



Why we believe Bitcoin may be the most
important technology of this decade.

ANDREESSEN HOROWITZ

About me

Just a quick introduction.



Balaji S. Srinivasan (@balajis)

CEO of 21.co, Partner at Andreessen Horowitz. PhD EE, Stanford. Co-founder/CTO of Counsyl (Thiel/FF), Stanford MOOC (200k students)

A screenshot of a magazine spread. The left page features a black and white portrait of Balaji Srinivasan in a suit. The right page has a red header "INNOVATORS UNDER 35". Below the header, it says "35 Innovators Under 35 2013". The main text discusses his company Counsyl's work in screening prospective parents for recessive diseases. A sidebar on the right lists categories: Introduction, Inventors, Entrepreneurs, and Visionaries.



ANDREESSEN
HOROWITZ

Counsyl



What is this Internet thing anyway?

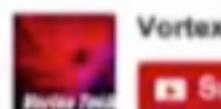
Step back with me to 1994.

What is "Internet"?

This is how things played out two decades ago.



1994: "Today": "What is the Internet, Anyway?"



VortexTech

Subscribe

1,444

1,578,633

4,592 57

+ Add to Share ... More

What is "Bitcoin"?

That's what we'll talk about today.

The Andreessen Horowitz Thesis on Bitcoin

Five key facts about Bitcoin that inform our thinking, and answers to some FAQs.

BITCOIN IS A PROTOCOL

Payments are now packets



BITCOIN HAS A NETWORK EFFECT

Four sides: Miners, Devs, Merchants, Users



Miners

Developers Merchants

Users

BITCOIN IS HERE TO STAY

Extraordinary institutional/sovereign support



BITCOIN IS BIGGER THAN GOOGLE

Mining now world's largest supercomputer



> Google

BITCOIN IS OPEN SOURCE

Extensible, programmable, rapidly improving



THE A16Z BITCOIN FAQ

And the most important q in Bitcoin.



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

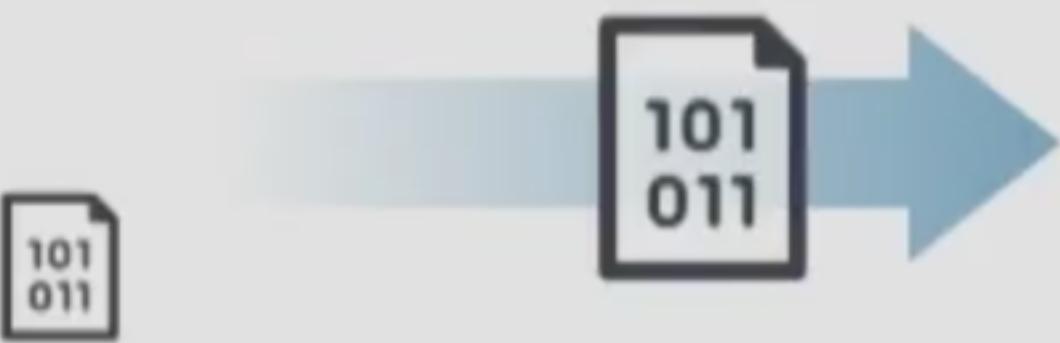
A hands B physical cash.

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

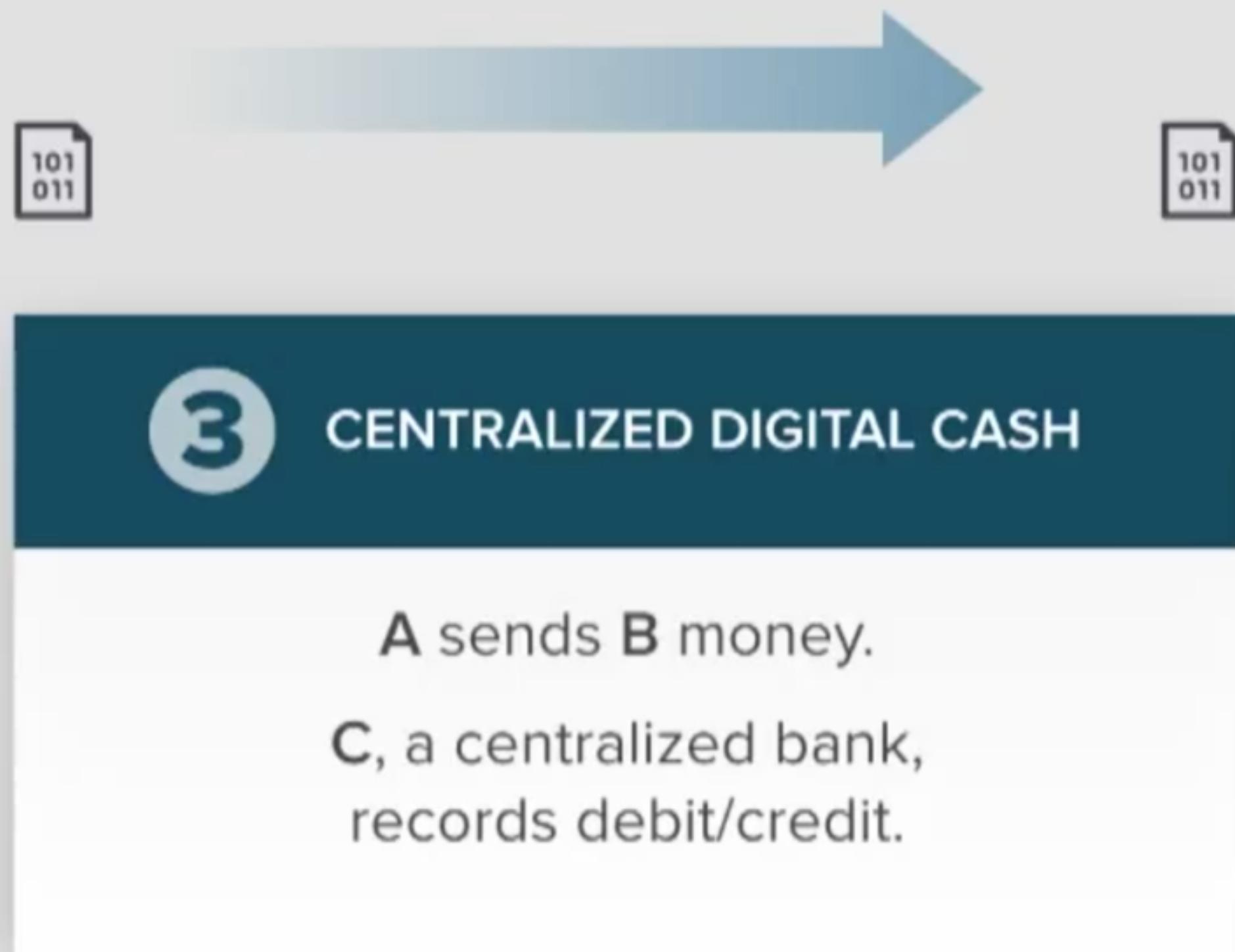
A emails B the serial numbers on a bill.

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.



Bitcoin solves in a decentralized way

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



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

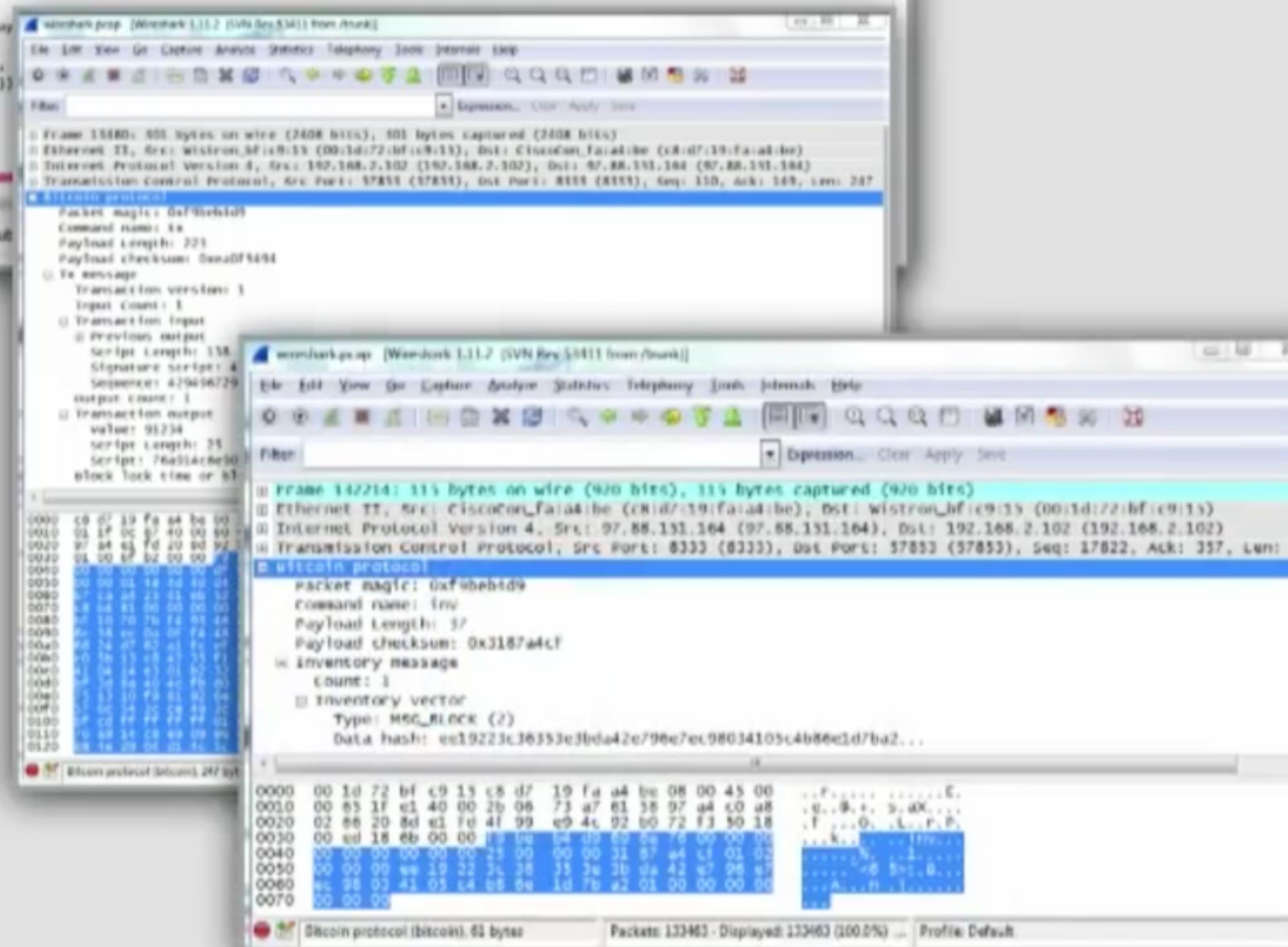
A transaction is literally a series of bytes broadcast over the internet to a P2P network of miners, with ack after mining.

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.

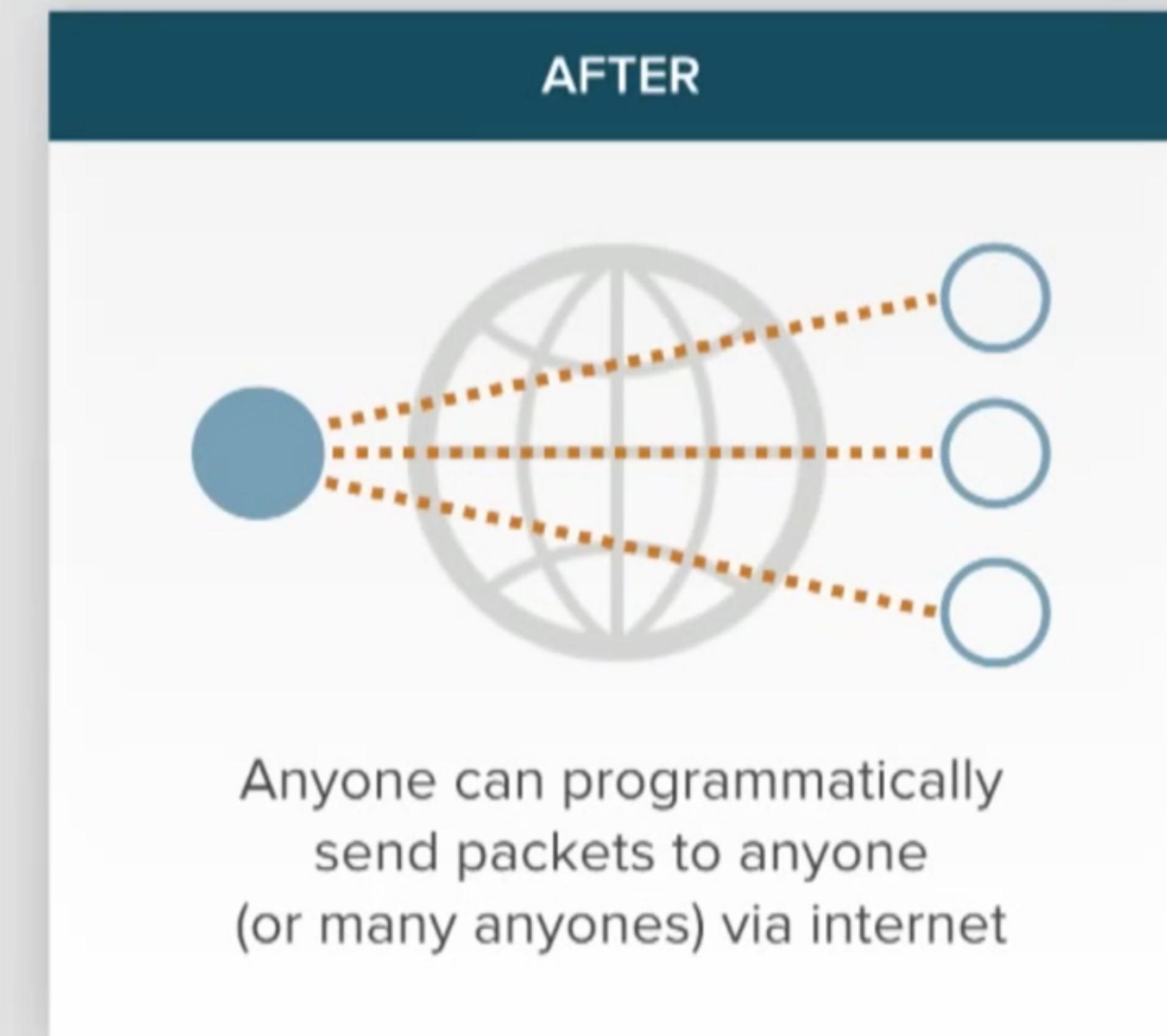
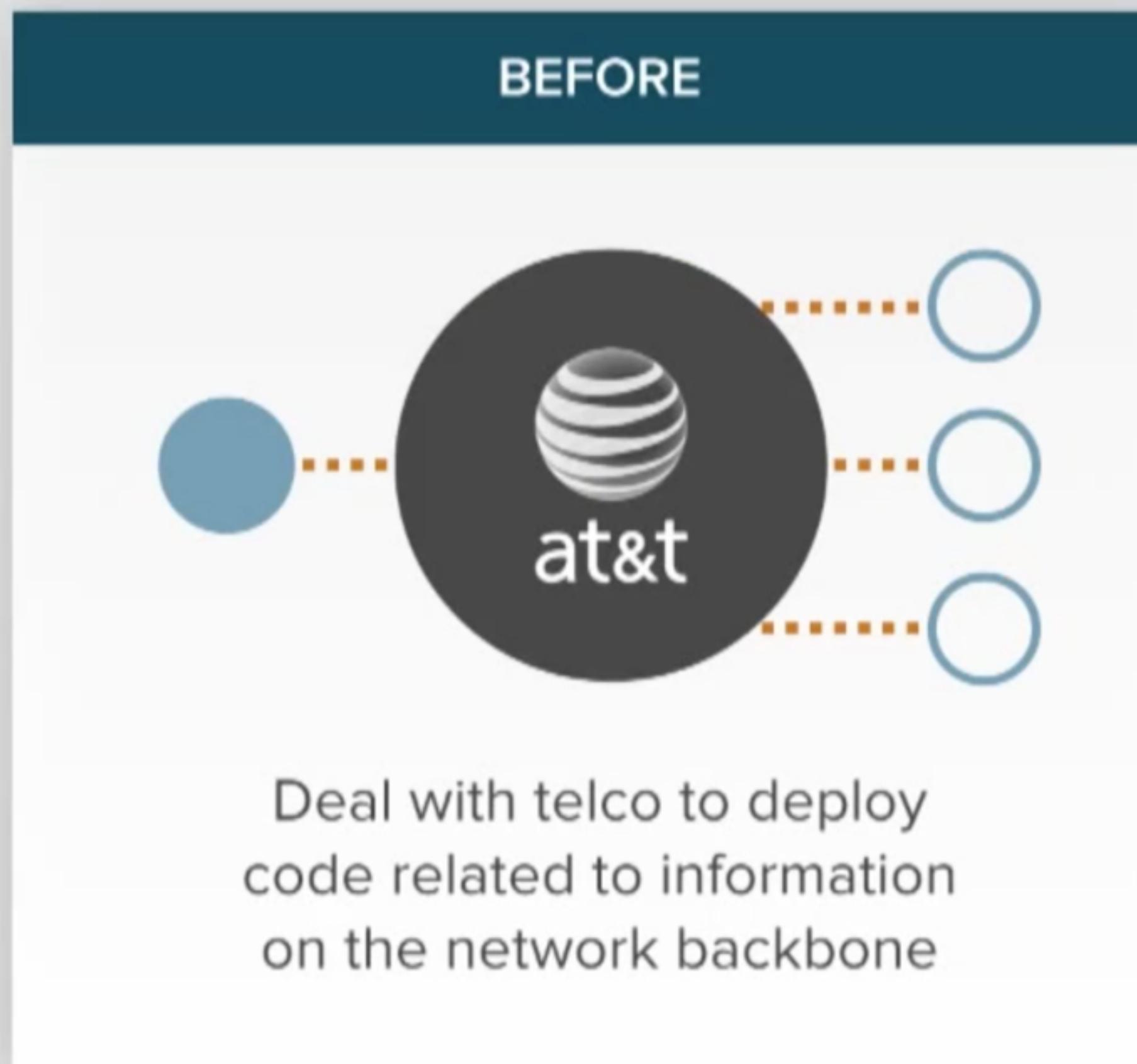
```
1 def getTxMsg(payload):
2     return nautilus.getMessage(nautilus, "tx", payload)
3
4 sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
5 sock.connect(("77.88.151.164", 8333))
6
7 sock.send(nautilus.getVersionMsg())
8 sock.recv(1000) # receive version
9 sock.recv(1000) # receive verack
10 sock.send(nautilus.getTxMsg("81800000"))
```

