658037"}
```

A live demo of "TCP/IP for transactions"

This is why we compare Bitcoin to the Internet

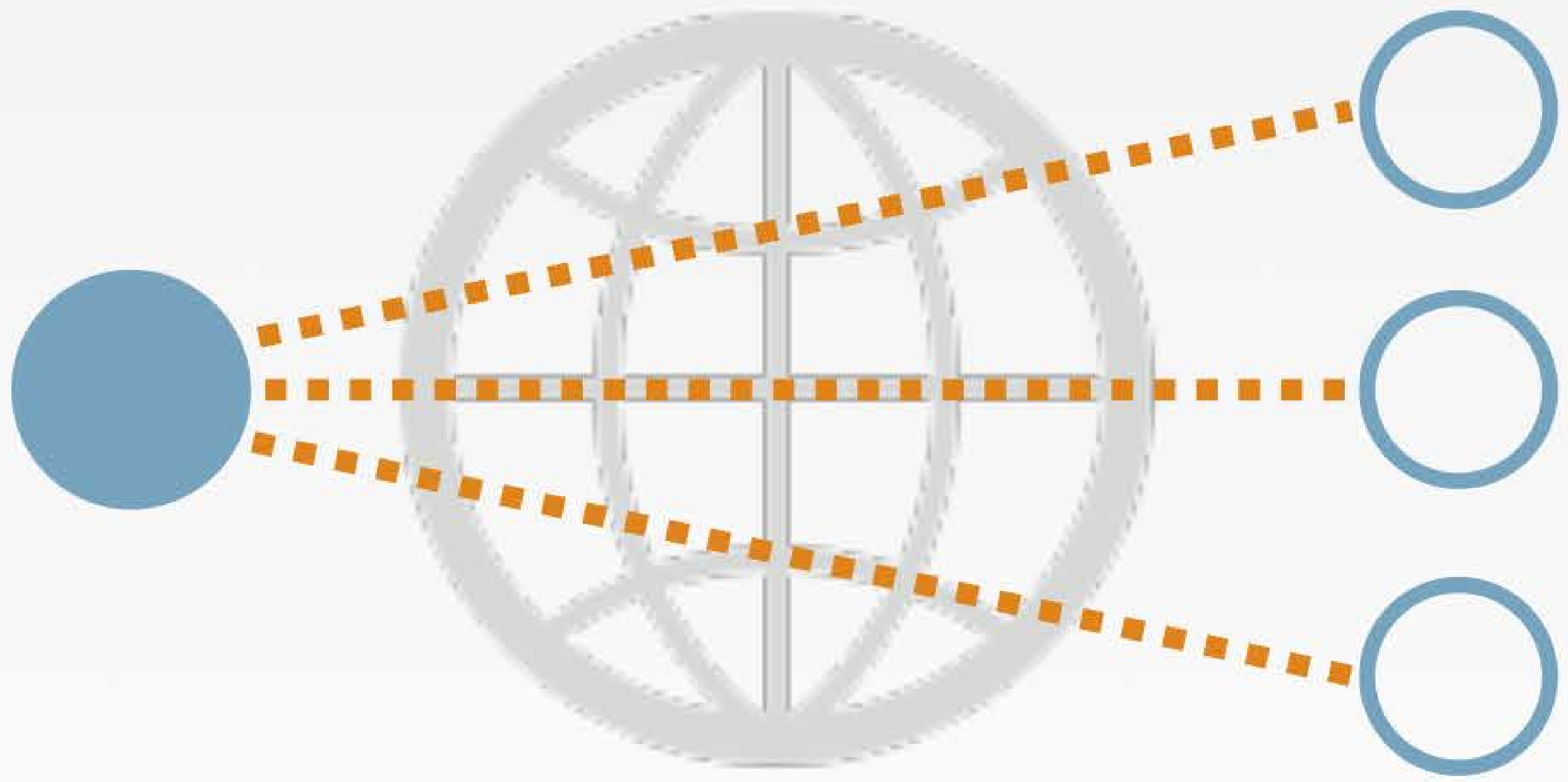
The internet disintermediated telcos, replacing with programmable packet-based communication.

BEFORE



Deal with telco to deploy
code related to information
on the network backbone

AFTER

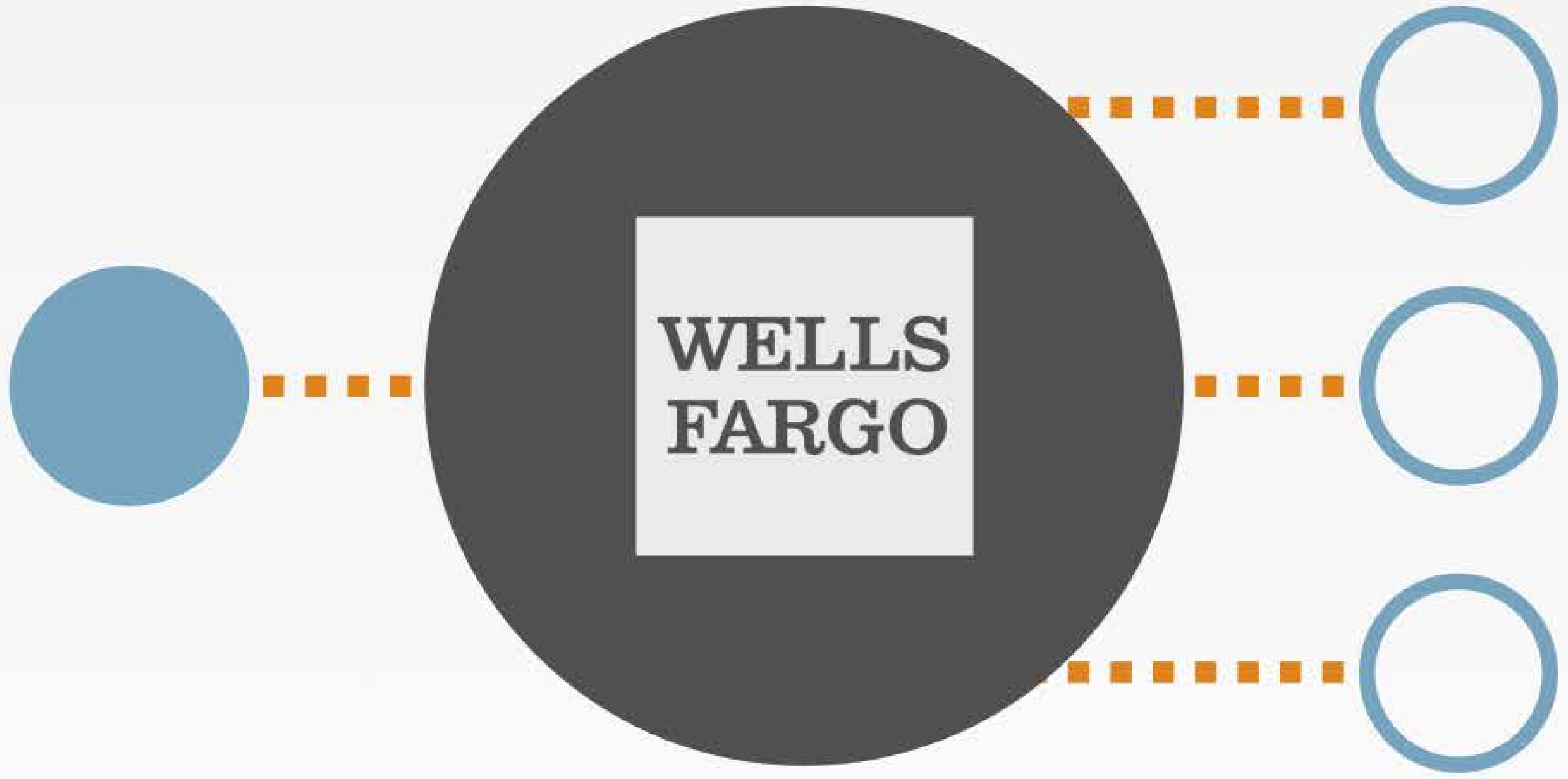


Anyone can programmatically
send packets to anyone
(or many anyones) via internet

Bitcoin disintermediates banks

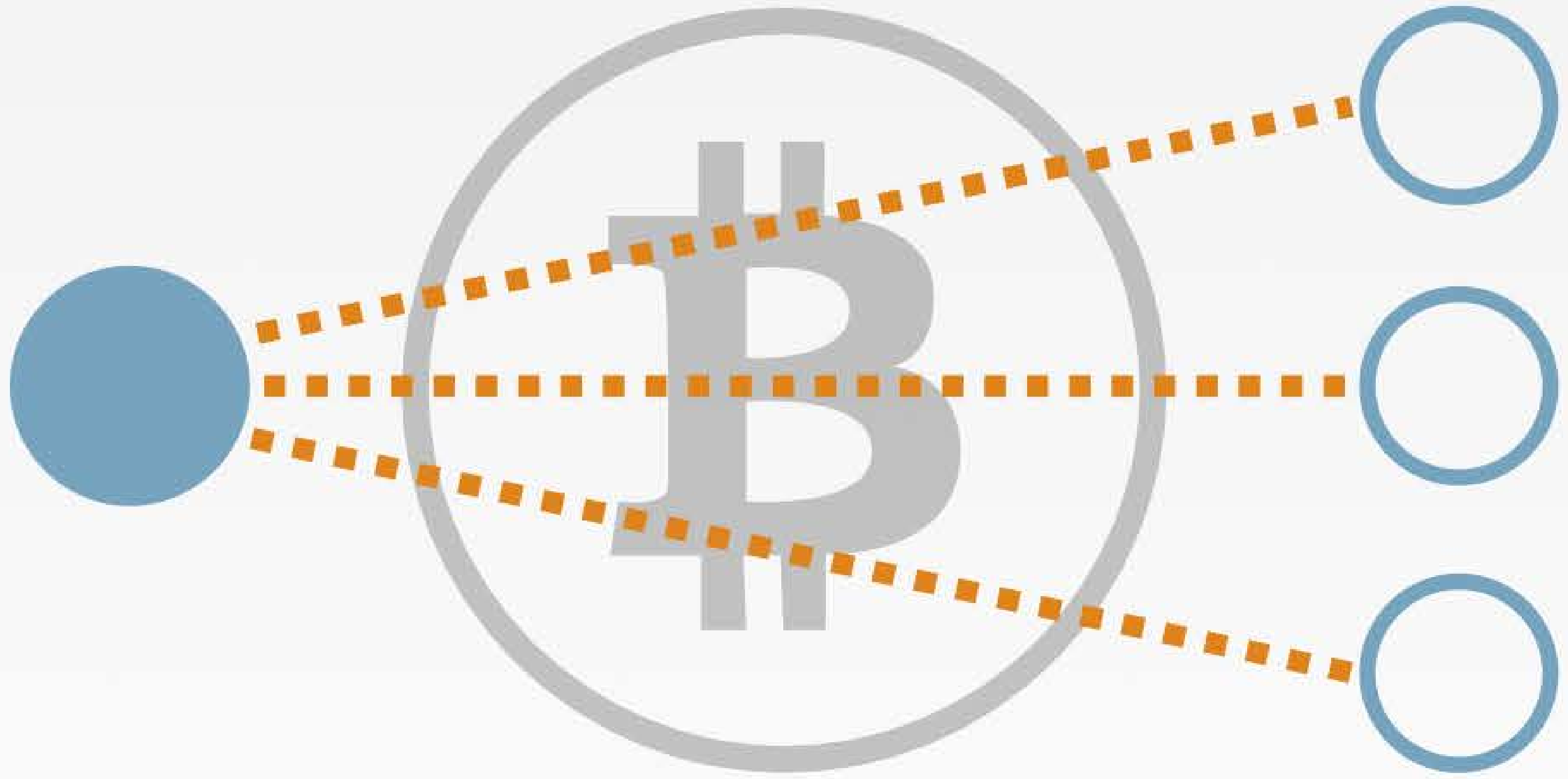
Similarly, Bitcoin disintermediates Fedwire/ACH/SWIFT, replacing with programmable packet-based money.

BEFORE



Deal with bank to deploy
code related to value
in the banking system

AFTER



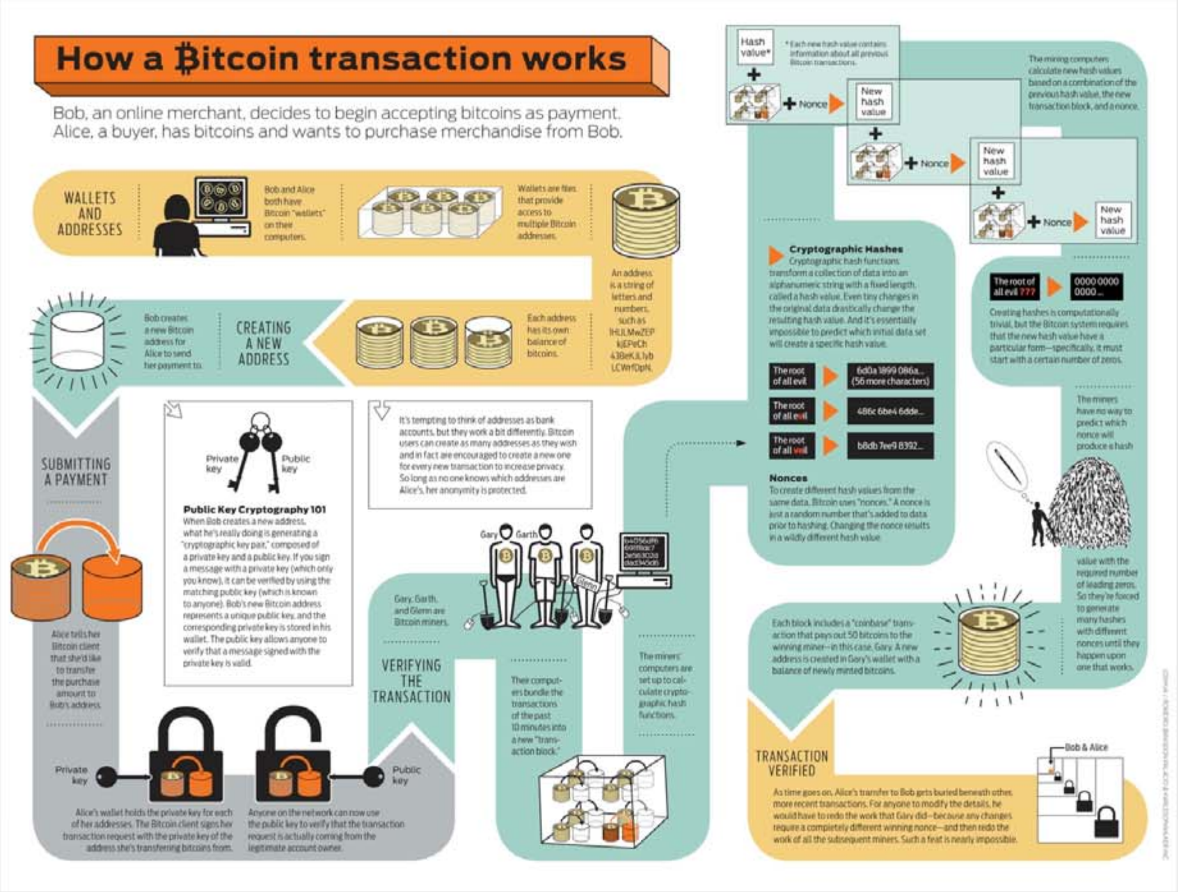
Anyone can programmatically
send value to anyone
(or many anyones) via internet

The Problem

Bitcoin mining is highly lucrative - and competitive

Background

Bitcoin mining: a worldwide computational race, held every 10 mins.
Mining combines transaction authentication with seignorage.



How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addesses. The Bitcoin client signs her transaction request with the private key of the address she's transfering bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

* Each new hash value contains information about all previous Bitcoin transactions.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil → 6d0a 1899 086a... (56 more characters)

The root of all evil → 486c 6be4 6dde...

The root of all veil → b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ??? → 0000 0000 0000...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

A Brief History of Mining

Mining has moved at Bitcoin time, recapitulating the entire history of computer development in a few years.

CPU

2009-2010

GPU

2010-2013

FPGA

2011-2013

DESKTOP ASIC

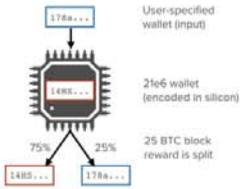
2013-2014

ASIC FARM (21E6)

2013-2014

THE NEXT STEP

2015 onward...



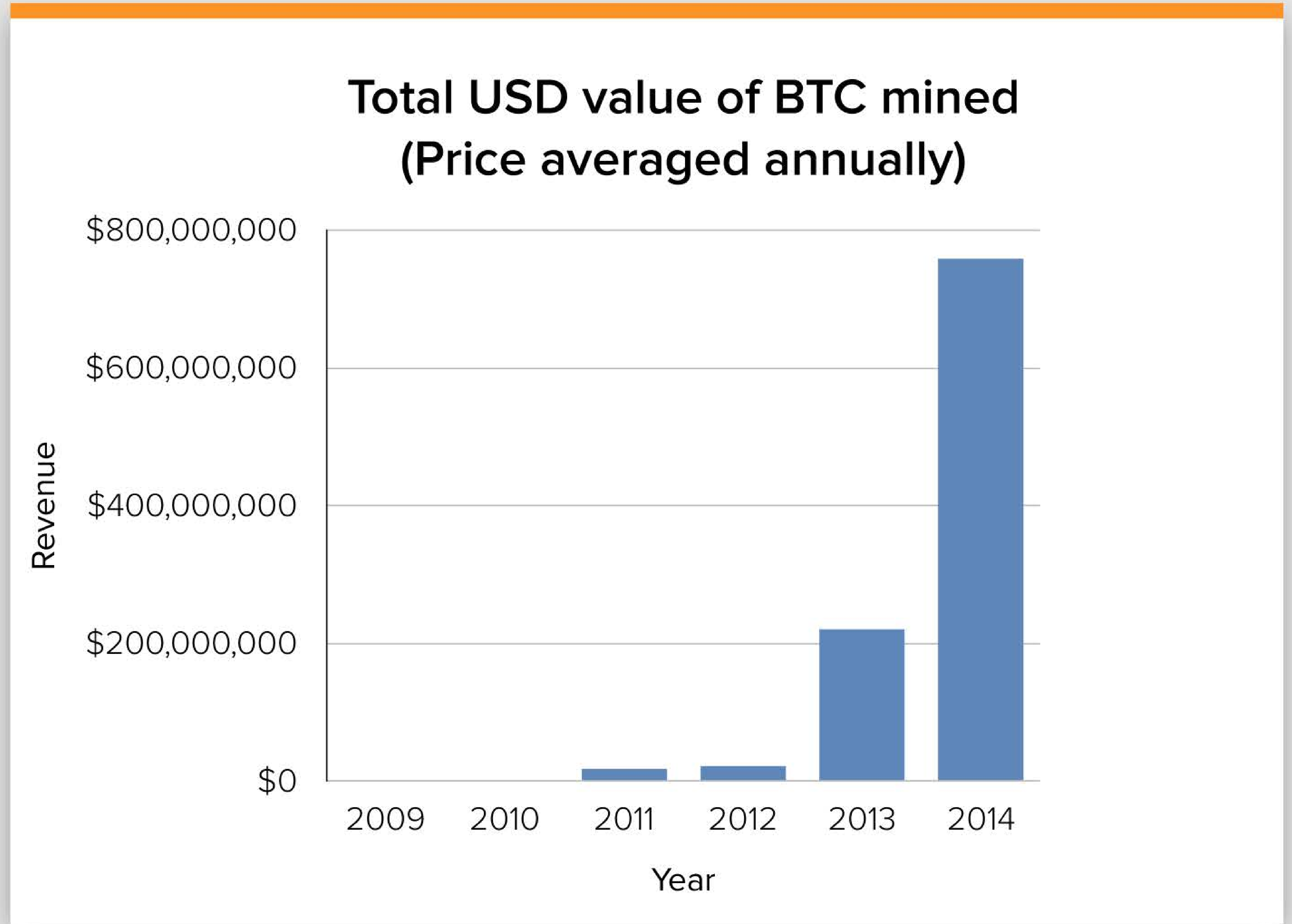
User-specified wallet (input)

21e6 wallet (encoded in silicon)

25 BTC block reward is split

Mining is Growing Exponentially

Any market that goes from $0 to $750M+ in four years is worth taking seriously.

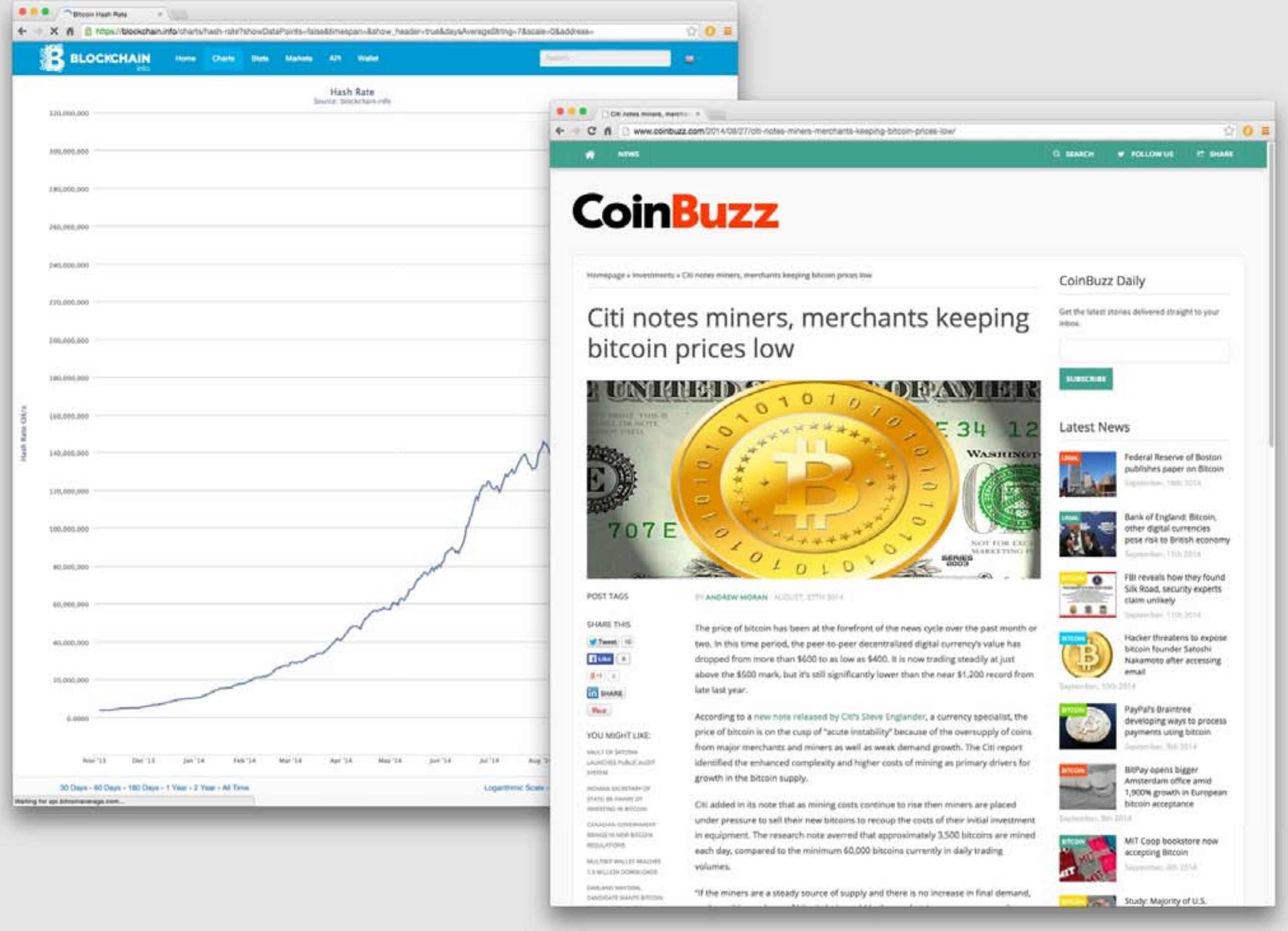


Incredible growth, even with price volatility

From $0 in 2010 to $750M+ in 2014!

Problem

Mining has thus become very competitive: hash rate is up 100X Y/Y. Because miners selling to pay electricity, price temporarily depressed.



Homepage » Investments » Citi notes miners, merchants keeping bitcoin prices low

Citi notes miners, merchants keeping bitcoin prices low

BY ANDREW MORAN . AUGUST, 27TH 2014

The price of bitcoin has been at the forefront of the news cycle over the past month or two. In this time period, the peer-to-peer decentralized digital currency's value has dropped from more than $600 to as low as $400. It is now trading steadily at just above the $500 mark, but it's still significantly lower than the near $1,200 record from late last year.

According to a new note released by Citi's Steve Englander, a currency specialist, the price of bitcoin is on the cusp of "acute instability" because of the oversupply of coins from major merchants and miners as well as weak demand growth. The Citi report identified the enhanced complexity and higher costs of mining as primary drivers for growth in the bitcoin supply.

Citi added in its note that as mining costs continue to rise then miners are placed under pressure to sell their new bitcoins to recoup the costs of their initial investment in equipment. The research note averred that approximately 3,500 bitcoins are mined each day, compared to the minimum 60,000 bitcoins currently in daily trading volumes.

"If the miners are a steady source of supply and there is no increase in final demand,

YOU MIGHT LIKE:

VAULT OF SATOSHI LAUNCHES PUBLIC AUDIT SYSTEM

INDIANA SECRETARY OF STATE: BE AWARE OF INVESTING IN BITCOIN

CANADIAN GOVERNMENT BRINGS IN NEW BITCOIN REGULATIONS

MULTIBIT WALLET REACHES 1.5 MILLION DOWNLOADS

OAKLAND MAYORAL CANDIDATE WANTS BITCOIN

CoinBuzz Daily

Get the latest stories delivered straight to your inbox.

Latest News

LEGAL Federal Reserve of Boston publishes paper on Bitcoin
September, 16th 2014

LEGAL Bank of England: Bitcoin, other digital currencies pose risk to British economy
September, 11th 2014

BITCOIN FBI reveals how they found Silk Road, security experts claim unlikely
September, 11th 2014

BITCOIN Hacker threatens to expose bitcoin founder Satoshi Nakamoto after accessing email
September, 10th 2014

BITCOIN PayPal's Braintree developing ways to process payments using bitcoin
September, 9th 2014

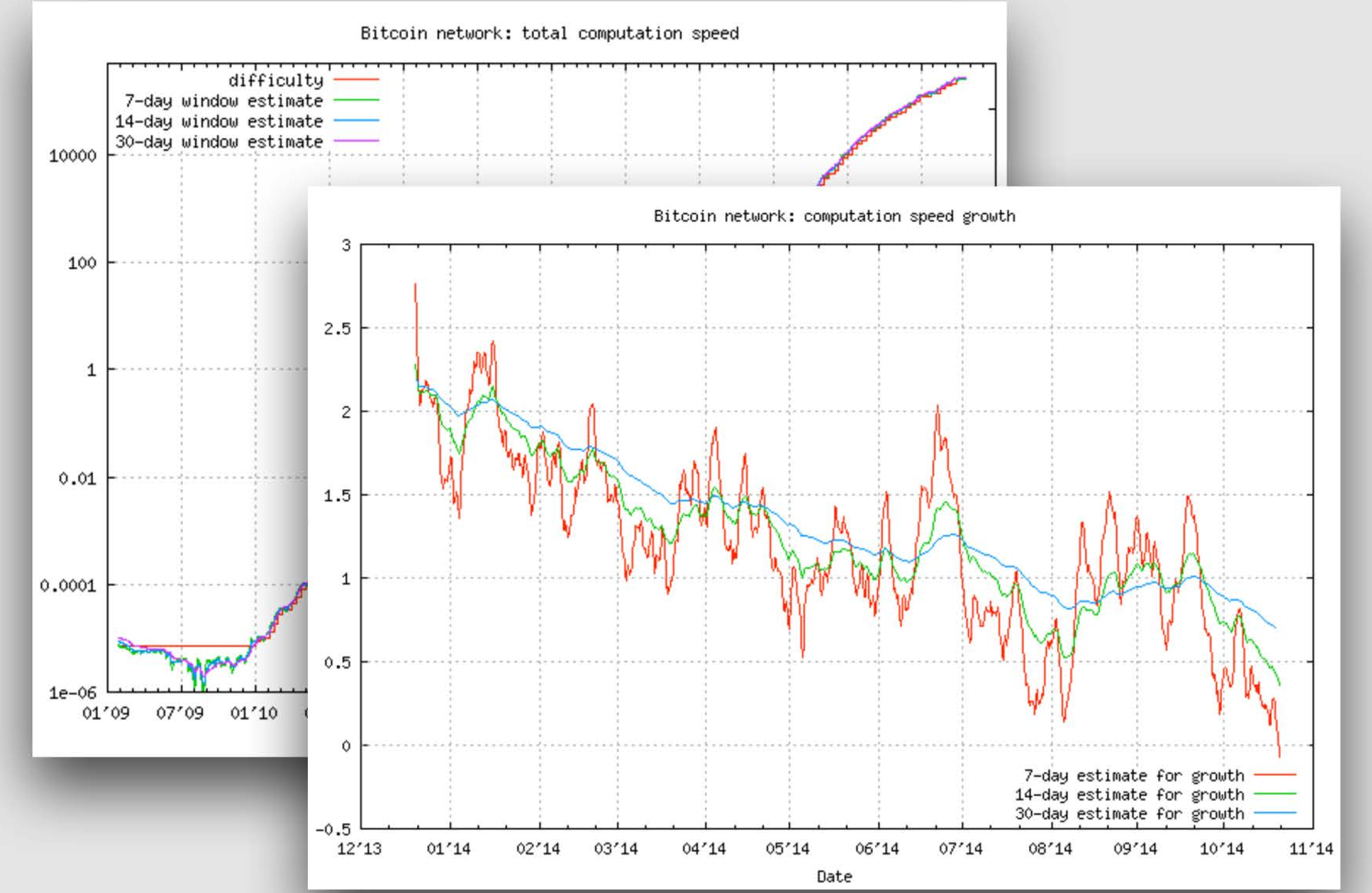
BITCOIN BitPay opens bigger Amsterdam office amid 1,900% growth in European bitcoin acceptance
September, 8th 2014

BITCOIN MIT Coop bookstore now accepting Bitcoin
September, 8th 2014

BITCOIN Study: Majority of U.S.

Partial Solution

A mining shakeout is happening, and hashrate growth is slowing. Moore's law now a limit. And 21E6 is the only miner w/ Intel fab chip.



- Cost for new company to enter is now prohibitive
- Bitcoin mining consumes more power than Google in 2011!
- Hashrate growth rapidly decelerating. Daily growth under 0.5%, down from 2%
- Limits to growth: technology, capital, power, scale

Partial Solution

A mining shakeout is happening, and hashrate growth is slowing. Moore's law now a limit. And 21E6 is the only miner w/ Intel fab chip.

	Best Today	Max	Gain	Notes
Tech	.22 W / Gh/s at 22nm (21E6)	~.15 W/ GH/s at 14nm	**1-2X**	21E6 v2: 0.57 W / GH/s 21E6 v3: 0.22 W / GH/s **Moore's law limits first**
Power	~300 MW (176 PH/s)	10+ GW (10 nuclear plants)	>100 X	10X may be noticeable (esp outside 1st world) 10 GW = 1% of world
Capital	~$1.5M / PH/s ~$500M-$1B?	VC: 15-25B/year Consumer: 100B+ / year	>10-100X	Many individual miners today
Nodes	~40k ASIC servers, 1e6 chips (21E6)	Goog alone: 2.5M CPU servers	>100 X	Loosest upper bound here

Approaching Moore's law: best efficiency likely ~0.15 W / GH/s @ 14nm

- Cost for new company to enter is now prohibitive
- Bitcoin mining consumes more power than Google in 2011!
- Hashrate growth rapidly decelerating. Daily growth under 0.5%, down from 2%
- Limits to growth: technology, capital, power, scale

21E6 vs. the Competition

We already enjoy a significant technological advantage, and are the only chip built at Intel's custom foundry.

Competitor	Location	Technology	W / GH/s	Notes
Bitfury	Georgia	55nm UMC	0.8	28nm chip failed; recently raised $20m
KNCMiner	Sweden	20nm TSMC	0.6	Chip below spec; de-focused with altcoin miner
AntMiner	China	28nm	0.8	Primarily equipment vendor; targeting home miners
ASICMiner	China	40nm	1.1	Chip below spec; cash-flow issues
Spondoolies	Israel	28nm TSMC	0.65	Chip below spec; equipment vendor only
Cointerra	US	28nm GF	1.1	Chip below spec; being sued by customers
21E6 (v2)	**US**	**22nm Intel**	**0.57**	**First and only Intel FinFET Bitcoin chip**
21E6 (v3)	**US**	**22nm Intel**	**0.22**	**Taped out 8/24, silicon due in November**

Approaching Moore's law: best efficiency is likely ~0.15 W / GH/s @ 14nm

Doubling Down is One Approach

So given ongoing shakeout, under many scenarios, simply scaling existing business is a reasonable alternative.

	IO (V1->V3)	CyrusOne (V2)	Brownfield (V3)
System Cost	$2,000	0	$2,450
Number of Systems	3250	7904	1900
System Speed (TH/s)	5.2	2	5.2
Power/System (kW)	1.3	1.3	1.3
Deployment Cost	$120,000	0	$250,000
Rent ($/KW/month)	90	80	3
Electricity Rate ($/kWh)	0.09	0.075	0.05
Deployment Month	Jan 2015	Already Deployed	Mar 2015
Turn-off Month	Aug 2016	Apr 2015	Beyond Nov 2017
Total Expense	$18,392,540	$6,884,384	$7,891,230
BTC Generated	55,528	32,272	30,427
USD Generated	$50,796,729	$32,512,126	$27,834,559
USD Profit	$32,404,189	$24,250,865	$19,943,329
Cost per BTC	$331.23	$232.45	$259.35
Avg BTC Price in Period	$456.21	$362.32	$600.35

Assumptions

Hashrate growth tied to BTC appreciation, with delay

Some additional, slowing irrationality in hashrate growth