[minimalSendTxn.py hosted with GitHub](#)



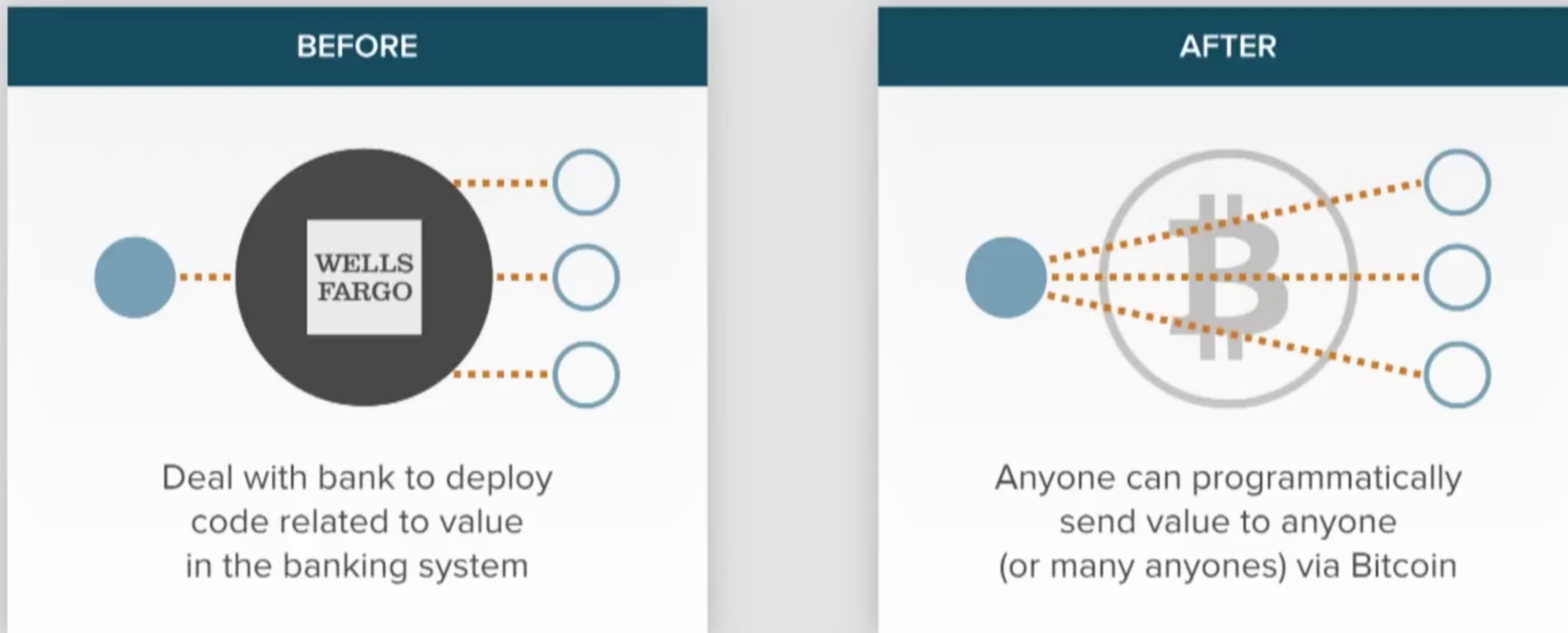
This is why we compare Bitcoin to the Internet

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



Bitcoin disintermediates banks

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



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.

15qSxP1SQcUX3o4nhkfdbgyoWEFMomJ4r

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**.

Bitcoin is here to stay

Institutional acceptance now beyond tipping point

Bitcoin Timeline

Over the last 18 months, 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

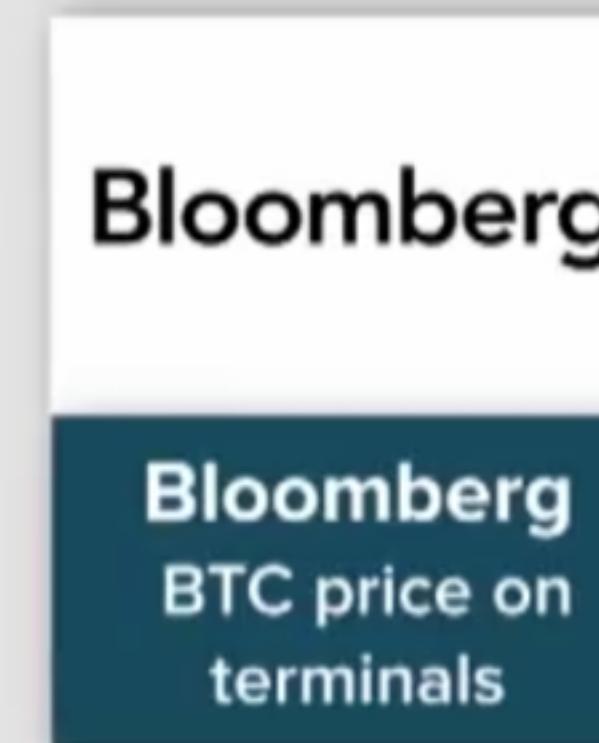
Finance



NASDAQ
Endorses Bitcoin ETF



BitBeat
Daily coverage of Bitcoin news



Bloomberg
BTC price on terminals

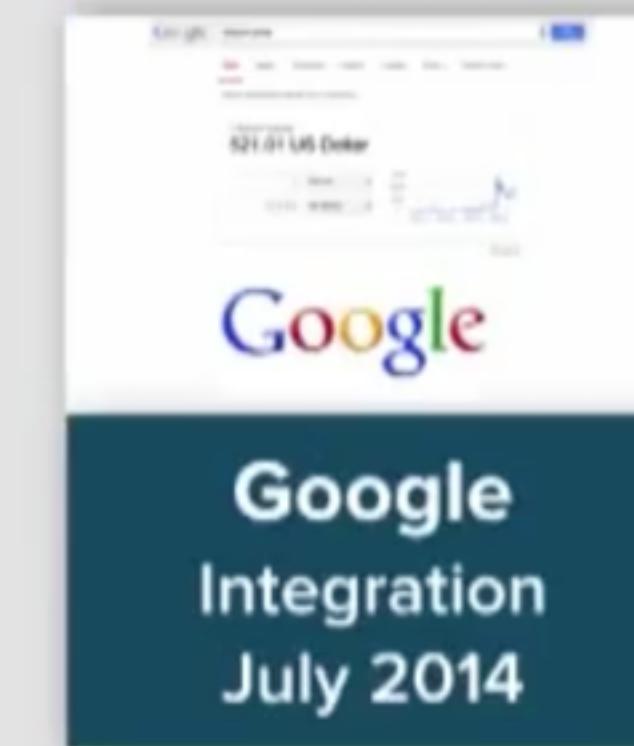


Wall Street
Reports from GS, MS, BofA, Citi

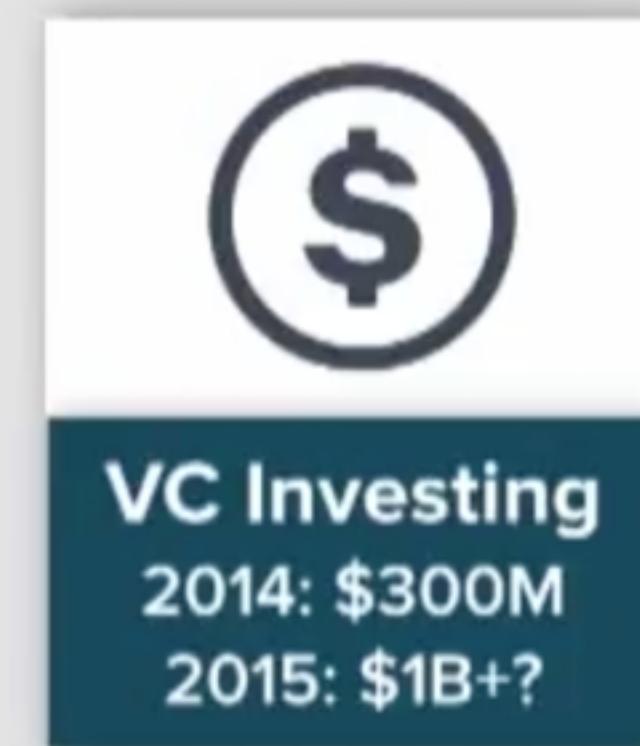
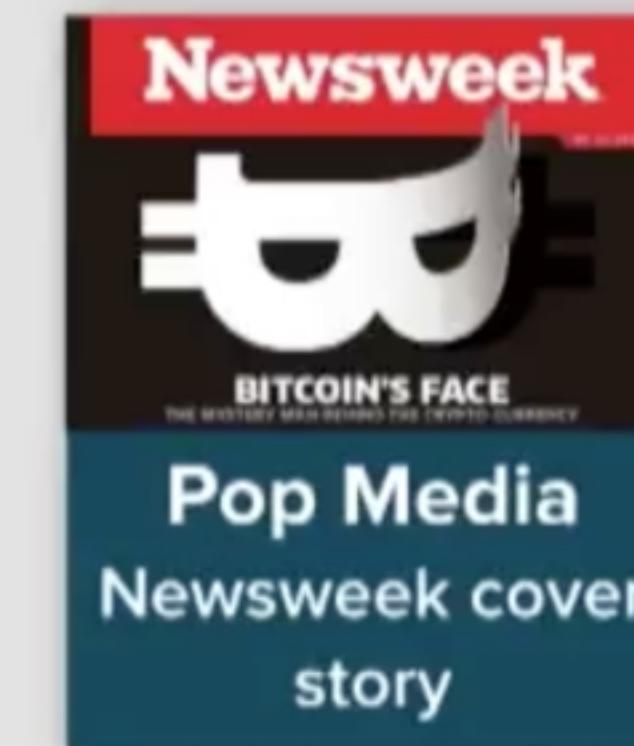
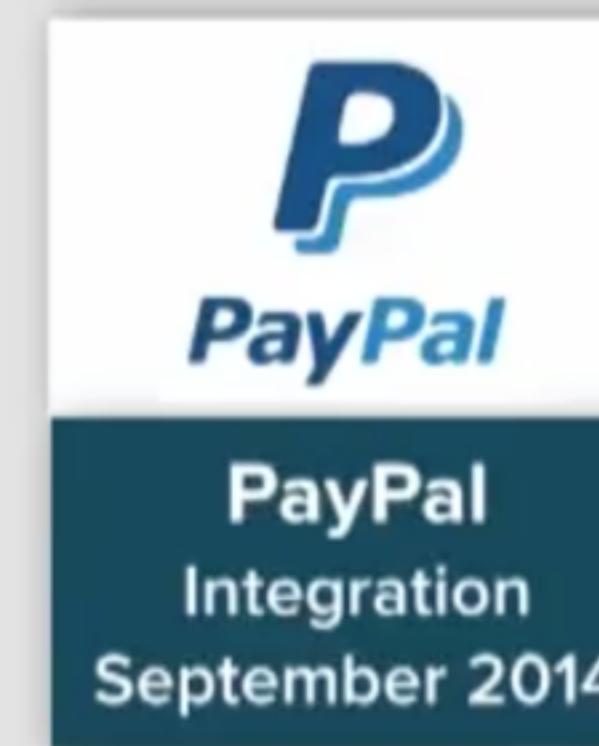
Bitcoin Timeline

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

Tech



Market



Federal Reserve

Past, present, and alternative Federal Reserve chairs on Bitcoin.

BUSINESS INSIDER

MARKETS

BERNANKE: Bitcoin 'Not a Promised Land'

STEVEN PERLBERG NOV. 18, 2013, 12:20 PM 4,29,862 16

The beautiful thing about Bitcoin, digital currency enthusiasts will tell you, is that it doesn't have a central bank.

So with eyes on today's Bitcoin Senate hearing, where does the world's most powerful central banker stand on the elusive cryptocurrency?

Yellen on Bitcoin: Fed Does Not Have Authority to Regulate It

12:43 pm ET Feb 27, 2014 FOREX

In Bitcoin Debate, Larry Summers Sides with the History of Change

ARTICLE COMMENTS (10)

BITCOIN FED FEDERAL RESERVE

Email Print

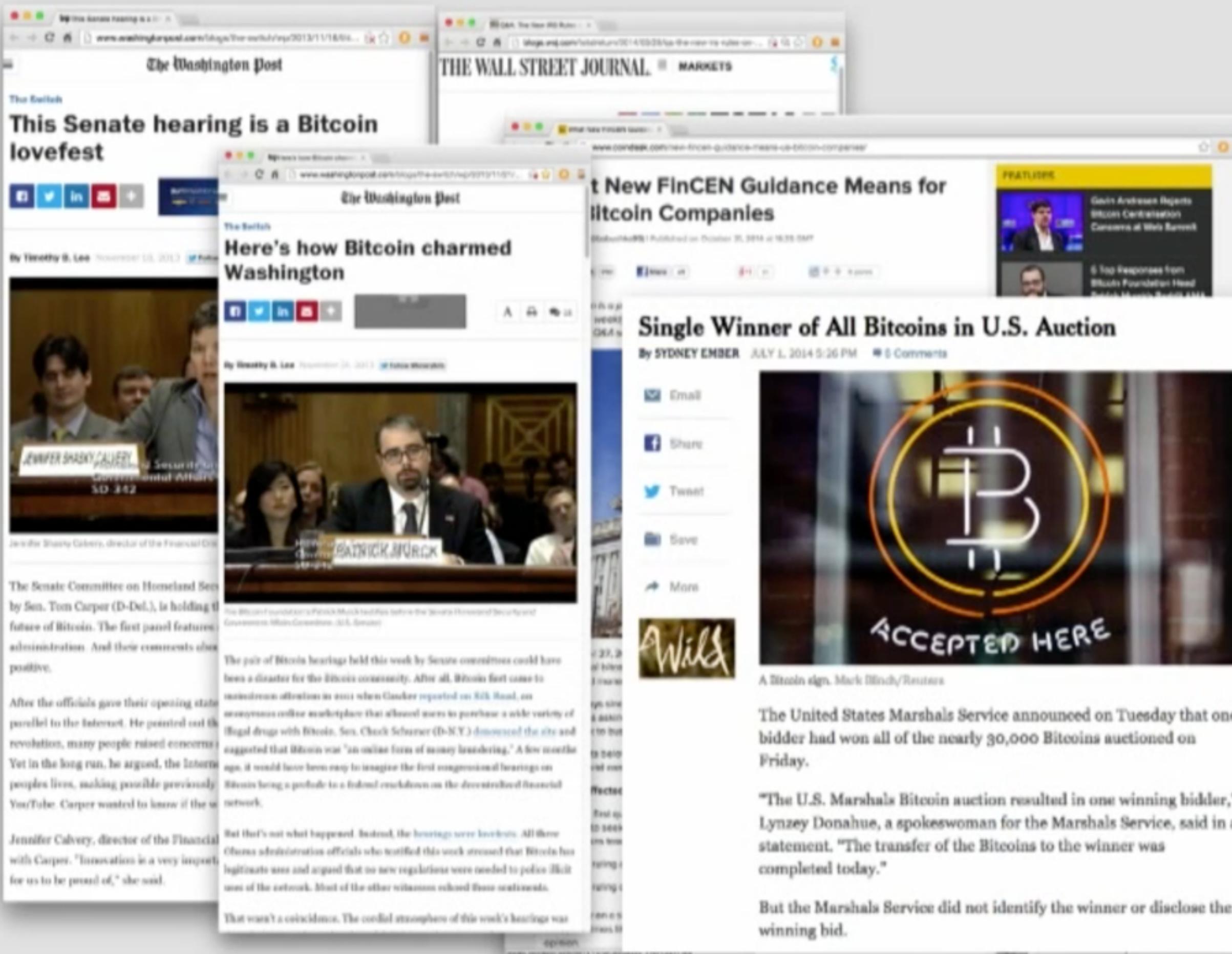
By MICHAEL J. CASEY CONNECT

Larry Summers has a warning for bitcoin's naysayers: ignore change at your own peril.