BTC price flat through Q1 2015, then slow appreciation

USD numbers based on BTC hold, sell in Nov 2017

Q: But how do we put it completely out of reach?
Is there a way to make Bitcoin mining an unfair fight?

But can we put mining out of reach?

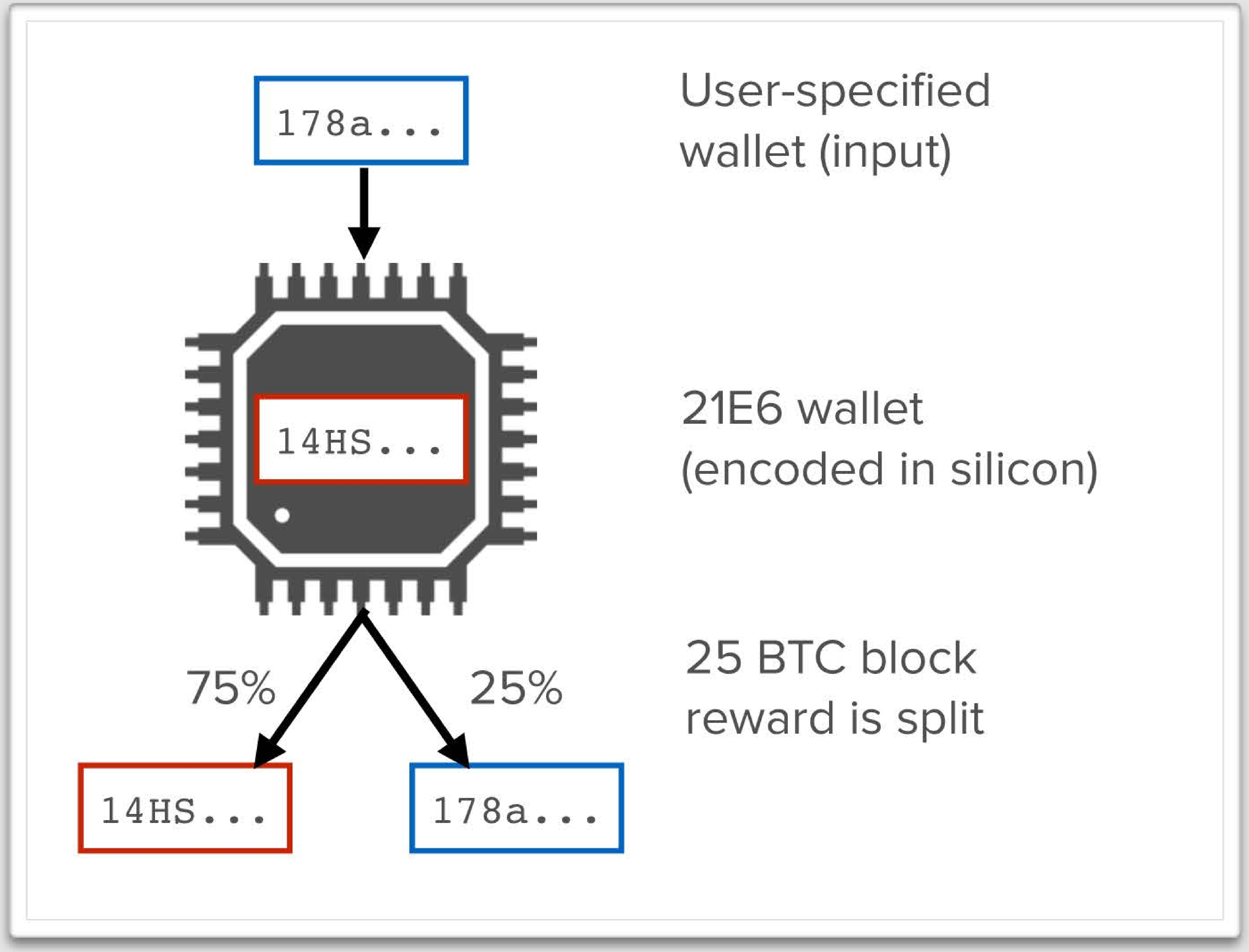
Is there any way to decommoditize Bitcoin mining?

Yes.

Introducing the 21E6 BitSplit chip.

The BitSplit Distributed Mining Chip

An embeddable version of our DC chip that exploits a protocol subtlety: mining proceeds can be sent to multiple accounts.



User-specified wallet (input)

21E6 wallet (encoded in silicon)

25 BTC block reward is split

How the 21E6 BitSplit Network Works

The existing 21E6 datacenters are crucial. The initial critical mass of mining (at least >1%) is required to bootstrap a mining pool.

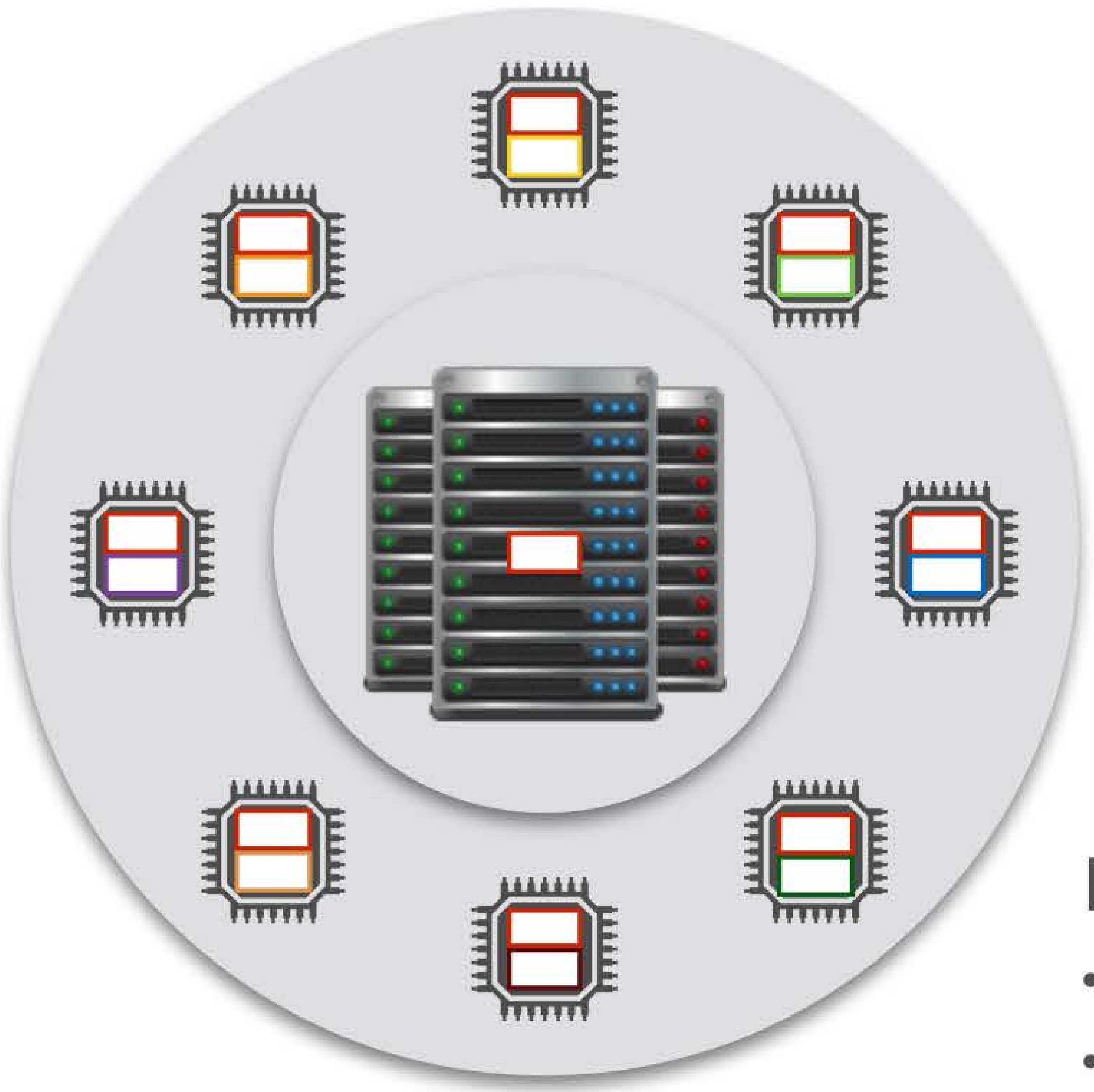
21E6 datacenters

- Core of pool
- 20,000+ servers
- ~3-5% of mining
- 26+ MW
- Guarantee blocks

Bitcoin inside

How the 21E6 BitSplit Network Works

The network of all BitSplit chips now connects to that pool. Each has a different user wallet address for depositing BTC.



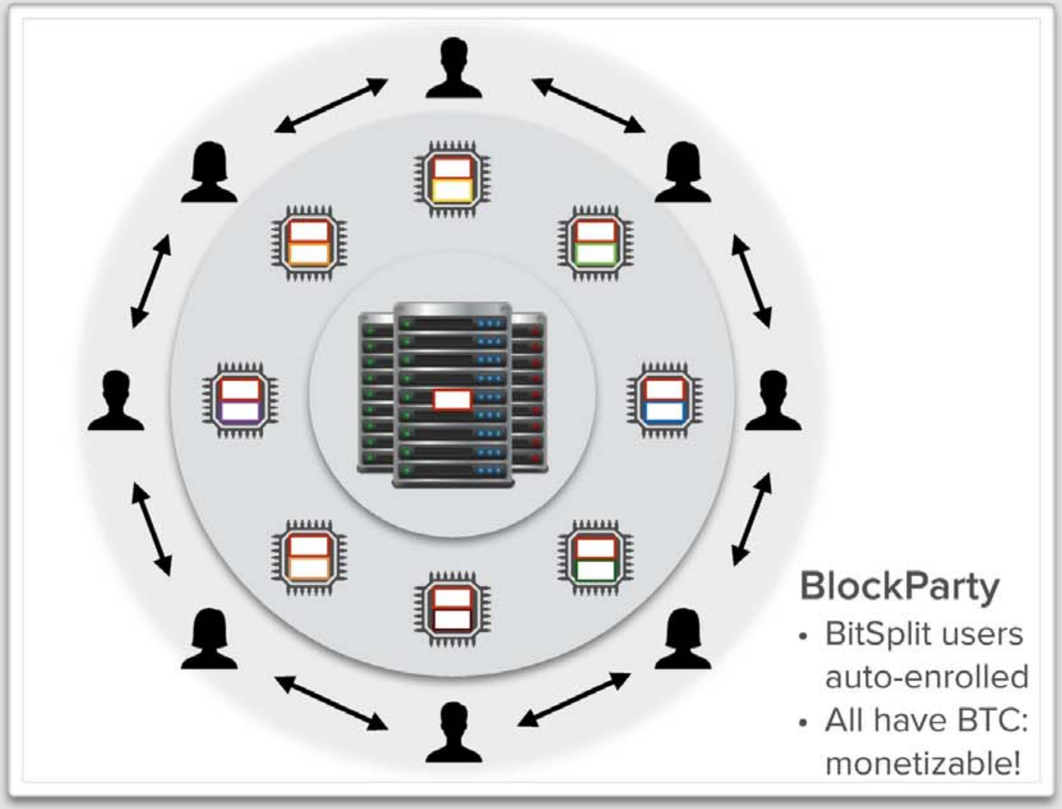
BitSplit chips

- Connect to pool
- Get pro-rata BTC
- "Zero opex"
- Huge scalability

Bitcoin inside

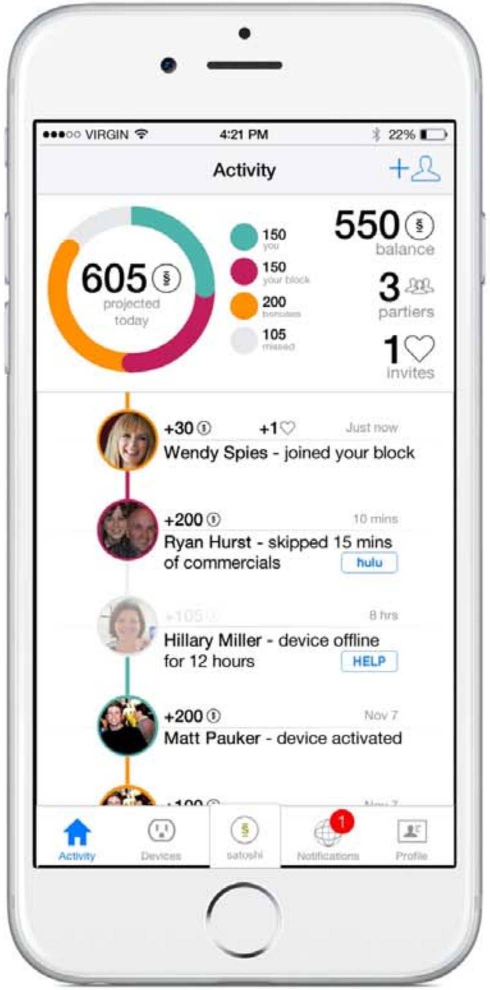
How the 21E6 BitSplit Network Works

Observation: the BitSplit pool is a social network in embryo.
Introducing BlockParty, the 21E6 social network.



BlockParty

- BitSplit users auto-enrolled
- All have BTC: monetizable!



+30 +1 Just now
Wendy Spies - joined your block

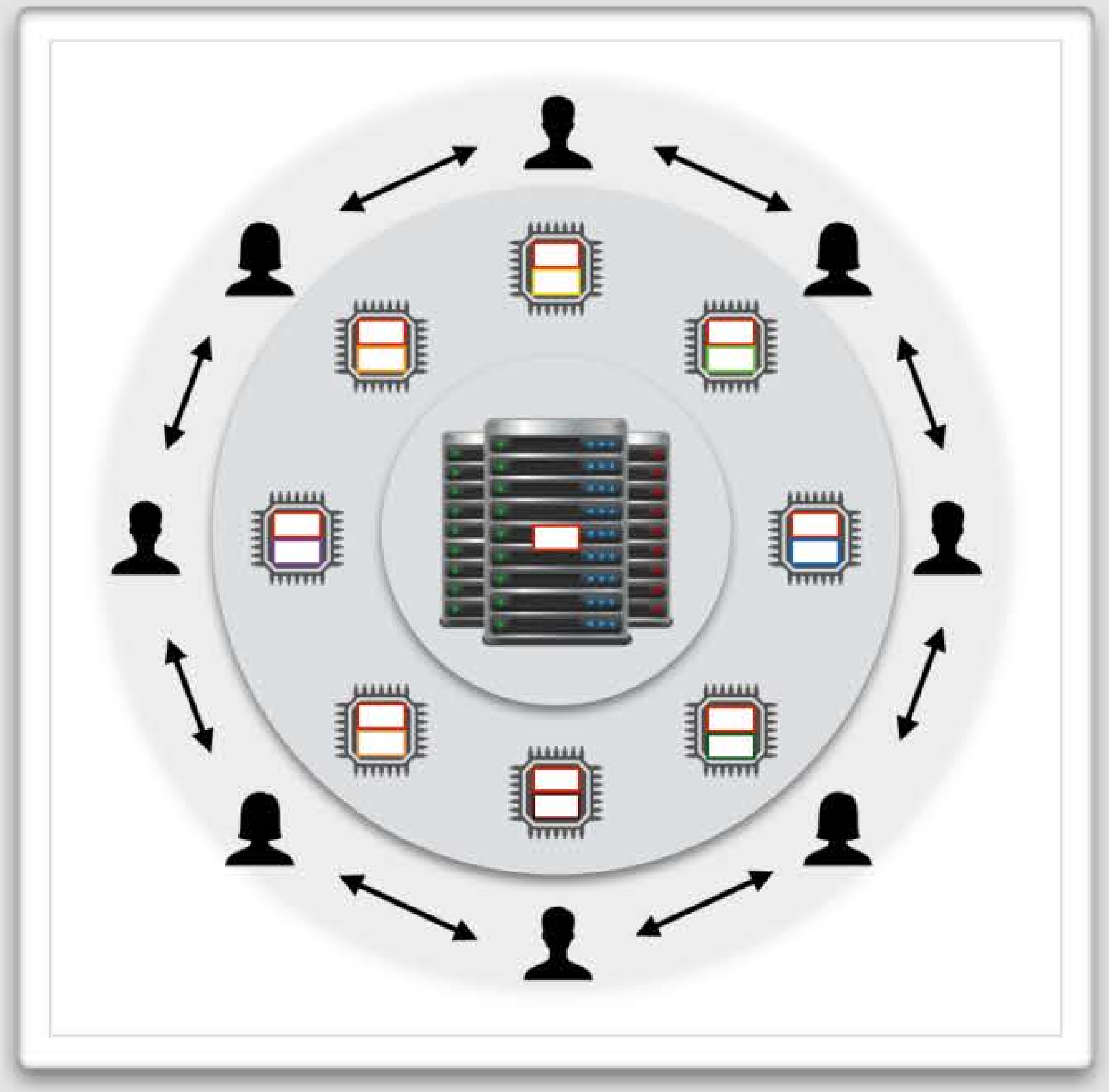
+200 10 mins
Ryan Hurst - skipped 15 mins of commercials hulu

+105 8 hrs
Hillary Miller - device offline for 12 hours HELP

+200 Nov 7
Matt Pauker - device activated

Our Datacenters Enable BitSplit

Without the datacenter core, the BitSplit chip wouldn't work. Only a pool provides the critical mass to win blocks reliably.



	No Pool	Pool
Hash %	0.00002% (chip)	0.00002% (chip) + 5% (pool)
Time to block	**34,722 days**	**~200 minutes**
Mean BTC/day	0.72 mBTC	0.72 mBTC
Median BTC/day	**0 mBTC**	**0.72 mBTC**

Calculations for 50 GH/s BitSplit, 5% pool, 250 PH/s global

Where a BitSplit Goes

A BitSplit can be embedded in a variety of line-powered devices, from our first-party USB hub to laptops to Sony Playstations.

USB HUB
BTC for applications

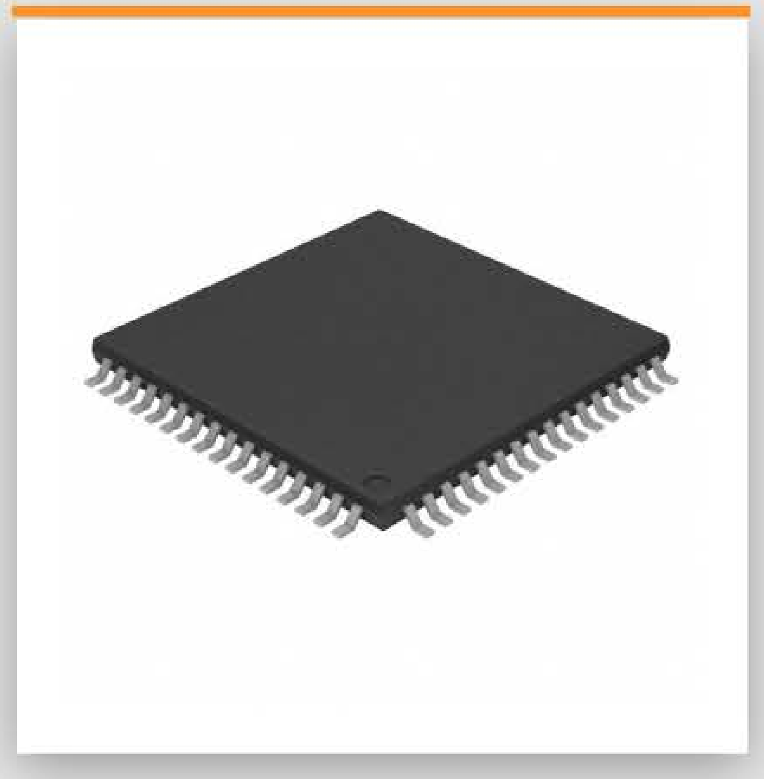
PC
BTC for applications

ROUTER
BTC for bandwidth

GAME CONSOLE
BTC for in-game purchases

PHONE CHARGER
BTC for mobile apps

DIRECT CHIPSET
Zero opex and capex



"There is no reason for any individual to have a computer in their home."

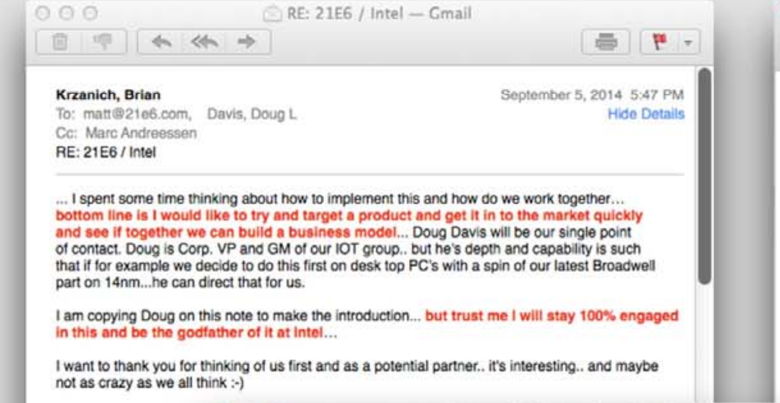
Ken Olsen, DEC (1977)

"A computer on every desk and in every home."

Bill Gates, Microsoft (1977)

Customer Pipeline

Any hardware manufacturer is a potential customer for the BitSplit chip. Those that own fabs are even better.



RE: 21E6 / Intel — Gmail

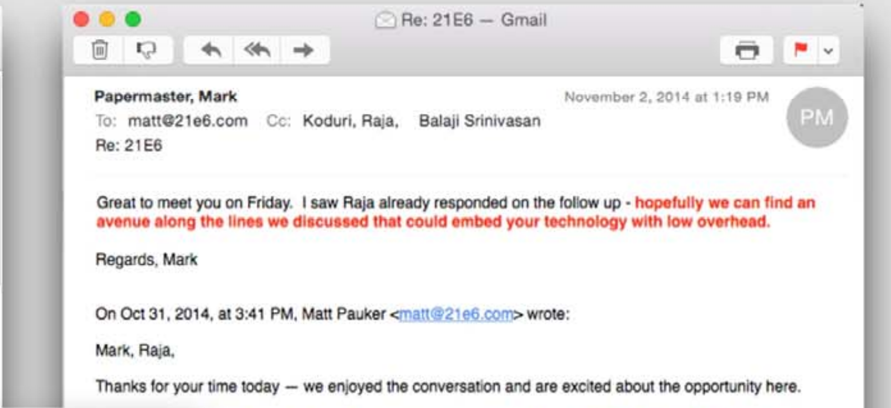
Krzanich, Brian September 5, 2014 5:47 PM
To: matt@21e6.com, Davis, Doug L
Cc: Marc Andreessen
RE: 21E6 / Intel

... I spent some time thinking about how to implement this and how do we work together... **bottom line is I would like to try and target a product and get it in to the market quickly and see if together we can build a business model**... Doug Davis will be our single point of contact. Doug is Corp. VP and GM of our IOT group.. but he's depth and capability is such that if for example we decide to do this first on desk top PC's with a spin of our latest Broadwell part on 14nm...he can direct that for us.

I am copying Doug on this note to make the introduction... **but trust me I will stay 100% engaged in this and be the godfather of it at Intel**...

I want to thank you for thinking of us first and as a potential partner.. it's interesting.. and maybe not as crazy as we all think :-)

BK



Re: 21E6 — Gmail

Papermaster, Mark November 2, 2014 at 1:19 PM
To: matt@21e6.com Cc: Koduri, Raja, Balaji Srinivasan
Re: 21E6

Great to meet you on Friday. I saw Raja already responded on the follow up - **hopefully we can find an avenue along the lines we discussed that could embed your technology with low overhead.**

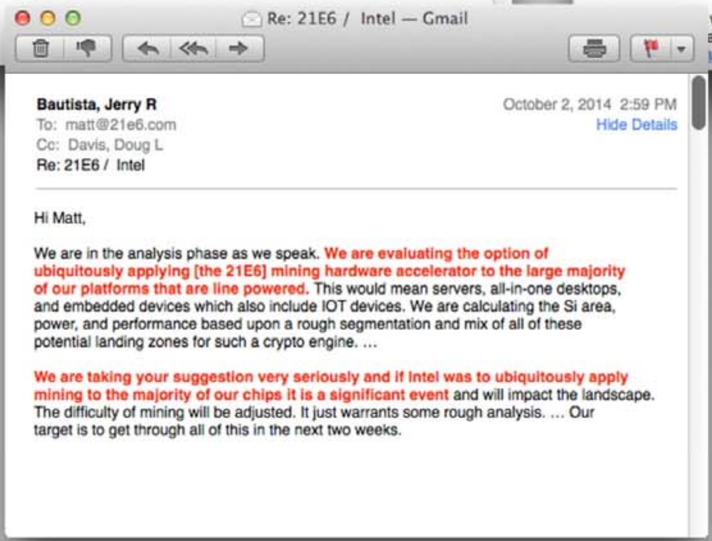
Regards, Mark

On Oct 31, 2014, at 3:41 PM, Matt Pauker <matt@21e6.com> wrote:

Mark, Raja,

Thanks for your time today — we enjoyed the conversation and are excited about the opportunity here.

was too large for email, so I've uploaded it here: https://docsend.com/view/9ejfyzs. We've
a recorded version of the bandwidth auction
ayer.vimeo.com/video/109632262. Please let us know if you have any questions.



Re: 21E6 / Intel — Gmail

Bautista, Jerry R October 2, 2014 2:59 PM
To: matt@21e6.com
Cc: Davis, Doug L
Re: 21E6 / Intel

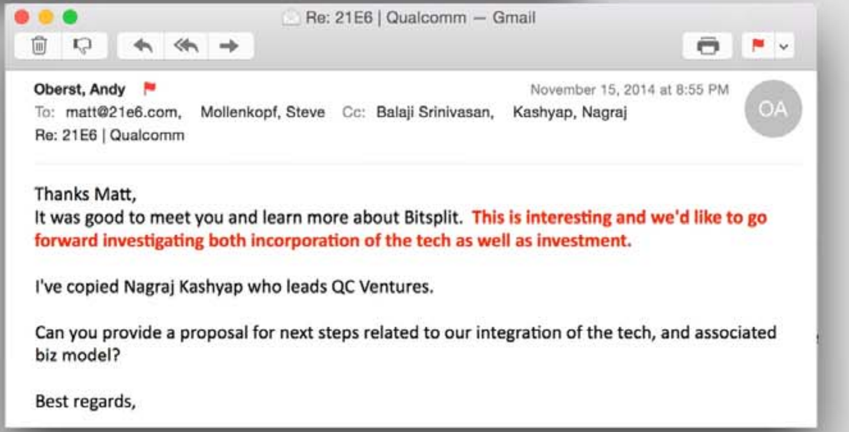
Hi Matt,

We are in the analysis phase as we speak. **We are evaluating the option of ubiquitously applying [the 21E6] mining hardware accelerator to the large majority of our platforms that are line powered.** This would mean servers, all-in-one desktops, and embedded devices which also include IOT devices. We are calculating the Si area, power, and performance based upon a rough segmentation and mix of all of these potential landing zones for such a crypto engine. ...

We are taking your suggestion very seriously and if Intel was to ubiquitously apply mining to the majority of our chips it is a significant event and will impact the landscape. The difficulty of mining will be adjusted. It just warrants some rough analysis. ... Our target is to get through all of this in the next two weeks.

Additional C-level discussions with:

- Cisco
- Facebook
- IBM



Re: 21E6 | Qualcomm — Gmail

Oberst, Andy November 15, 2014 at 8:55 PM
To: matt@21e6.com, Mollenkopf, Steve Cc: Balaji Srinivasan, Kashyap, Nagraj
Re: 21E6 | Qualcomm

Thanks Matt,
It was good to meet you and learn more about Bitsplit. **This is interesting and we'd like to go forward investigating both incorporation of the tech as well as investment.**

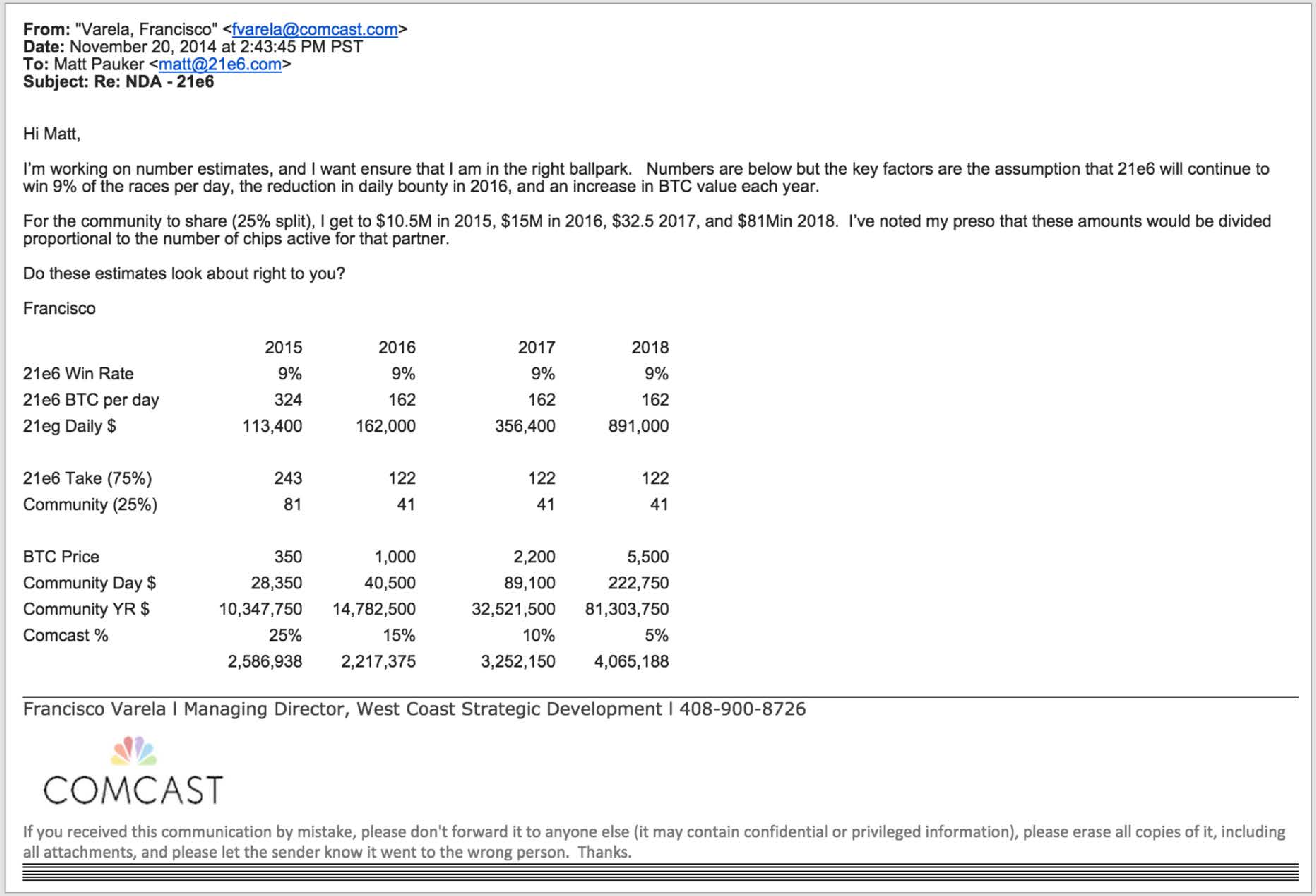
I've copied Nagraj Kashyap who leads QC Ventures.

Can you provide a proposal for next steps related to our integration of the tech, and associated biz model?

Best regards,

Customer Pipeline

Any hardware manufacturer is a potential customer for the BitSplit chip. Those that own fabs are even better.



From: "Varela, Francisco" <fvarela@comcast.com>
Date: November 20, 2014 at 2:43:45 PM PST
To: Matt Pauker <matt@21e6.com>
Subject: Re: NDA - 21e6

Hi Matt,

I'm working on number estimates, and I want ensure that I am in the right ballpark.   Numbers are below but the key factors are the assumption that 21e6 will continue to win 9% of the races per day, the reduction in daily bounty in 2016, and an increase in BTC value each year.

For the community to share (25% split), I get to $10.5M in 2015, $15M in 2016, $32.5 2017, and $81Min 2018. I've noted my preso that these amounts would be divided proportional to the number of chips active for that partner.

Do these estimates look about right to you?

Francisco

	2015	2016	2017	2018
21e6 Win Rate	9%	9%	9%	9%
21e6 BTC per day	324	162	162	162
21eg Daily $	113,400	162,000	356,400	891,000
21e6 Take (75%)	243	122	122	122
Community (25%)	81	41	41	41
BTC Price	350	1,000	2,200	5,500
Community Day $	28,350	40,500	89,100	222,750
Community YR $	10,347,750	14,782,500	32,521,500	81,303,750
Comcast %	25%	15%	10%	5%
	2,586,938	2,217,375	3,252,150	4,065,188

Francisco Varela I Managing Director, West Coast Strategic Development I 408-900-8726

COMCAST

If you received this communication by mistake, please don't forward it to anyone else (it may contain confidential or privileged information), please erase all copies of it, including all attachments, and please let the sender know it went to the wrong person. Thanks.

The Implications of BitSplit

We've figured out how to mainstream Bitcoin while decommoditizing mining.

FOR 21E6

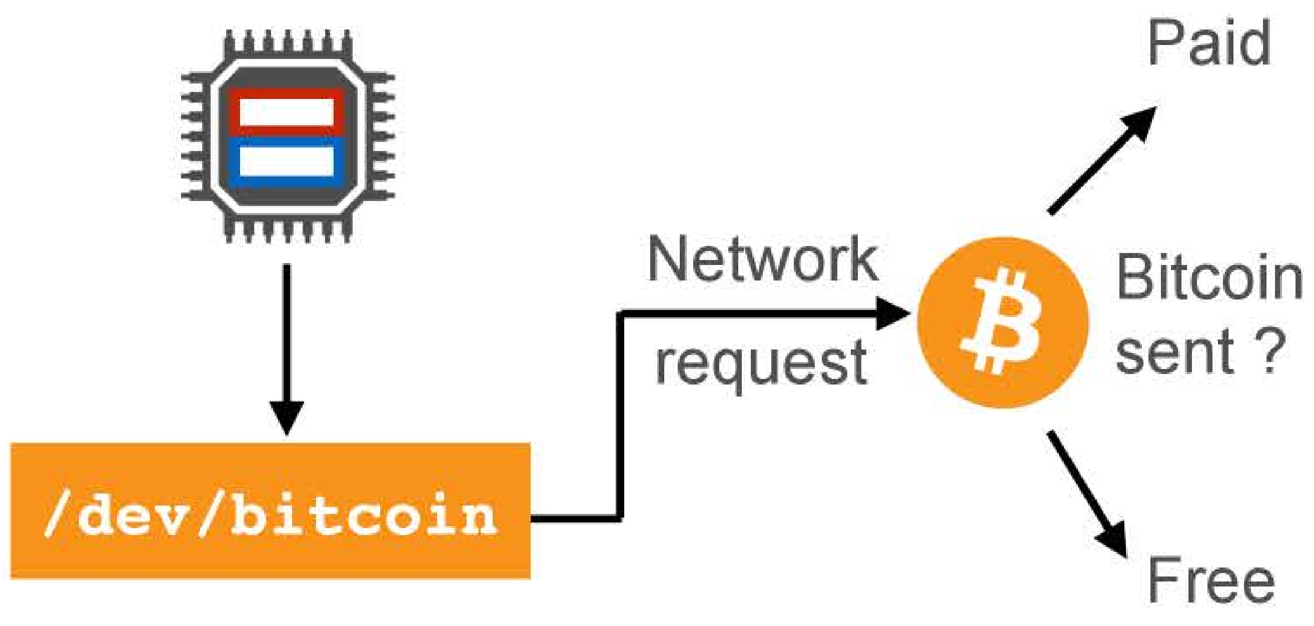
A transformatively lower cost of mining

FOR OEMs