US Federal Government

After Senate hearings in late 2013, IRS ruling, FINCEN, and large FBI sale have now effectively legalized Bitcoin at federal level.



US State Governments

New York, California, and Texas are all now legalizing or have signaled significant positive sentiment. More states are following.

The screenshot displays three separate news articles side-by-side:

- Forbes Article:** "California Banks Support Comptroller's Bitcoin Regulation" by Arman Batali. It discusses the California Banking Department's proposal to regulate Bitcoin.
- Bloomberg Article:** "New York Vvina With California to Write Bitcoin Rules" by Michael Bobelian. It notes that New York is drafting regulations alongside California.
- CoinDesk Article:** "5 US States Poised to Promote Bitcoin-Friendly Regulation" by Daniel Cawrey. It lists five US states (New York, California, Texas, Florida, and Colorado) that are considering friendly regulations for Bitcoin.

Below the articles is a map of the United States with state boundaries, indicating the locations of the five states mentioned in the article.



UK, Japan, Israel Governments

Extremely positive attitude from many foreign governments, even more so than the US.

the guardian

George Osborne hails Britain into bitcoin

A government review will explore the best currencies, and the role that cryptocurrencies play in the economy. The Treasury has launched a review to look at how Britain can accept the new currency.

THE WALL STREET JOURNAL

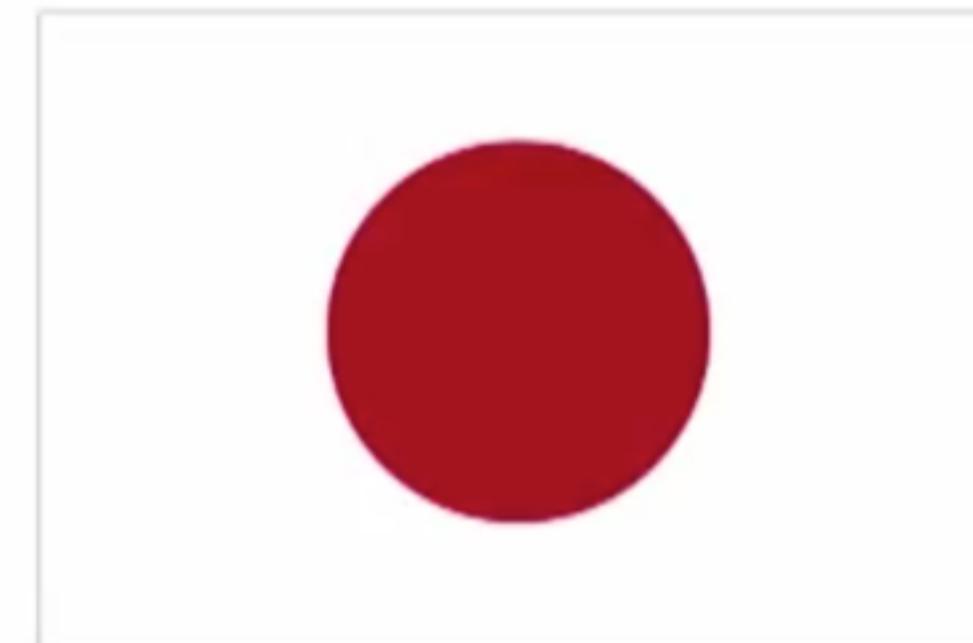
Japan Ruling Party to Hold Off Regulating Bitcoin

The Japanese Ruling Party has decided not to regulate Bitcoin, despite calls for it to do so.

The Jewish Daily FORWARD

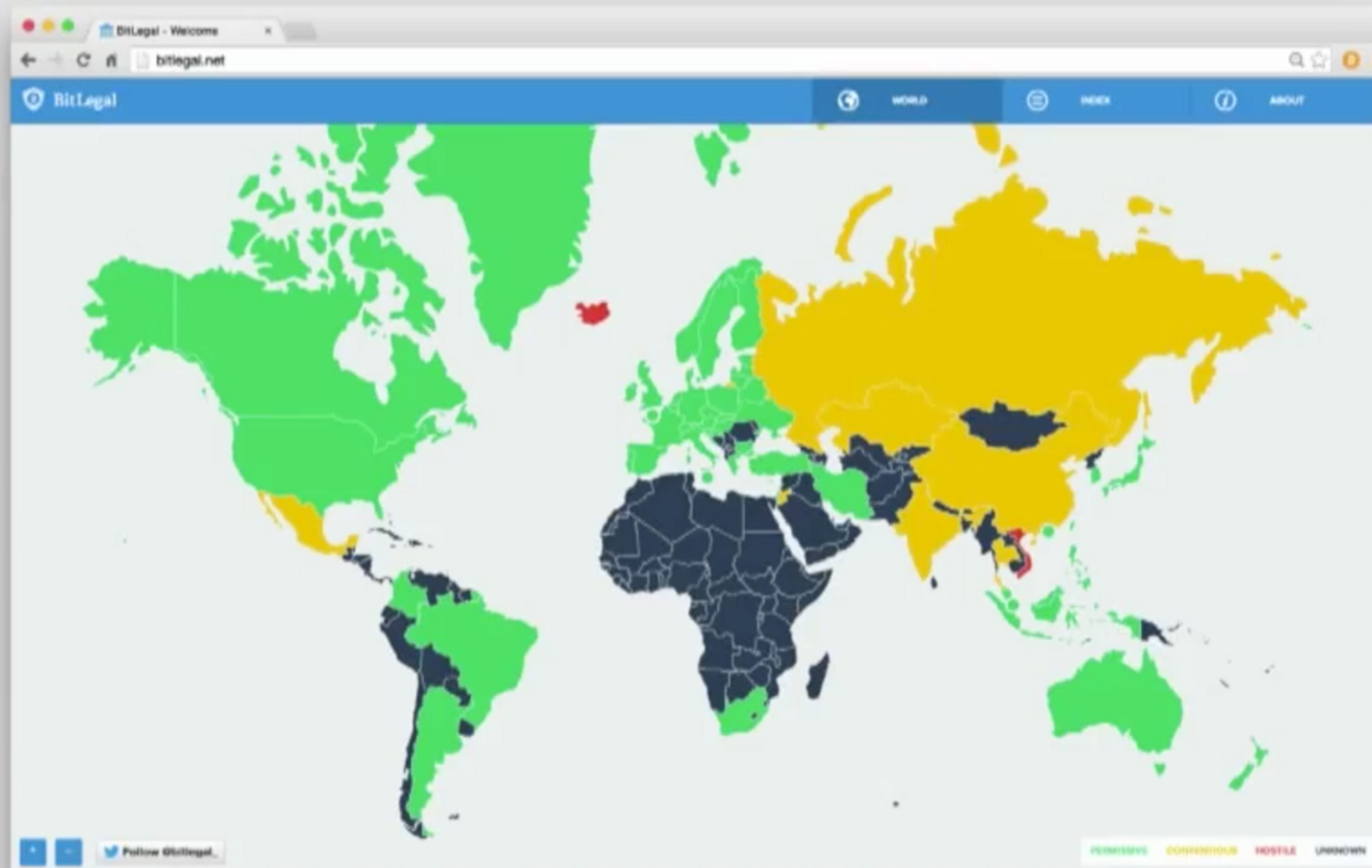
Bitcoin Makes Aliyah as Virtual Currency Gains Favor in Israel

ATMs Split Out Scanable Cash in Tel Aviv



International Governments

Surprisingly few govts have restricted it worldwide; even China/Russia in practice are slowing vs banning.



About

BitLegal tracks the evolving regulatory landscape of virtual currency around the world.

Team
Zachary Taylor - Founder
A freelance web developer based out of Philadelphia interested in disruptive and unique applications of virtual currency.

Contact
All inquiries can be directed to info@bitlegal.io.

Donations
Your support is much appreciated! You can contribute to our beer fund at the following address:
16182fQ6been34Shjn4lf2x7CLJ4mowJ4FEP

Disclaimer

BitLegal provides information about a developing area of the law and it is designed to help users make decisions about their own legal needs. Use of this site, or the information contained herein, does not create an attorney-client relationship. The content on this site is not offered as, does not constitute, and should not be relied upon as a source of legal advice. Legal information is not the same as legal advice. Legal advice is the application of law to an individual's specific circumstances. Nothing on this website should be considered a substitute for professional legal advice.

Online users should not act or rely upon any information in this site without first directly consulting legal counsel of their own. We recommend you consult a lawyer if you want.

Institutional Finance

WSJ, Bloomberg, NASDAQ embracing Bitcoin. GS: "All About Bitcoin"

The image shows a Mac desktop with four browser windows open:

- newsbtc.com**: Headline: "Wall Street Journal Launches BitBeat: Your Daily Bitcoin Round-up". By Eric Calore, February 5, 2014.
- Bloomberg NOW**: Headline: "BITCOIN NOW ON BLOOMBERG". Article by Bloomberg, dated April 30, 2014.
- cointelegraph.com**: Headline: "Nasdaq's LaValle: Bitcoin ETF is "A Turning Point"".
- www.paymentcardadvocacy.org**: Headline: "Global Macro Research Top of Mind". March 11, 2014. Issue 21. Article: "All About Bitcoin".

WSJ

NASDAQ®

Bloomberg

Goldman Sachs

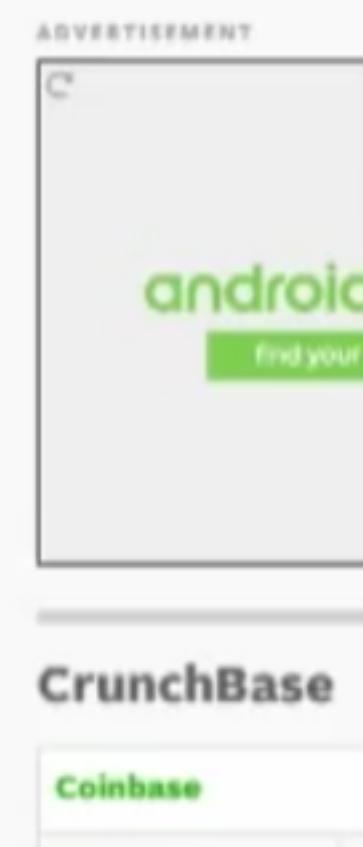
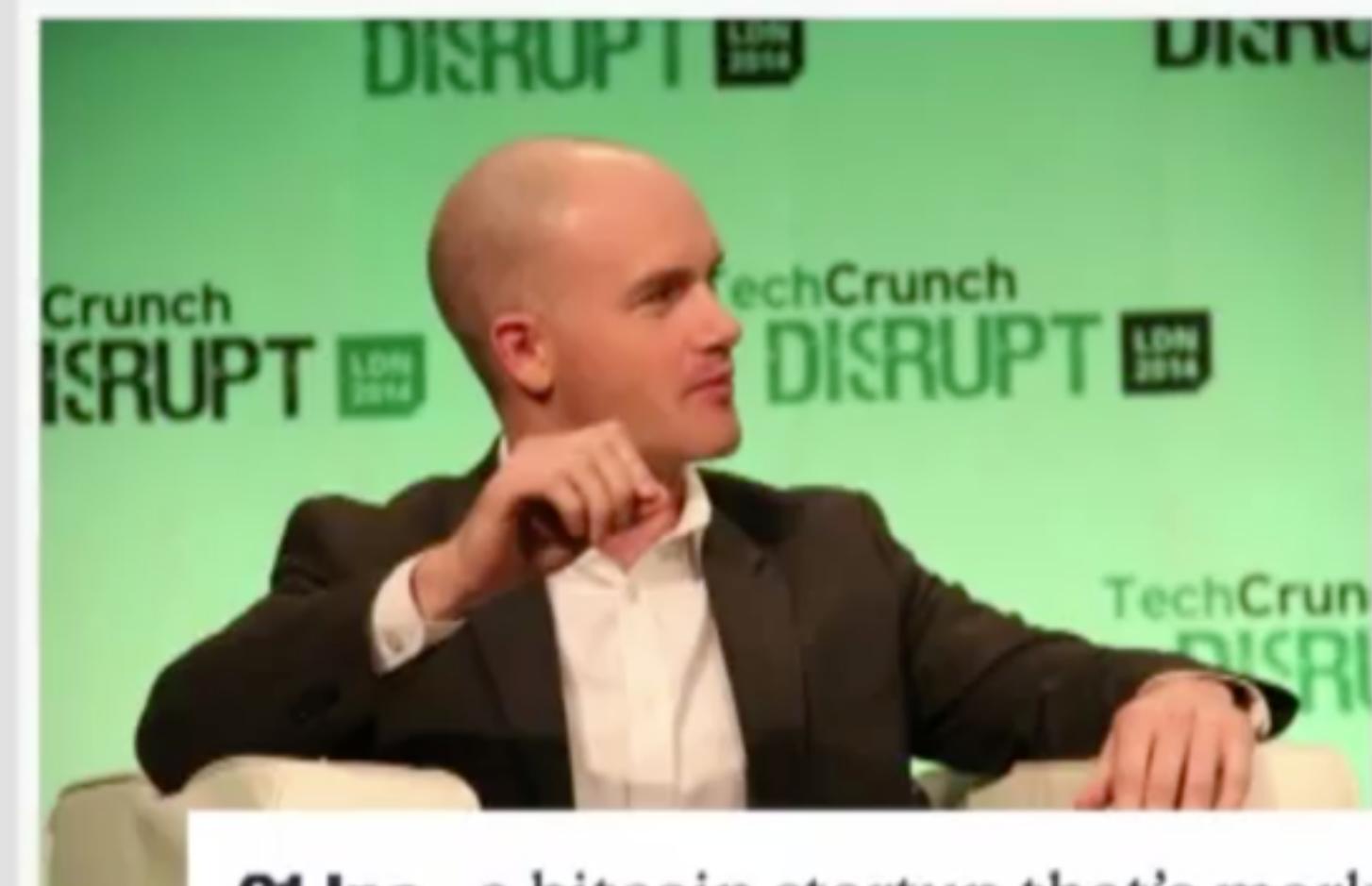
Institutional Finance and Govt

NYSE, USAA, BBVA investing in Coinbase. Summers joining 21 SAB.

Coinbase Confirms \$75M Raise From DFJ, NYSE, Strategic Banking Partners

Posted Jan 20, 2015 by Kim-Mai Cutler (@kimmaicutler)

754 SHARES



21 Inc., a bitcoin startup that's marketing chips that let devices such as smartphones mine for the digital currency, just added former Treasury Secretary Larry Summers to its advisory board. ([Wall Street Journal](#))



BBVA

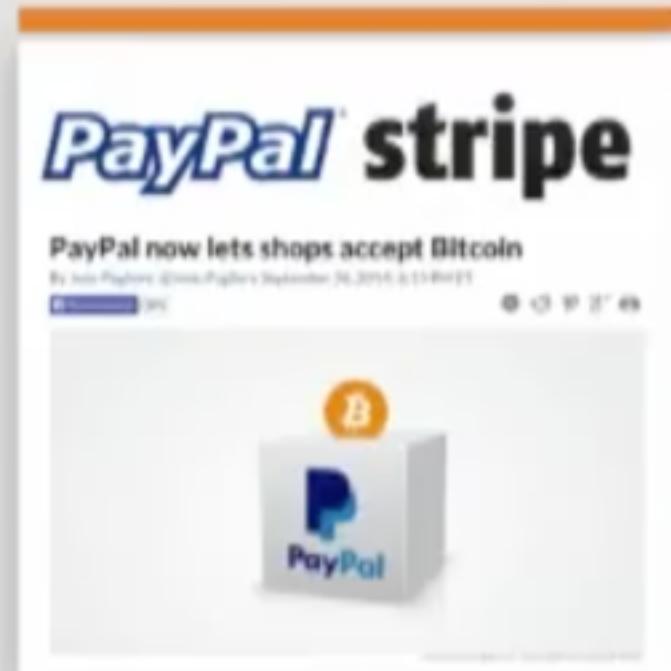


"What's your Bitcoin Strategy?"

Major organizations in different sectors are now executing on their Bitcoin strategy.

PAYMENTS

Paypal, Stripe using Bitcoin



MERCHANTS

Accepting Bitcoin for goods



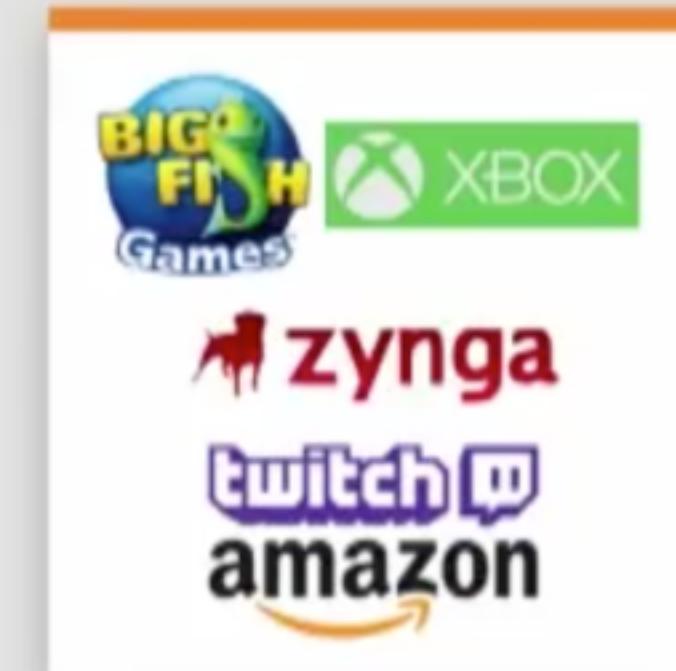
NEWSMEDIA

Regular Bitcoin coverage



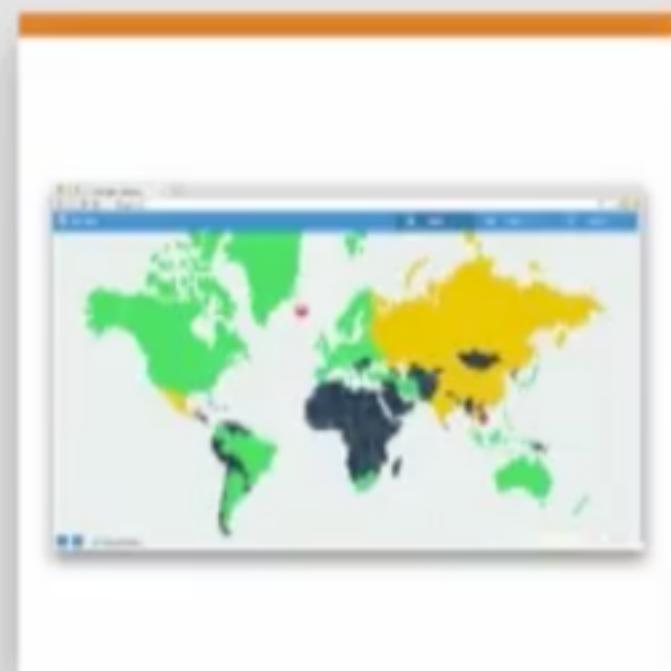
GAMING

In-game pts, Twitch Turbo



GOVERNMENTS

Very positive in many countries



VENTURE CAPITAL

Investing >\$300M



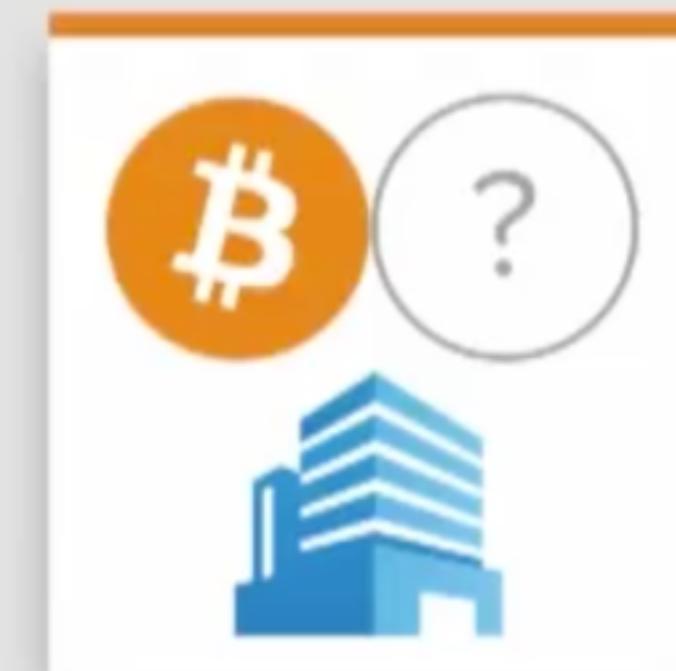
INVESTMENT BANKING

Coverage & CIO attention



BITCOIN STRATEGY

What fits your org?

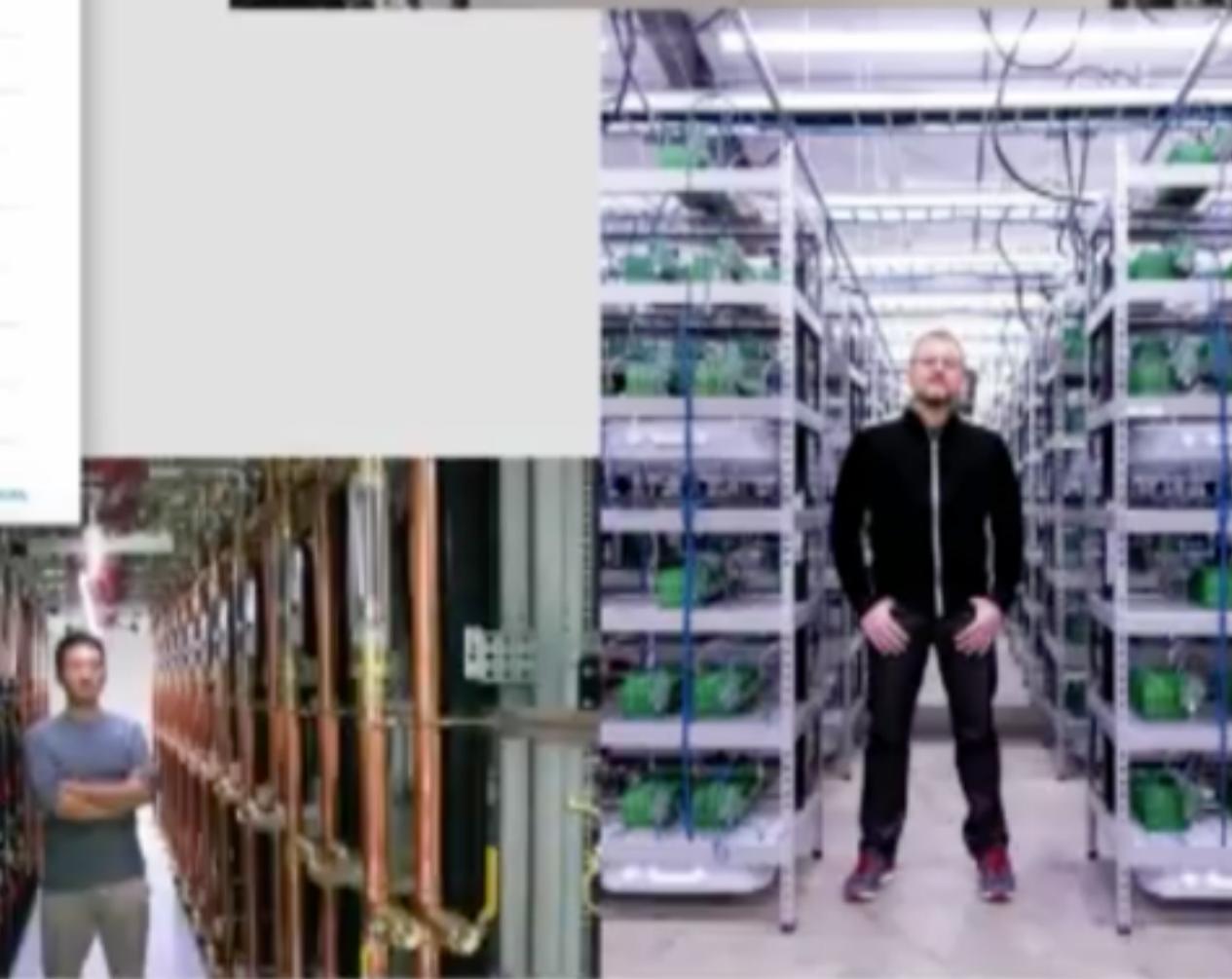
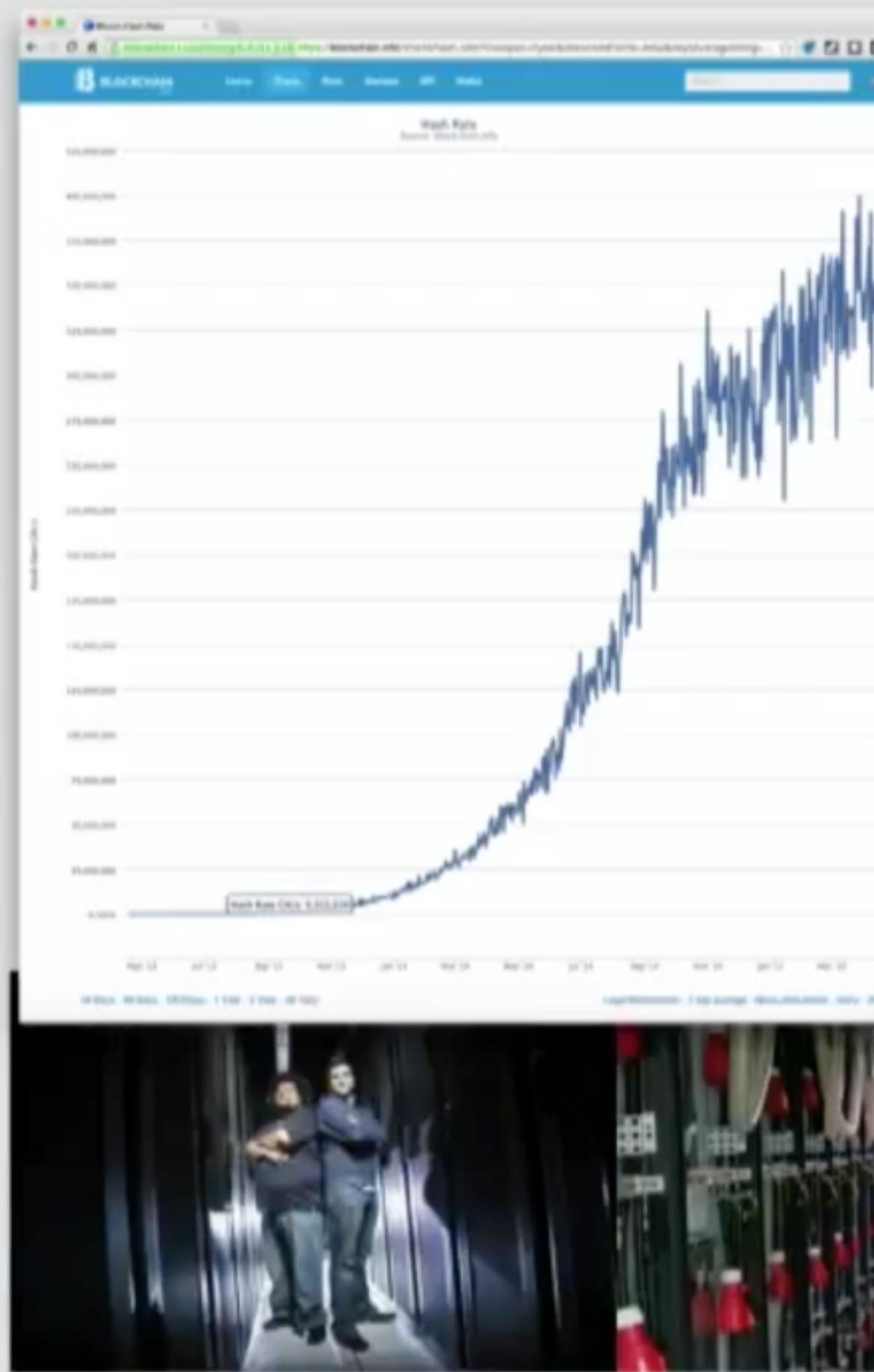


Bitcoin is bigger than Google

Mining consumes more power than Google in 2011.
All of Google today would represent <1% of mining.

Bitcoin mining up >100X, now S-curve

The degree of mining buildout over the last two years has not fully been appreciated in the popular press.



Google search results for "Bitcoin mining". The top result is a link to [Are You a Bitcoin Miner? - bitcoinaffiliatenetwork.com](http://areyouabitcoinminer.com). Other results include "What is Bitcoin Mining?" and "How to become the best Bitcoin Miner". The right side shows sponsored ads for mining hardware like AntMiner S5, S7, and S9.

Google CPUs: <1% of Bitcoin hashrate

CPUs/GPUs are now 1,000-10,000X less efficient than ASICs. Thus even 10 million Google servers are less than 1% of global hashrate!

James Pearn
Shared publicly · Jan 25, 2012

How many servers does Google have?
My estimate: 1,791,040 as of January 2012
And projection: 2,376,640 in early 2013

This Goo Mining hardware comparison
con See also: Non-specialized hardware comparison
con Below are some statistics about the mining performance of various hardware used in a Bitcoin mining rig. For GP
Sat and other hardware not specifically designed for bitcoin mining see here.
Notes:
Goo • Mhash/s = millions hashes per second (double sha256 raw speed performance; may not be very energy effici
secl some models)
serv • Mhash/J = millions hashes per joule (energy efficiency; 1 joule of energy is 1 watt during 1 second: 1 J = 1 W
if M • W = 1 Intel
pow amc

ASIC	Model	p/t	Mhash/s	Mhash/J	Mhash / \$ ^[1] / ^[2]	ACP [W]	Clock [GHz]	Version
	Xeon E5630 (dual)	2x4/8	8	0.1	80	2.53	0.3.17/Win7-64	source
An	Xeon E6520 (dual)	2x4/8	24.7			2.53	ufasoft v0.10	windows
An	Xeon E7220	2/2	6.3	?	80	2.93	ufasoft v0.10	Centos
An	Xeon E7320 (dual)	2x2	1.5			2.8	cgminer v1.2.8	2x2.8 cores
An	Xeon E7450 (quad)	4x8/24	60			2.40	ufasoft v0.13	-t 24
An	Xeon E7520 (dual)	2x4/16	18		95	1.87	ufasoft v0.10	windows 2008 R2 64bit (-t 16)
	Xeon W3680	6/12	18		130	3.33	cpuminer v1.0.2 --algo=4way	Ubuntu 11.04 64bit

Google

- 10^{e6} servers x 1-10 MH/s per CPU x 10 CPUs/server
- $= 10^7$ servers x 10^7 (H/s) per CPU x 10^1 CPUs per server
- $= 10^{15}$ H/s

VS

Bitcoin

- 350×10^{e15} H/s (global)



Non-specialized hardware comparison

Contents [hide]
1 Graphics cards
1.1 AMD (ATI)
1.2 Nvidia
2 CPUs/GPUs
2.1 AMD
2.2 AHM
2.3 Intel
2.4 Other
3 See Also

Graphics cards

Due to the rising hashrate of the Bitcoin network caused by the introduction of ASICs to the market, GPU mining Bitcoins has become impractical. The hashrate of most GPU units is below 1GH/s, and as of 2014, some single ASIC units are able to reach speeds of over 1.000GH/s while consuming far less power than a GPU. The information in this table is preserved for historical interest, but does not include many GPUs which were released after the advent of ASIC mining.

AMD (ATI)

Stream SDK 2.5 seems to have resolved many of the problems with earlier versions. Everyone's setup will be unique so this should only be a guide or starting point, not an absolute.

Model	Mhash/s	Mhash/J	Mhash/s/\$ ^[1]	Watts	Clock
3410	0.89	0.074	?	12(?)	222
3XXX					
42XX					
4350	6.90	0.346	0.16	20	575
4350	7.2				600

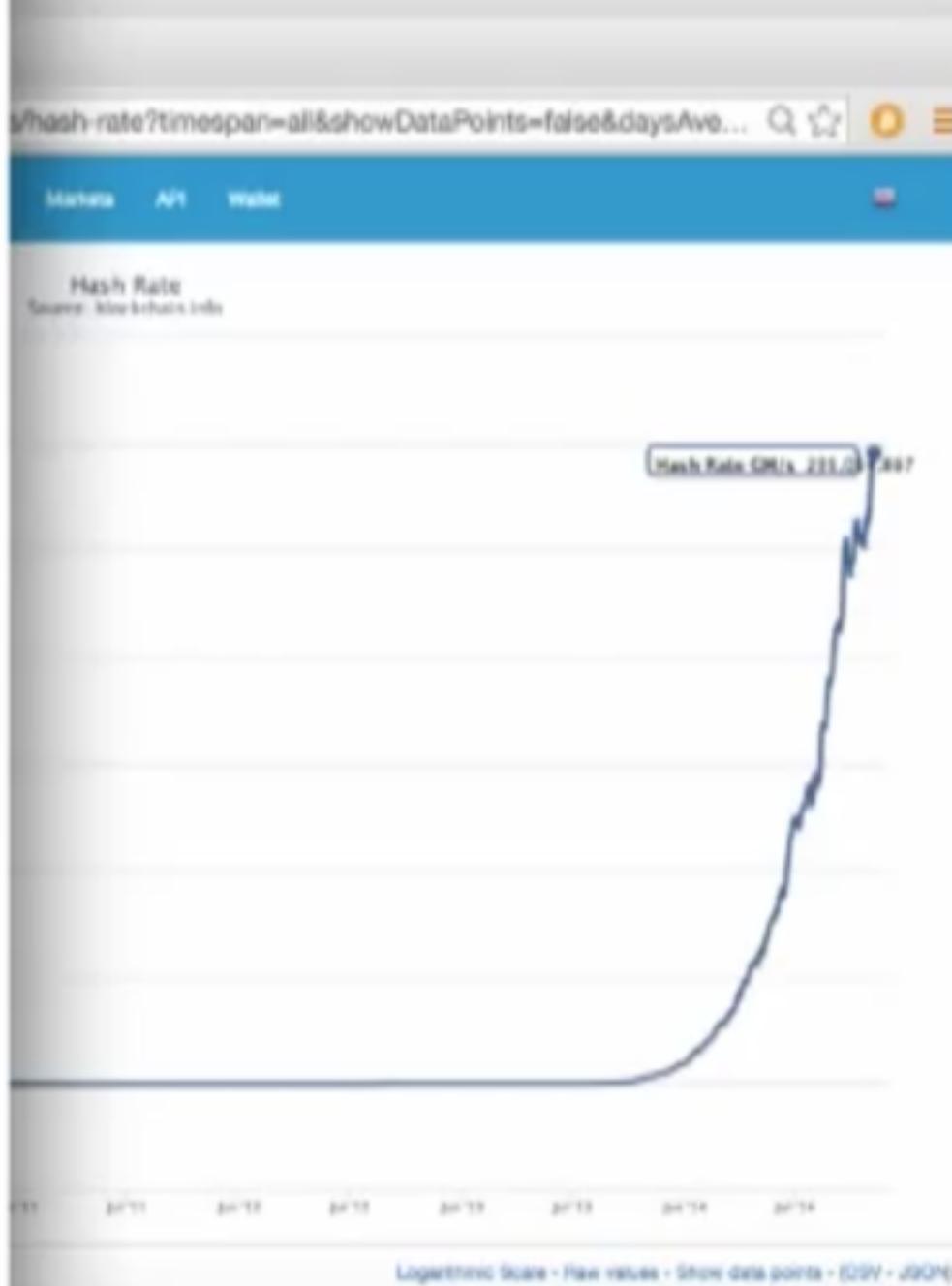
Google 2011: less power than Bitcoin

The Bitcoin network now consumes at least 300MW of power (assuming 1 MW/PH/s) - more than all of Google did in 2011.