Increased sales from Bitcoin hardware

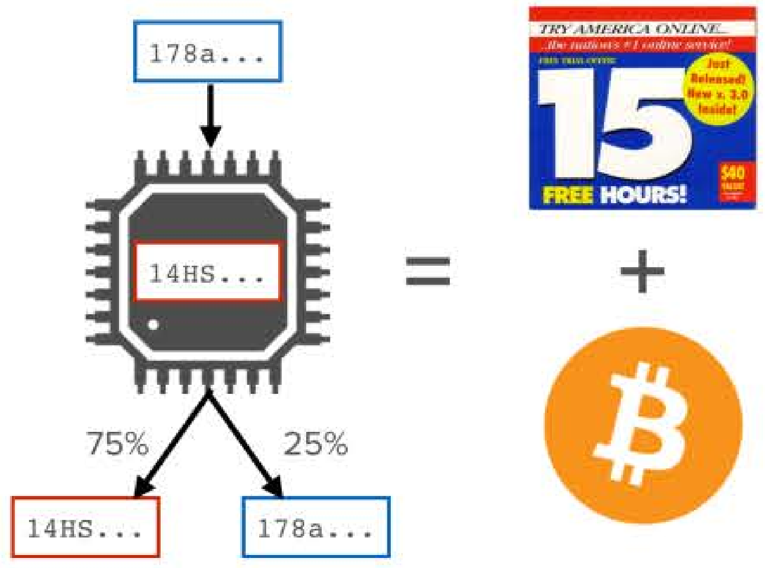
FOR USERS

Infinite BTC by default for applications



FOR EVERYONE

Mainstreams protocol: "AOL CD of Bitcoin"



For 21E6: BitSplit Decommoditizes Mining

To understand why, let's review up-front (capex) & recurring (opex) costs for different mining paradigms.

Platform	Our per-unit capex	Our per-unit opex	Our BTC share	Our BTC price	Estimated impact on USD/BTC price
Desktop (sell)	<$0 (user pays)	$0 (user pays)	0%	infinite	No share of BTC mined
Desktop (buy)	high	high	100%	high	Not space/power efficient
ASIC farm	lower	lower	100%	lower	Negative (opex sell off)
BitSplit device	$8-40	$0 (user pays)	~75%	low	Positive (no sell off)
BitSplit chipset	$0	$0 (user pays)	~75%	lowest	Highly positive (default)

DESKTOP MINER

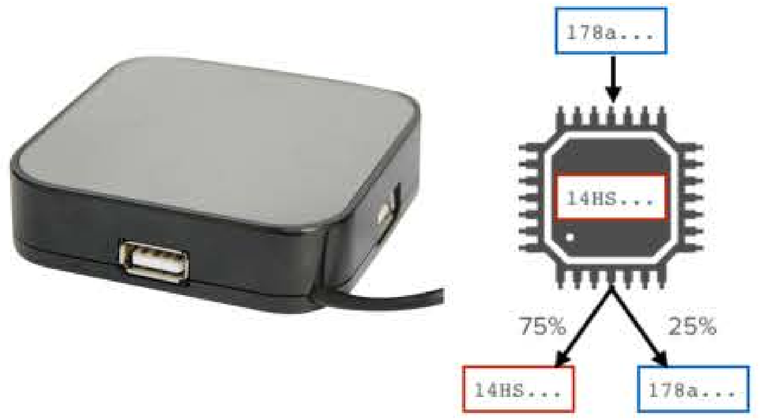
Single-purpose

ASIC FARM

Datacenter

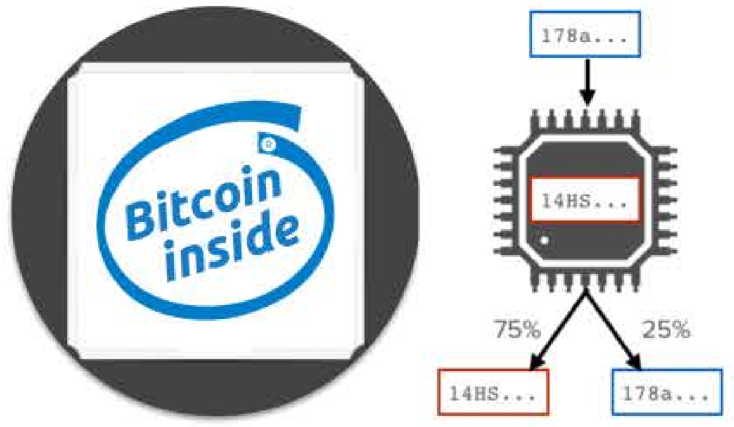
BITSPLIT DEVICE

Multifunctional w/ BTC



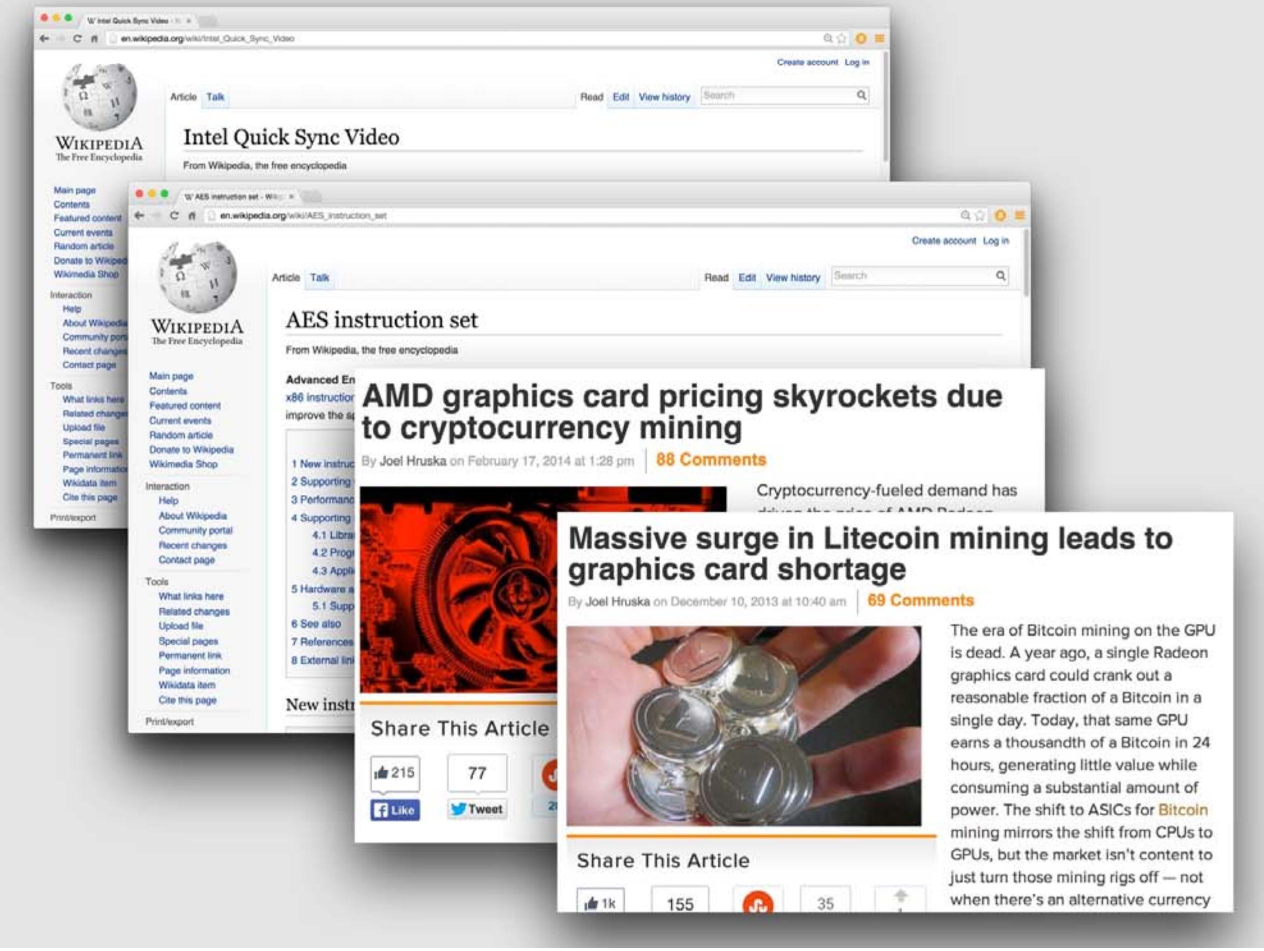
BITSPLIT CHIPSET

Available by default



For OEM: BitSplit means sales (and/or BTC)

Built-in support for next big thing likely means sales bump.
Examples: H.264, AES encoding/decoding, and Bitcoin GPUs.



Intel Quick Sync Video

From Wikipedia, the free encyclopedia

AES instruction set

From Wikipedia, the free encyclopedia

Advanced En
x86 instructior
improve the s

1 New instruc
2 Supporting
3 Performanc
4 Supporting
4.1 Libra
4.2 Progr
4.3 Appli
5 Hardware a
5.1 Supp
6 See also
7 References
8 External lin

New instr

AMD graphics card pricing skyrockets due to cryptocurrency mining

By Joel Hruska on February 17, 2014 at 1:28 pm | 88 Comments

Cryptocurrency-fueled demand has

Massive surge in Litecoin mining leads to graphics card shortage

By Joel Hruska on December 10, 2013 at 10:40 am | 69 Comments

The era of Bitcoin mining on the GPU is dead. A year ago, a single Radeon graphics card could crank out a reasonable fraction of a Bitcoin in a single day. Today, that same GPU earns a thousandth of a Bitcoin in 24 hours, generating little value while consuming a substantial amount of power. The shift to ASICs for Bitcoin mining mirrors the shift from CPUs to GPUs, but the market isn't content to just turn those mining rigs off — not when there's an alternative currency

Unbeatable Economics

1st-party device economics similar to DC; OEM economics are unbeatable…other than BitSplit Inside.

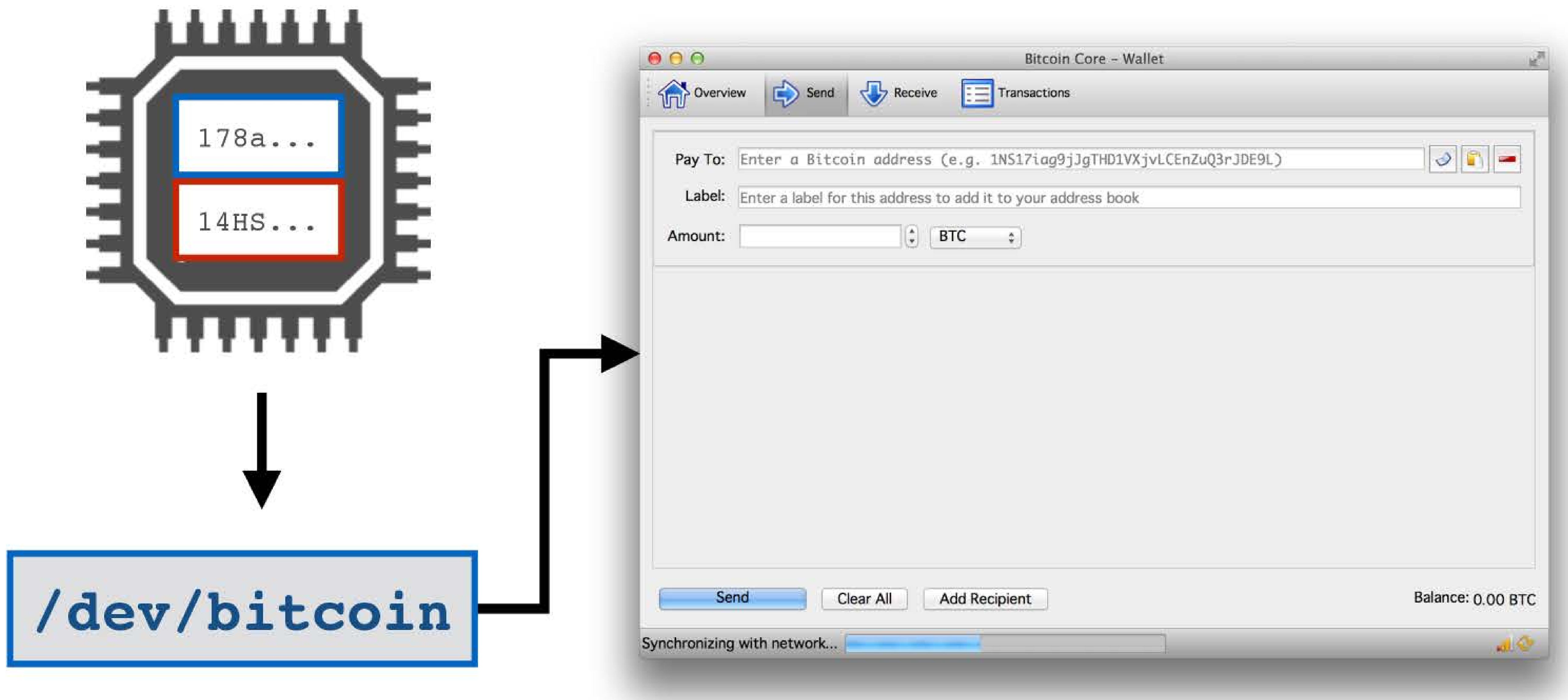
	IO (V1->V3)	CyrusOne (V2)	Brownfield (V3)	BitSplit Charger	BitSplit Chip	BitSplit Inside
System Cost	$2,000	0	$2,450	$35	$8	$0
Number of Systems	3250	7904	1900	250,000	1,000,000	10,000,000
System Speed (TH/s)	5.2	2	5.2	0.0375	0.0625	0.02
Power/System (kW)	1.3	1.3	1.3	0.015	0.015	0.005
Deployment Cost	$120,000	0	$250,000	0	0	0
Rent ($/KW/month)	90	80	3	0	0	0
Electricity Rate ($/kWh)	0.09	0.075	0.05	0	0	0
Other Monthly Opex						0.01
Deployment Month	Jan 2015	Already Deployed	Mar 2015	Mar 2015	Aug 2015	Oct 2015
Turn-off Month	Aug 2016	Apr 2015	Beyond Nov 2017	Beyond Nov 2017	Beyond Nov 2017	Beyond Nov 2017
Total Expense	$18,392,540	$6,884,384	$7,891,230	$8,750,000	$8,000,000	$100,000
BTC Generated	55,528	32,272	30,427	28,872	121,839	322,360
USD Generated	$50,796,729	$32,512,126	$27,834,559	$26,411,842	$111,457,994	$294,895,040
USD Profit	$32,404,189	$24,250,865	$19,943,329	$17,661,842	$103,457,994	$292,495,040
Cost per BTC	$331.23	$232.45	$259.35	$303.06	**$65.66**	**$7.45**
Avg BTC Price in Period	$456.21	$362.32	$600.35	$600.35	$639.57	$656.30

For Users: BTC By Default

For users, an embedded BitSplit provides **`/dev/bitcoin`**, a continually replenished source of Bitcoin for applications.

BitSplit chip

Bitcoin app (such as a client)



Pay To: Enter a Bitcoin address (e.g. 1NS17iag9jJgTHD1VXjvLCEnZuQ3rJDE9L)

Label: Enter a label for this address to add it to your address book

Amount: BTC

Balance: 0.00 BTC

Synchronizing with network...

Provides constantly replenished source of BTC

Example: a bundled Bitcoin client can now send/receive out of box

/dev/random

From Wikipedia, the free encyclopedia

In Unix-like operating systems, **/dev/random** is a special file that serves as a blocking pseudorandom number generator. It allows access to environmental noise collected from device drivers and other sources.[1] Not all operating systems implement the same semantics for /dev/random.

Special device files

- /dev/full
- /dev/null
- **/dev/random and /dev/urandom**
- /dev/zero

This box: view · talk · edit

Contents [hide]

1 Linux
2 FreeBSD
3 OpenBSD
4 Mac OS X and iOS
5 Other operating systems
6 EGD as an alternative
7 See also
8 References
9 External links

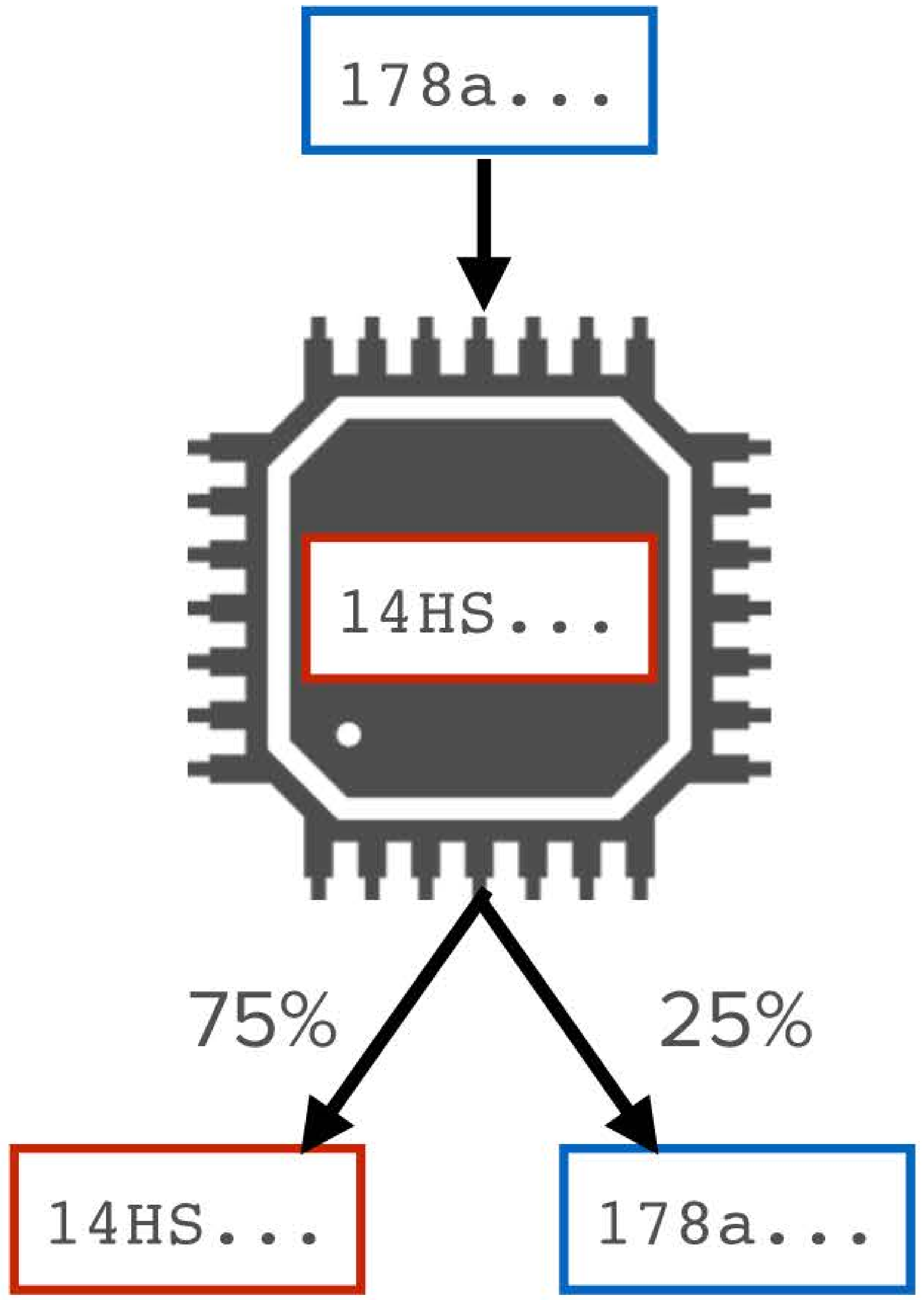
The Unit Economics of BitSplit

Under a wide range of assumptions, BitSplits produce annual per-user gross revenue comparable to Facebook's annual RPU ($8.84)

Bitcoin Price (USD/BTC)

Hashrate (PH/s)	$300	$500	$1000	$2000	Satoshis
256	$76.99	$128.32	$256.64	$513.28	25.6M
512	$38.50	$64.16	$128.32	$256.64	12.8M
1024	$19.25	$32.08	$64.16	$128.32	6.4M
2048	$9.62	$16.04	$32.08	$64.16	3.2M
4096	$4.81	$8.02	$16.04	$32.08	1.6M

Per-user gross revenue for 50 GH/s BitSplit



$$R = \frac{H}{H+G} NBTP$$

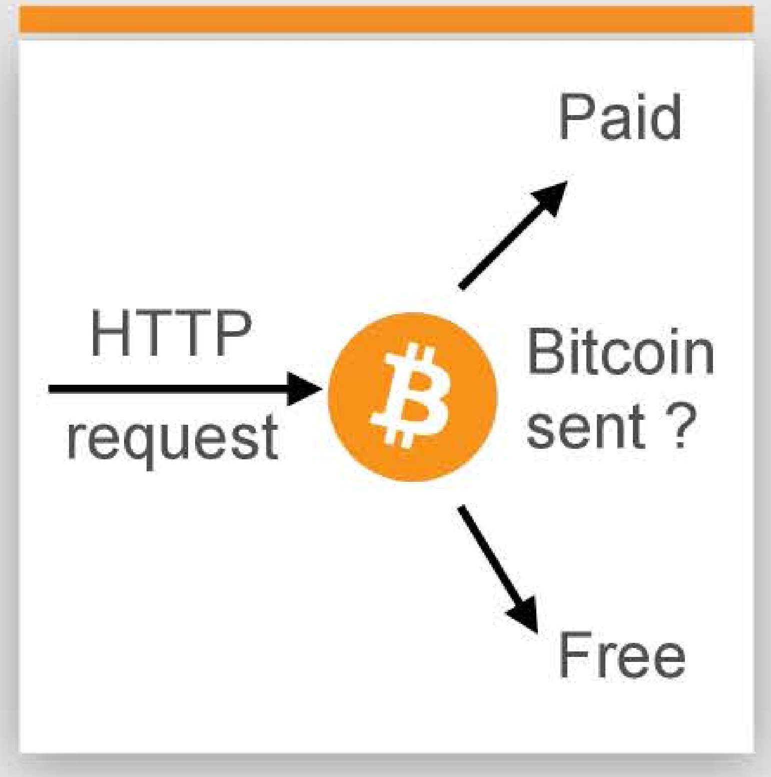
R : Gross annual revenue
H : Bitsplit hashrate, 50 GH/s
G : Global hashrate
N : 144 blocks per day
B : 25 BTC per block
T : 365 days per year
P : USD/BTC price

For Users: BitSplit Enables Applications

Default hardware and software support for the next major Internet protocol enables a wide suite of applications.

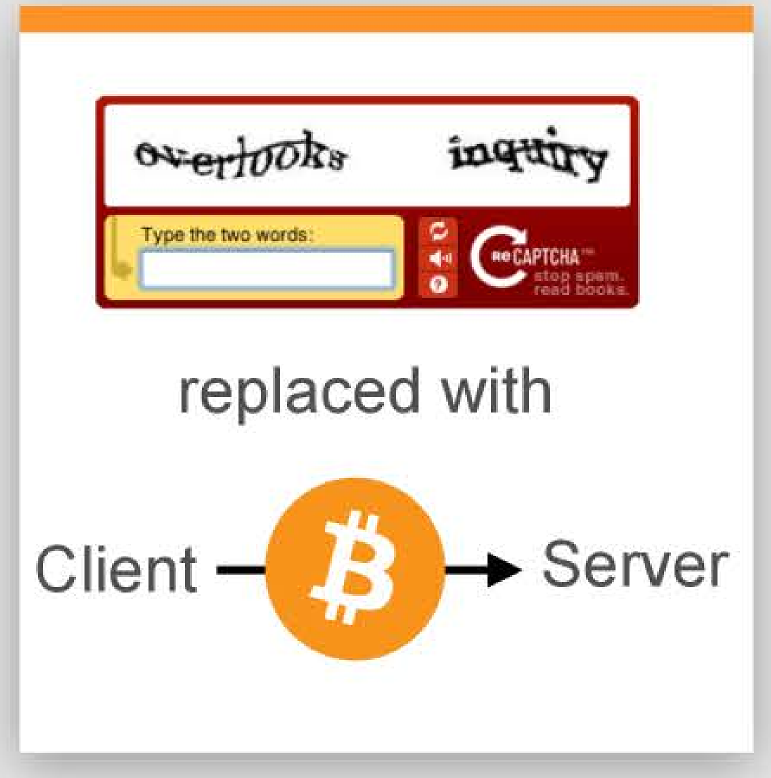
ERROR 402

Branch on BTC payment



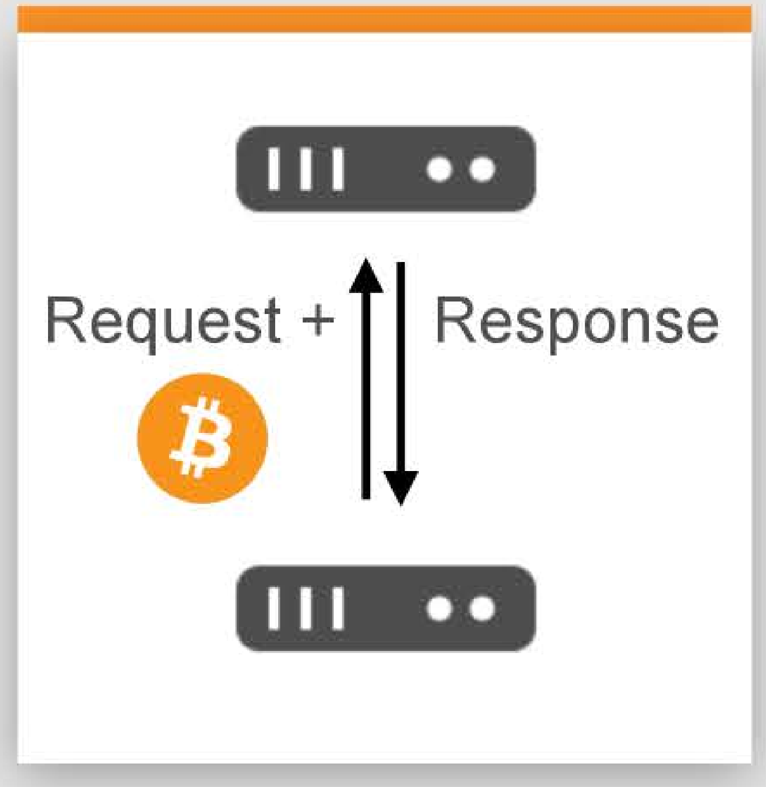
BITCOIN CAPTCHA

Make spam unprofitable



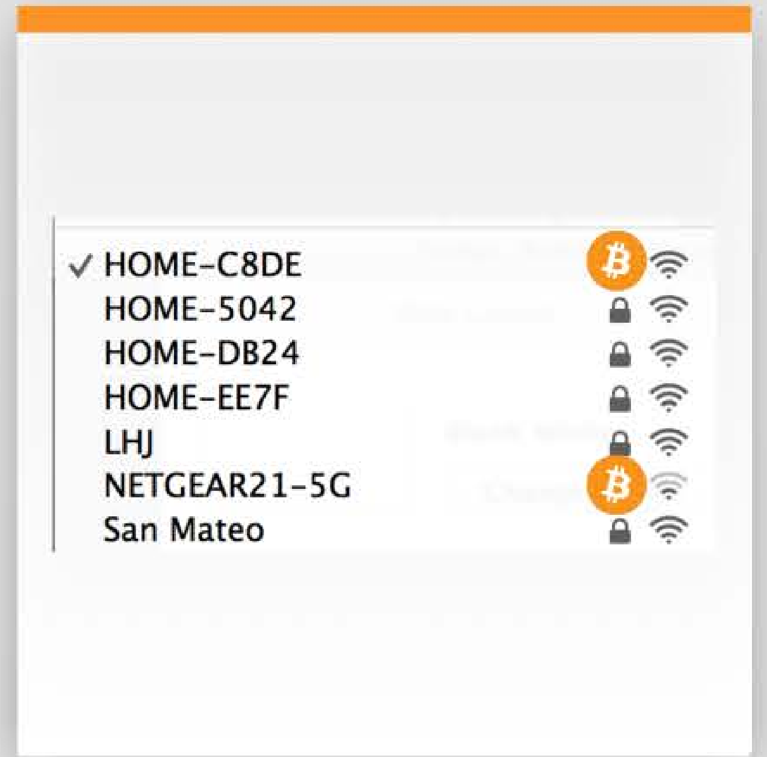
PAID APIS

BTC for API call



PAID WIFI

BTC for access

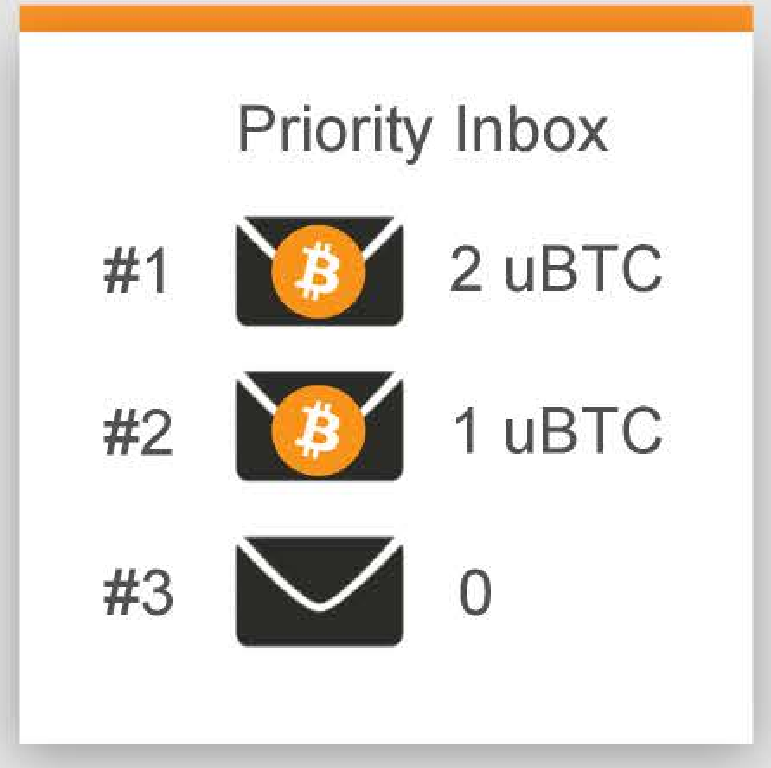


BITSIGN

Blockchain notary

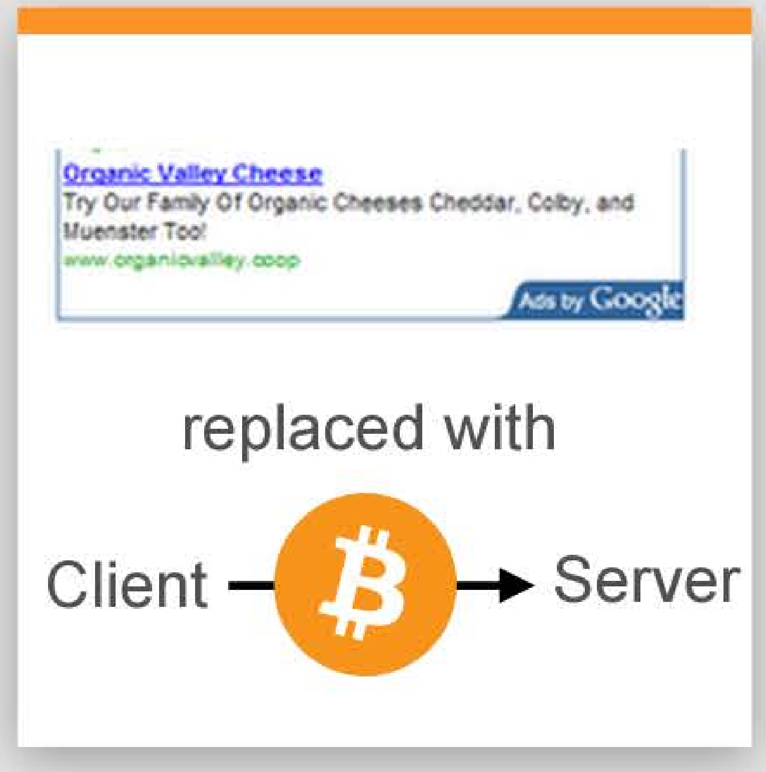
SPAMLESS EMAIL

Priority inbox by BTC



AD-FREE BROWSING

Send BTC, see ad-free



MORE

Just the start...

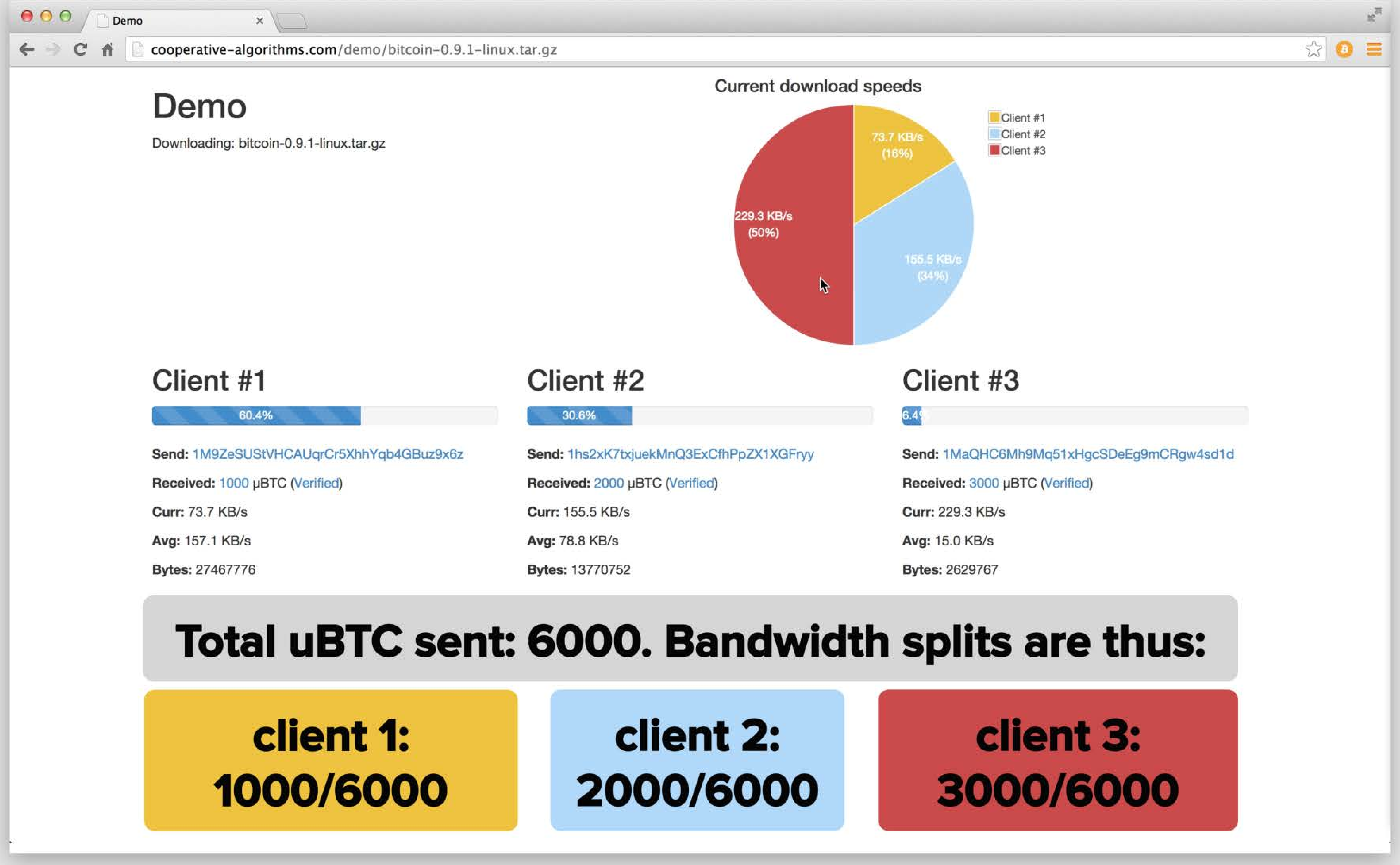
Demo: Realtime Bandwidth Auction with Bitcoin

We've developed a series of demos that show the price-independent utility of an infinite stream of BTC.

Bitcoin as a Protocol

Application 1: Using Bitcoin to conduct a realtime bandwidth auction

Alex Chia[1,2], Matt Pauker[2], Balaji S. Srinivasan[1,2]
1: Stanford Bitcoin Group (balajis@stanford.edu)
2: 21E6 (matt@21e6.com)



Demo

Downloading: bitcoin-0.9.1-linux.tar.gz

Client #1

Send: 1M9ZeSUStVHCAUqrCr5XhhYqb4GBuz9x6z

Received: 1000 µBTC (Verified)

Curr: 73.7 KB/s

Avg: 157.1 KB/s

Bytes: 27467776

Client #2

Send: 1hs2xK7txjuekMnQ3ExCfhPpZX1XGFryy

Received: 2000 µBTC (Verified)

Curr: 155.5 KB/s

Avg: 78.8 KB/s

Bytes: 13770752

Client #3

Send: 1MaQHC6Mh9Mq51xHgcSDeEg9mCRgw4sd1d

Received: 3000 µBTC (Verified)

Curr: 229.3 KB/s

Avg: 15.0 KB/s

Bytes: 2629767

Total uBTC sent: 6000. Bandwidth splits are thus:

client 1: 1000/6000

client 2: 2000/6000

client 3: 3000/6000

player.vimeo.com/video/109632262

Demo: Paid API usage with Bitcoin

We've developed a new protocol that shows how to use Bitcoin to pay for any Internet-accessible resource.

Bitcoin as a Protocol

Application 2: Using BTC to programmatically pay for an arbitrary digital good

Alex Chia[1,2], Matt Pauker[2], Balaji S. Srinivasan[1,2]
1: Stanford Bitcoin Group (balajis@stanford.edu)
2: 21E6 (matt@21e6.com)

CLIENT INITIATES HTTP REQUEST

SERVER DENIES, ASKS FOR .001 BTC

CLIENT REREQUESTS AND ATTACHES BTC

SERVER RETURNS RESOURCE FOR BTC

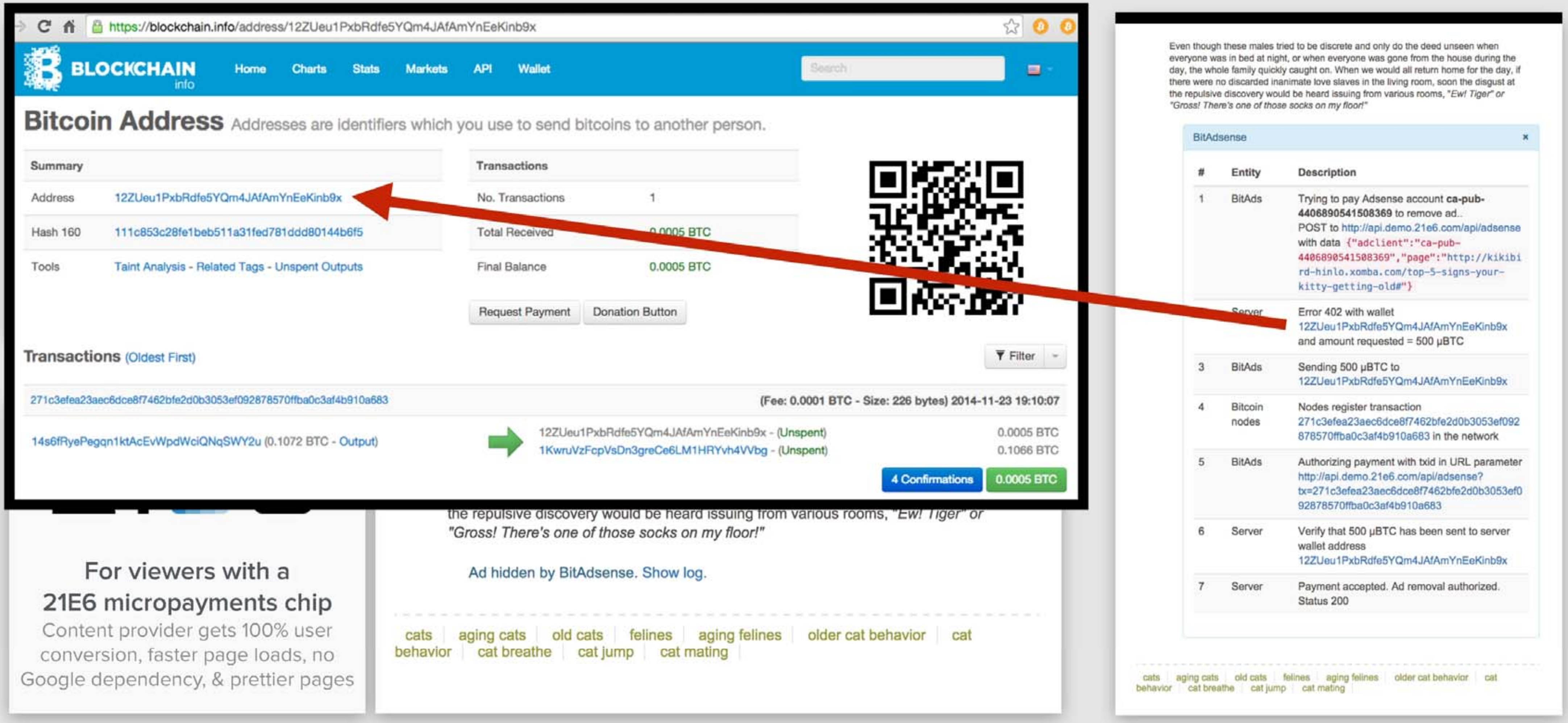
```
demo@402demo:~$ bitcurl -X POST -d '{"to":
6502071548,"msg":"hello world via bitcurl"}'
http://api.demo.21e6.com/api/twilio -v
Requesting http://api.demo.21e6.com/api/twilio
Status 402
Bitcoin address: 1Gy4AvTeA2LftFdMm2TfBojV1LfcT22KRr
Price in BTC: 0.001
Transaction id:
6428b54af4e2f03bf5d806472d2081d4a0dac7f53d156906f9c8aeec6
01cb34b
Retrying request with txid..
Status 200
{"status":"ok","message_id":"SM04d5c769e8a847098c16da328b
658037"}
demo@402demo:~$
```