Google never says how many servers are running in its data centers. The new estimate is based on information the company shared with Stanford professor Jonathan Koomey, who has just released an [updated report](#) on data center energy usage.

Google's David Jacobowitz, a program manager on the Green Energy team, told Koomey that the electricity used by the company's data centers was less than 1% of 198.8 billion kWh – the estimated total global data center energy usage for 2010. That means that Google may be running its entire global data center network in an energy footprint of roughly 220 megawatts of power.

"Google's data center electricity use is about 0.01% of total worldwide electricity use and less than 1 percent of global data center electricity use in 2010," Koomey writes, while cautioning that his numbers represent educated guesses extrapolated from the company's information. "This result is in part a function of the higher infrastructure efficiency of Google's facilities compared to in-house data centers, which is consistent with efficiencies of other cloud computing installations, but it also reflects lower electricity use per server for Google's highly optimized servers."



Global hashrate	300 PH/s
Mining ASIC power usage	1 W / GH/s = 1 MW / PH/s
Total mining power usage	>300MW
Google 2011 (est.)	220MW

Bitcoin is open source

A programmable and customizable OS for money

Bitcoin is to Paypal as Linux is to Windows

It is open-source, decentralized, programmable, and extensible.

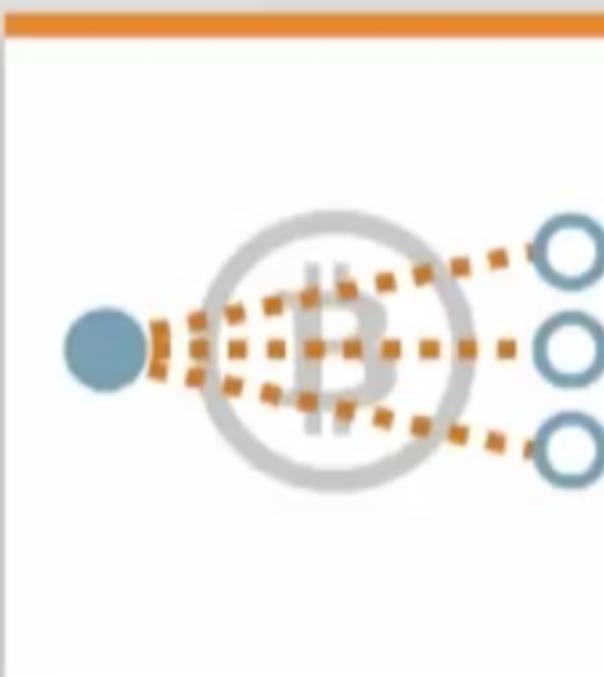
EVERY ENTITY

Banking for anything



EVERY DEVICE

Connected? Send/receive.



EVERY COUNTRY

Available worldwide



EVERY AMOUNT

From micro to macro

Sending
.000000001 BTC

1GSwxxelCRfzwCISqvGMH2zv5symVbrCNn - [Spent]

Sending
550,000 BTC

1MRc2RlbqAzRUVTelJ7muMPtvrS9HAvr - [Spent]

EXTENSIBLE

Modify code, add features

A screenshot of a GitHub repository page for "TOSHI" (An Open Source Bitcoin Node For Developers). The page includes a brief description, a logo, and a link to the repository's code.

UNFREEZABLE

Full personal control

A screenshot of a news article from theguardian.com. The headline reads "PayPal freezes, then restores account of crowdfunded secure email startup". The article discusses how PayPal's actions affected a company called ProtonMail.

FREE & OPEN SOURCE

Forkable on Github

A screenshot of a GitHub repository page for "bitcoin / bitcoin". The page shows the repository's details, including its name and a link to the code.

MUCH MORE

Multisig, Blockchain, Contracts!

A diagram illustrating the extensibility of Bitcoin. It shows a central node connected to four boxes: "Assurance Contracts", "Smart Property", "Autonomous Agents", and "Distributed Markets".

Examples of Forking & Modification

Bitcoin is an open-source commons that people can fork & rapidly improve without paying anything.

Introducing Toshi - An 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 implementation 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



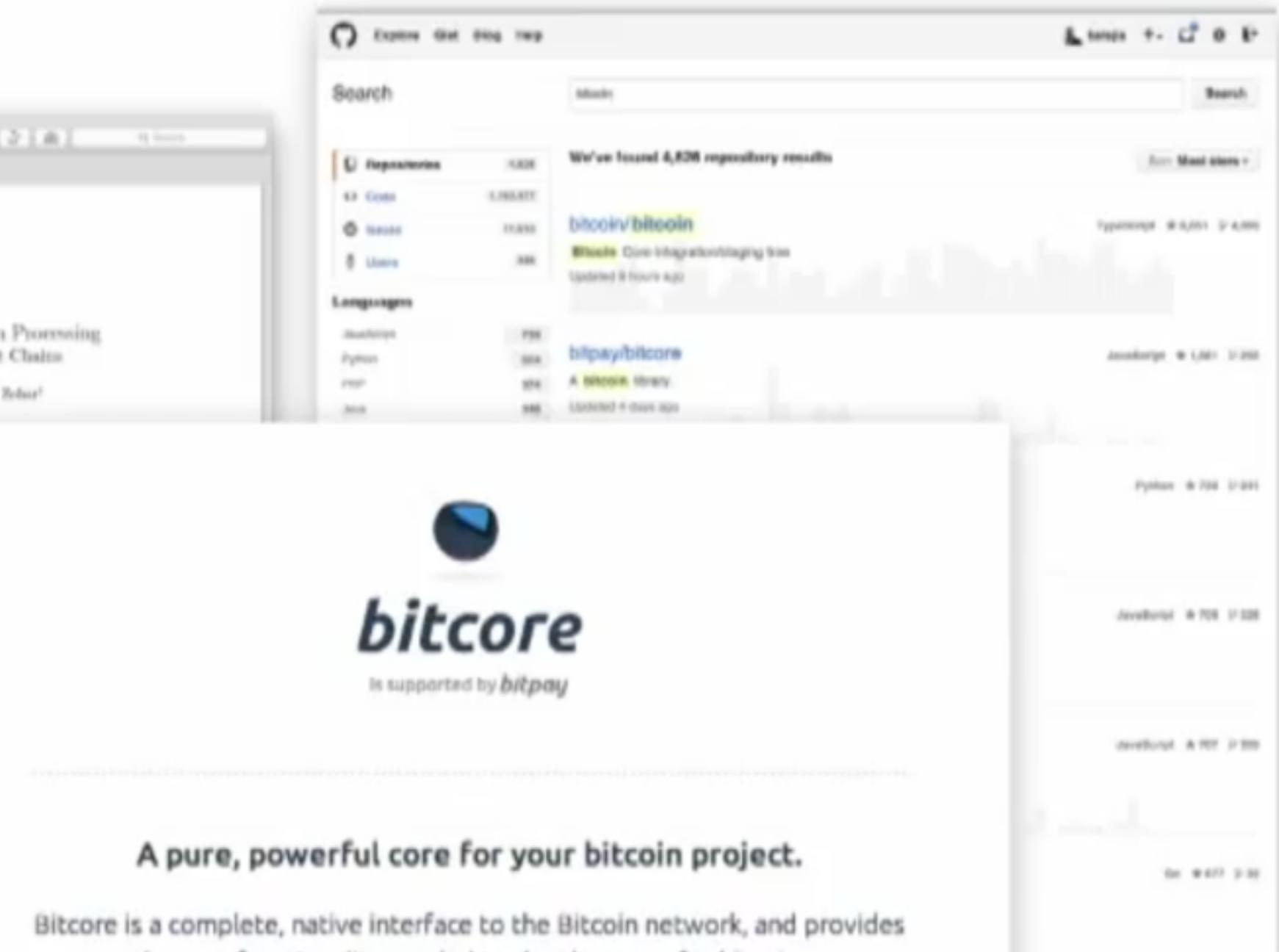
Have a Snack, Pay with Bitcoins
Toshi Beutel¹, Christian Decker¹, Lennart Ebele¹, Roger Wattenhofer², Stefan Wanka¹
¹ETH Zurich, Switzerland (toshi.cs.berkeley.edu/toshi/bitcoin)
²Microsoft Research (research.microsoft.com)

B. REVISION
Bitcoins were introduced as a peer-to-peer electronic payment system in 2009. However due to the nature of the transaction confirmation in Bitcoin, it is not well suited for payment. Most often quick transaction confirmation, low fees and a consensus that allows for the reuse of the same bitcoins multiple times are the key requirements. We evaluate the performance of the current system using double-spending attacks and show that employing our technique, the success of such attacks decreases to less than 0.001%. Moreover, we present a real world application. We modified a snack vending machine to accept Bitcoin payments, and make use of fast transaction confirmation.

E. INTRODUCTION
Today, we are witnessing that an increasing number of payments in our economy are initiated rapidly and easily. Today businesses are forced upon a customer and established companies are looking for new ways to expand their existing payment methods. In the last years, several new payment systems like Google Wallet or PayPal simplified fast and reliable money exchange. These approaches have in common that they rely on a central trusted authority to process payments. In contrast, the Bitcoin currency and payment system offers a completely decentralized payment infrastructure based on a peer-to-peer network. Even though there is no central trust authority the Bitcoin network can provide reliable instantaneous money transfer.

However, due to the decentralized nature of Bitcoin, transactions can only be confirmed if the majority of participating nodes accept them. This transaction confirmation process can take several minutes. Although often touted as the major advantage of Bitcoin it is not fit for transactions that require fast clearing of transactions. While this delay is not problematic for most online purchases, it prevents the use of Bitcoin in situations where a transaction confirmation is required in the order of seconds, such as paying in a supermarket or at a small vending machine.

In this paper, we present a technique that improves the trade-off between transaction speed and confirmation reliability in the Bitcoin network. In addition to our double-spending experiments that quantify this trade-off, we implemented the fast transaction clearing in a common ready-to-use machine that can accept bitcoins as a payment and dispense the product within seconds.



bitcore
bitpay/bitcore
A **Bitcoin** library.
Updated 8 hours ago

Abstract
Bitcoin is a potentially disruptive new crypto-currency protocol which is quickly gaining popularity. One of the main reasons for its success is whether or not it has high volume of transactions originated from a global community. We investigate the bottleneck on the rate of transaction processing of both the bandwidth available to make a transaction and the efficiency of Bitcoin's transaction processing. The results confirm that the bottleneck is on the rate of transaction processing and not the bandwidth available to make a transaction. We propose upon the original analysis and results, we are able to give bounds on the number of transactions processed. Relying on previously published assumptions we show these bounds are currently more interesting bandwidth needed to make all transactions. We also implement improvements to the protocol, namely the use of multi-signature transactions resulting in a significant reduction in the size of the transaction.

Finally, we present an easily implementable model to predict the number of transactions per second. The model is especially useful when the network experiences high rates, increases in the number of transactions processed per second and the transaction size. The prediction model is accurate. The block processing time can be accurately predicted - a 1000 fold speedup compared to today's off processor binary transactions per second.

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.

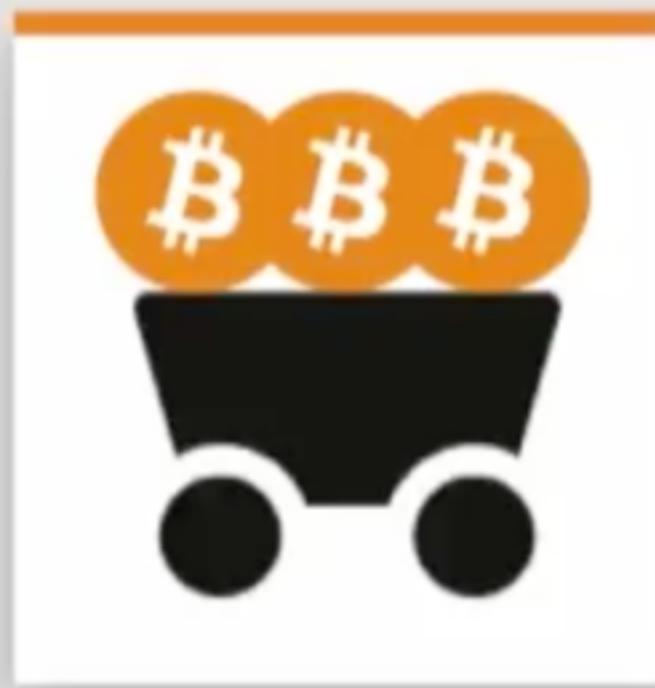
Get Started

Bitcoin has a network effect

Four-sides: Miners, Devs, Merchants, Users

Bitcoin has a four-sided network effect

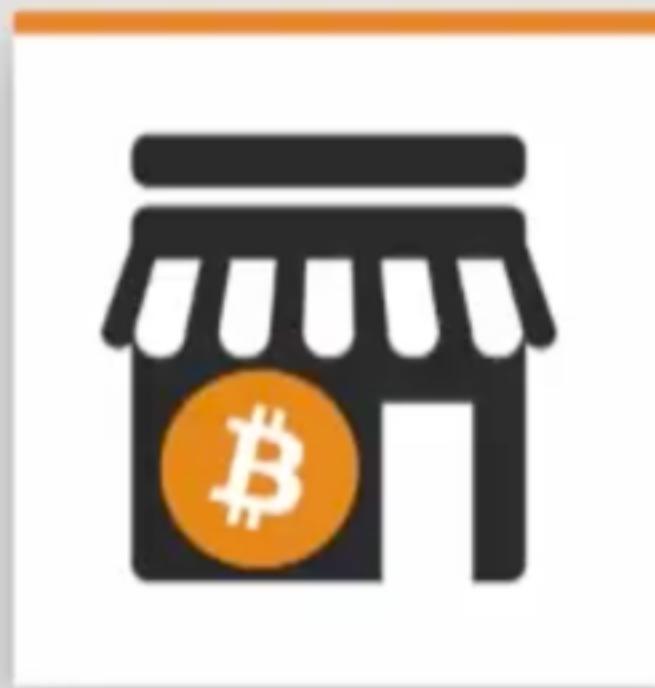
Four groups: miners, developers, users, and merchants.



Miners
Verify transactions,
receive BTC.