```
demo@402demo:~$ bitcurl -X POST -d '{"to":6502071548,"msg":"hello world via bitcurl"}' http://api.demo.21e6.com/api/twilio -v
Requesting http://api.demo.21e6.com/api/twilio
Status 402
Bitcoin address: 1Gy4AvTeA2LftFdMm2TfBojV1LfcT22KRr
Price in BTC: 0.001
Transaction id: 6428b54af4e2f03bf5d806472d2081d4a0dac7f53d156906f9c8aeec601cb34b
Retrying request with txid..
Status 200
{"status":"ok","message_id":"SM04d5c769e8a847098c16da328b658037"}
```

api.demo.21e6.com

Demo: Trade BTC for Time via Responsive Monetization

This is live in the Blockchain; try clicking 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x



https://blockchain.info/address/12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
BLOCKCHAIN info
Home
Charts
Stats
Markets
API
Wallet
Search

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
Hash 160	111c853c28fe1beb511a31fed781ddd80144b6f5
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	0.0005 BTC
Final Balance	0.0005 BTC

Transactions (Oldest First)

271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683 (Fee: 0.0001 BTC - Size: 226 bytes) 2014-11-23 19:10:07

14s6fRyePegqn1ktAcEvWpdWciQNqSWY2u (0.1072 BTC - Output) → 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x - (Unspent) 0.0005 BTC
1KwruVzFcpVsDn3greCe6LM1HRYvh4VVbg - (Unspent) 0.1066 BTC

For viewers with a 21E6 micropayments chip

Content provider gets 100% user conversion, faster page loads, no Google dependency, & prettier pages

the repulsive discovery would be heard issuing from various rooms, *"Ew! Tiger" or "Gross! There's one of those socks on my floor!"*

Ad hidden by BitAdsense. Show log.

cats | aging cats | old cats | felines | aging felines | older cat behavior | cat behavior | cat breathe | cat jump | cat mating |

Even though these males tried to be discrete and only do the deed unseen when everyone was in bed at night, or when everyone was gone from the house during the day, the whole family quickly caught on. When we would all return home for the day, if there were no discarded inanimate love slaves in the living room, soon the disgust at the repulsive discovery would be heard issuing from various rooms, *"Ew! Tiger" or "Gross! There's one of those socks on my floor!"*

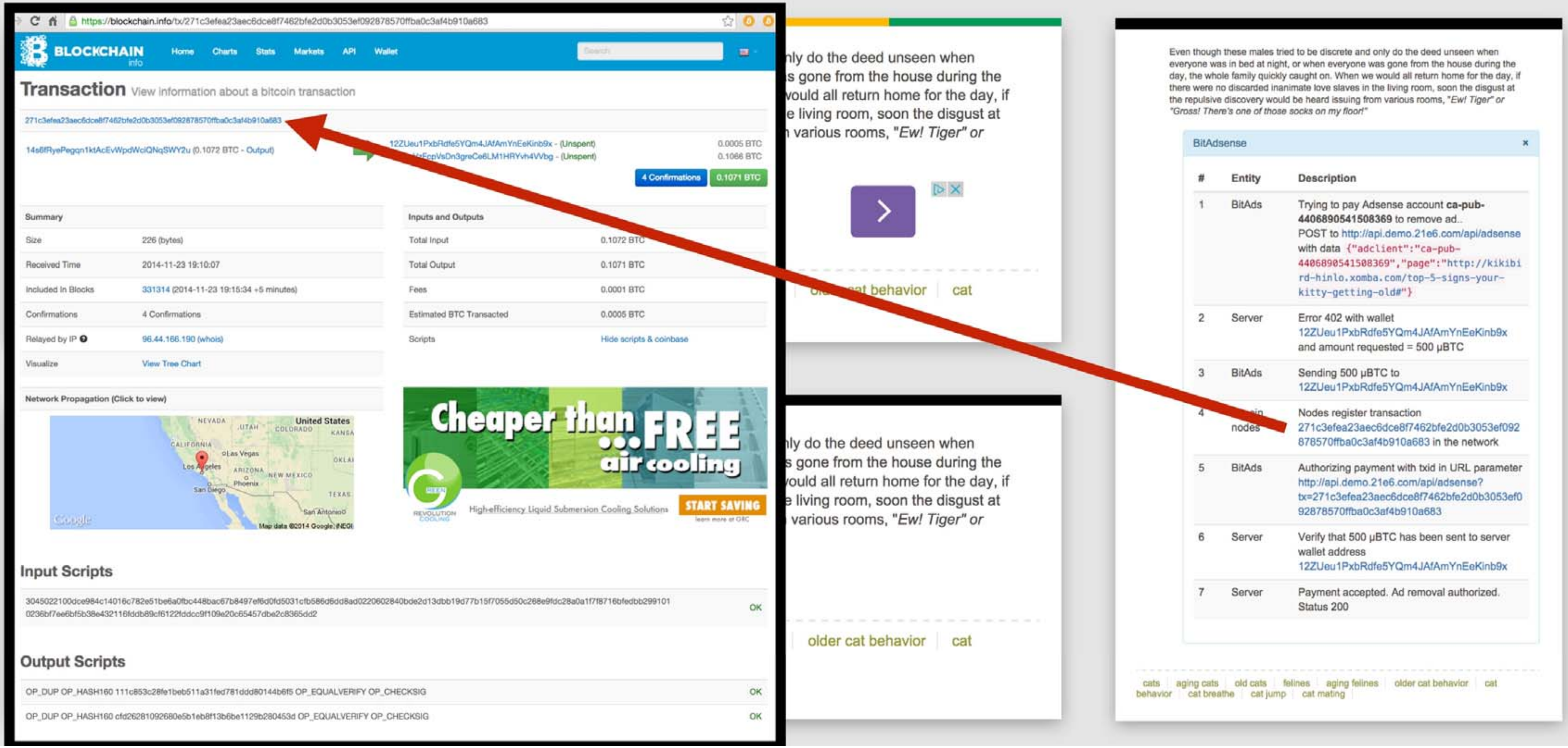
BitAdsense ×

#	Entity	Description
1	BitAds	Trying to pay Adsense account **ca-pub-4406890541508369** to remove ad.. POST to http://api.demo.21e6.com/api/adsense with data `{"adclient":"ca-pub-4406890541508369","page":"http://kikibird-hinlo.xomba.com/top-5-signs-your-kitty-getting-old#"}`
	Server	Error 402 with wallet 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x and amount requested = 500 µBTC
3	BitAds	Sending 500 µBTC to 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
4	Bitcoin nodes	Nodes register transaction 271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683 in the network
5	BitAds	Authorizing payment with txid in URL parameter http://api.demo.21e6.com/api/adsense?tx=271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683
6	Server	Verify that 500 µBTC has been sent to server wallet address 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
7	Server	Payment accepted. Ad removal authorized. Status 200

cats | aging cats | old cats | felines | aging felines | older cat behavior | cat behavior | cat breathe | cat jump | cat mating |

Demo: Trade BTC for Time via Responsive Monetization

This is live in the Blockchain; tx 271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683



https://blockchain.info/tx/271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683

Transaction View information about a bitcoin transaction

271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683

14s6fRyePegqn1ktAcEvWpdWciQNqSWY2u (0.1072 BTC - Output)

12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x - (Unspent) 0.0005 BTC
VzFcpVsDn3greCe6LM1HRYvh4Vbg - (Unspent) 0.1066 BTC

4 Confirmations 0.1071 BTC

Summary	
Size	226 (bytes)
Received Time	2014-11-23 19:10:07
Included In Blocks	331314 (2014-11-23 19:15:34 +5 minutes)
Confirmations	4 Confirmations
Relayed by IP	96.44.166.190 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.1072 BTC
Total Output	0.1071 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	0.0005 BTC
Scripts	Hide scripts & coinbase

Network Propagation (Click to view)

Input Scripts

```
3045022100dce984c14016c782e51be6a0fbc448bac67b8497ef6d0fd5031cfb586d6dd8ad0220602840bde2d13dbb19d77b15f7055d50c268e9fdc28a0a1f7f8716bfedbb299101
0236bf7ee6bf5b38e432116fddb89cf6122fddcc9f109e20c65457dbe2c8365dd2                                  OK
```

Output Scripts

```
OP_DUP OP_HASH160 111c853c28fe1beb511a31fed781ddd80144b6f5 OP_EQUALVERIFY OP_CHECKSIG     OK
OP_DUP OP_HASH160 cfd26281092680e5b1eb8f13b6be1129b280453d OP_EQUALVERIFY OP_CHECKSIG     OK
```

nly do the deed unseen when
s gone from the house during the
vould all return home for the day, if
e living room, soon the disgust at
various rooms, "*Ew! Tiger*" or

older cat behavior | cat

nly do the deed unseen when
s gone from the house during the
vould all return home for the day, if
e living room, soon the disgust at
various rooms, "*Ew! Tiger*" or

older cat behavior | cat

Even though these males tried to be discrete and only do the deed unseen when everyone was in bed at night, or when everyone was gone from the house during the day, the whole family quickly caught on. When we would all return home for the day, if there were no discarded inanimate love slaves in the living room, soon the disgust at the repulsive discovery would be heard issuing from various rooms, "*Ew! Tiger*" or "*Gross! There's one of those socks on my floor!*"

BitAdsense ×

#	Entity	Description
1	BitAds	Trying to pay Adsense account **ca-pub-4406890541508369** to remove ad.. POST to http://api.demo.21e6.com/api/adsense with data `{"adclient":"ca-pub-4406890541508369","page":"http://kikibird-hinlo.xomba.com/top-5-signs-your-kitty-getting-old#"}`
2	Server	Error 402 with wallet 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x and amount requested = 500 μBTC
3	BitAds	Sending 500 μBTC to 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
4	Blockchain nodes	Nodes register transaction 271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683 in the network
5	BitAds	Authorizing payment with txid in URL parameter http://api.demo.21e6.com/api/adsense?tx=271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683
6	Server	Verify that 500 μBTC has been sent to server wallet address 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
7	Server	Payment accepted. Ad removal authorized. Status 200

cats | aging cats | old cats | felines | aging felines | older cat behavior | cat behavior | cat breathe | cat jump | cat mating

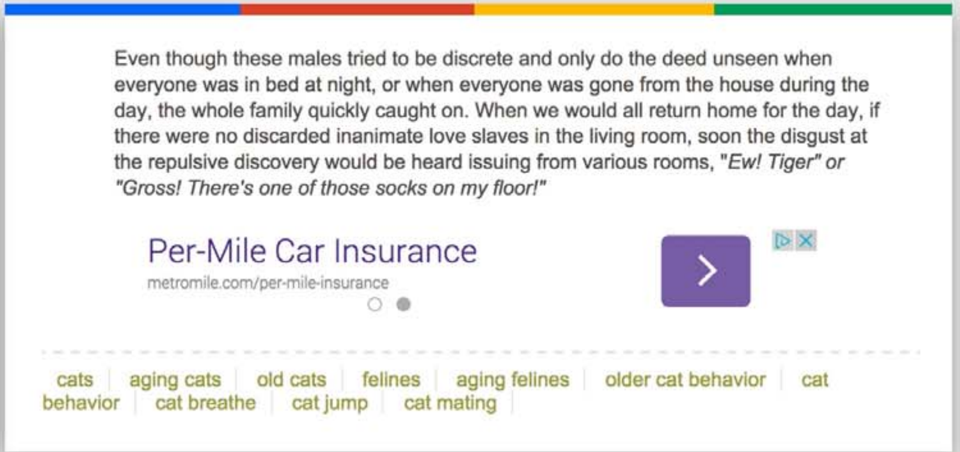
Demo: Trade BTC for Time via Responsive Monetization

Content providers paste in JS snippet; enable fallback to AdSense for non-micropayments capable computers

Google Ads | AdSense

For viewers without a 21E6 micropayments chip

Content provider continues to serve AdSense for clients without micropayments capability (just like responsive web design)



Even though these males tried to be discrete and only do the deed unseen when everyone was in bed at night, or when everyone was gone from the house during the day, the whole family quickly caught on. When we would all return home for the day, if there were no discarded inanimate love slaves in the living room, soon the disgust at the repulsive discovery would be heard issuing from various rooms, *"Ew! Tiger" or "Gross! There's one of those socks on my floor!"*

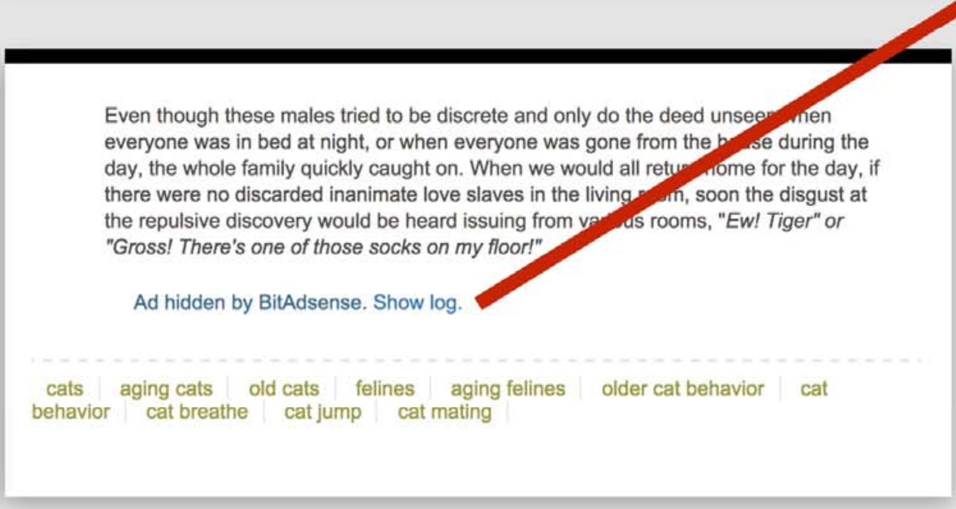
Per-Mile Car Insurance
metromile.com/per-mile-insurance

cats | aging cats | old cats | felines | aging felines | older cat behavior | cat behavior | cat breathe | cat jump | cat mating |

21E6

For viewers with a 21E6 micropayments chip

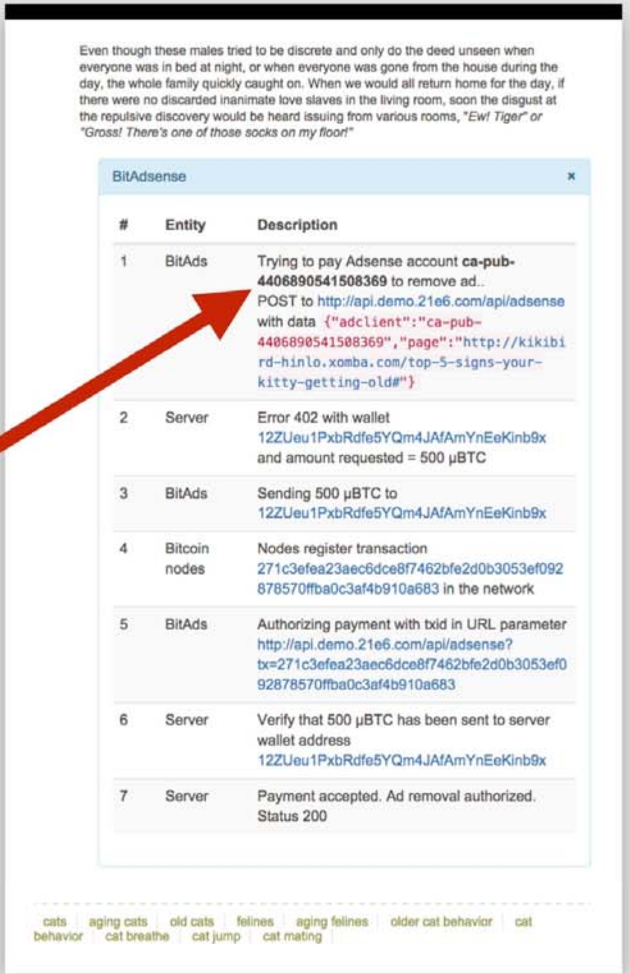
Content provider gets 100% user conversion, faster page loads, no Google dependency, & prettier pages



Even though these males tried to be discrete and only do the deed unseen when everyone was in bed at night, or when everyone was gone from the house during the day, the whole family quickly caught on. When we would all return home for the day, if there were no discarded inanimate love slaves in the living room, soon the disgust at the repulsive discovery would be heard issuing from various rooms, *"Ew! Tiger" or "Gross! There's one of those socks on my floor!"*

Ad hidden by BitAdsense. Show log.

cats | aging cats | old cats | felines | aging felines | older cat behavior | cat behavior | cat breathe | cat jump | cat mating |



Even though these males tried to be discrete and only do the deed unseen when everyone was in bed at night, or when everyone was gone from the house during the day, the whole family quickly caught on. When we would all return home for the day, if there were no discarded inanimate love slaves in the living room, soon the disgust at the repulsive discovery would be heard issuing from various rooms, *"Ew! Tiger" or "Gross! There's one of those socks on my floor!"*

BitAdsense ×

#	Entity	Description
1	BitAds	Trying to pay Adsense account **ca-pub-4406890541508369** to remove ad.. POST to http://api.demo.21e6.com/api/adsense with data `{"adclient":"ca-pub-4406890541508369","page":"http://kikibird-hinlo.xomba.com/top-5-signs-your-kitty-getting-old#"}`
2	Server	Error 402 with wallet 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x and amount requested = 500 µBTC
3	BitAds	Sending 500 µBTC to 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
4	Bitcoin nodes	Nodes register transaction 271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683 in the network
5	BitAds	Authorizing payment with txid in URL parameter http://api.demo.21e6.com/api/adsense?tx=271c3efea23aec6dce8f7462bfe2d0b3053ef092878570ffba0c3af4b910a683
6	Server	Verify that 500 µBTC has been sent to server wallet address 12ZUeu1PxbRdfe5YQm4JAfAmYnEeKinb9x
7	Server	Payment accepted. Ad removal authorized. Status 200

cats | aging cats | old cats | felines | aging felines | older cat behavior | cat behavior | cat breathe | cat jump | cat mating |

What we're shipping in Q1

First party device: USB charger.

Educate on chip & protocol via MOOC.

BitSplit Go-To-Market Strategy

“A miner in every device and every hand”. Start with our own device to prove a point, and then expand.

CapEx

Phase 1: USB charging hub (1st-party device)

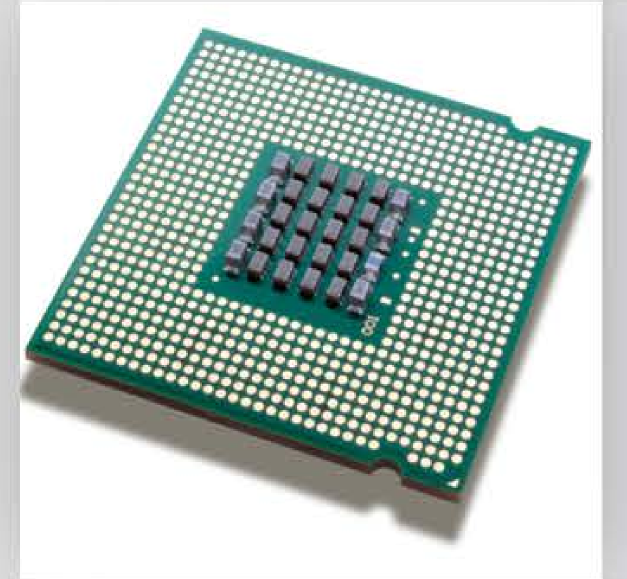
- 21E6-produced consumer devices to seed market
- Launch device in Q1
- Zero OpEx, low CapEx

$35

Phase 2: OEM

- 21E6 chip in every net-enabled device; optional rev-share with OEM
- Routers, printers, gaming consoles, set-top boxes, …
- Zero OpEx, tiny CapEx (just cost of chip)

$8



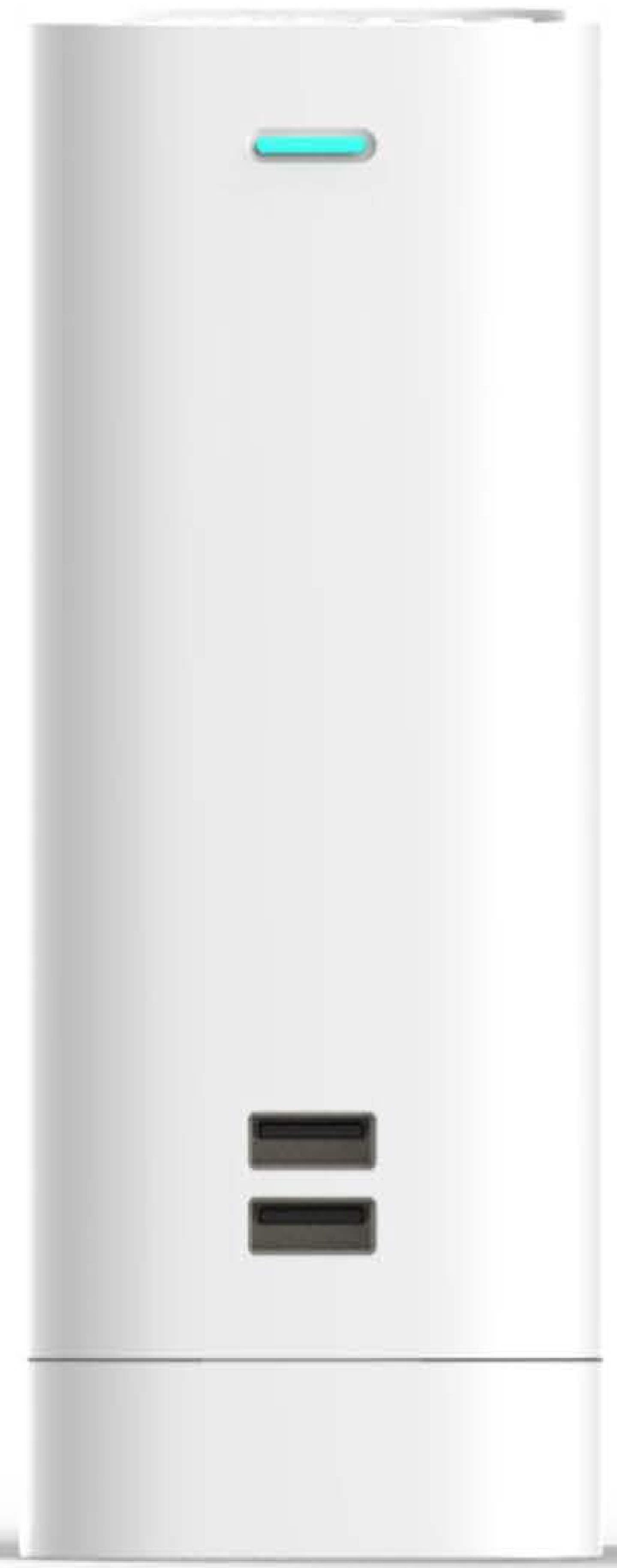
Phase 3: “Bitcoin Inside”

- Mining capability embedded directly in chipsets (e.g., for IoT)
- No extra hardware required for device manufacturer
- Zero OpEx, **zero CapEx**

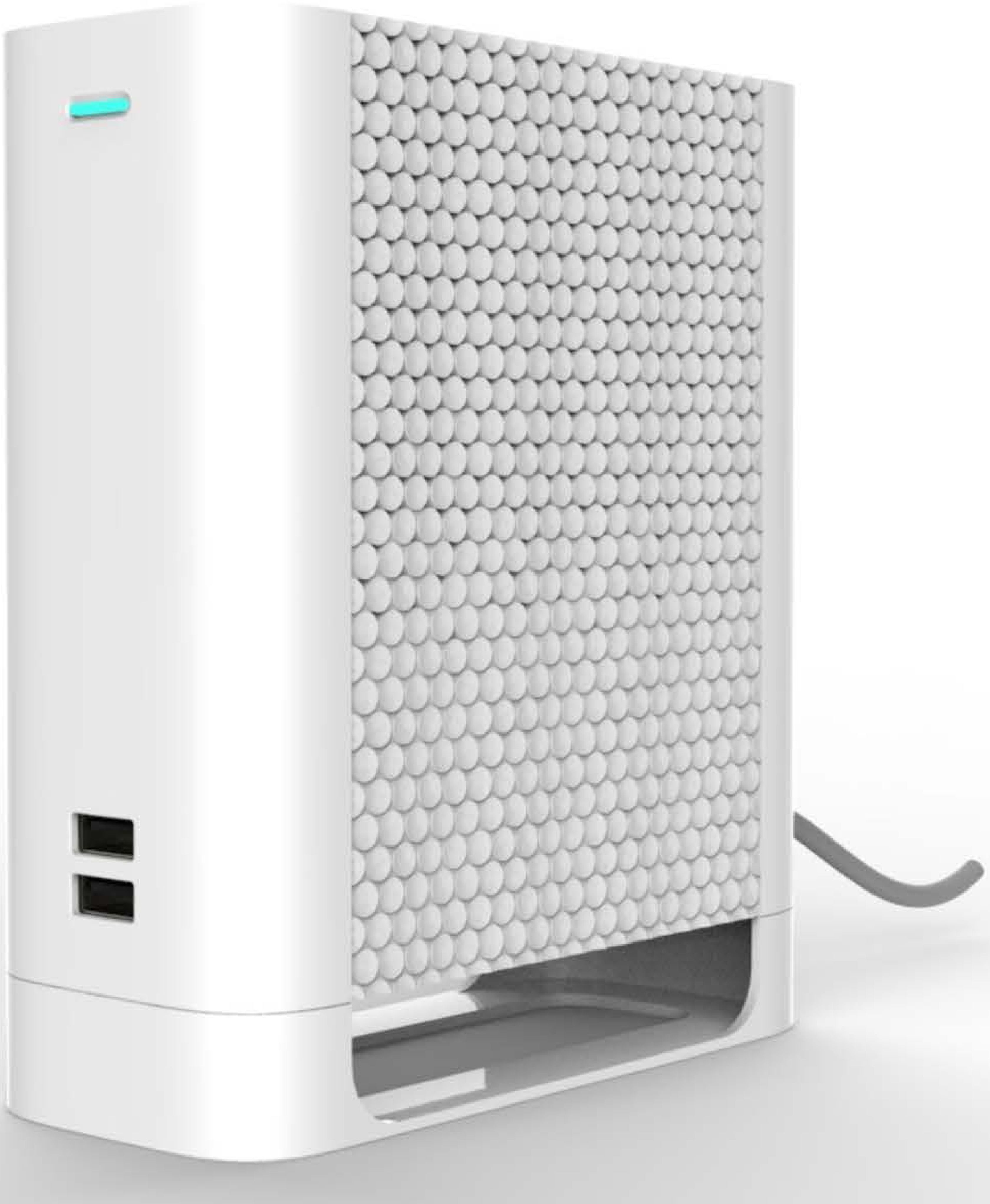
$0

BitSplit Go-To-Market: Phase 1

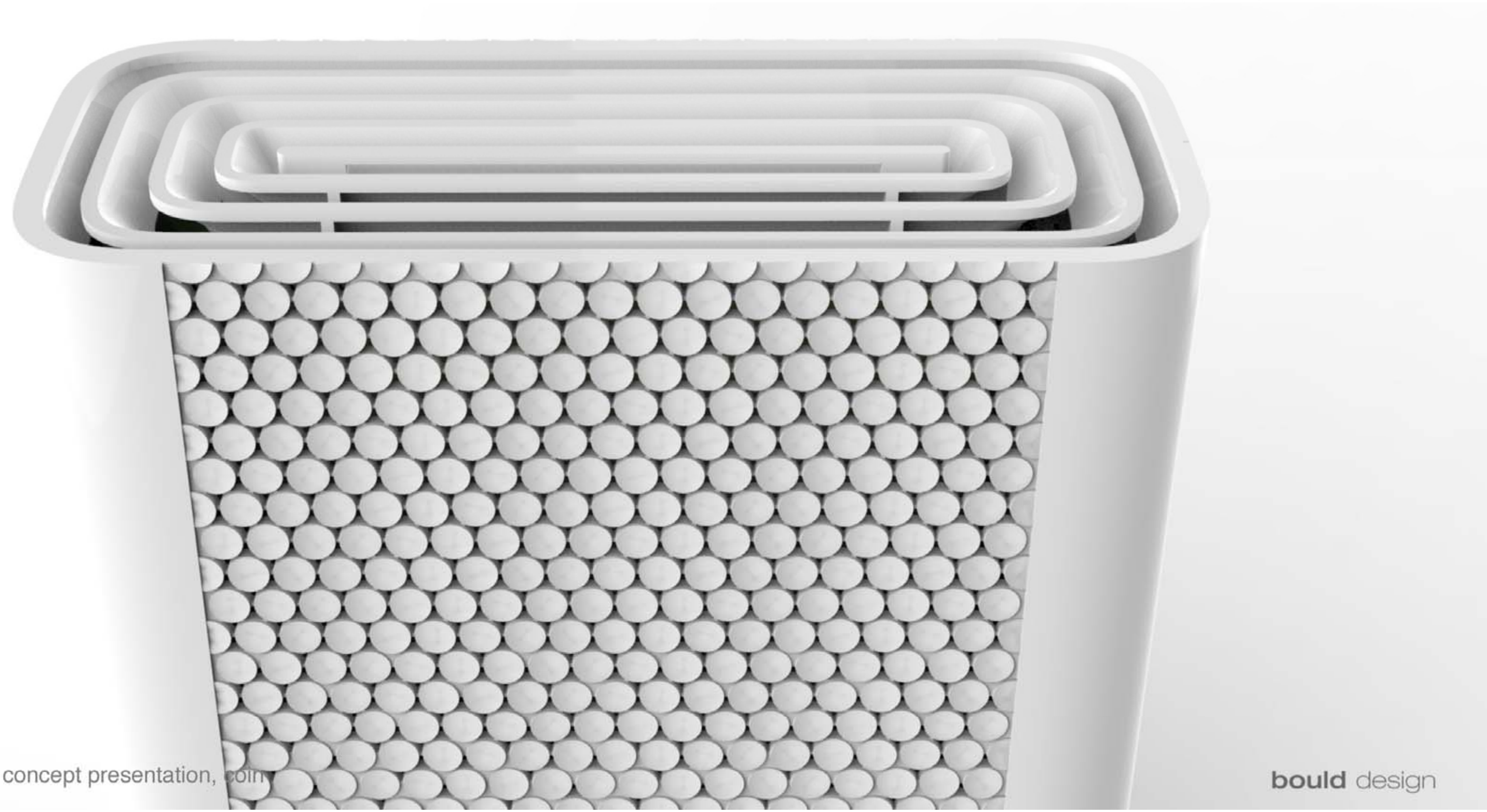
Proof-of-concept device targeting developers & early adopters



ID: 21E6 3D concept presentation, coin

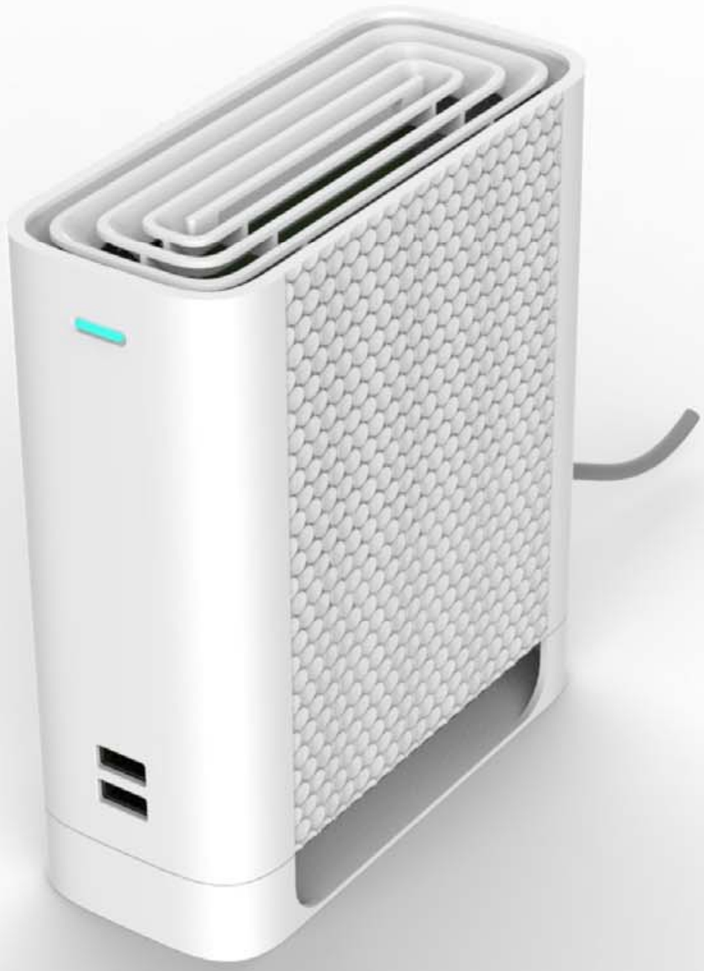


ID: 21E6 3D concept presentation, coin



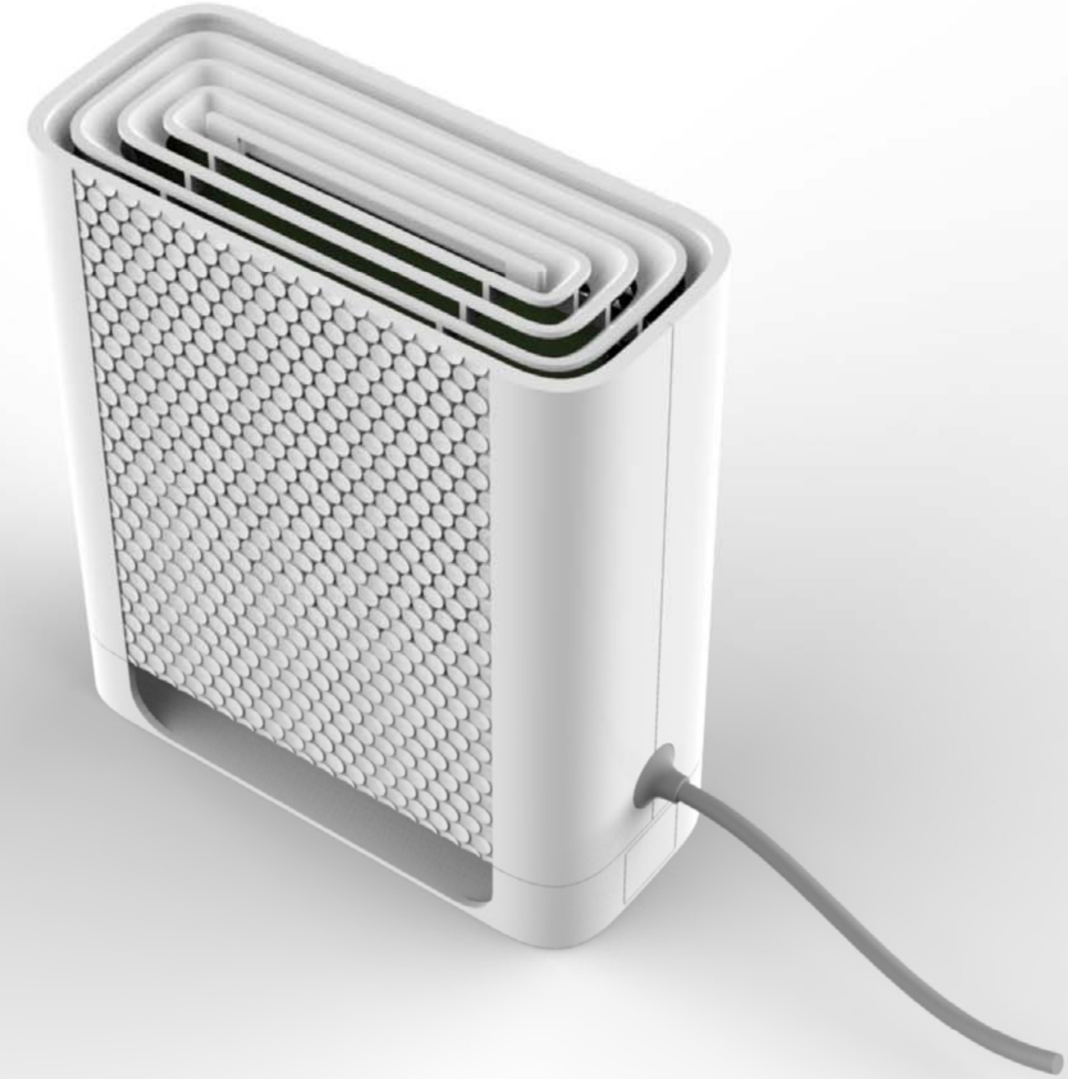
ID: 21E6 3D concept presentation, coin

21E6 confidential, 11.19.2014

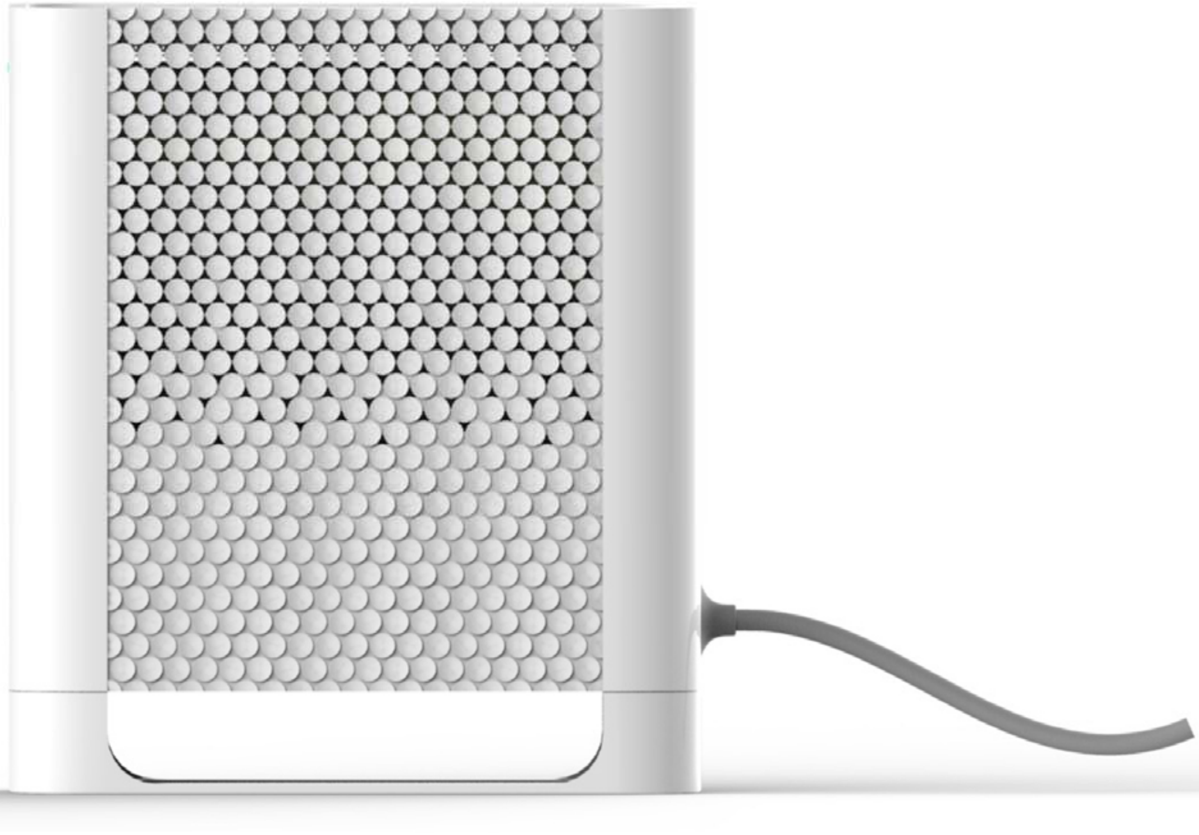


ID: 21E6 3D concept presentation, coin

bould design



ID: 21E6 3D concept presentation, coin



ID: 21E6 3D concept presentation, coin

BitSplit Go-To-Market Strategy

The first 1-5 million units? Target developers, developers, developers, developers through our channels.

APIs for BTC

NumPy

Amazon Elastic MapReduce

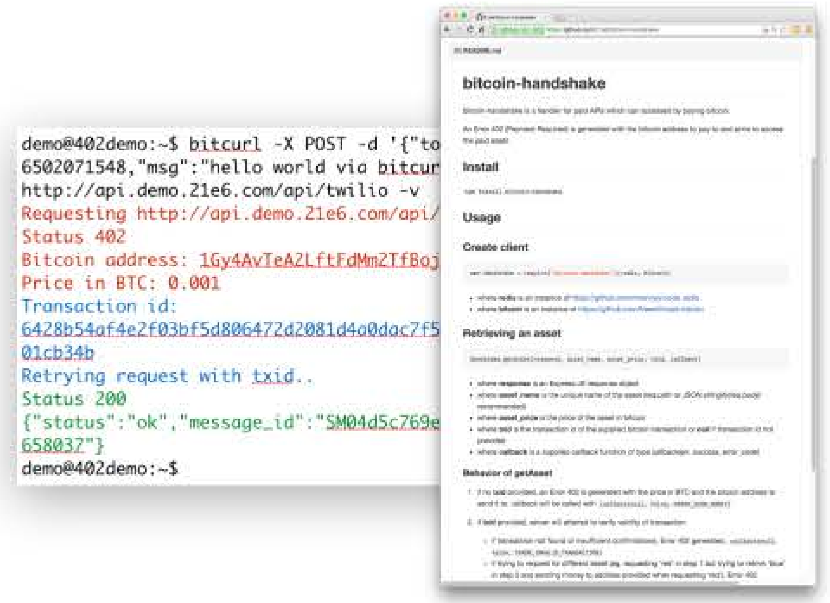
Google translate

Natural Language Toolkit

SciPy.org

GSL - GNU Scientific Library

402 API handshake