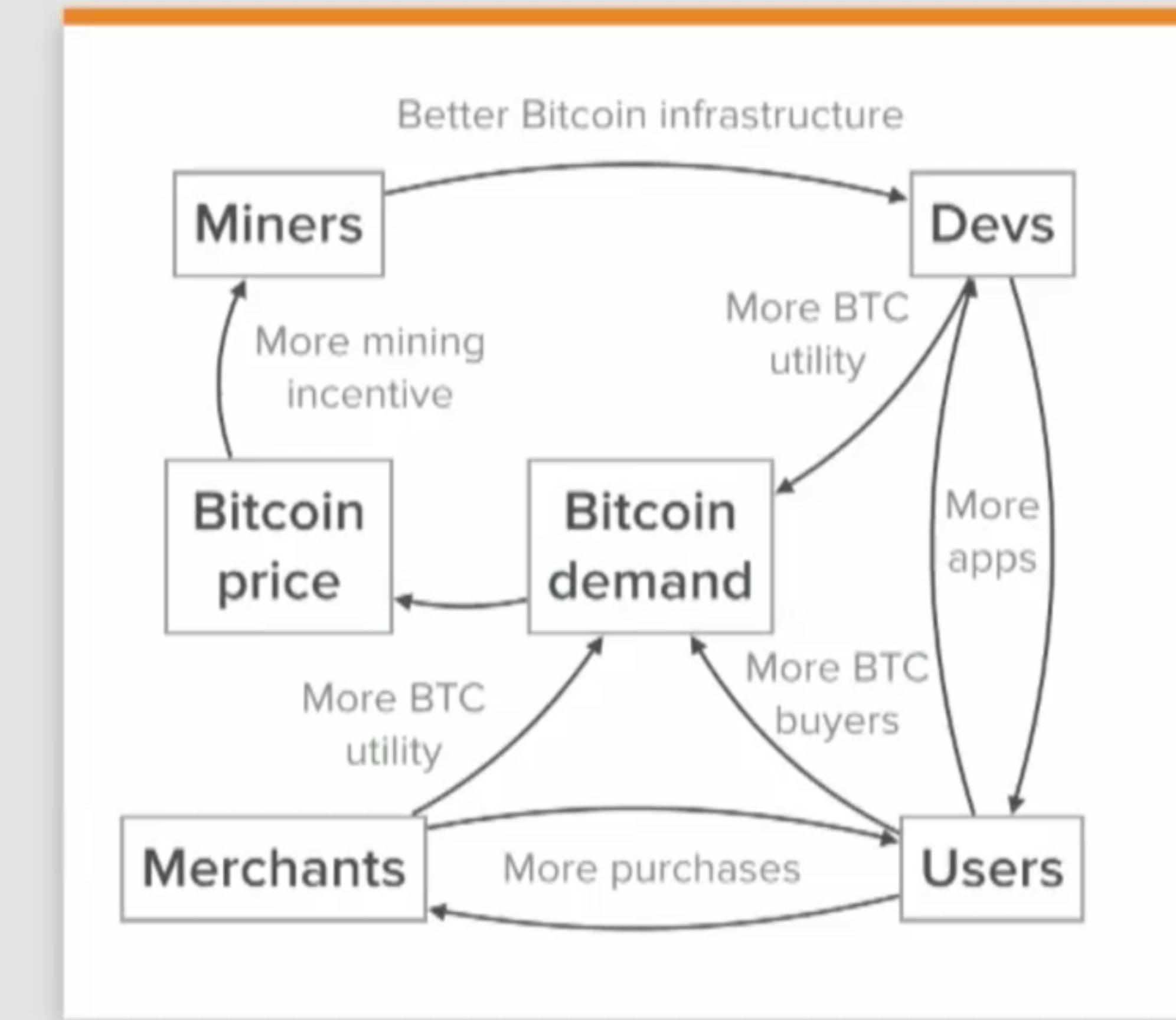
Devs
Write Bitcoin apps.



Merchants
Accept Bitcoin for goods.



Users
Use Bitcoin for goods & apps.



The 4-Sided Network Effect

Every node increases value for other nodes.

Users: Adoption Metrics

From a year-on-year perspective, even given price volatility, adoption is actually way up across the board.

Key Bitcoin Adoption Metrics

	Quarterly			Last 12 Months	
	Mar-15	Dec-14	Q/Q Δ	Mar-14	Δ
Commerce					
Wallets	8,457,207	7,396,772	14%	4,448,142	2x
Merchants	88,000	82,000	7%	52,704	2x
Merchants' annual revenue (\$bn)	180	180	0%	2	78x
ATMs	374	342	9%	47	8x
Unique bitcoin addresses	203,189	157,377	29%	137,342	1x
Industry					
All-time VC investment (\$m)	\$676	\$447	51%	\$164	4x
Number of VC-backed startups	103	89	16%	47	2x
Media					
Mainstream media mentions	458	580	-10%	2,594	-82%
Technology					
Network hash rate (billion/second)	346,028,956	313,142,289	11%	41,813,922	8x
Github no. of updated repositories	27,857	23,249	20%	9,915	3x
Valuation					
Bitcoin market capitalization (\$bn)	\$3.4	\$4.3	-21%	\$5.3	-36%

Data sources and notes: CoinDesk, [Blockchain.info](#), [BitcoinPulse](#), [Github](#), [Coin ATM Radar](#). Figures are cumulative from start of records, except unique bitcoin addresses and media mentions, which are figures for the quarter ending that month.



Most figures up 3-10X. Hashrate up 200X!

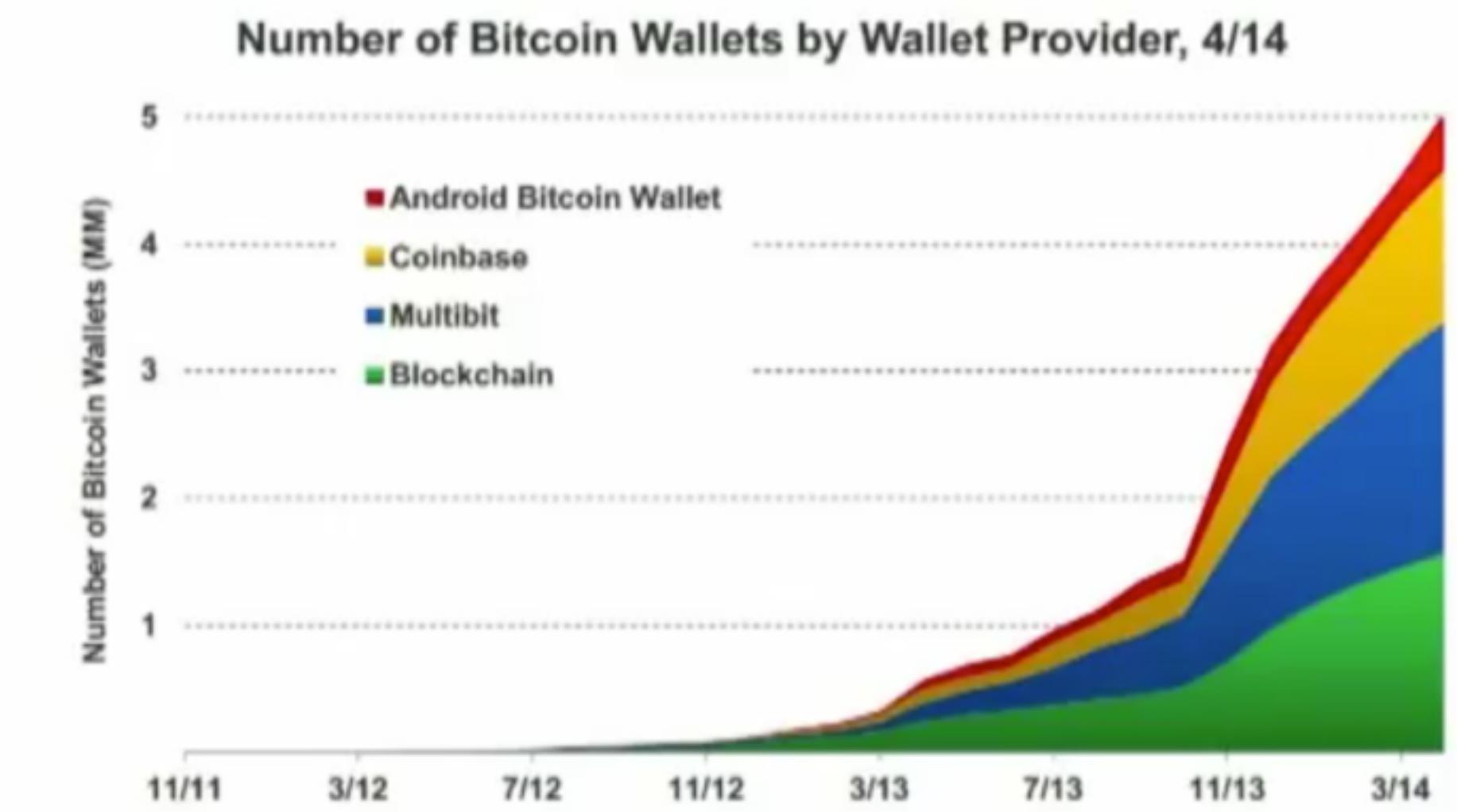
2014: year of institutional acceptance

Users: More than 8M Wallets

Were 5M public wallets as of May 2014.

Were 8M as of Nov 2014 (Coinbase + Blockchain + ...)

Fact that ~5MM Bitcoin Wallets (+8x Y/Y) Exist
Proves Extraordinary Interest in Cryptocurrencies



@KPCB

Source: CoinDesk. Largest wallet providers (Blockchain / MultBit / Coinbase / Bitcoin Wallet) at ~4.9MM wallets account for majority of Bitcoin wallets created.

53



8M user wallets means ~100-1000X growth left

Potential to ultimately get to billions

Users: Record Transaction Volumes

All-time record transaction volumes are now being posted.



The long-term transaction volume trend is clear

Core developer roadmap scales tx volume to many billions per day

Users: Record Transaction Volumes

All-time record transaction volumes are now being posted.



A Scalability Roadmap

ON OCTOBER 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.

There are other ideas for how to make Bitcoin scale, and whenever practical I like to choose “all of the above” for how to solve a problem, because nobody is smart enough to choose The One True Solution every time. So I won’t be surprised or disappointed if development wanders off this roadmap in a different direction.

Initial Download

Everybody who runs the Bitcoin Core reference implementation the first time is annoyed by an absurdly long wait for it to download and then index the

The long-term transaction volume trend is clear

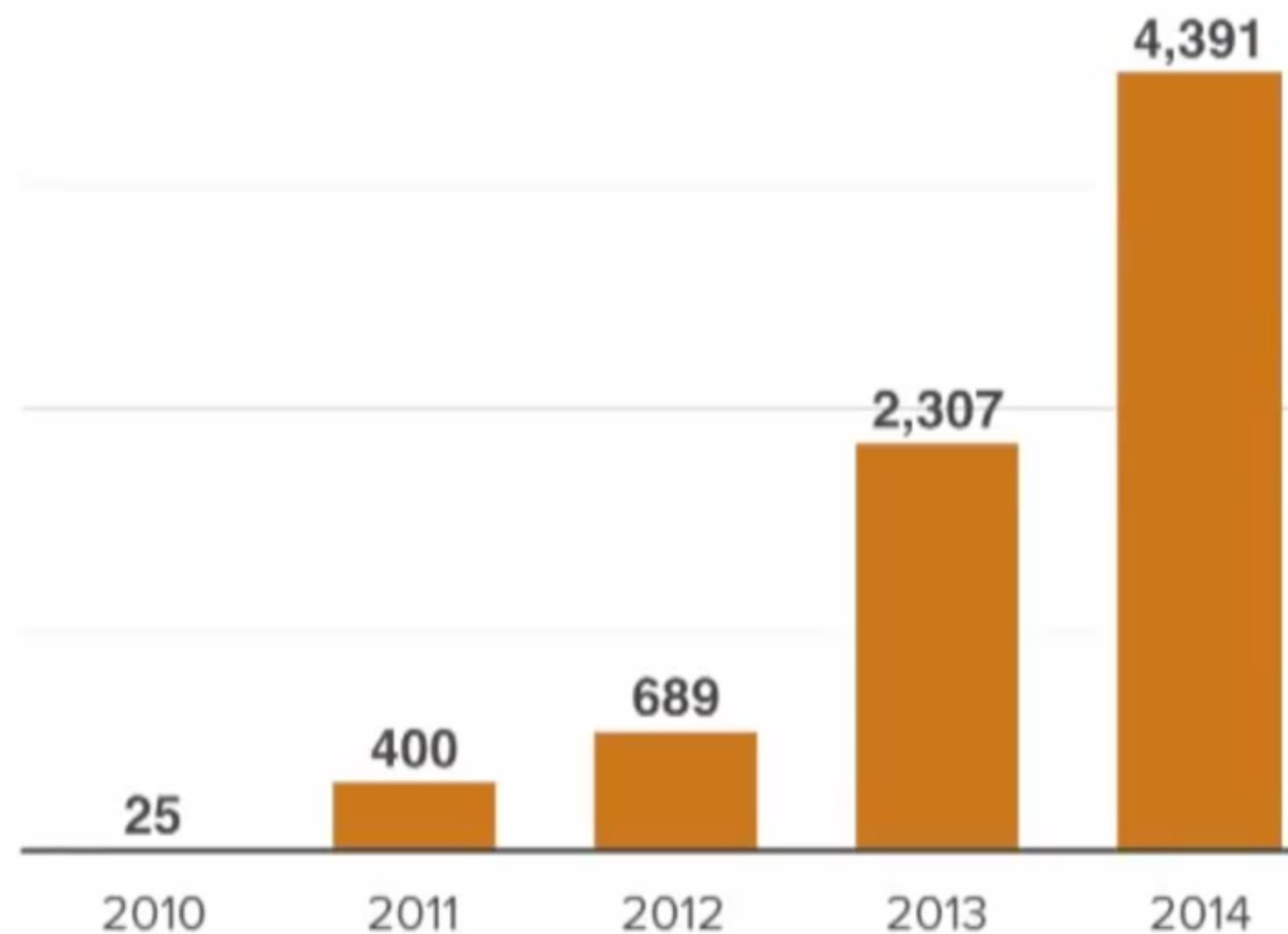
Core developer roadmap scales tx volume to many billions per day



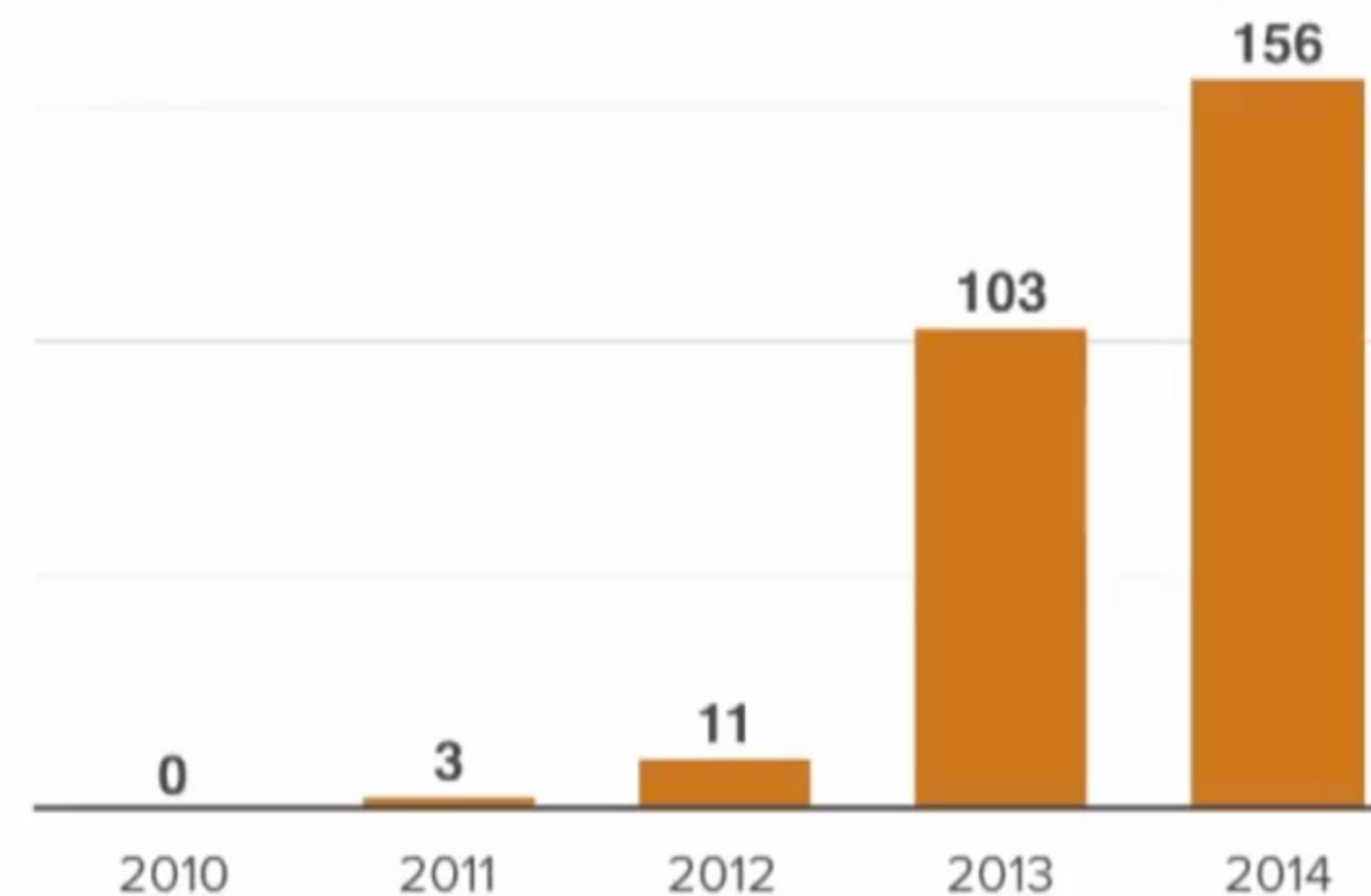
Developers: Huge Open Source & Startup Traction

The community of Bitcoin developers & entrepreneurs is rapidly increasing.

GITHUB REPOS



ANGELLIST INVESTMENTS



Price: The Short-Term View

Why is price down now? Miners have to sell in bulk to pay electricity bills, artificially depressing price with large sell orders.



The a16z Bitcoin FAQ

Let's talk through some FAQs - and the most important q

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 Instances	Amit Yagle	Active
10	MultSig Transaction Instruction	Asim Farmer	Draft
11	id of a Bitcoin Transaction	Gavin Andresen	Accepted
12	OP_ECD	Gavin Andresen	Withdrawn
13	Address Format for use in script hash	Gavin Andresen	Pending
14	Protocol Version and User Agent	Asim Farmer, Patrick Butcher	Accepted
15	Witness	Amit Yagle	Withdrawn
16	Pay To Script Hash	Gavin Andresen	Accepted
17	OP_DUP and OP_NODUP (OP_2)	Luke Dashjr	Withdrawn
18	Timestamps	Luke Dashjr	Draft
19	Multisig Transactions: Low Priority	Luke Dashjr	Draft
20	URI Scheme	Luke Dashjr	Pending
21	URI Scheme	Micah Lee, Matt Corallo	Accepted
22	getnewtxid - Functionality	Luke Dashjr	Accepted
23	getnewtxid - Fixed Mixing	Luke Dashjr	Accepted
24	Business Remittance	Peter Voulgaris	Accepted
25	Ping message	Micah Lee	Accepted
26	Peer-to-Peer Decentralized Wallets	Peter Voulgaris	Accepted
27	SmartLocks	Asim Farmer	Draft
28	Block ID, Height or Sequence	Gavin Andresen	Accepted
29	Margin message	Jeff Garzik	Accepted
30	Relay Services	Markus Haas	Draft
31	Beacon Mining	Markus Haas 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

Powered by Lightning by [Joe Pamer](#) (open source), Collected



Modifiable?