```
demo@402demo:~$ bitcurl -X POST -d '{"to
6502071548,"msg":"hello world via bitcur
http://api.demo.21e6.com/api/twilio -v
Requesting http://api.demo.21e6.com/api/
Status 402
Bitcoin address: 1Gy4AvTeA2LftFdMmZTfBoj
Price in BTC: 0.001
Transaction id:
6428b54af4e2f03bf5d806472d2081d4a0dac7f5
01cb34b
Retrying request with txid..
Status 200
{"status":"ok","message_id":"SM04d5c769e
658037"}
demo@402demo:~$
```

bitcoin-handshake

Install

Usage

Create client

Retrieving an asset

Behavior of getAsset

Bitsplit devices

Immediate Utility

Hundreds of zero signup 402-paid APIs available at api.21e6.com on day 0

ANDREESSEN HOROWITZ

Product Hunt

twitter

GitHub

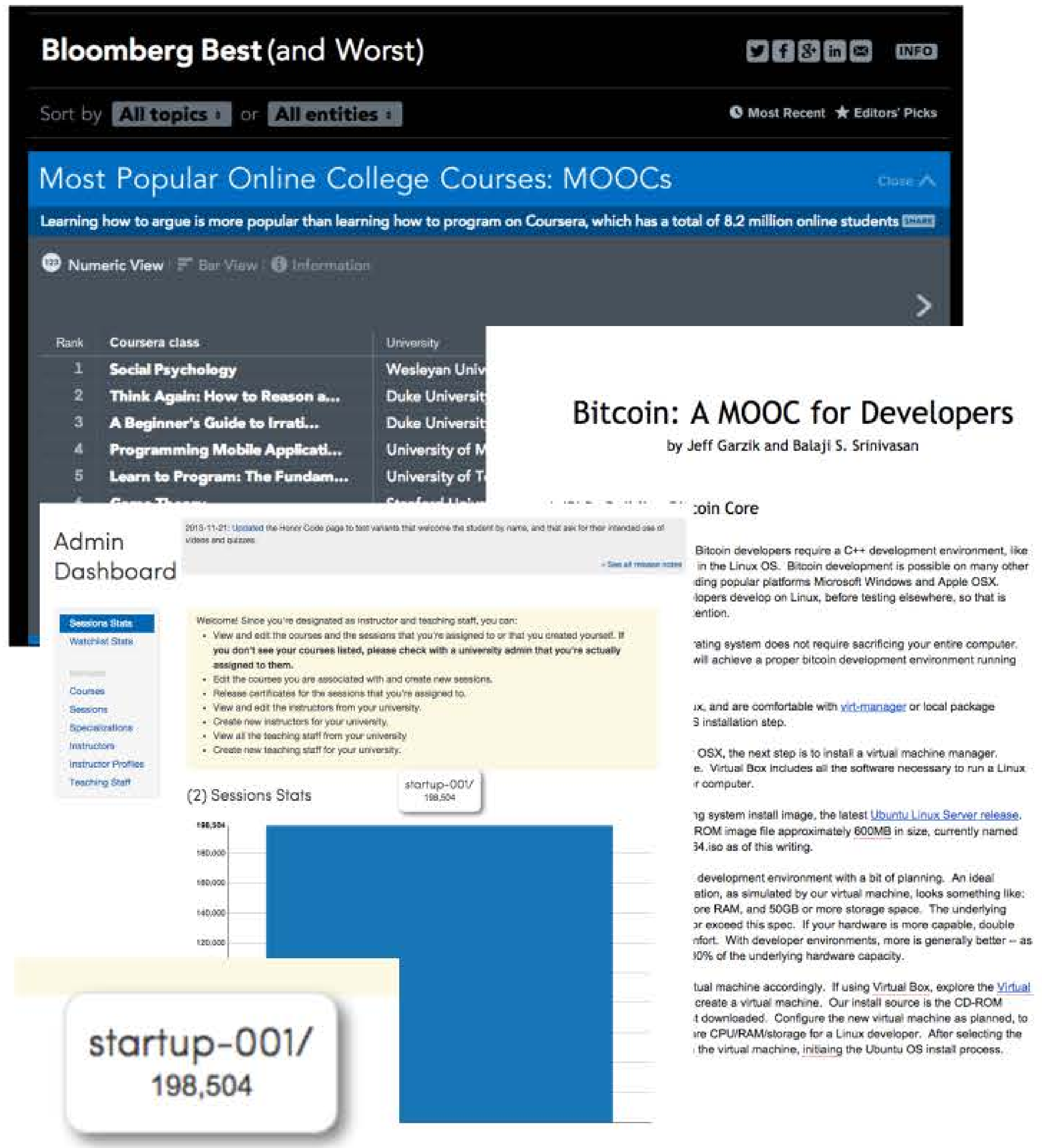
AngelList

reddit

UDACITY

Push via our channels

We have the relationships to put this all over AngelList, Github, Twitter, etc.



Bloomberg Best (and Worst)

Sort by All topics or All entities

Most Recent ★ Editors' Picks

Most Popular Online College Courses: MOOCs

Learning how to argue is more popular than learning how to program on Coursera, which has a total of 8.2 million online students

Numeric View | Bar View | Information

Rank	Coursera class	University
1	Social Psychology	Wesleyan Univ
2	Think Again: How to Reason a...	Duke Universit
3	A Beginner's Guide to Irrati...	Duke Universit
4	Programming Mobile Applicati...	University of M
5	Learn to Program: The Fundam...	University of T

Bitcoin: A MOOC for Developers

by Jeff Garzik and Balaji S. Srinivasan

:oin Core

Bitcoin developers require a C++ development environment, like in the Linux OS. Bitcoin development is possible on many other ding popular platforms Microsoft Windows and Apple OSX. lopers develop on Linux, before testing elsewhere, so that is ention.

ating system does not require sacrificing your entire computer. will achieve a proper bitcoin development environment running

ıx, and are comfortable with virt-manager or local package 3 installation step.

OSX, the next step is to install a virtual machine manager. e. Virtual Box includes all the software necessary to run a Linux r computer.

ng system install image, the latest Ubuntu Linux Server release, ROM image file approximately 600MB in size, currently named 34.iso as of this writing.

development environment with a bit of planning. An ideal ation, as simulated by our virtual machine, looks something like: ore RAM, and 50GB or more storage space. The underlying or exceed this spec. If your hardware is more capable, double nfort. With developer environments, more is generally better -- as 30% of the underlying hardware capacity.

tual machine accordingly. If using Virtual Box, explore the Virtual create a virtual machine. Our install source is the CD-ROM t downloaded. Configure the new virtual machine as planned, to re CPU/RAM/storage for a Linux developer. After selecting the the virtual machine, initiaing the Ubuntu OS install process.

Admin Dashboard

2015-11-21: Updated the Honor Code page to test variants that welcome the student by name, and that ask for their intended use of videos and quizzes.

Welcome! Since you're designated as instructor and teaching staff, you can:

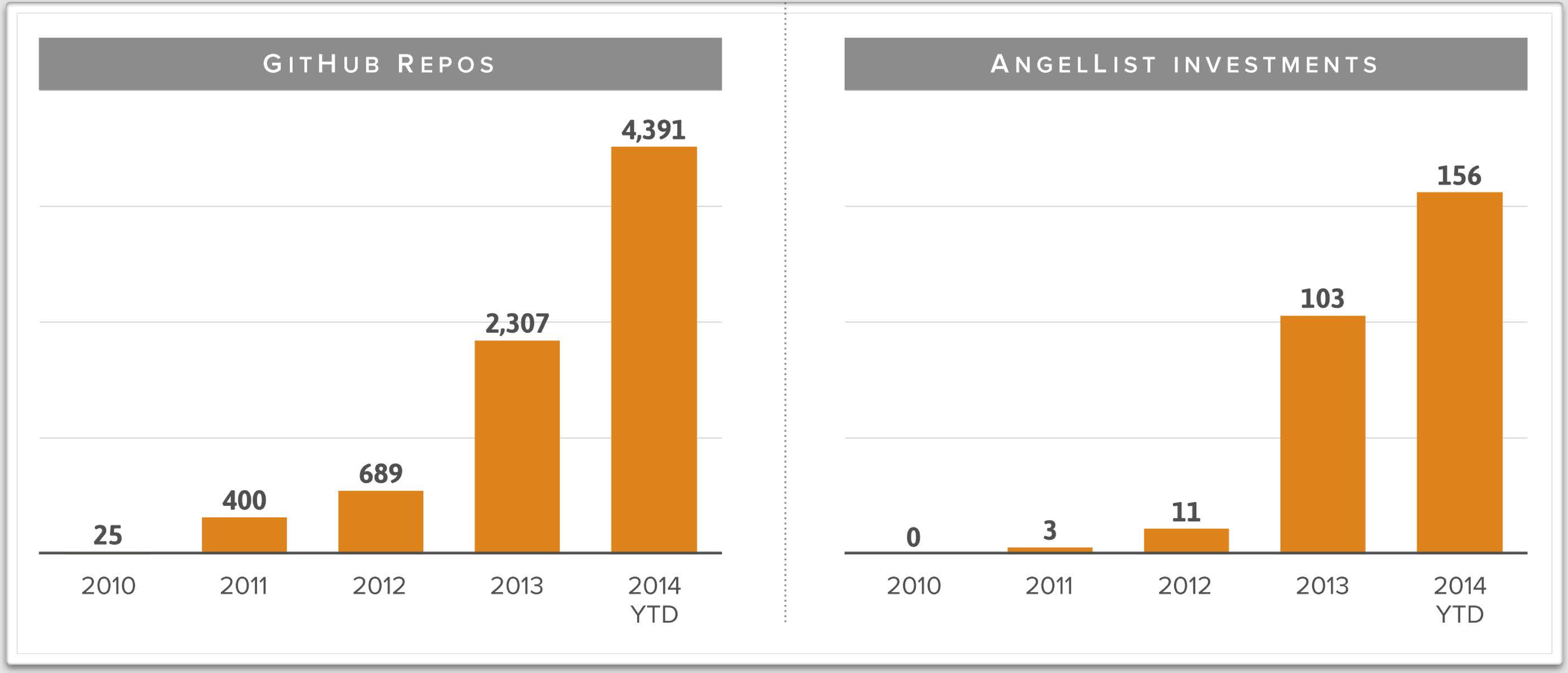
- View and edit the courses and the sessions that you're assigned to or that you created yourself. If **you don't see your courses listed, please check with a university admin that you're actually assigned to them.**
- Edit the courses you are associated with and create new sessions.
- Release certificates for the sessions that you're assigned to.
- View and edit the instructors from your university.
- Create new instructors for your university.
- View all the teaching staff from your university.
- Create new teaching staff for your university.

Educate via Bitcoin MOOC

Taught one of most popular MOOCs ever. Now teaching Bitcoin MOOC w/ core dev.

Earliest BitSplit Adopters will be Developers & Entrepreneurs

BitSplit devices have built-in monetization. And community of Bitcoin devs & entrepreneurs already large.

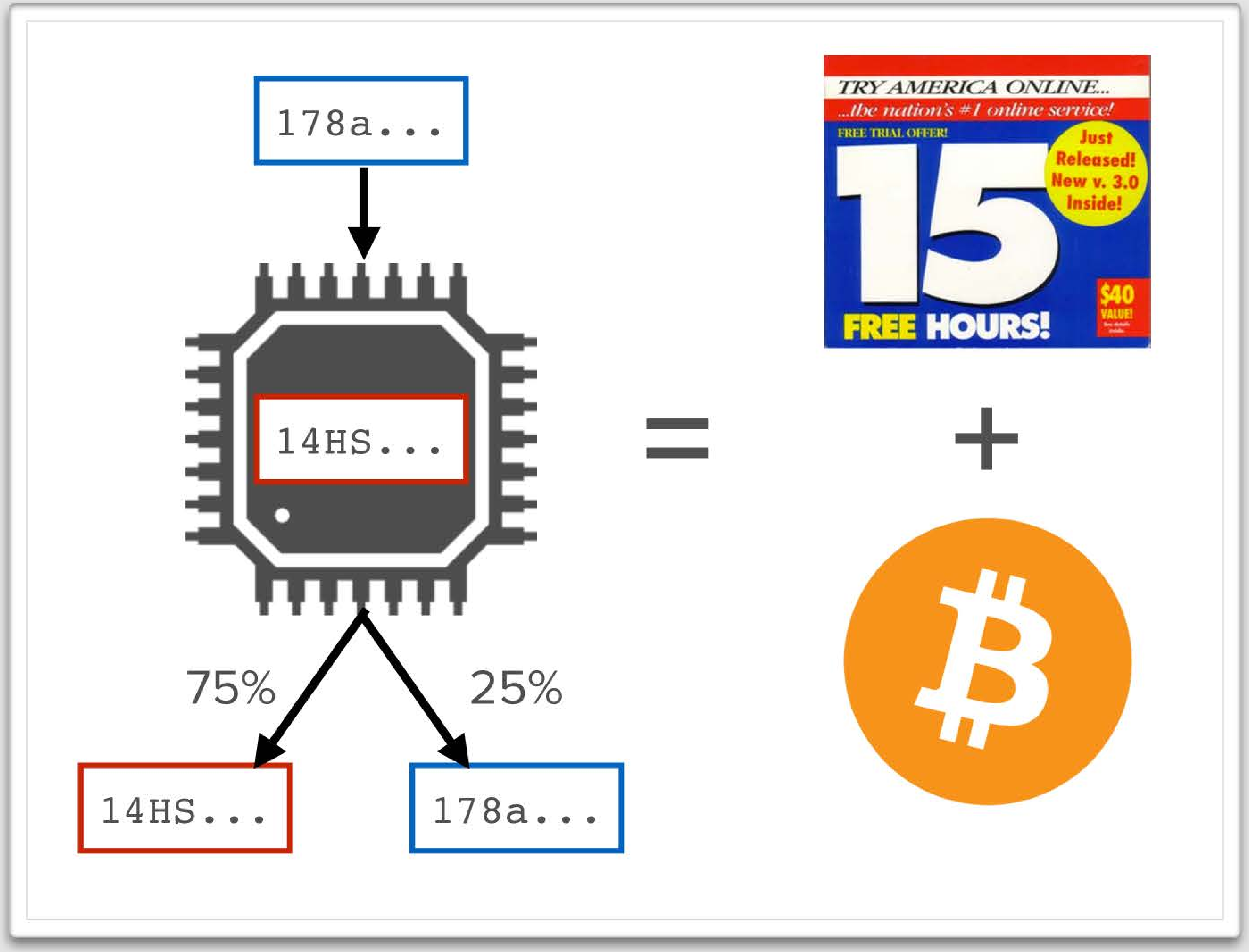


GitHub Repos

AngelList investments

For All: BitSplit Mainstreams Bitcoin

The AOL CD of Bitcoin: give every user a free trial of Bitcoin at near-zero marginal cost. A proven model to onboard millions.



- Solves the chicken-and-egg problem
- Only way to get BTC to millions of people
- No credit card or bank account required
- Users more likely to spend $5 than $5k
- Power of defaults (IE, Google/FF)

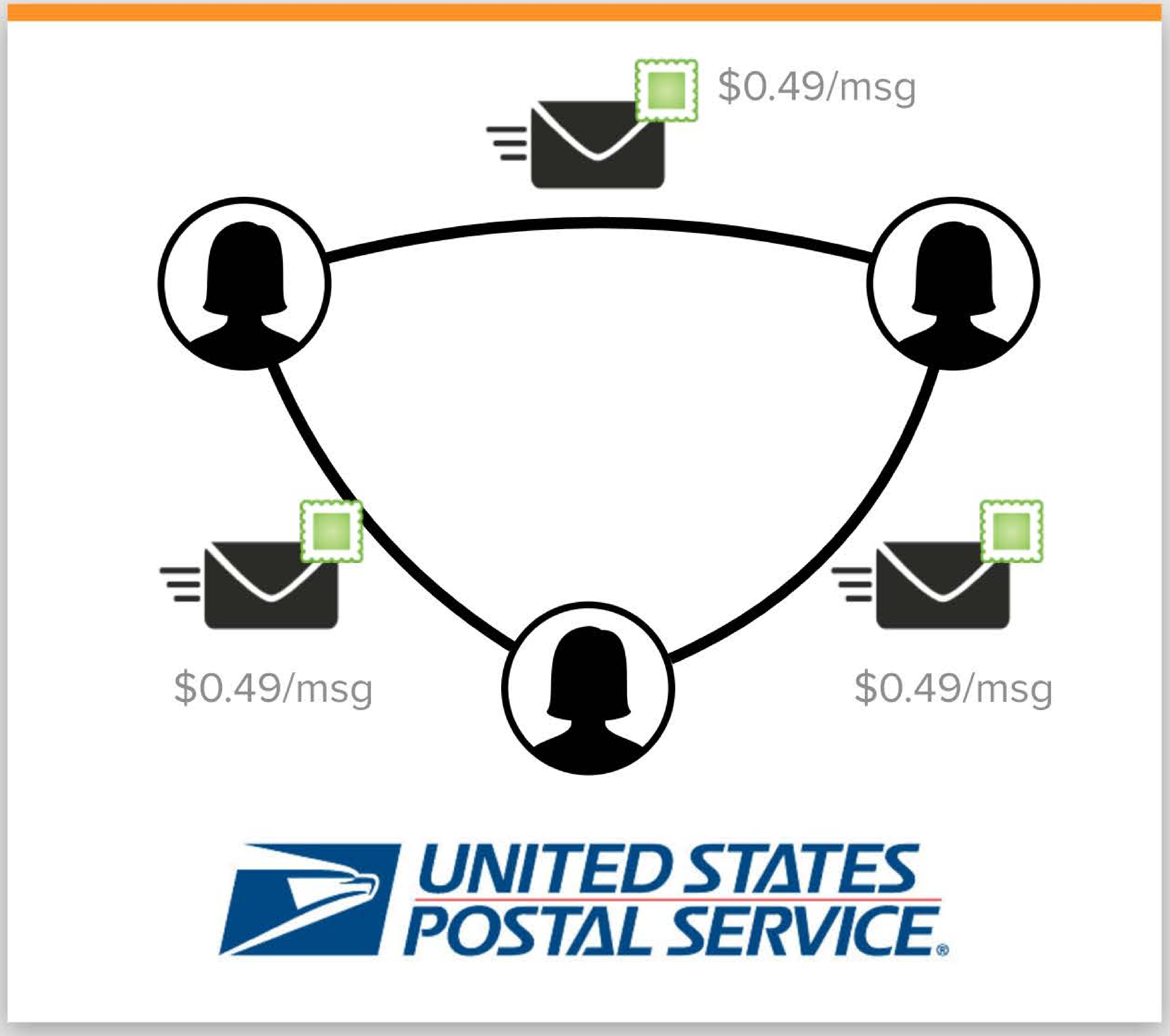
Monetizing the future of money

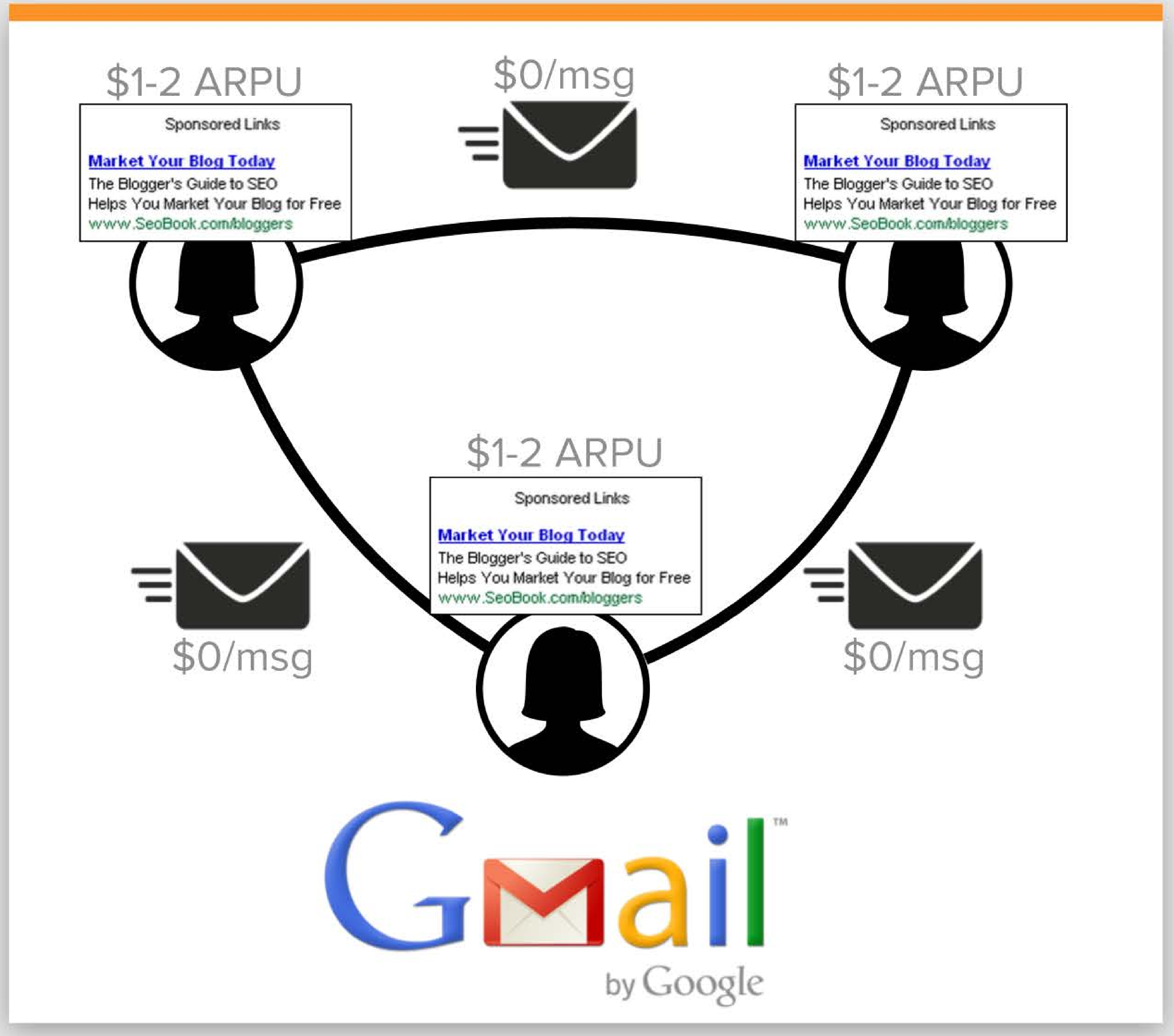
Three strategies for revenue growth

- BitSplit share of mined BTC
- Increased BTC price
- Bitcoin subscription rev for applications

Monetize the Nodes, not the Edges

The USPS monetized physical mail via stamps on the edges. Gmail (FB, TWTR) monetize via ads on the nodes.





Mail was once monetized via edge fees

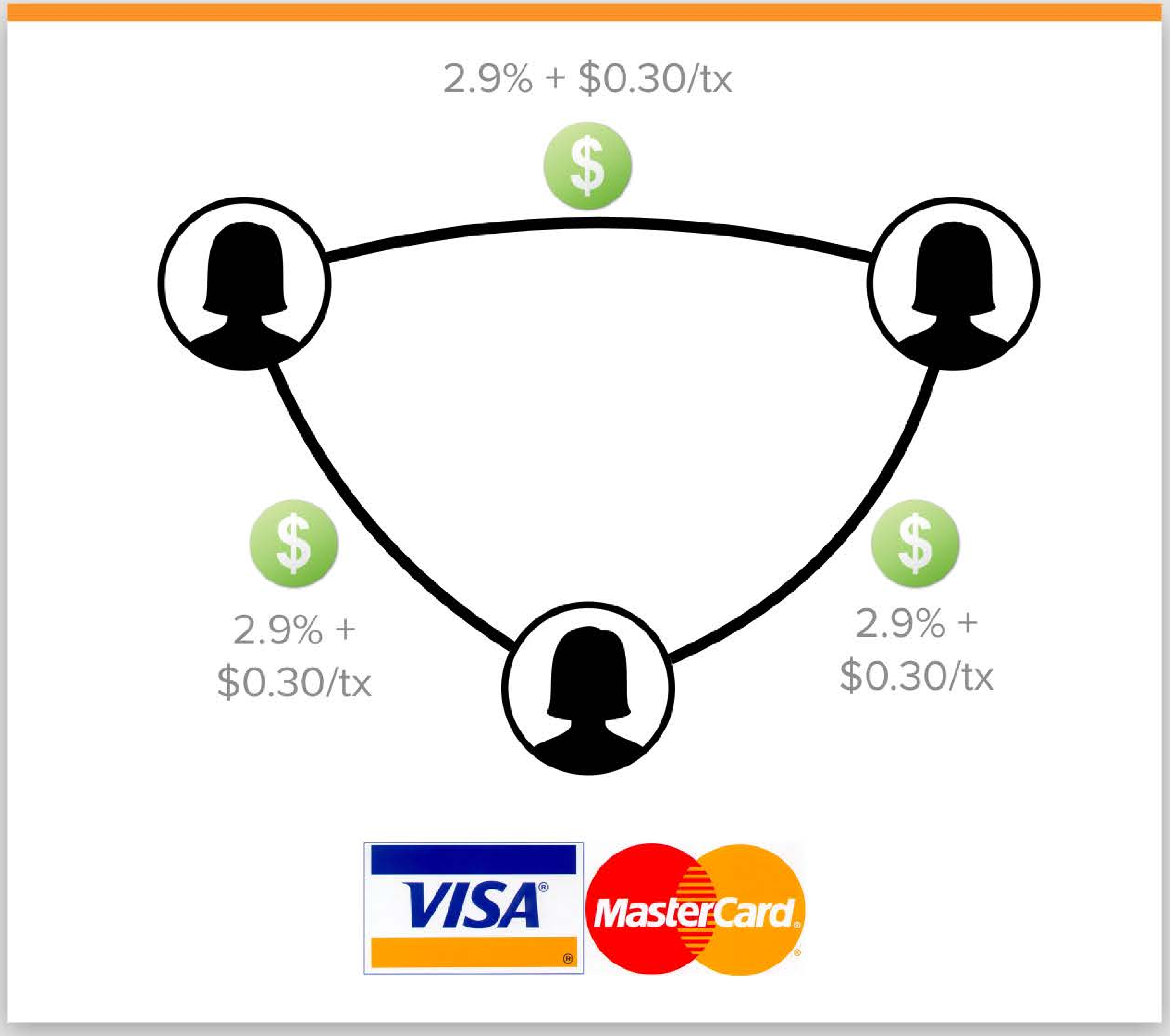
The USPS charge: one stamp for every message sent.

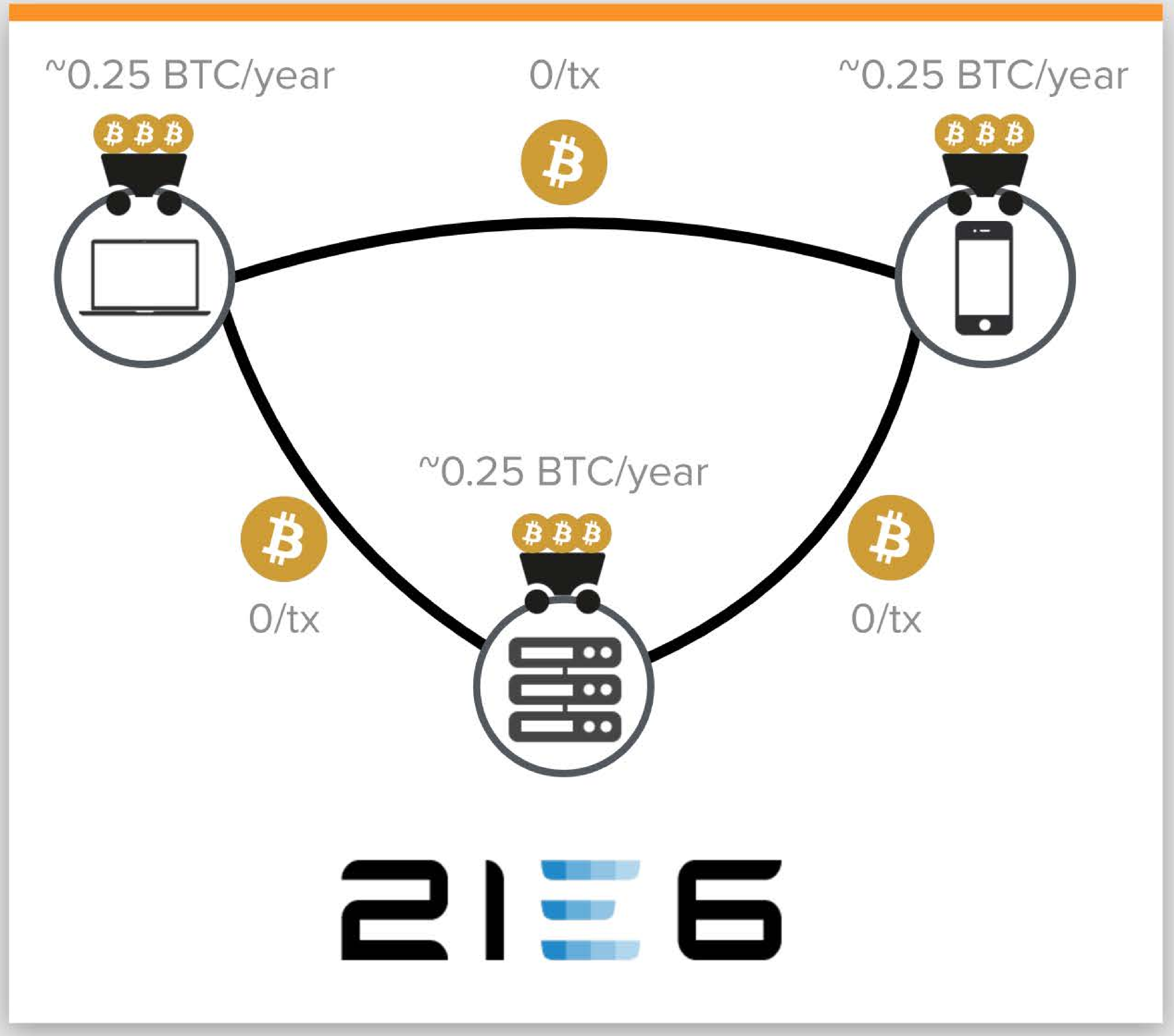
Email is now monetized via node fees

To promote network effect, no edge fees. Ads on nodes.

Monetize the Nodes, not the Edges

Similarly, to encourage growth of machine economy: waive transaction fees & monetize via mining on nodes.





Transactions once monetized via edge fees

The Visa charge: transaction fees for every bit of value sent.

Transactions now monetized via node fees

To promote network effect, no edge fees. Mining on nodes.

Series C

We have 30M of $75M spoken for to grow from enormous miner into the company that makes Bitcoin happen.

Datacenter

- Upgrade of V1 servers to V3 (2.5 PH/s → 17 PH/s)
- New V3 brownfield deployment
- Evaluating increased investment based on price/hashrate trend

BitSplit

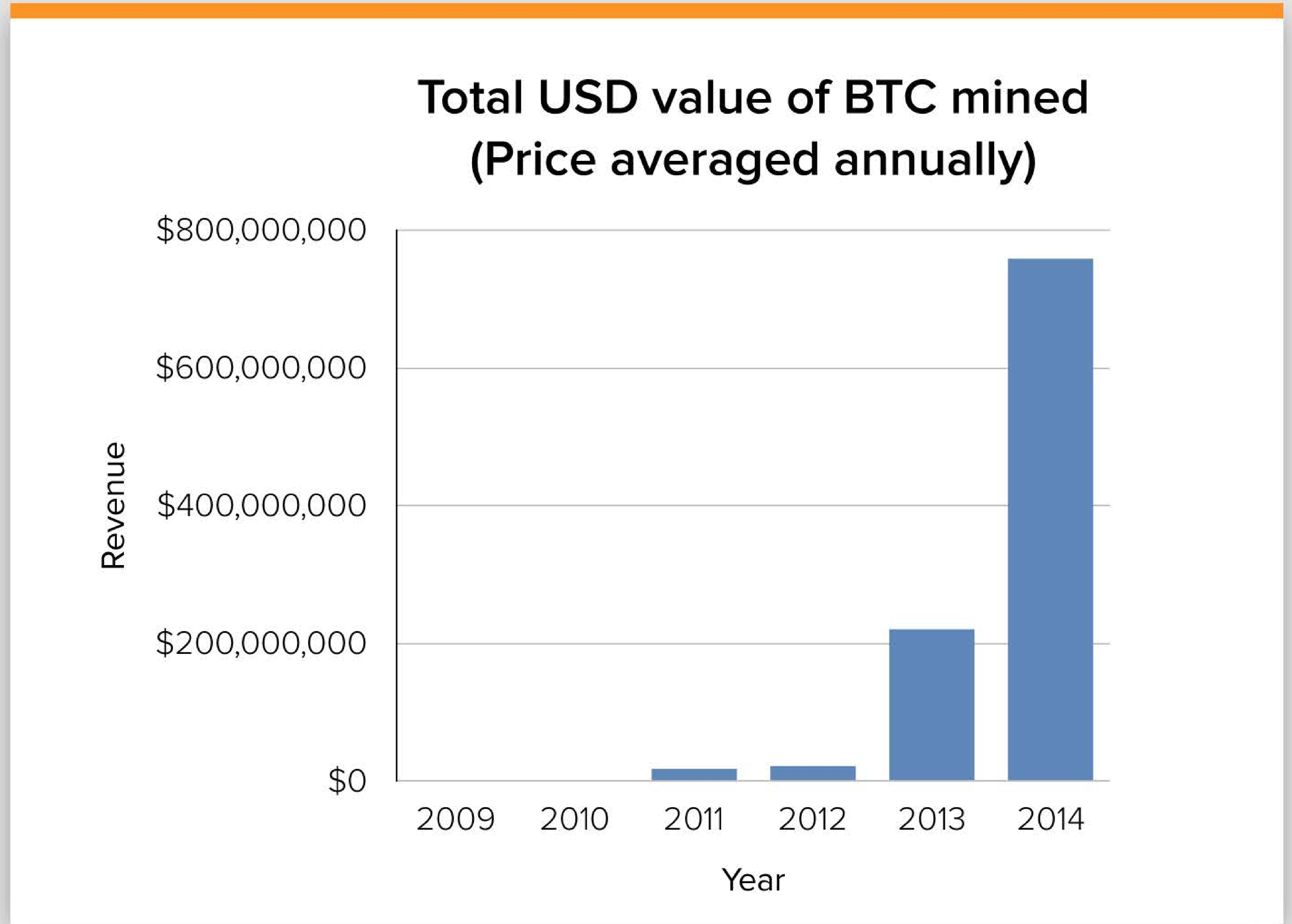
- 250,000 21E6 devices to seed market
- OEM program to enable 3rd parties (device & chipset manufacturers)
- Will evaluate additional first-party devices based on uptake

Summary

Just three premises to believe

Premise 1: Exponential growth

Any market that goes from $0 to $750M+ in four years is worth taking seriously.

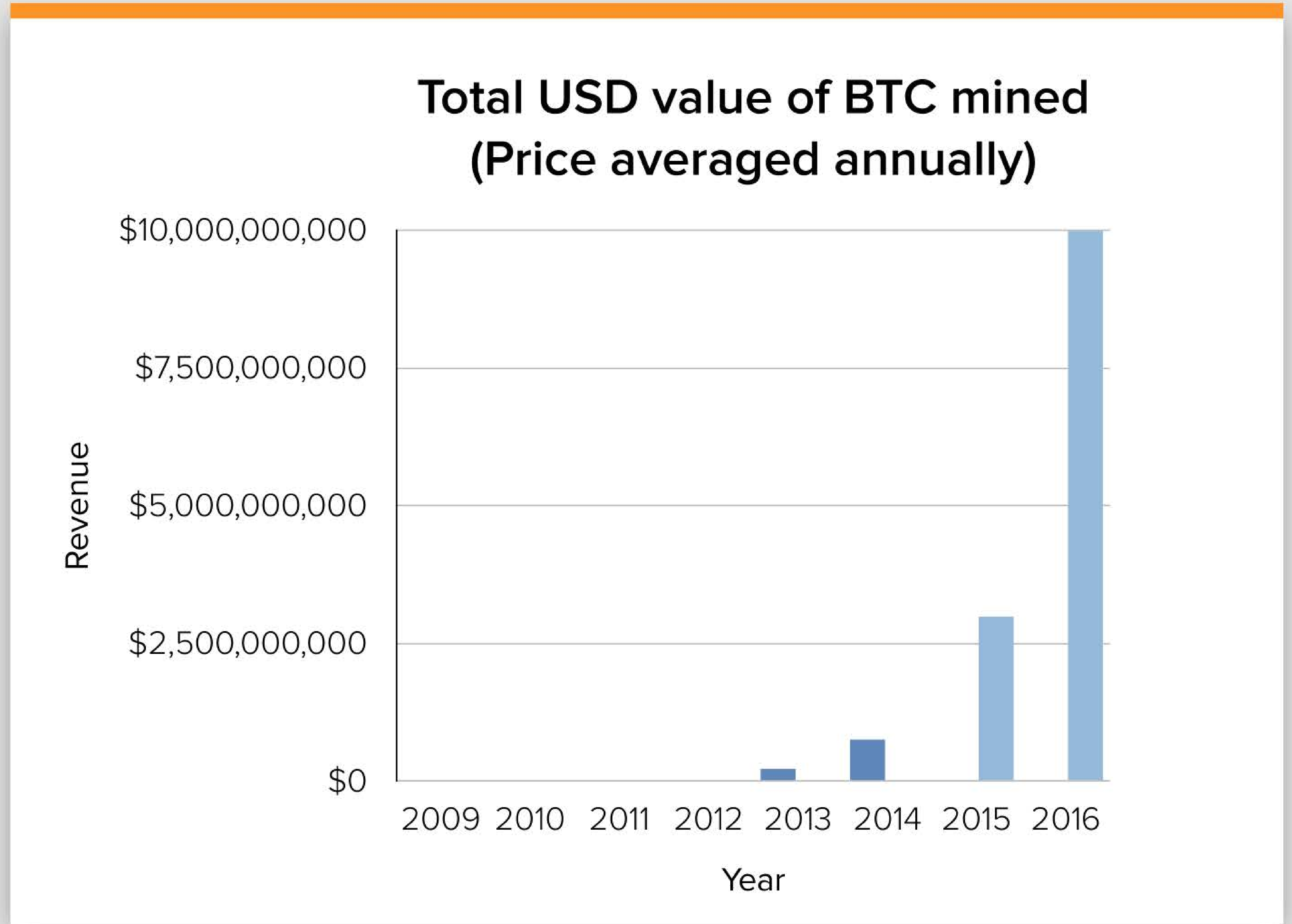


Incredible growth, even with price volatility

From $0 in 2010 to $750M+ in 2014!

Premise 1: Exponential growth

Any market that goes from $0 to $750M+ in four years is worth taking seriously.

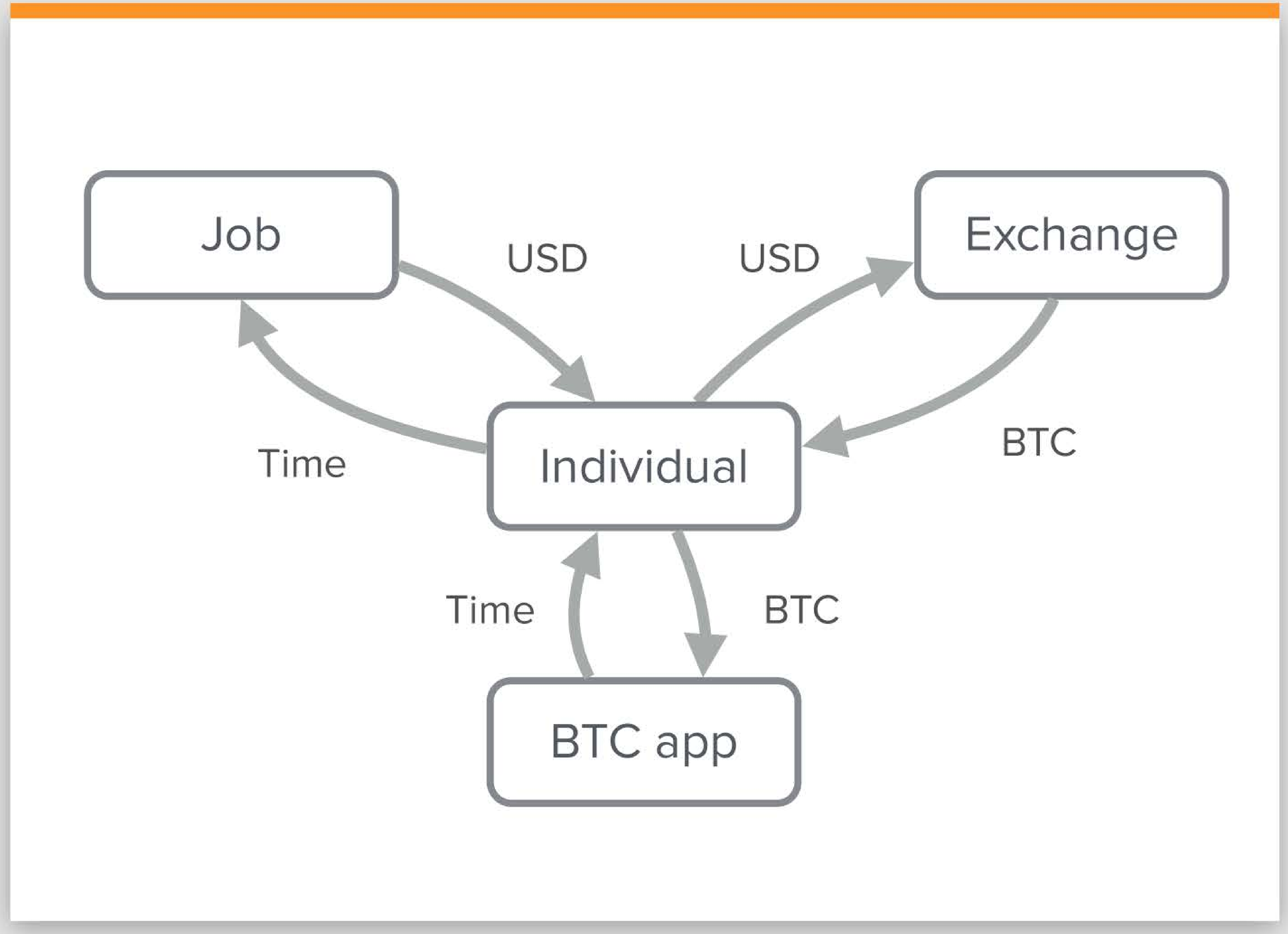


If this continues, it's the big one

Few other markets with potential for this type of exponential growth

Premise 2: Apps boost demand

The sole determinant of price in a supply-constrained market is demand. And Bitcoin apps cause increased demand.

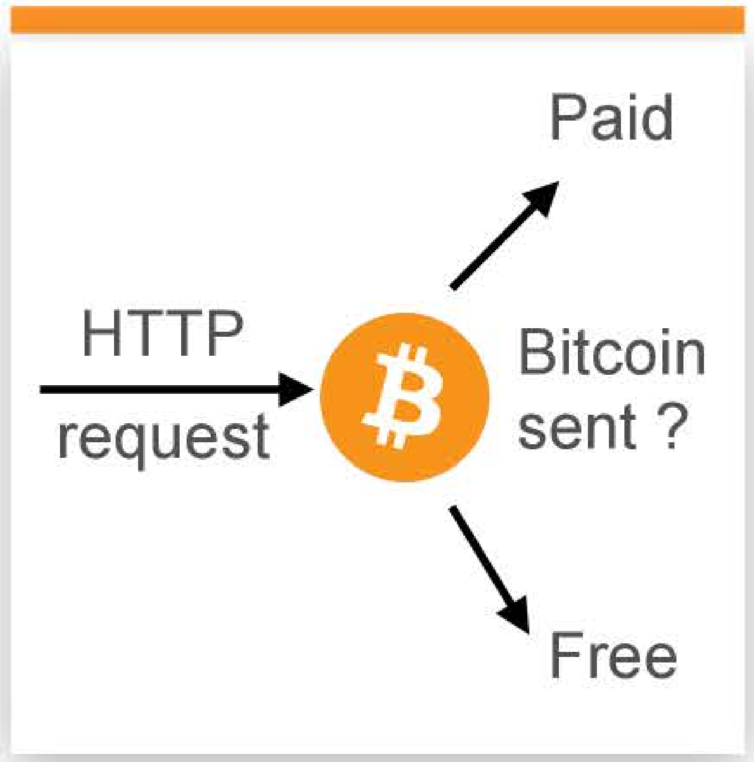


We know people will pay money for time

The demos show Bitcoin - and only BTC - can be used for this purpose

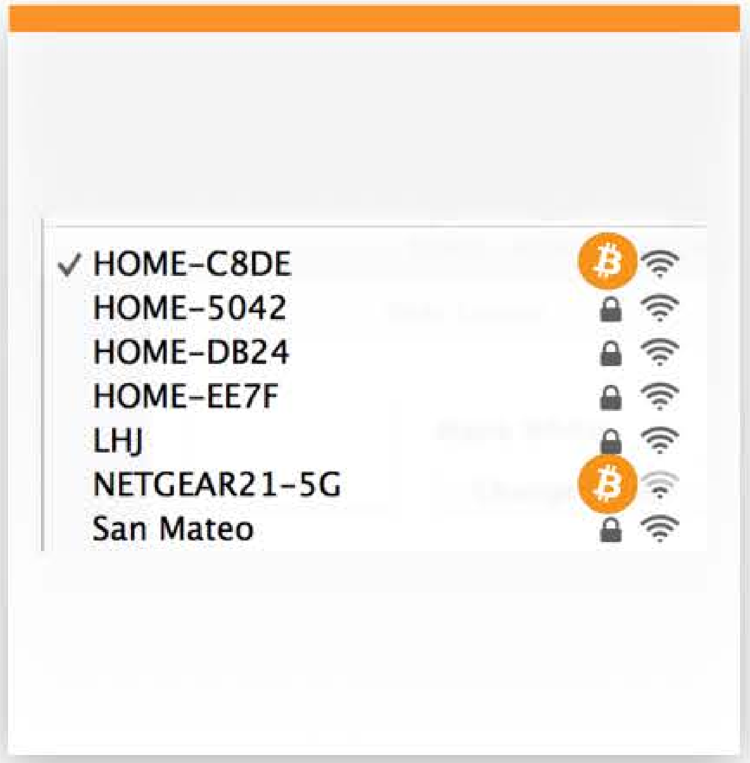
ERROR 402

Branch on BTC payment



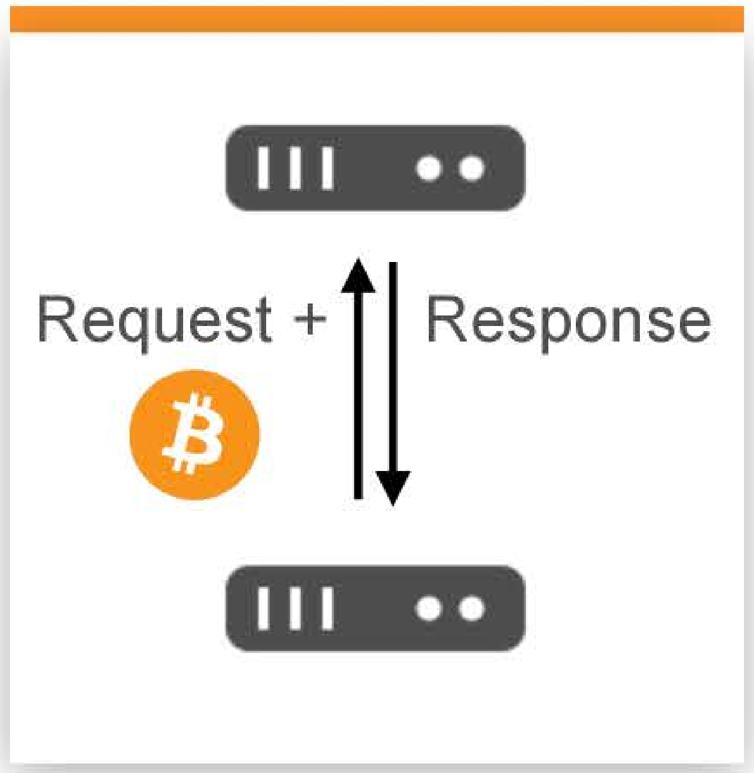
PAID WIFI

BTC for access


✓ HOME-C8DE
HOME-5042
HOME-DB24
HOME-EE7F
LHJ
NETGEAR21-5G
San Mateo

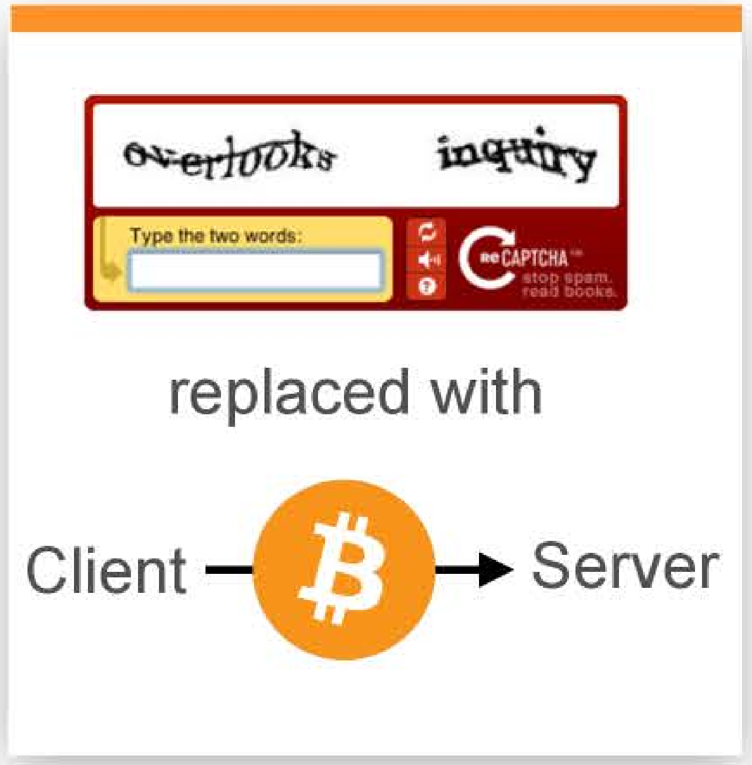
PAID APIS

BTC for API call



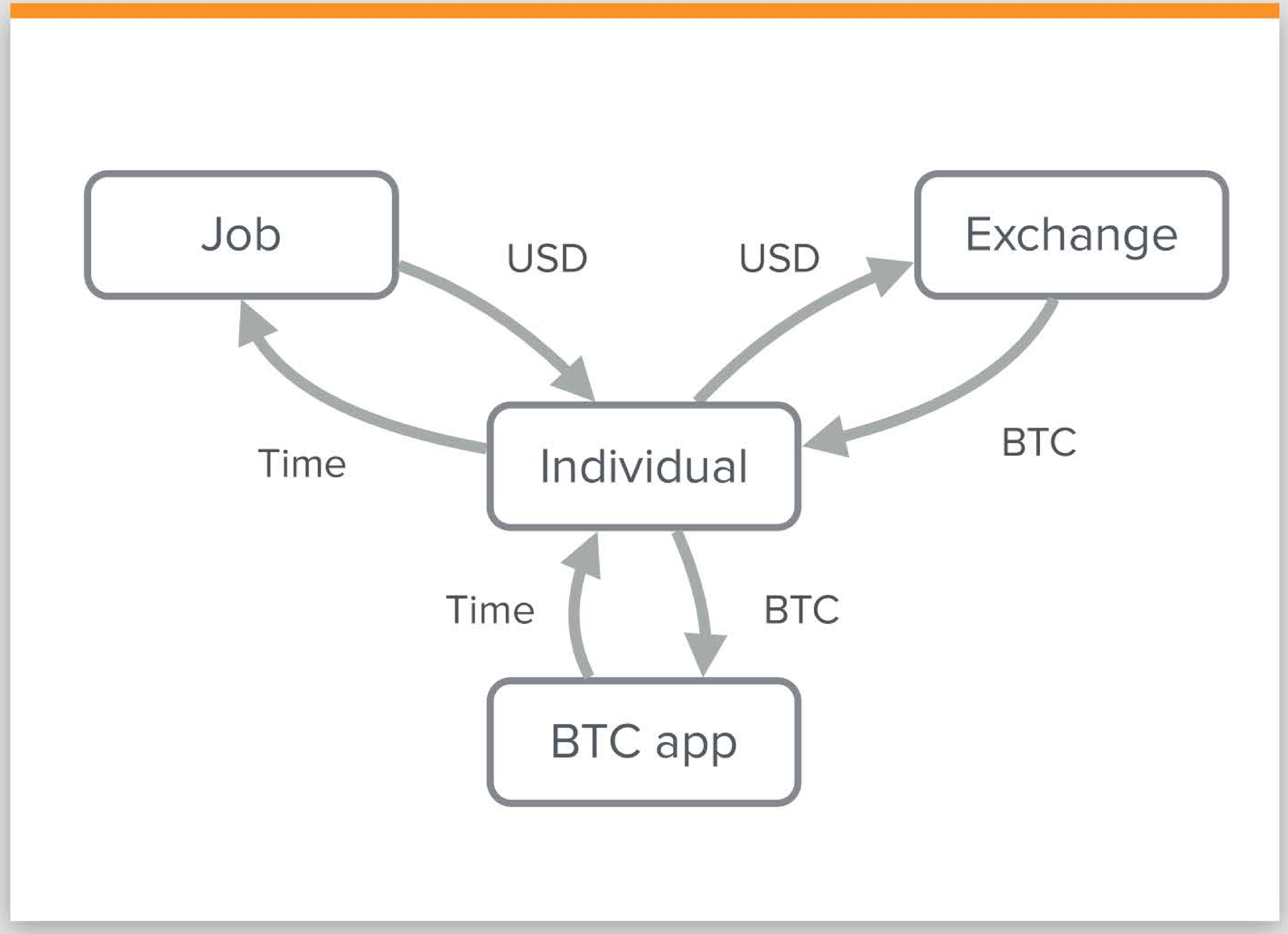
BITCOIN CAPTCHA

Make spam unprofitable



Premise 2: Apps boost demand

The sole determinant of price in a supply-constrained market is demand. And Bitcoin apps cause increased demand.



We know people will pay money for time

The demos show Bitcoin - and only BTC - can be used for this purpose

BITSIGN

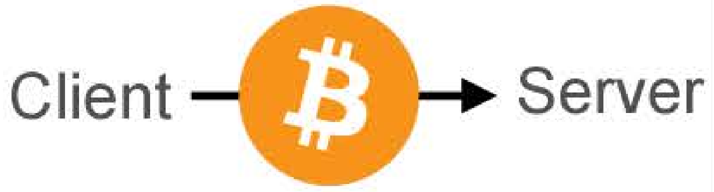
Blockchain notary

AD-FREE BROWSING

Send BTC, see ad-free

Organic Valley Cheese
Try Our Family Of Organic Cheeses Cheddar, Colby, and Muenster Too!
www.organicvalley.coop
Ads by Google

replaced with



SPAMLESS EMAIL

Priority inbox by BTC

Priority Inbox

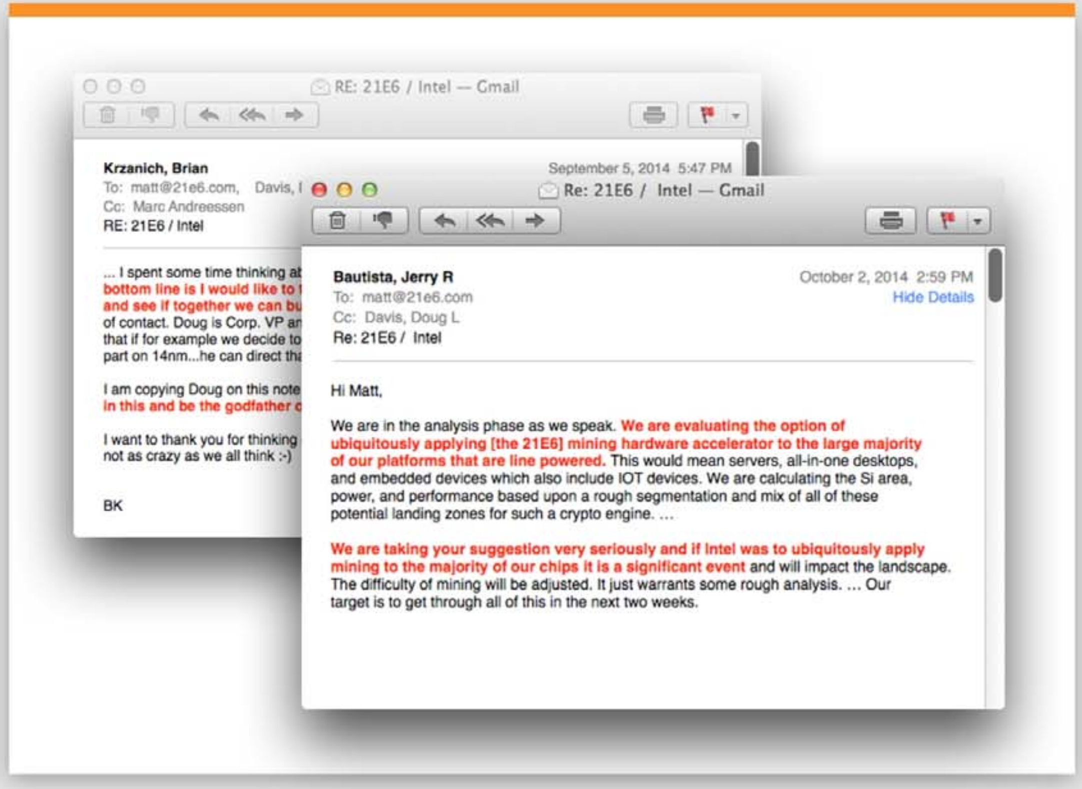
#1	✉	2 uBTC
#2	✉	1 uBTC
#3	✉	0

MORE

Just the start...

Premise 3: We can make margins

Finally, based on distribution contacts, we have a plan to make commanding margins: distributed chips mining for us for free.



Krzanich, Brian
To: matt@21e6.com, Davis, I
Cc: Marc Andreessen
RE: 21E6 / Intel
September 5, 2014 5:47 PM

... I spent some time thinking ab
bottom line is I would like to t
and see if together we can bu
of contact. Doug is Corp. VP an
that if for example we decide to
part on 14nm...he can direct tha

I am copying Doug on this note
in this and be the godfather o

I want to thank you for thinking
not as crazy as we all think :-)

BK

Bautista, Jerry R
To: matt@21e6.com
Cc: Davis, Doug L
Re: 21E6 / Intel
October 2, 2014 2:59 PM

Hi Matt,

We are in the analysis phase as we speak. **We are evaluating the option of ubiquitously applying [the 21E6] mining hardware accelerator to the large majority of our platforms that are line powered.** This would mean servers, all-in-one desktops, and embedded devices which also include IOT devices. We are calculating the Si area, power, and performance based upon a rough segmentation and mix of all of these potential landing zones for such a crypto engine. …

We are taking your suggestion very seriously and if Intel was to ubiquitously apply mining to the majority of our chips it is a significant event and will impact the landscape. The difficulty of mining will be adjusted. It just warrants some rough analysis. … Our target is to get through all of this in the next two weeks.

Intel and AMD both in process

And Facebook, Cisco, Qualcomm, IBM...

21E6

How to mainstream Bitcoin (...and mine it for less than $10/BTC)

2013	Design the world’s best Bitcoin mining chip
2014	Prove it scales by mining millions in BTC
2015	A miner in every device and in every hand

21E6

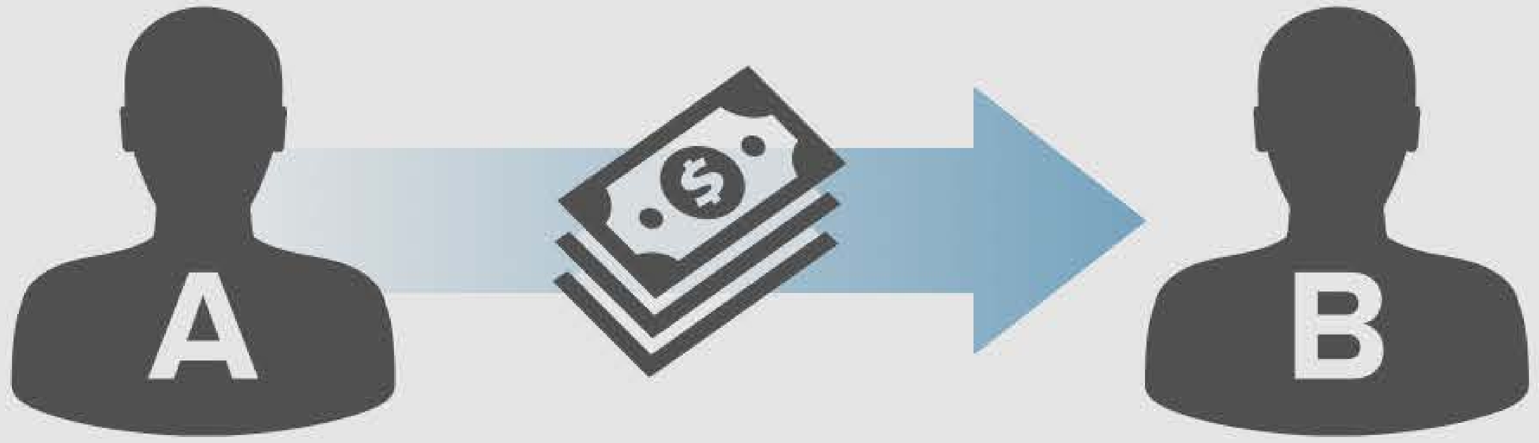
Appendix

Bitcoin is a Protocol

Payments are now packets

In what sense is Bitcoin a protocol?

To understand the progression of ideas, begin with physical cash.



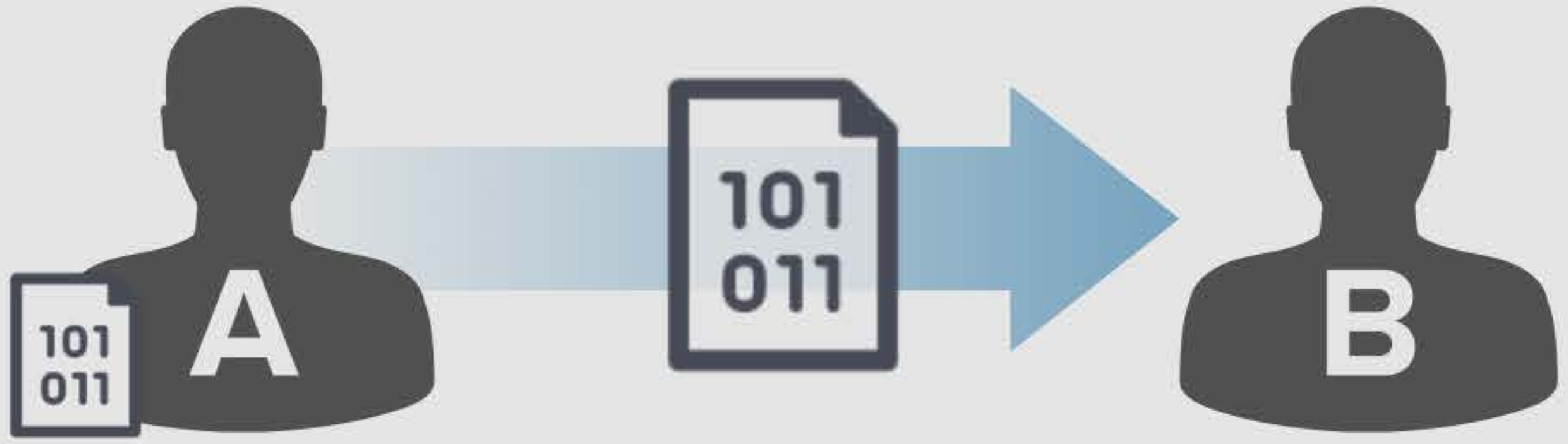
1 PHYSICAL CASH

A hands **B** physical cash.

Implicit property: **A** no longer has the bill, and **B** knows **A** has transferred it.

Many tried to create a "digital cash"

But naively transplanting cash to the digital world doesn't work.



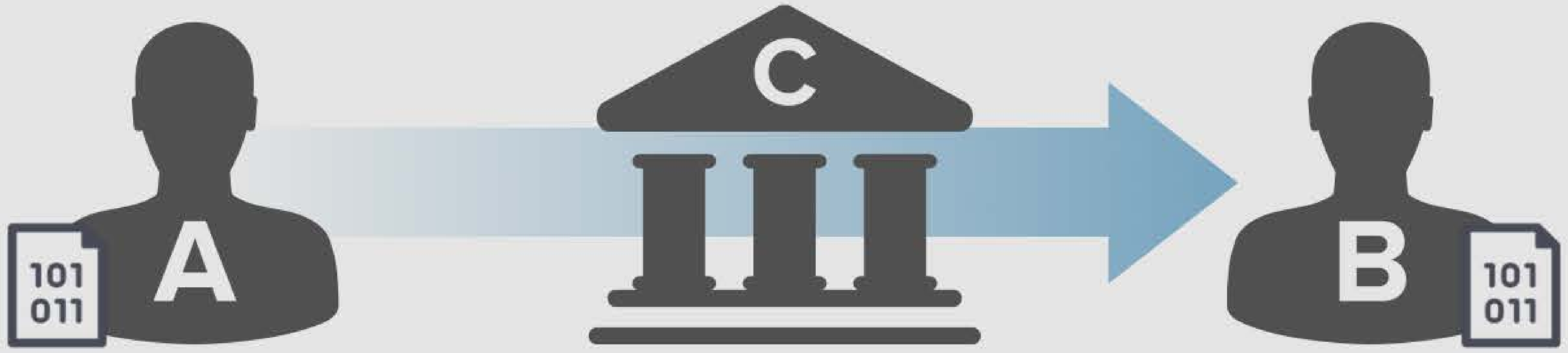
2 NAIVE DIGITAL CASH

A emails **B** the serial numbers on a bill.

But **A** still has those serial numbers — and temptation to “double spend”.

Banks solve this in a centralized way

Each transaction is recorded in a central database, with update permitted only by a short list of trusted financial intermediaries.



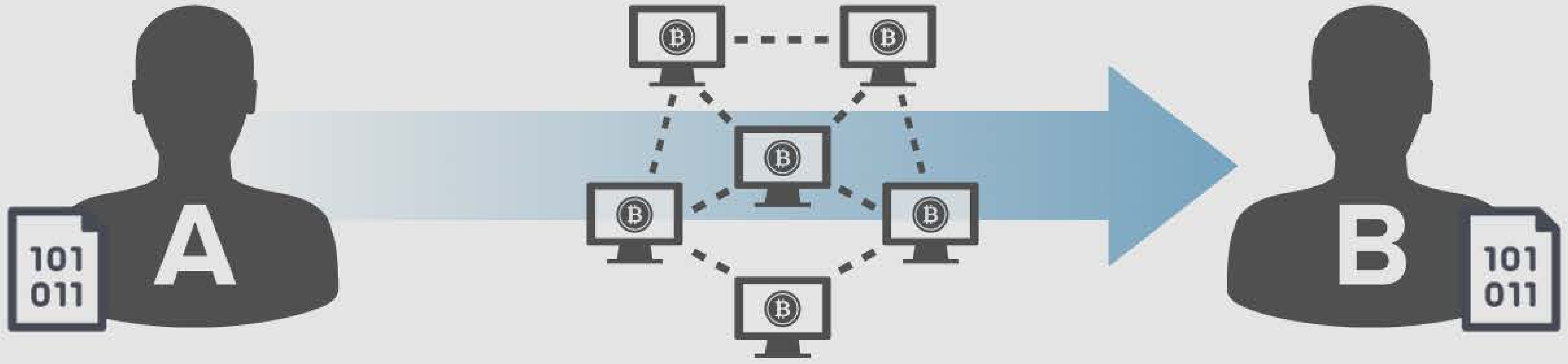
3 CENTRALIZED DIGITAL CASH

A sends **B** money.

C, a centralized bank, records debit/credit.

Bitcoin solves in a decentralized way

Each transaction is pushed out to a distributed database (the Blockchain), updated by a decentralized network of miners.



4 DECENTRALIZED DIGITAL CASH

A sends **B** money.

A global network of "miners" now records the debit/credit.

How does Bitcoin solve the decentralization problem?

Key idea: Byzantine Generals. Permits update of distributed blockchain database in adversarial environment.

Double spending prevented by the blockchain, a distributed ledger of all transactions

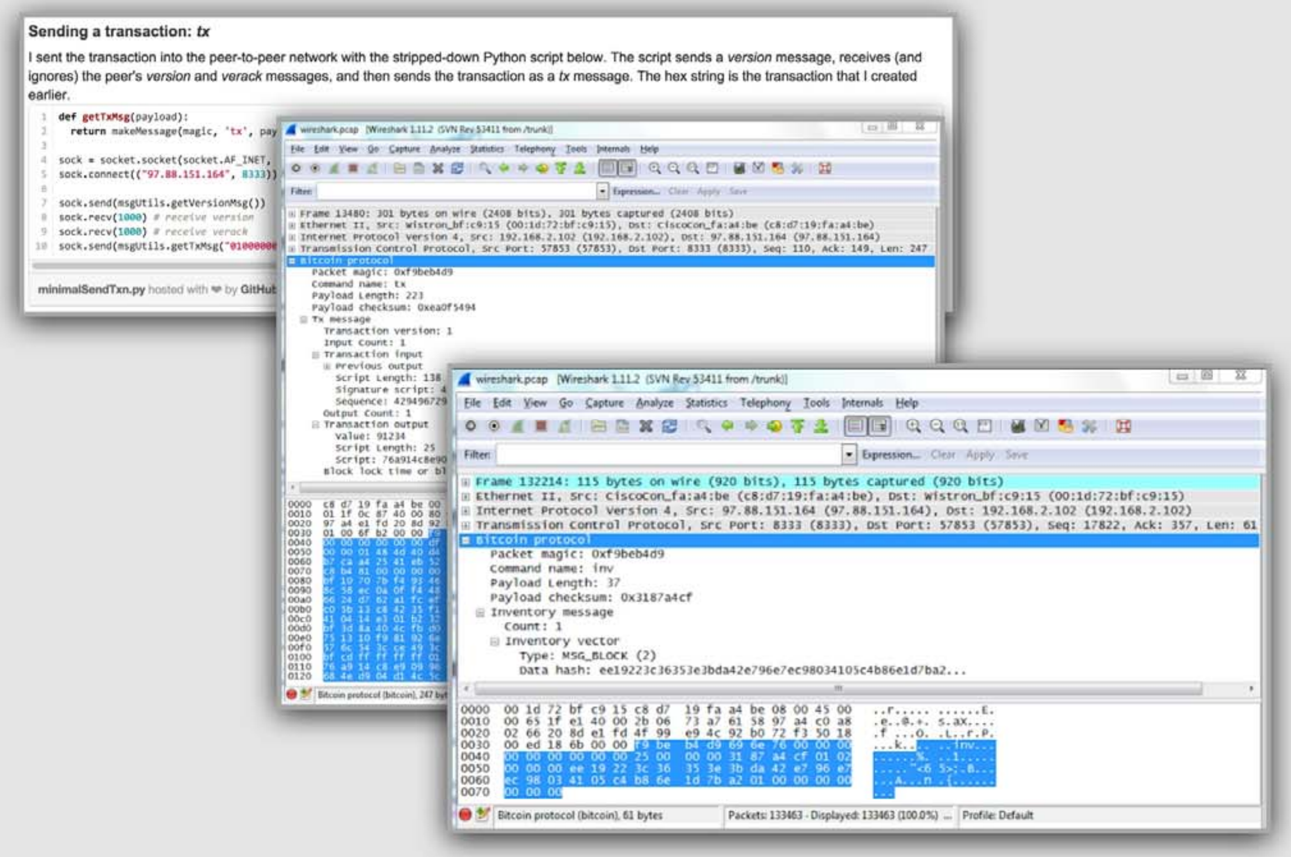
Transactions are aggregated into blocks and chained together to form the blockchain

The majority decision is represented by the longest chain, which has the greatest computation invested in it

The system remains secure if the majority of computational power remains controlled by honest participants

In other words: Bitcoin is a protocol

A transaction is literally a series of bytes broadcast over the internet to a P2P network of miners, with ack after mining.



Sending a transaction: *tx*

I sent the transaction into the peer-to-peer network with the stripped-down Python script below. The script sends a *version* message, receives (and ignores) the peer's *version* and *verack* messages, and then sends the transaction as a *tx* message. The hex string is the transaction that I created earlier.