Yes. Like IETF, BIPs/patches regularly incorporated.

Important: Bitcoin protocol itself has not been hacked.

I Tried Hacking Bitcoin And I Failed

BY DAN KAMINSKY, DANKAMINSKY.COM

APR. 12, 2013, 10:45 AM 6,704,607 12

Seriously though, as an engineer and 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.

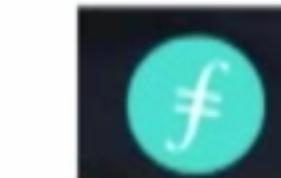
Scaling will be nontrivial, but Internet pushed communications up to 10000/day. Bitcoin will do same for transactions.

Scalable?

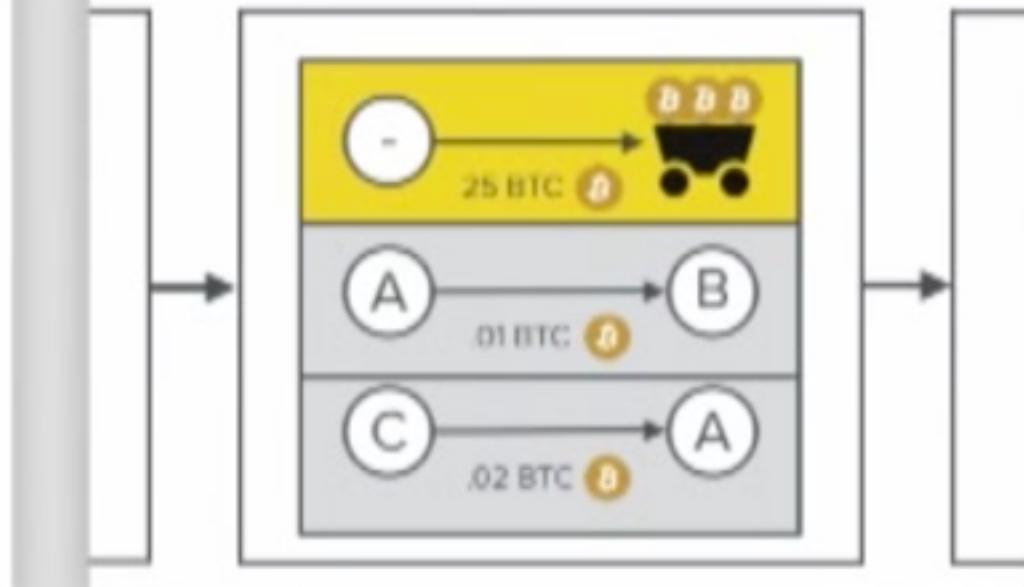
Yes. Core devs have published billion tx roadmap.

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

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.

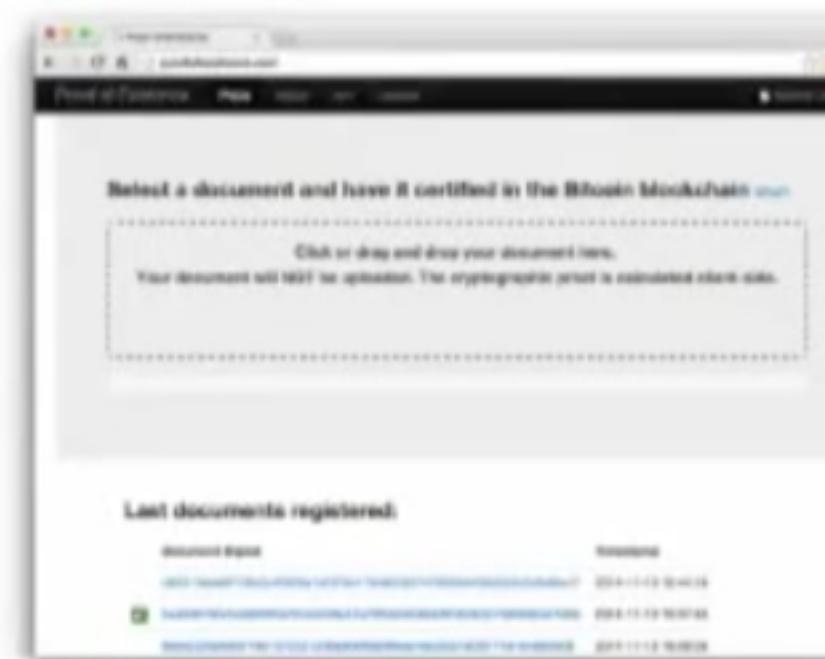
BUSINESS SOFTWARE security, cloud & services, bitcoin

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

Jeremy Kirk

May 28, 2013 4:00 AM ET

Manuel Arango, a 23-year-old developer in Argentina, has an idea for Bitcoin that doesn't focus on money. Arango, who works in game development, launched a service this week called [Invoicelock](#). 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.



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 Endorses Bitcoin ETF



WSJ BitBeat
Daily coverage of Bitcoin news

Altcoins: lack traction, 10X reason



Stellar/Ripple: no compelling advantages vs Bitcoin

How does this compare to Bitcoin?

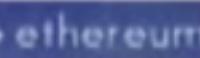
The main differences between Stellar and Bitcoin are the following:

- 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 users can set their currency in their currency of choice (flat or digital).

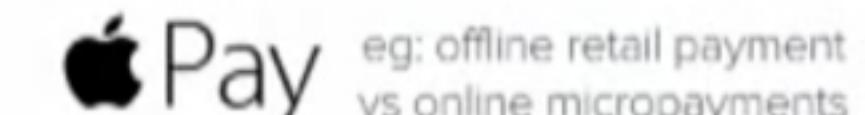
The issue is that the stellar currency itself will be mostly a behind-the-scenes currency, and that the stellar network won't help provide more liquidity between currencies.

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 HTTP

And perhaps the most frequent question...

What about the Bitcoin price?

Price: The Long-Term View

Understanding price begins with understanding market depth: the empirical balance of buy and sell orders.



- Miner sell pressure:
25 BTC/block x 144 blocks/day x \$250 = \$900k/day
- A stable price means buy and sell identically balanced
- Price migration up/down signals imbalance



For price to increase, must have more buy than sell orders

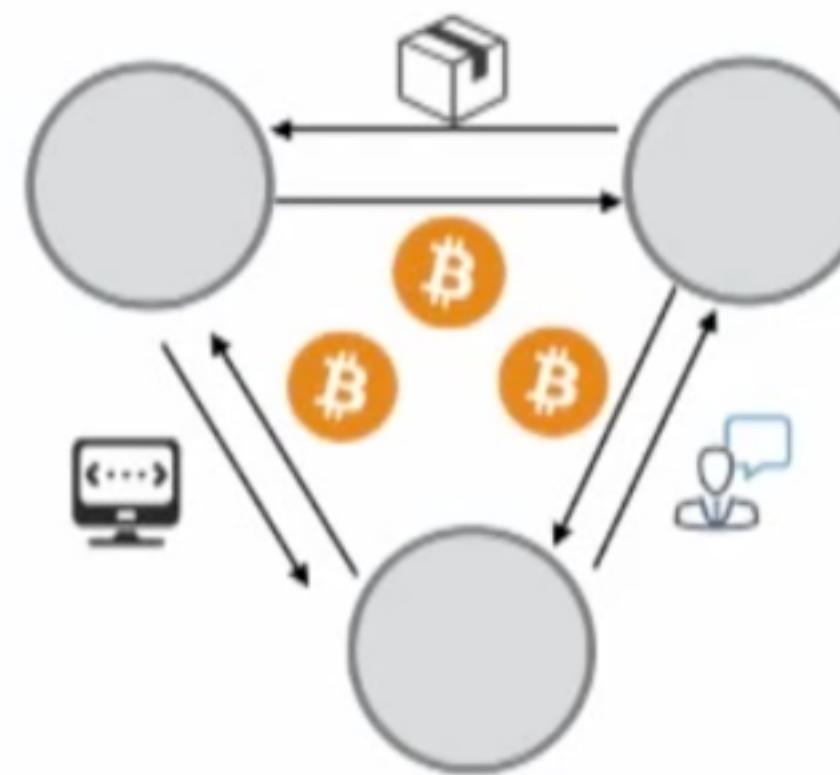
Why would that happen besides simple speculation?

Price: The Long-Term View

In the long term, maintaining and increasing the Bitcoin price further will mean the multiyear task of building the Bitcoin economy.

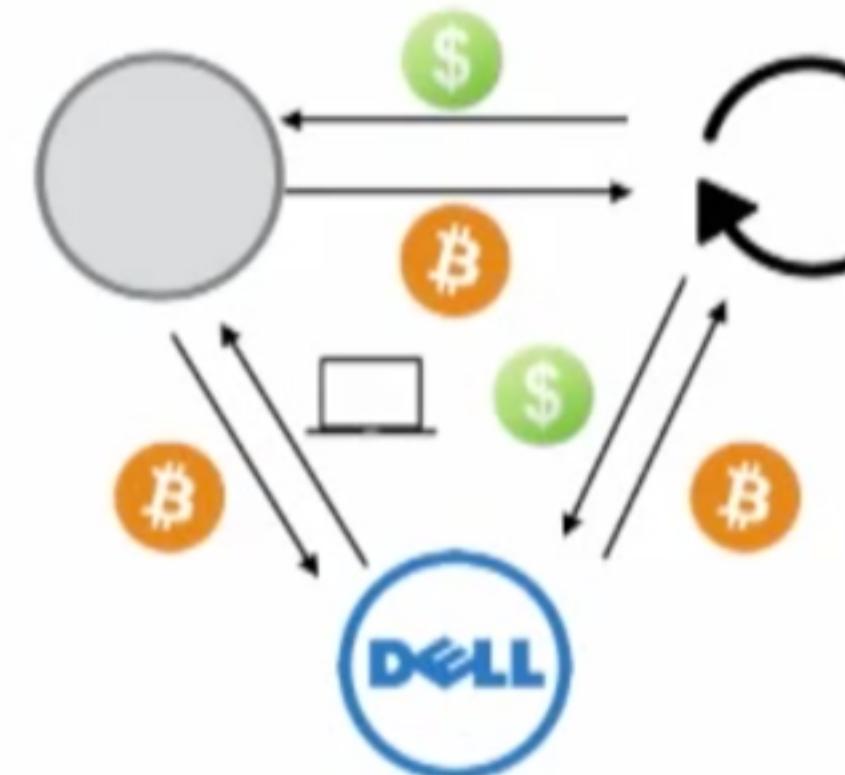
Good:

- buy BTC above market price
- trade BTC for valuable goods and services



Bad:

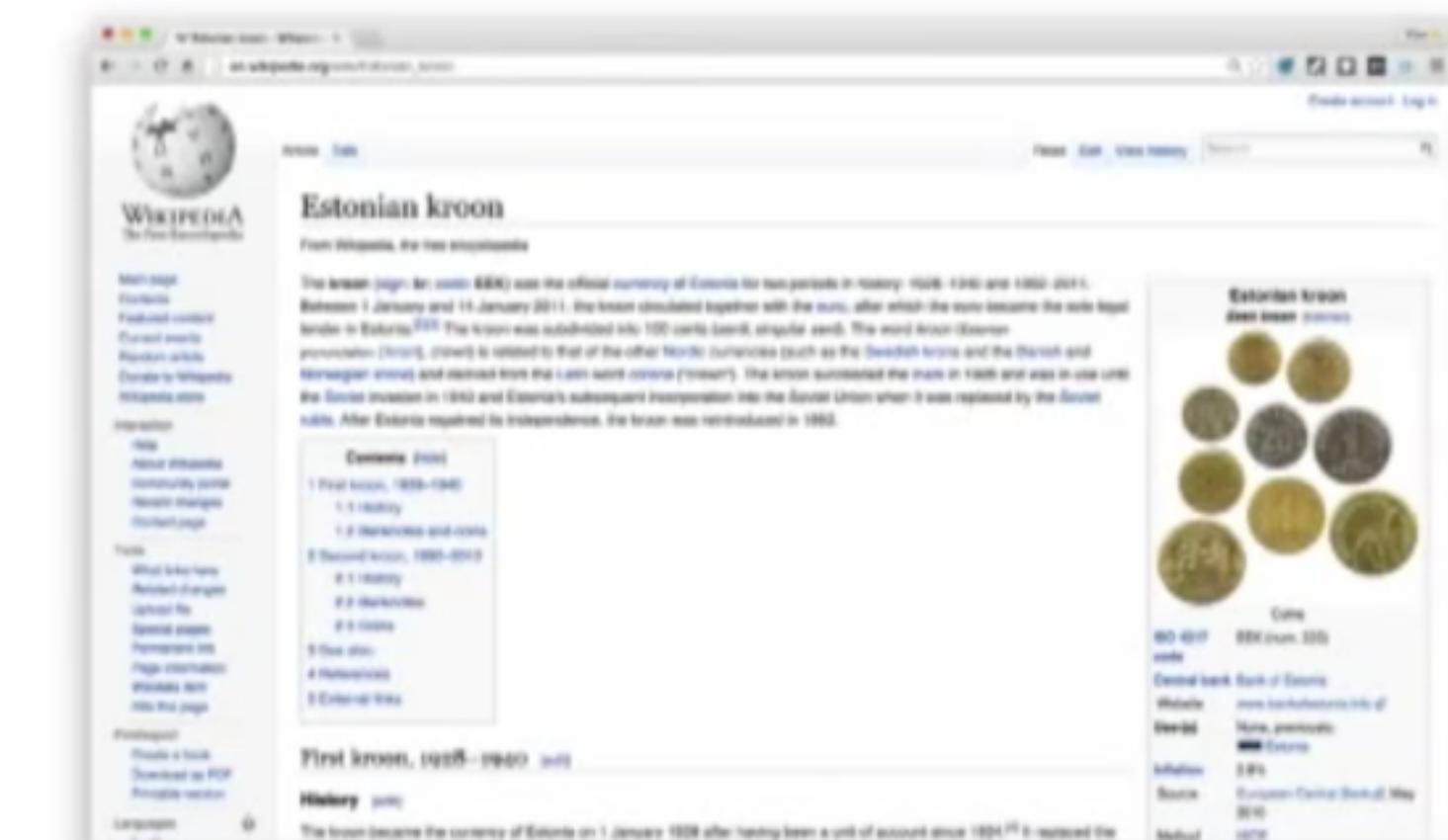
- sell BTC
- receive BTC and sell to pay bills



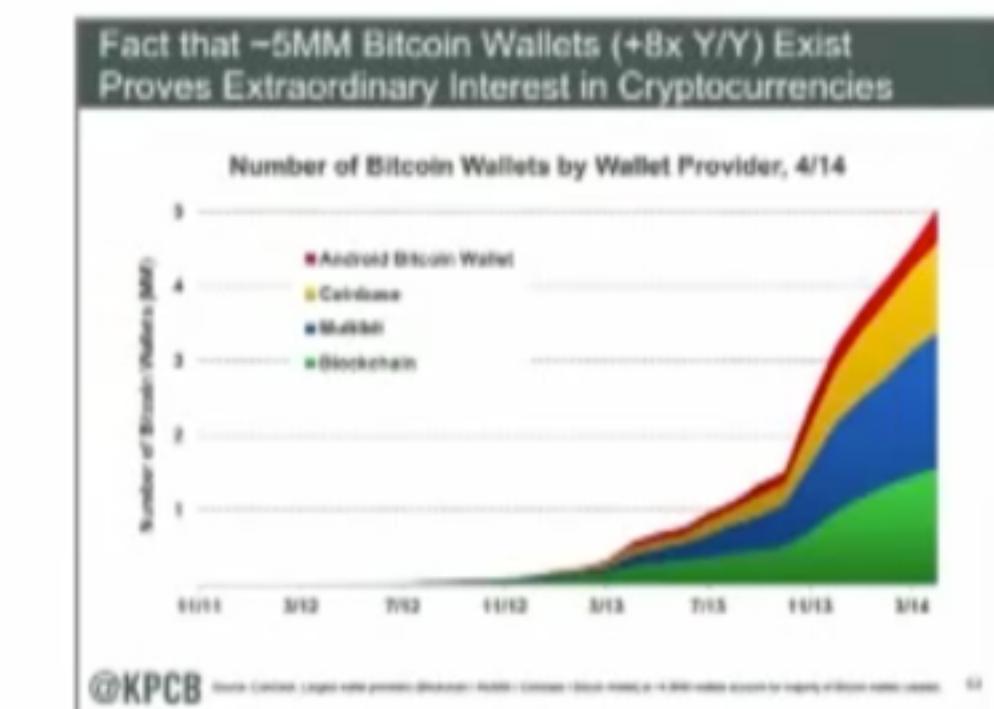
To increase the price we need closed loops.