```
def getTxMsg(payload):
  return makeMessage(magic, 'tx', pay

sock = socket.socket(socket.AF_INET,
sock.connect(("97.88.151.164", 8333))

sock.send(msgUtils.getVersionMsg())
sock.recv(1000) # receive version
sock.recv(1000) # receive verack
sock.send(msgUtils.getTxMsg("0100000
```

minimalSendTxn.py hosted with ❤ by GitHub

wireshark.pcap [Wireshark 1.11.2 (SVN Rev 53411 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
⊞ Frame 13480: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits)
⊞ Ethernet II, Src: Wistron_bf:c9:15 (00:1d:72:bf:c9:15), Dst: CiscoCon_fa:a4:be (c8:d7:19:fa:a4:be)
⊞ Internet Protocol Version 4, Src: 192.168.2.102 (192.168.2.102), Dst: 97.88.151.164 (97.88.151.164)
⊞ Transmission Control Protocol, Src Port: 57853 (57853), Dst Port: 8333 (8333), Seq: 110, Ack: 149, Len: 247
⊟ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: tx
    Payload Length: 223
    Payload checksum: 0xea0f5494
  ⊟ Tx message
      Transaction version: 1
      Input Count: 1
    ⊟ Transaction input
      ⊞ Previous output
        Script Length: 138
        Signature script: 4
        Sequence: 429496729
      Output Count: 1
    ⊟ Transaction output
        Value: 91234
        Script Length: 25
        Script: 76a914c8e90
      Block lock time or bl

0000  c8 d7 19 fa a4 be 00
0010  01 1f 0c 87 40 00 80
0020  97 a4 e1 fd 20 8d 92
0030  01 00 6f b2 00 00 f9
0040  00 00 00 00 00 00 df
0050  00 00 01 48 4d 40 d4
0060  b7 ca a4 25 41 eb 52
0070  c8 b4 81 00 00 00 00
0080  bf 10 70 7b f4 93 46
0090  8c 58 ec 0a 0f f4 48
00a0  66 24 d7 62 a1 fc ef
00b0  c0 3b 13 c8 42 35 f1
00c0  41 04 14 e3 01 b2 32
00d0  bf 3d 8a 40 4c fb d0
00e0  75 13 10 f9 81 92 6e
00f0  57 6c 34 3c ce 49 3c
0100  bf cd ff ff ff ff 01
0110  76 a9 14 c8 e9 09 96
0120  68 4e d9 04 d1 4c 5c
```

Bitcoin protocol (bitcoin), 247 byt

wireshark.pcap [Wireshark 1.11.2 (SVN Rev 53411 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

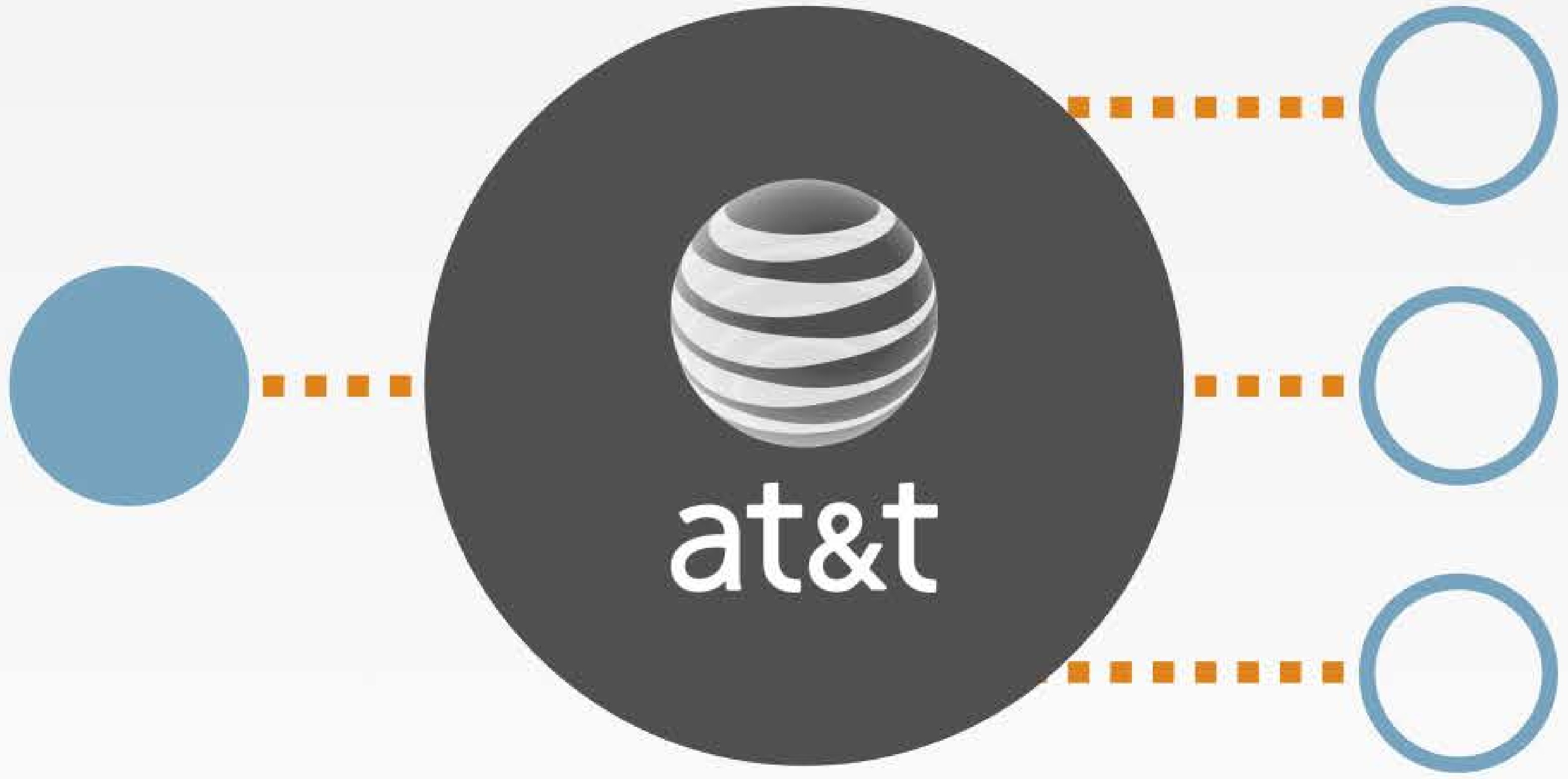
```
⊞ Frame 132214: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
⊞ Ethernet II, Src: CiscoCon_fa:a4:be (c8:d7:19:fa:a4:be), Dst: Wistron_bf:c9:15 (00:1d:72:bf:c9:15)
⊞ Internet Protocol Version 4, Src: 97.88.151.164 (97.88.151.164), Dst: 192.168.2.102 (192.168.2.102)
⊞ Transmission Control Protocol, Src Port: 8333 (8333), Dst Port: 57853 (57853), Seq: 17822, Ack: 357, Len: 61
⊟ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: inv
    Payload Length: 37
    Payload checksum: 0x3187a4cf
  ⊟ Inventory message
      Count: 1
    ⊟ Inventory vector
        Type: MSG_BLOCK (2)
        Data hash: ee19223c36353e3bda42e796e7ec98034105c4b86e1d7ba2...

0000  00 1d 72 bf c9 15 c8 d7  19 fa a4 be 08 00 45 00   ..r..... ......E.
0010  00 65 1f e1 40 00 2b 06  73 a7 61 58 97 a4 c0 a8   .e..@.+. s.aX....
0020  02 66 20 8d e1 fd 4f 99  e9 4c 92 b0 72 f3 50 18   .f ...O. .L..r.P.
0030  00 ed 18 6b 00 00 f9 be  b4 d9 69 6e 76 00 00 00   ...k.... ..inv...
0040  00 00 00 00 00 00 25 00  00 00 31 87 a4 cf 01 02   ......%. ..1.....
0050  00 00 00 ee 19 22 3c 36  35 3e 3b da 42 e7 96 e7   ....."<6 5>;.B...
0060  ec 98 03 41 05 c4 b8 6e  1d 7b a2 01 00 00 00 00   ...A...n .{......
0070  00 00 00                                           ...
```

Bitcoin protocol (bitcoin), 61 bytes | Packets: 133463 · Displayed: 133463 (100.0%) ... | Profile: Default

This is why we compare Bitcoin to the Internet

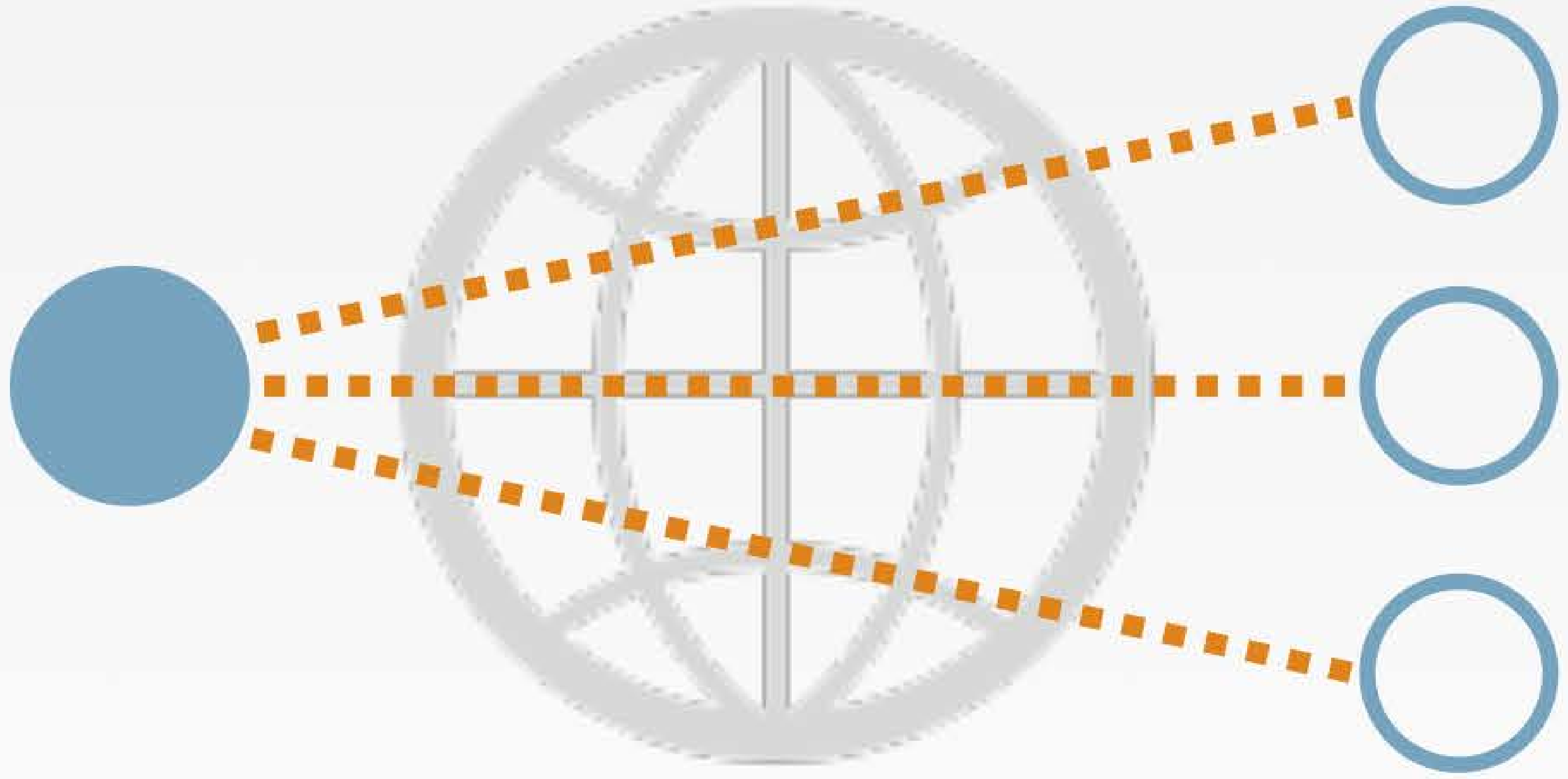
The internet disintermediated telcos, replacing with programmable packet-based communication.

BEFORE



Deal with telco to deploy
code related to information
on the network backbone

AFTER

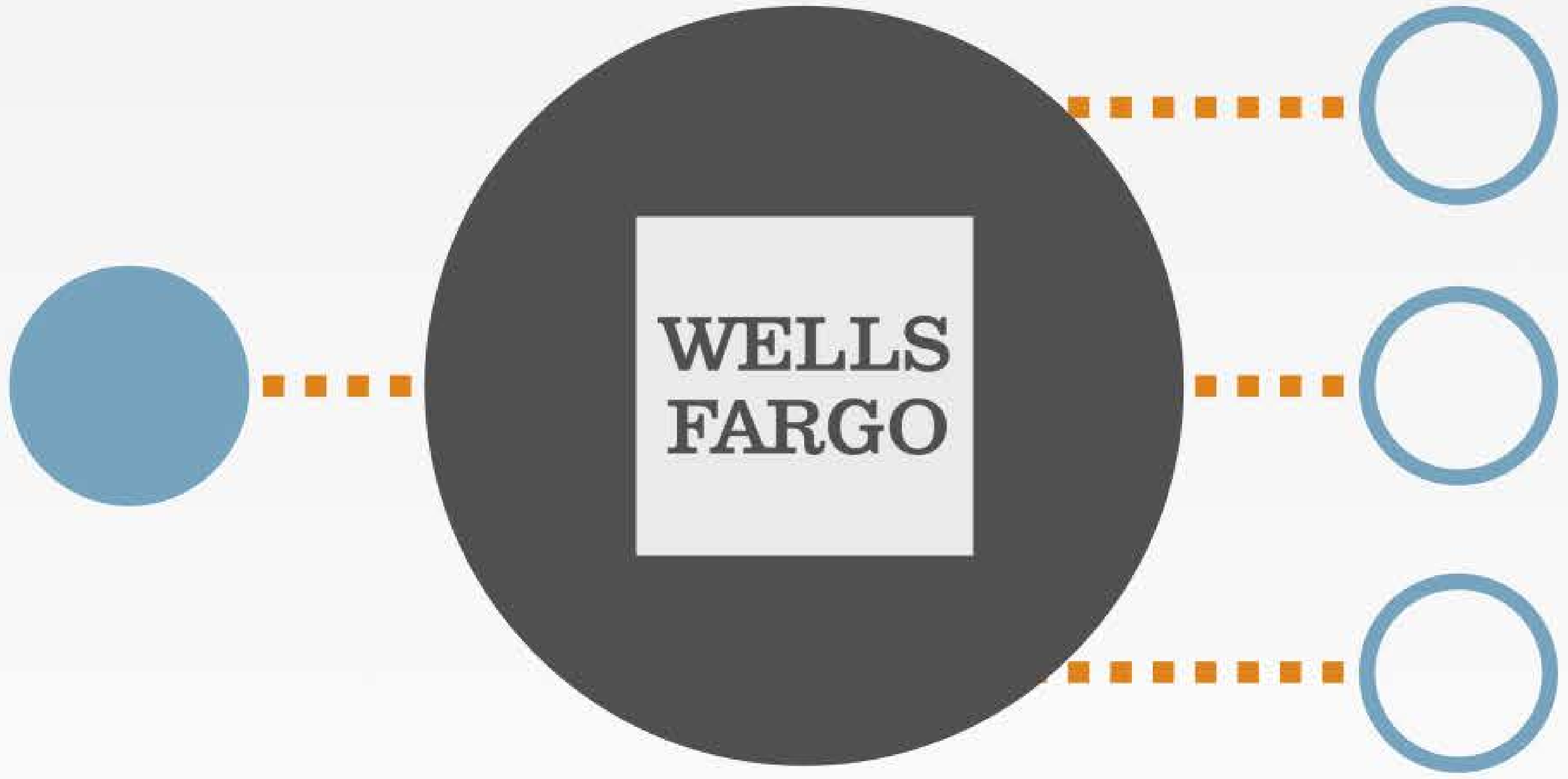


Anyone can programmatically
send packets to anyone
(or many anyones) via internet

Bitcoin disintermediates banks

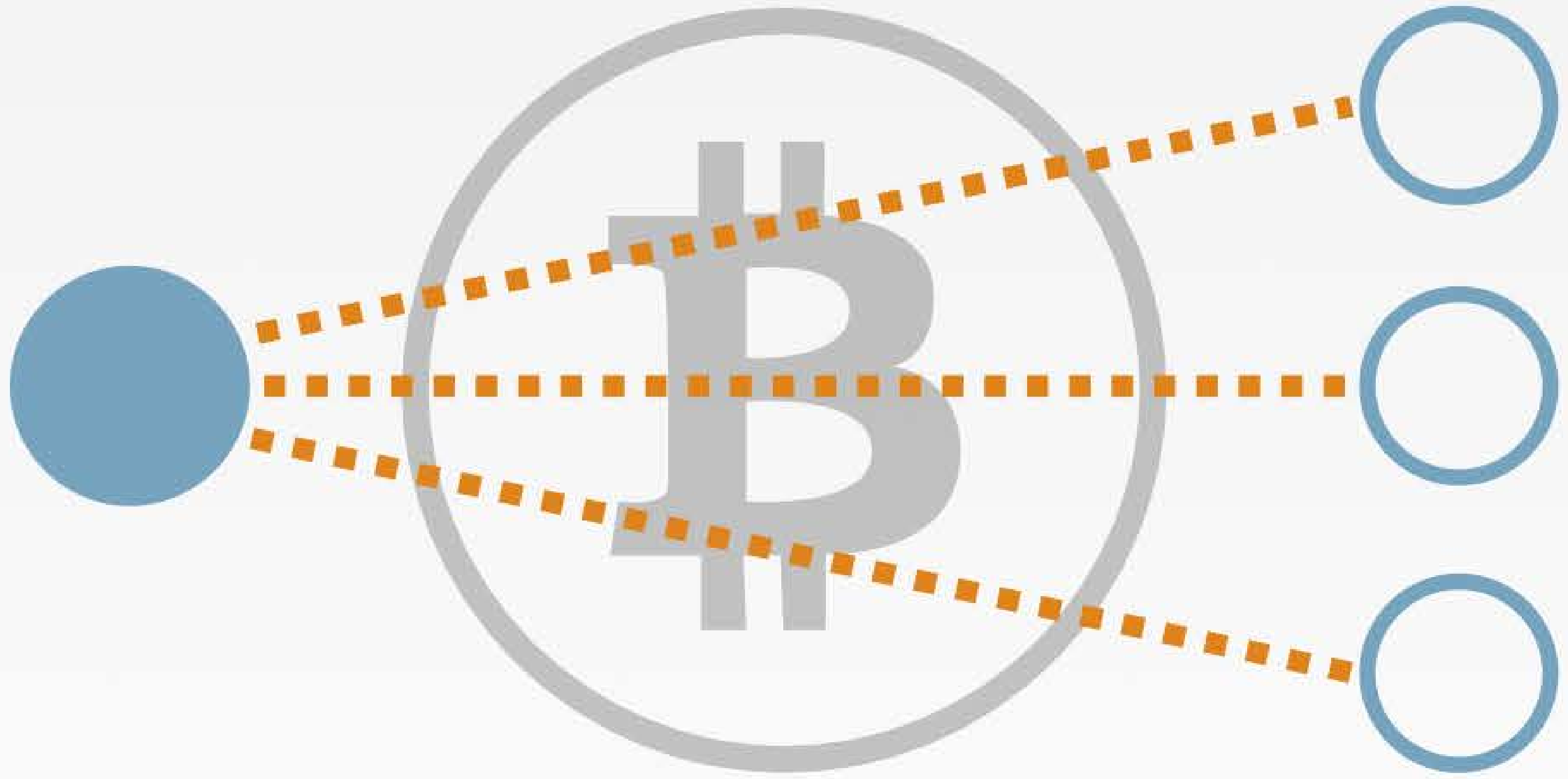
Similarly, Bitcoin disintermediates Fedwire/ACH/SWIFT, replacing with programmable packet-based money.

BEFORE



Deal with bank to deploy
code related to value
in the banking system

AFTER



Anyone can programmatically
send value to anyone
(or many anyones) via internet

To the end user, Bitcoin is like email

Like email, others can send to your public Bitcoin/email address - but only you can send out w/ your private key.

joe@gmail.com

Anyone can send you email if they know your public email address.

****

But **only you** can send email from that account with your private email password.

15qSxP1SQcUX3o4nhkfdbgyoWEFMomJ4rZ

Anyone can send you Bitcoin if they know your public Bitcoin address.

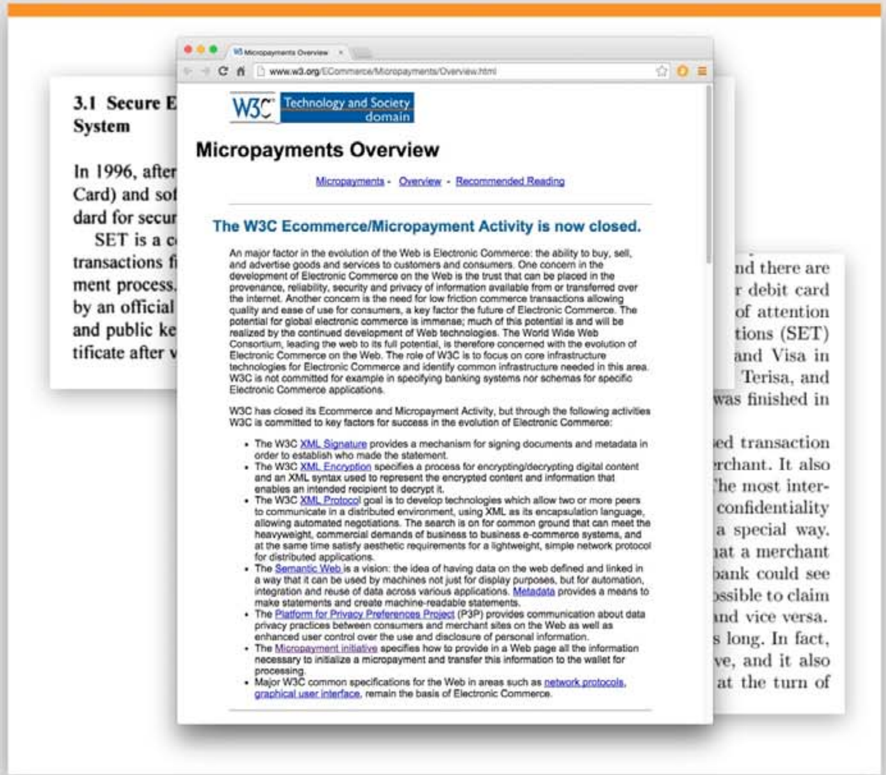
****

But **only you** can send Bitcoin from that address with your private Bitcoin key.

Just like there is no ‘email.com’ that owns email, there is no ‘bitcoin.com’ that owns Bitcoin; **the code is open-source.**

If Bitcoin existed in 1994, we'd have put it in the browser

At Netscape, we tried negotiating with Visa for years to put micropayments in the browser. It's finally time.


Micropayments Overview
www.w3.org/ECommerce/Micropayments/Overview.html
W3C Technology and Society domain

3.1 Secure E
System

In 1996, after
Card) and sof
dard for secur
SET is a c
transactions f
ment process.
by an official
and public ke
tificate after v

Micropayments Overview

Micropayments - Overview - Recommended Reading

The W3C Ecommerce/Micropayment Activity is now closed.

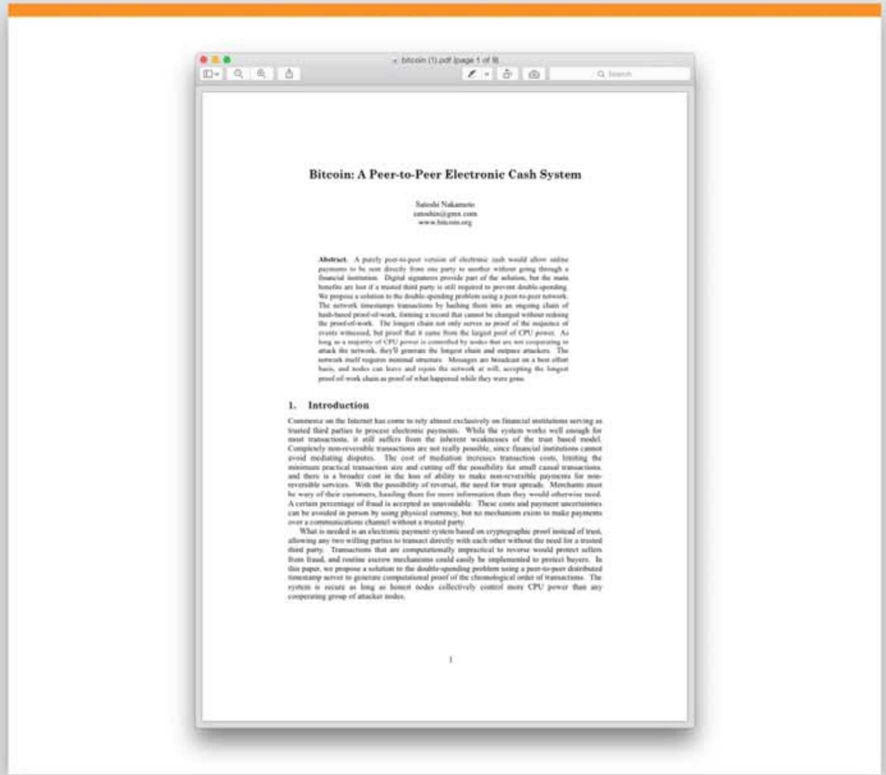
An major factor in the evolution of the Web is Electronic Commerce: the ability to buy, sell, and advertise goods and services to customers and consumers. One concern in the development of Electronic Commerce on the Web is the trust that can be placed in the provenance, reliability, security and privacy of information available from or transferred over the internet. Another concern is the need for low friction commerce transactions allowing quality and ease of use for consumers, a key factor the future of Electronic Commerce. The potential for global electronic commerce is immense; much of this potential is and will be realized by the continued development of Web technologies. The World Wide Web Consortium, leading the web to its full potential, is therefore concerned with the evolution of Electronic Commerce on the Web. The role of W3C is to focus on core infrastructure technologies for Electronic Commerce and identify common infrastructure needed in this area. W3C is not committed for example in specifying banking systems nor schemas for specific Electronic Commerce applications.

W3C has closed its Ecommerce and Micropayment Activity, but through the following activities W3C is committed to key factors for success in the evolution of Electronic Commerce:

- The W3C XML Signature provides a mechanism for signing documents and metadata in order to establish who made the statement.
- The W3C XML Encryption specifies a process for encrypting/decrypting digital content and an XML syntax used to represent the encrypted content and information that enables an intended recipient to decrypt it.
- The W3C XML Protocol goal is to develop technologies which allow two or more peers to communicate in a distributed environment, using XML as its encapsulation language, allowing automated negotiations. The search is on for common ground that can meet the heavyweight, commercial demands of business to business e-commerce systems, and at the same time satisfy aesthetic requirements for a lightweight, simple network protocol for distributed applications.
- The Semantic Web is a vision: the idea of having data on the web defined and linked in a way that it can be used by machines not just for display purposes, but for automation, integration and reuse of data across various applications. Metadata provides a means to make statements and create machine-readable statements.
- The Platform for Privacy Preferences Project (P3P) provides communication about data privacy practices between consumers and merchant sites on the Web as well as enhanced user control over the use and disclosure of personal information.
- The Micropayment initiative specifies how to provide in a Web page all the information necessary to initialize a micropayment and transfer this information to the wallet for processing.
- Major W3C common specifications for the Web in areas such as network protocols, graphical user interface, remain the basis of Electronic Commerce.

nd there are
r debit card
of attention
tions (SET)
and Visa in
Terisa, and
was finished in

ed transaction
rchant. It also
The most inter-
confidentiality
a special way.
at a merchant
bank could see
ssible to claim
nd vice versa.
s long. In fact,
ve, and it also
at the turn of



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, 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 non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

We tried to get micropayments into browser

In retrospect, lacked tech for web-style decentralization

People forgot, gave up. Then came Bitcoin.

Just like convergence device and VR, the 90s ideas now work

Bitcoin is like Linux

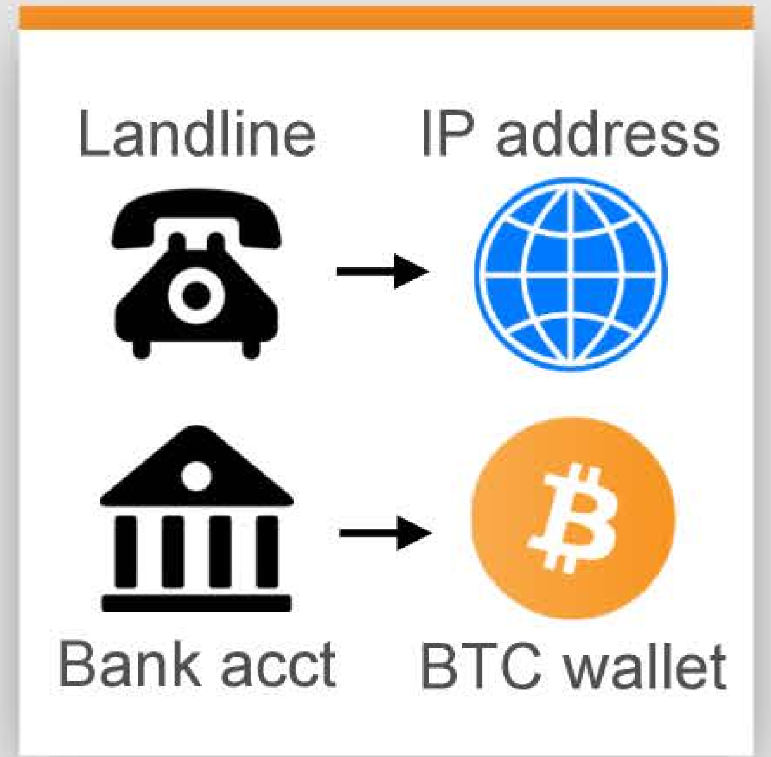
A programmable and customizable OS for money

Bitcoin is to Paypal as Linux is to Windows

We've already seen what happens when an open-source, decentralized, programmable version arises.

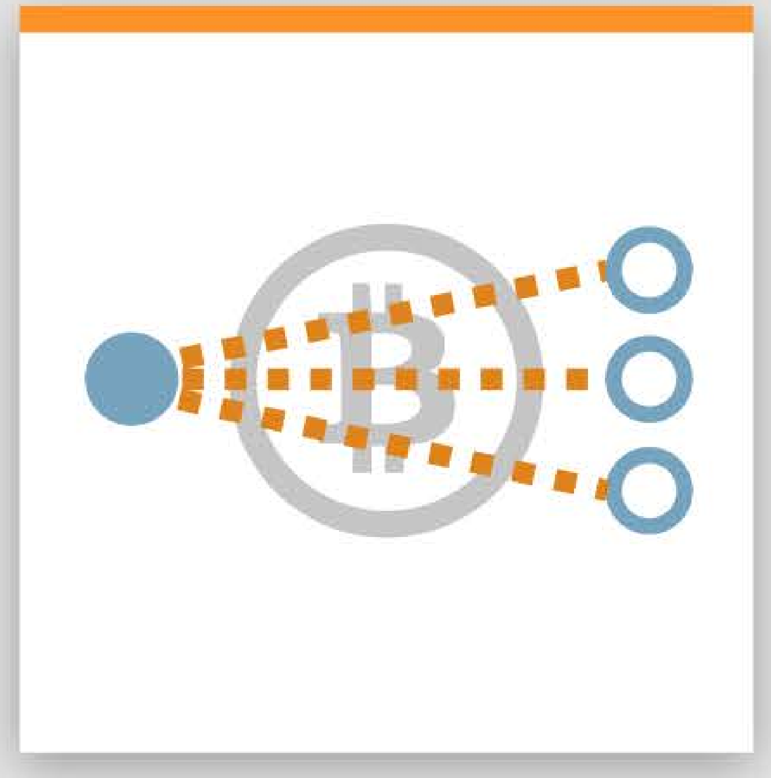
EVERY ENTITY

Banking for anything



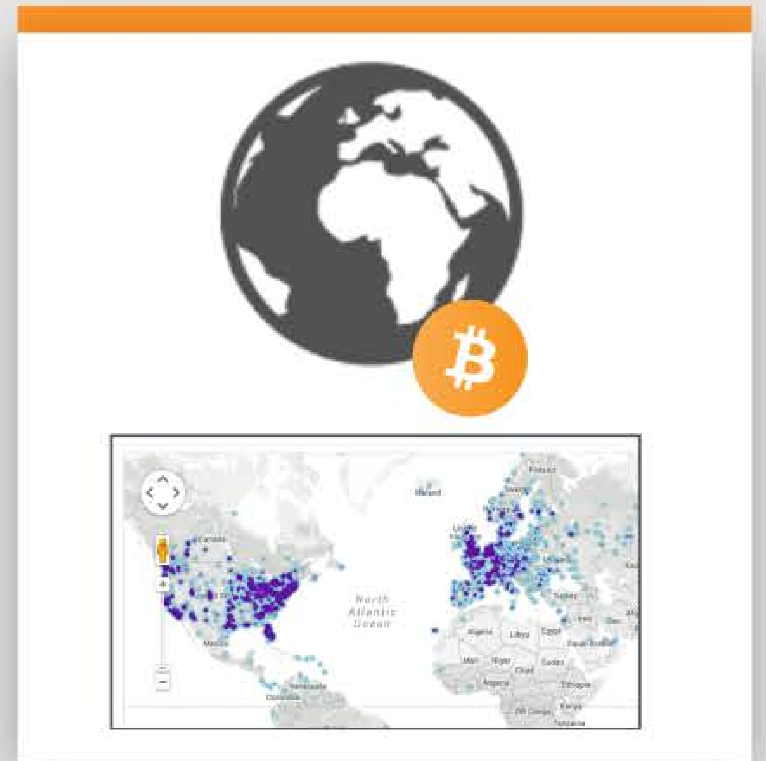
EVERY DEVICE

Connected? Send/receive.



EVERY COUNTRY

Available worldwide



EVERY AMOUNT

From micro to macro

Sending
.000000001 BTC

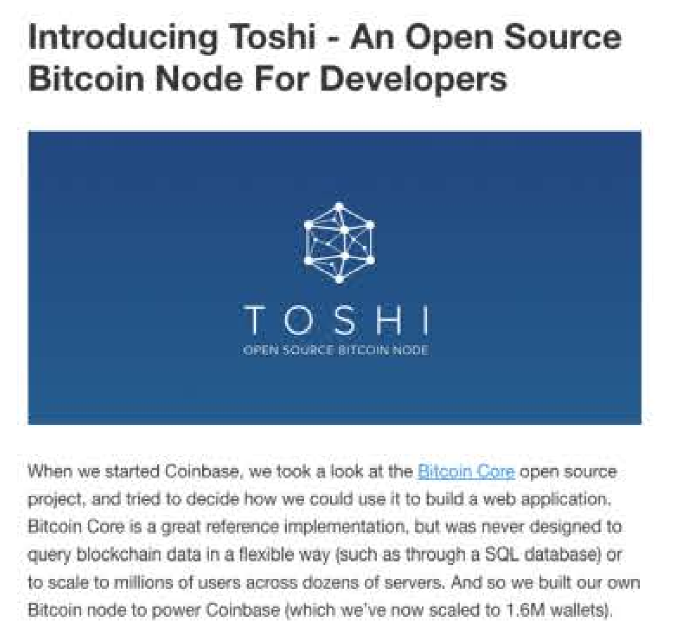
1GSwxzetCRFzwCiSqyvQMHZuSdymWbrENn - (Spent)

Sending
550,000 BTC

1M8s2S5bgAzSSzVTeL7zruvMPLvzSkEAuv - (Spent)

EXTENSIBLE

Modify code, add features

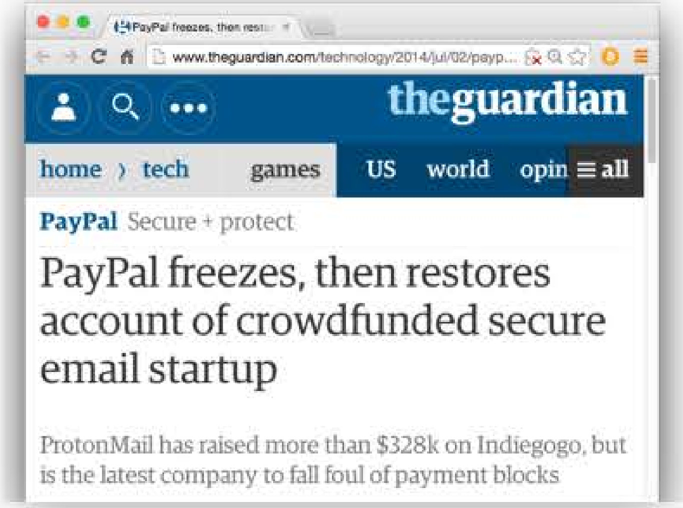


Introducing Toshi - An Open Source Bitcoin Node For Developers

When we started Coinbase, we took a look at the Bitcoin Core open source project, and tried to decide how we could use it to build a web application. Bitcoin Core is a great reference implementation, but was never designed to query blockchain data in a flexible way (such as through a SQL database) or to scale to millions of users across dozens of servers. And so we built our own Bitcoin node to power Coinbase (which we've now scaled to 1.6M wallets).

UNFREEZABLE

Full personal control


PayPal freezes, then resto
www.theguardian.com/technology/2014/jul/02/payp...
theguardian
home
tech
games
US
world
opin
≡ all

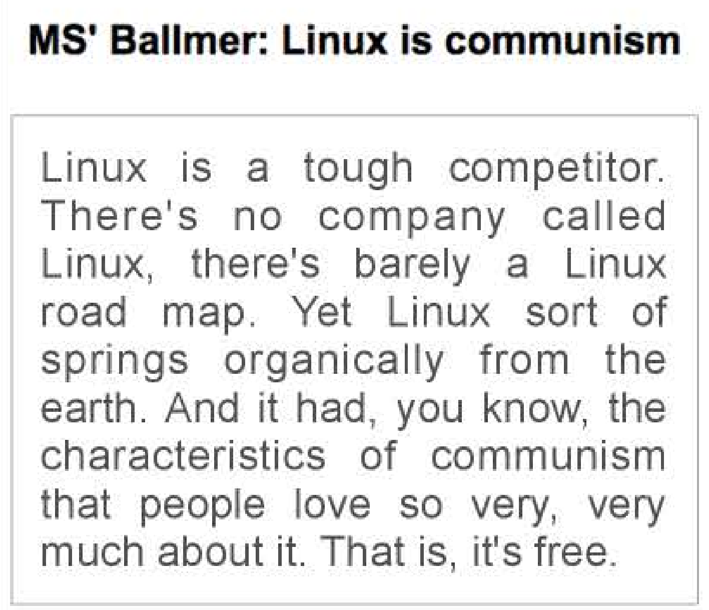
PayPal Secure + protect

PayPal freezes, then restores account of crowdfunded secure email startup

ProtonMail has raised more than $328k on Indiegogo, but is the latest company to fall foul of payment blocks

FREE & OPEN SOURCE

No toll from .com



MS' Ballmer: Linux is communism

Linux is a tough competitor. There's no company called Linux, there's barely a Linux road map. Yet Linux sort of springs organically from the earth. And it had, you know, the characteristics of communism that people love so very, very much about it. That is, it's free.

MUCH MORE

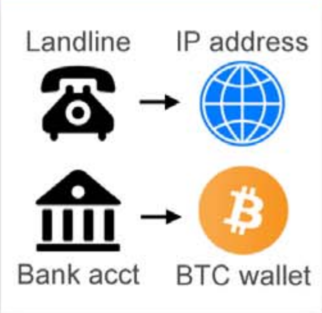
Multisig, Blockchain, Contracts!

Bitcoin is to Paypal as Linux is to Windows

We've already seen what happens when an open-source, decentralized, programmable version arises.

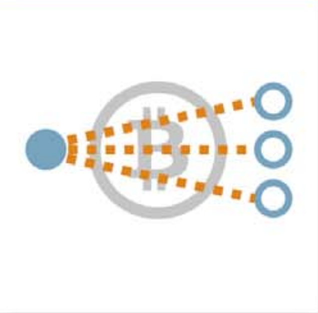
EVERY ENTITY

Banking for anything



EVERY DEVICE

Connected? Send/receive.



EVERY COUNTRY

Available worldwide

EVERY AMOUNT

From micro to macro

Sending
.000000001 BTC

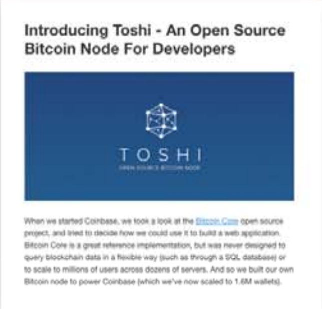
1GSwxzetCRFzwCiSqyvQMHZuSdymWbrENn - (Spent)

Sending
550,000 BTC

1MBs2S5bgAzSSzVTeL7zruvMPLvzSkEAuv - (Spent)

EXTENSIBLE

Modify code, add features

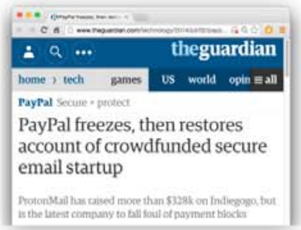


Introducing Toshi - An Open Source Bitcoin Node For Developers

When we started Coinbase, we took a look at the Bitcoin Core open source project, and tried to decide how we could use it to build a web application. Bitcoin Core is a great reference implementation, but was never designed to query blockchain data in a flexible way (such as through a SQL database) or to scale to millions of users across dozens of servers. And so we built our own Bitcoin node to power Coinbase (which we've now scaled to 1.6M wallets).

UNFREEZABLE

Full personal control



PayPal Secure + protect

PayPal freezes, then restores account of crowdfunded secure email startup

ProtonMail has raised more than $328k on Indiegogo, but is the latest company to fall foul of payment blocks

FREE & OPEN SOURCE

No toll from .com

MS' Ballmer: Linux is communism

Linux is a tough competitor. There's no company called Linux, there's barely a Linux road map. Yet Linux sort of springs organically from the earth. And it had, you know, the characteristics of communism that people love so very, very much about it. That is, it's free.

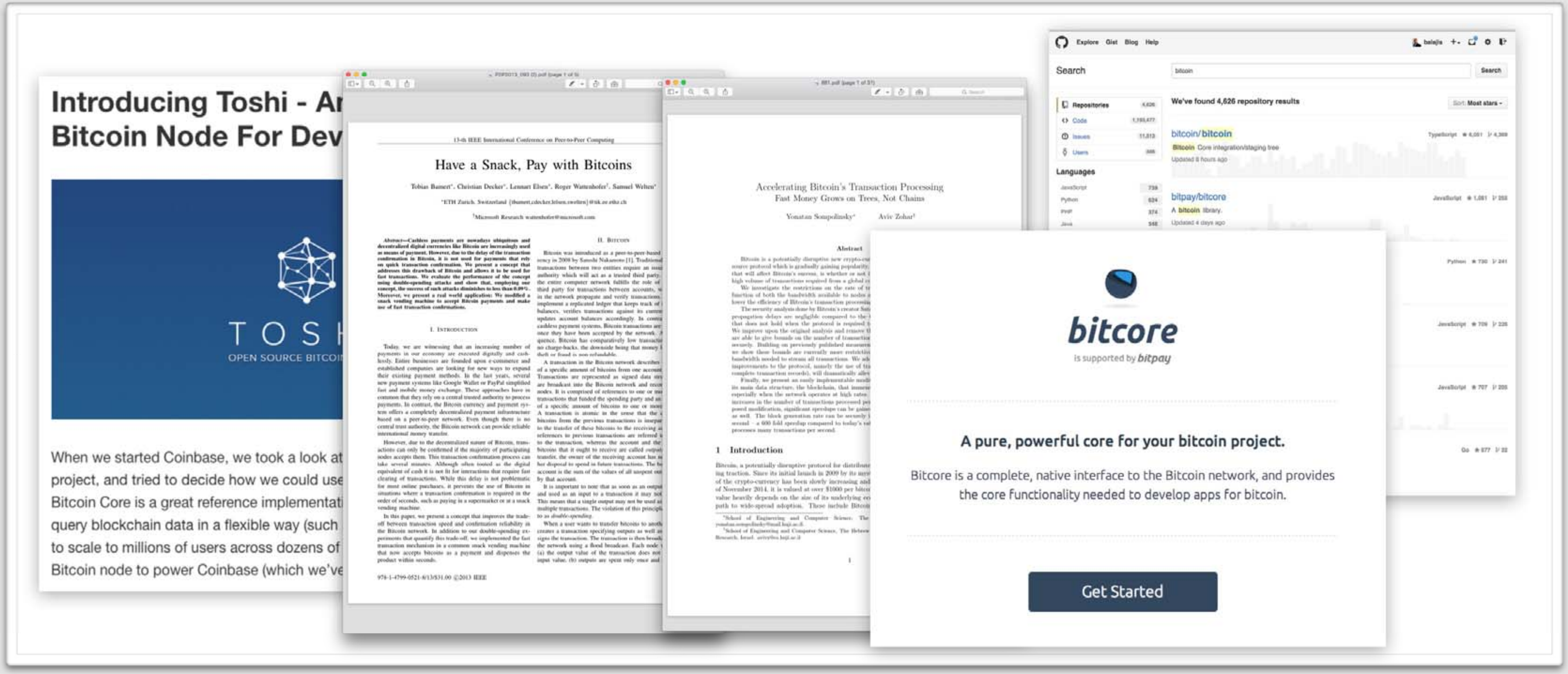
MUCH MORE

Multisig, Blockchain, Contracts!

Assurance Contracts
Transferable
Smart Property
Virtual Property
Autonomous Agents
Distributed Markets

Examples of Forking & Modification

Bitcoin, like Linux, is an open-source commons that people can fork & rapidly improve without paying a tax.



Introducing Toshi - Ar
Bitcoin Node For Dev

When we started Coinbase, we took a look at
project, and tried to decide how we could use
Bitcoin Core is a great reference implementati
query blockchain data in a flexible way (such
to scale to millions of users across dozens of
Bitcoin node to power Coinbase (which we've

13-th IEEE International Conference on Peer-to-Peer Computing

Have a Snack, Pay with Bitcoins

Tobias Bamert*, Christian Decker*, Lennart Elsen*, Roger Wattenhofer†, Samuel Welten*

*ETH Zurich, Switzerland {tbamert,cdecker,lelsen,swelten}@tik.ee.ethz.ch

†Microsoft Research wattenhofer@microsoft.com

Abstract—Cashless payments are nowadays ubiquitous and decentralized digital currencies like Bitcoin are increasingly used as means of payment. However, due to the delay of the transaction confirmation in Bitcoin, it is not used for payments that rely on quick transaction confirmation. We present a concept that addresses this drawback of Bitcoin and allows it to be used for fast transactions. We evaluate the performance of the concept using double-spending attacks and show that, employing our concept, the success of such attacks diminishes to less than 0.09%. Moreover, we present a real world application: We modified a snack vending machine to accept Bitcoin payments and make use of fast transaction confirmations.

I. Introduction

II. Bitcoin

978-1-4799-0521-8/13/$31.00 ©2013 IEEE

Accelerating Bitcoin's Transaction Processing
Fast Money Grows on Trees, Not Chains

Yonatan Sompolinsky* Aviv Zohar†

Abstract

1 Introduction

Search

bitcoin

Search

Repositories	4,626
Code	1,193,477
Issues	11,813
Users	888

Languages

JavaScript	739
Python	624
PHP	374
Java	348

We've found 4,626 repository results

Sort: Most stars

bitcoin/bitcoin — TypeScript ★ 6,051 ⑂ 4,369
Bitcoin Core integration/staging tree
Updated 8 hours ago

bitpay/bitcore — JavaScript ★ 1,081 ⑂ 252
A bitcoin library.
Updated 4 days ago

Python ★ 730 ⑂ 241

JavaScript ★ 709 ⑂ 226

JavaScript ★ 707 ⑂ 205

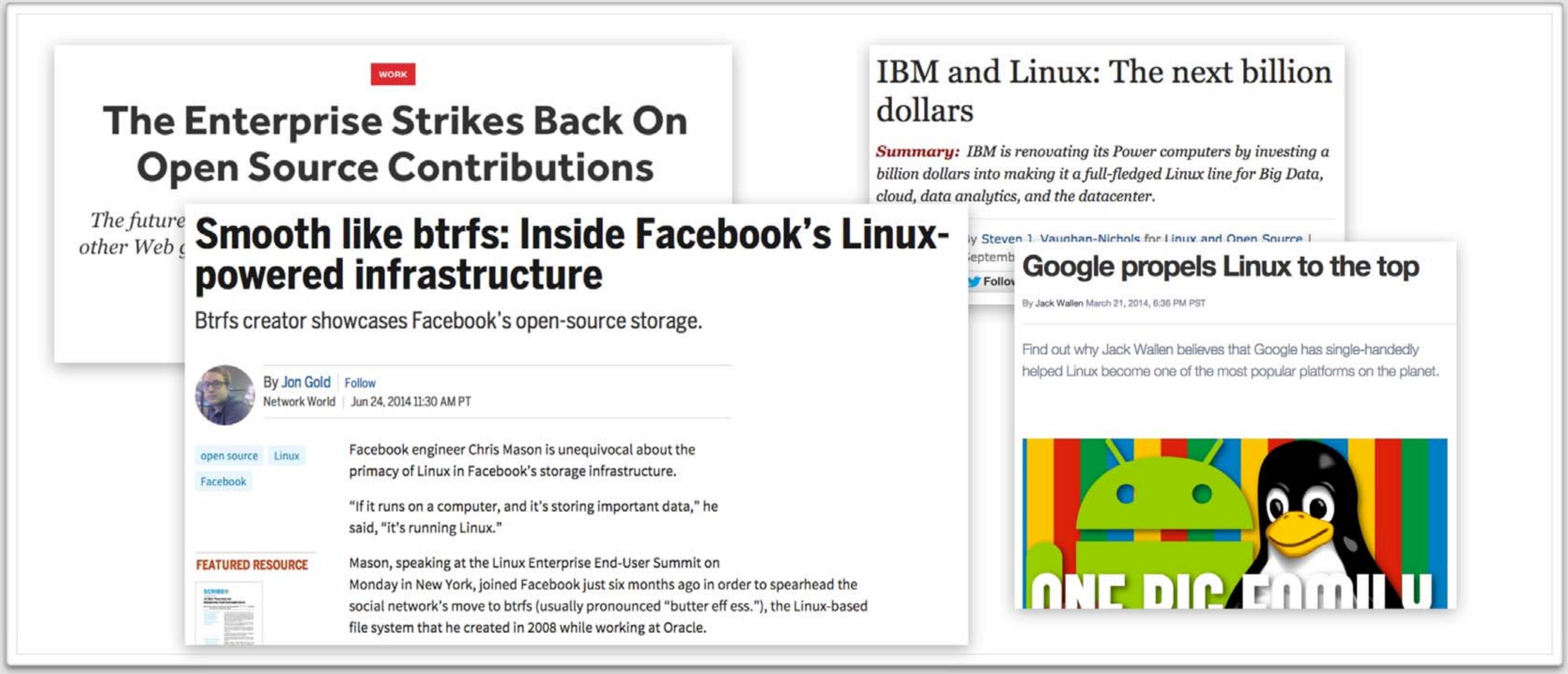
Go ★ 677 ⑂ 32

A pure, powerful core for your bitcoin project.

Bitcore is a complete, native interface to the Bitcoin network, and provides the core functionality needed to develop apps for bitcoin.

We've Seen This Movie Before

A forkable and modifiable payments system will dominate a centralized one for same reasons Linux > Windows.



WORK

The Enterprise Strikes Back On Open Source Contributions

The future
other Web g

Smooth like btrfs: Inside Facebook's Linux-powered infrastructure

Btrfs creator showcases Facebook's open-source storage.

By Jon Gold Follow
Network World | Jun 24, 2014 11:30 AM PT

open source Linux
Facebook

Facebook engineer Chris Mason is unequivocal about the primacy of Linux in Facebook's storage infrastructure.

"If it runs on a computer, and it's storing important data," he said, "it's running Linux."

FEATURED RESOURCE

Mason, speaking at the Linux Enterprise End-User Summit on Monday in New York, joined Facebook just six months ago in order to spearhead the social network's move to btrfs (usually pronounced "butter eff ess."), the Linux-based file system that he created in 2008 while working at Oracle.

IBM and Linux: The next billion dollars

Summary: *IBM is renovating its Power computers by investing a billion dollars into making it a full-fledged Linux line for Big Data, cloud, data analytics, and the datacenter.*

y Steven J. Vaughan-Nichols for Linux and Open Source |
eptemb
Follow

Google propels Linux to the top

By Jack Wallen March 21, 2014, 6:36 PM PST

Find out why Jack Wallen believes that Google has single-handedly helped Linux become one of the most popular platforms on the planet.