To have more buy than sell orders: build, not just speculate

There must be goods & services purchase-able only with Bitcoin



Estonia: 1.3M people with own currency (till 2011)
A modern economy on the Kroon



Bitcoin: 5M wallets for this digital currency

Q: Can we build a cloud economy?

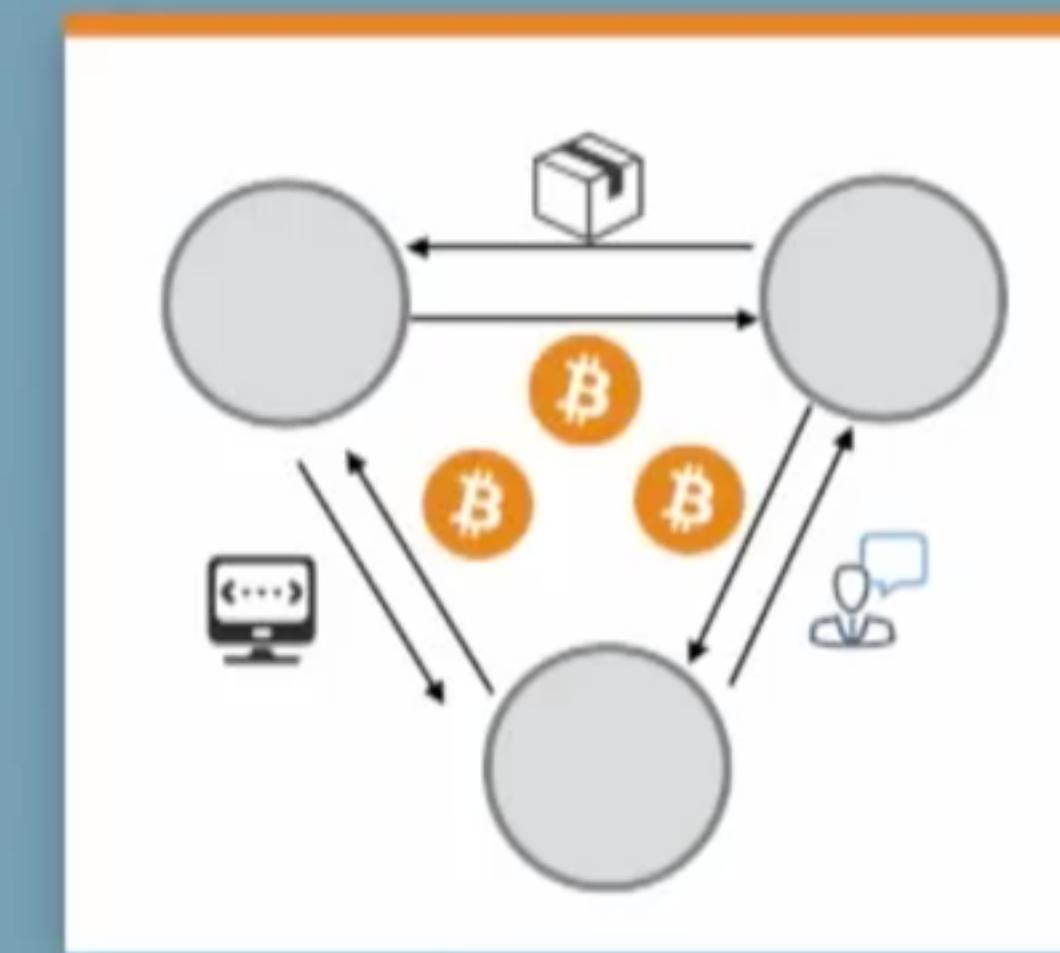
The answer to the most frequent question...

What about the Bitcoin price?

...is the most important question.

Can we build a cloud economy?

Can we build the closed loops?
Can we build a cloud economy?



Perhaps the most important q in Bitcoin.

Recap

Let's summarize.

The Andreessen Horowitz Thesis on Bitcoin

Five key facts about Bitcoin that inform our thinking, and answers to some FAQs.

BITCOIN IS A PROTOCOL

Payments are now packets



BITCOIN HAS A NETWORK EFFECT

Four sides: Miners, Devs, Merchants, Users



Miners

Developers Merchants

Users

BITCOIN IS HERE TO STAY

Extraordinary institutional/sovereign support



BITCOIN IS BIGGER THAN GOOGLE

Mining now world's largest supercomputer



> Google

BITCOIN IS OPEN SOURCE

Extensible, programmable, rapidly improving



THE A16Z BITCOIN FAQ

And the most important q in Bitcoin.



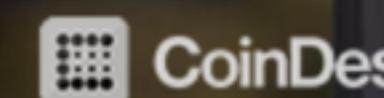
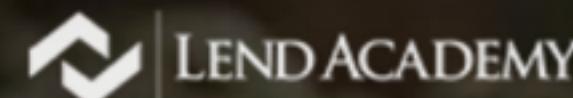
Mobile app ideas

[GET A LOAN](#)[INVEST IN LOANS](#)[RESOURCES](#)[LOGIN](#)[SIGN UP](#)

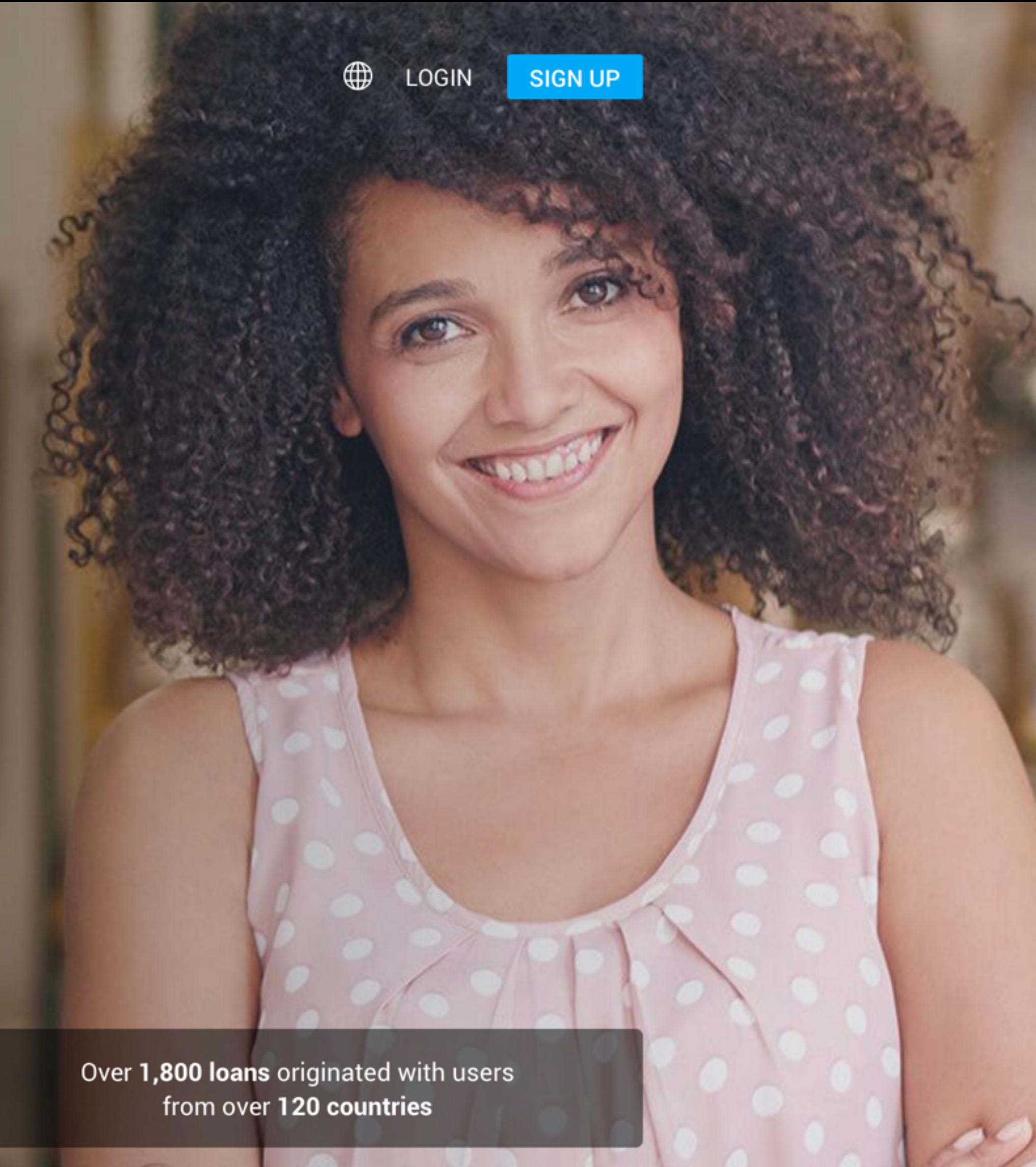
Borrow and invest without borders

[Apply for my loan](#)[Start earning today](#)

AS SEEN ON

**GIGAOM****Forbes**

Over 1,800 loans originated with users
from over 120 countries



Currency

BTC

ETH

ETC

XMR

ZEC

PASC

DASH

LTC



Calculated for
1 BTC = \$ 2778.93

Hashing Power

13

TH/s



Power consumption (w)

1350

Cost per KW/h (\$)

0.06

PROFIT RATIO PER DAY

480%

PROFIT PER MONTH

\$ 280.41

Profit per day
\$ 9.35

Day

Mined/day
Ƀ 0.004063

Power cost/Day
\$ 1.94

Profit per week
\$ 65.43

Week

Mined/week
Ƀ 0.02844

Power cost/Week
\$ 13.61

Profit per month
\$ 280.41

Month

Mined/month
Ƀ 0.1219

Power cost/Month
\$ 58.32

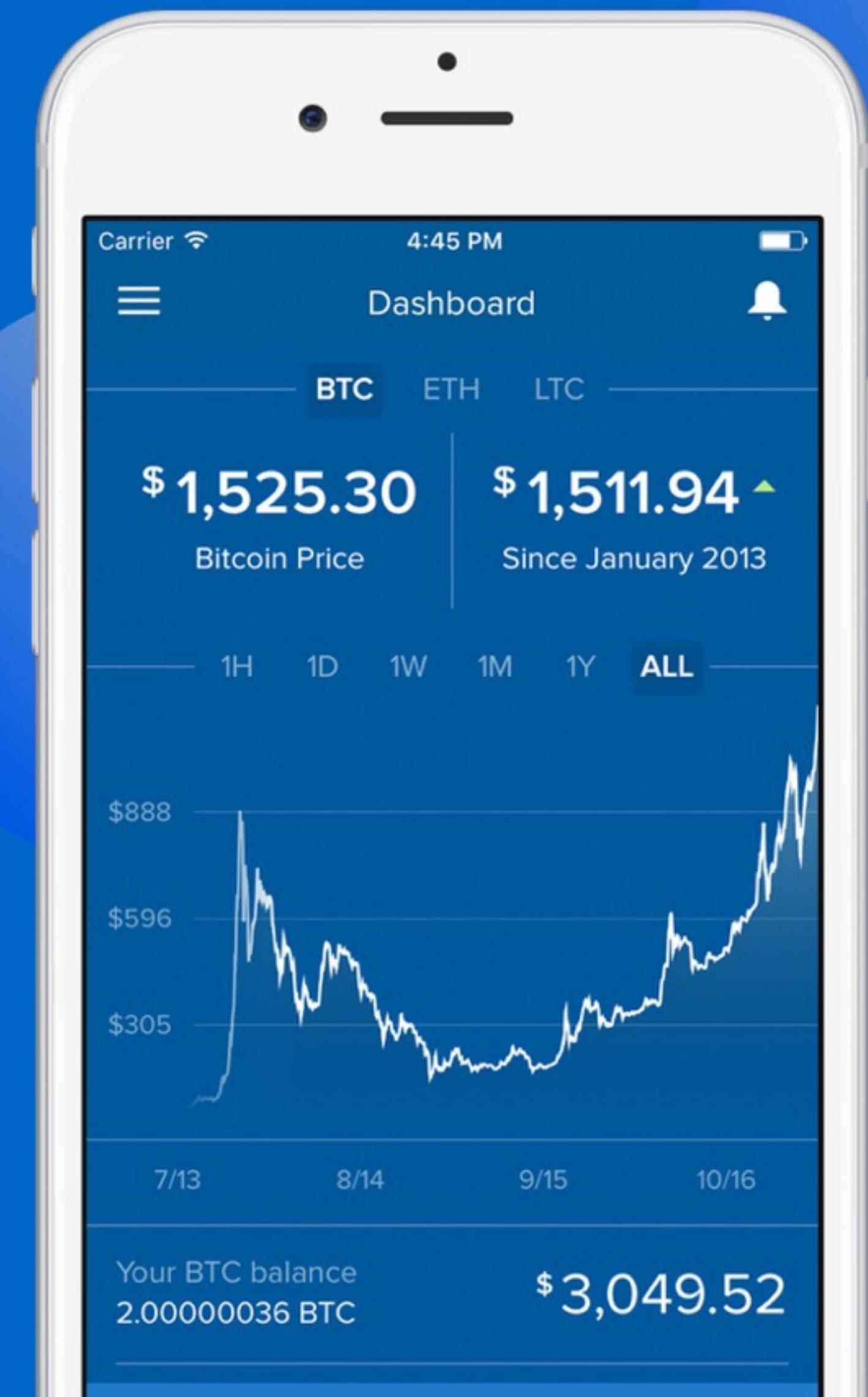
Profit per year
\$ 3,411.70

Year

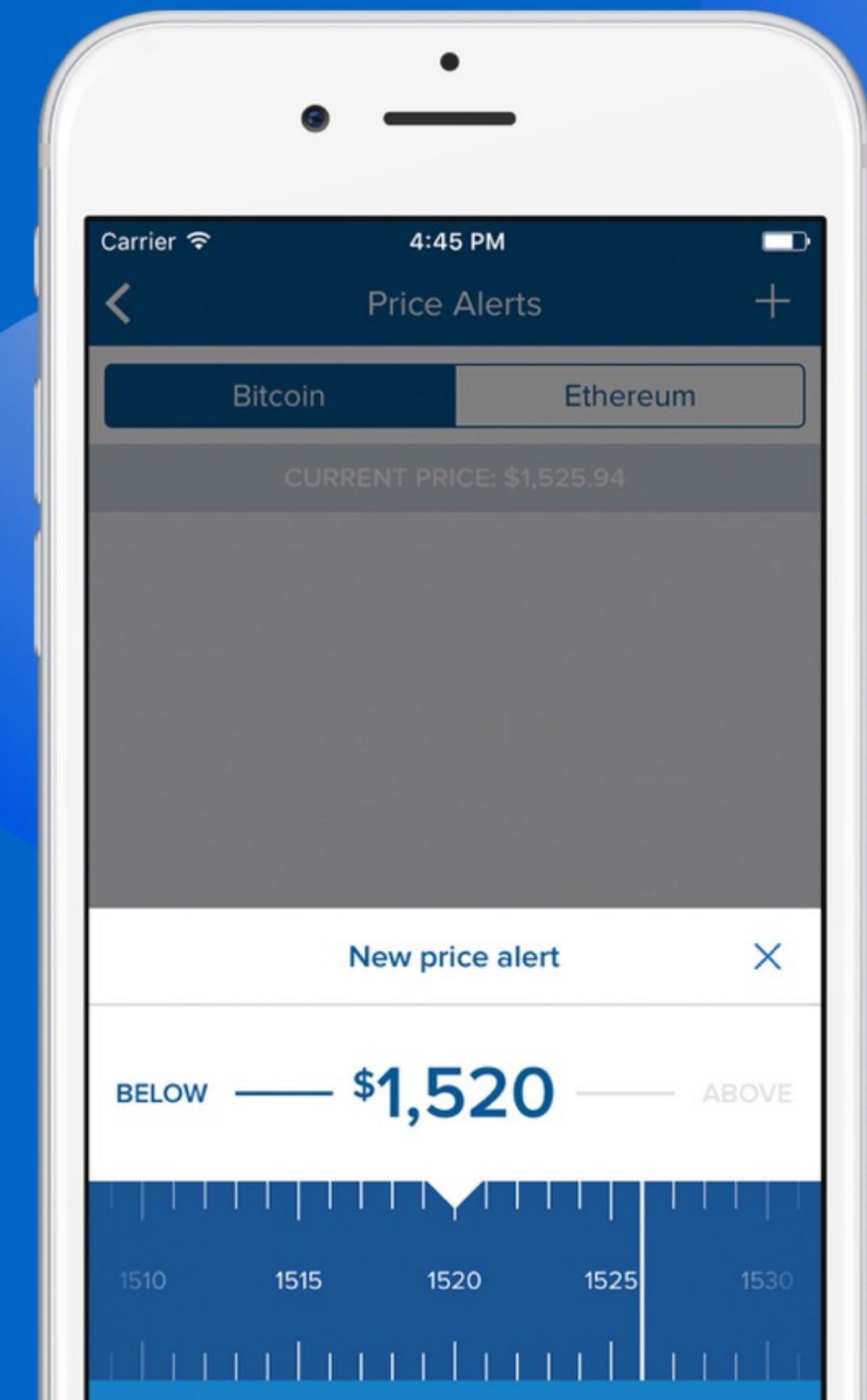
Mined/year
Ƀ 1.48

Power cost/Year
\$ 709.56

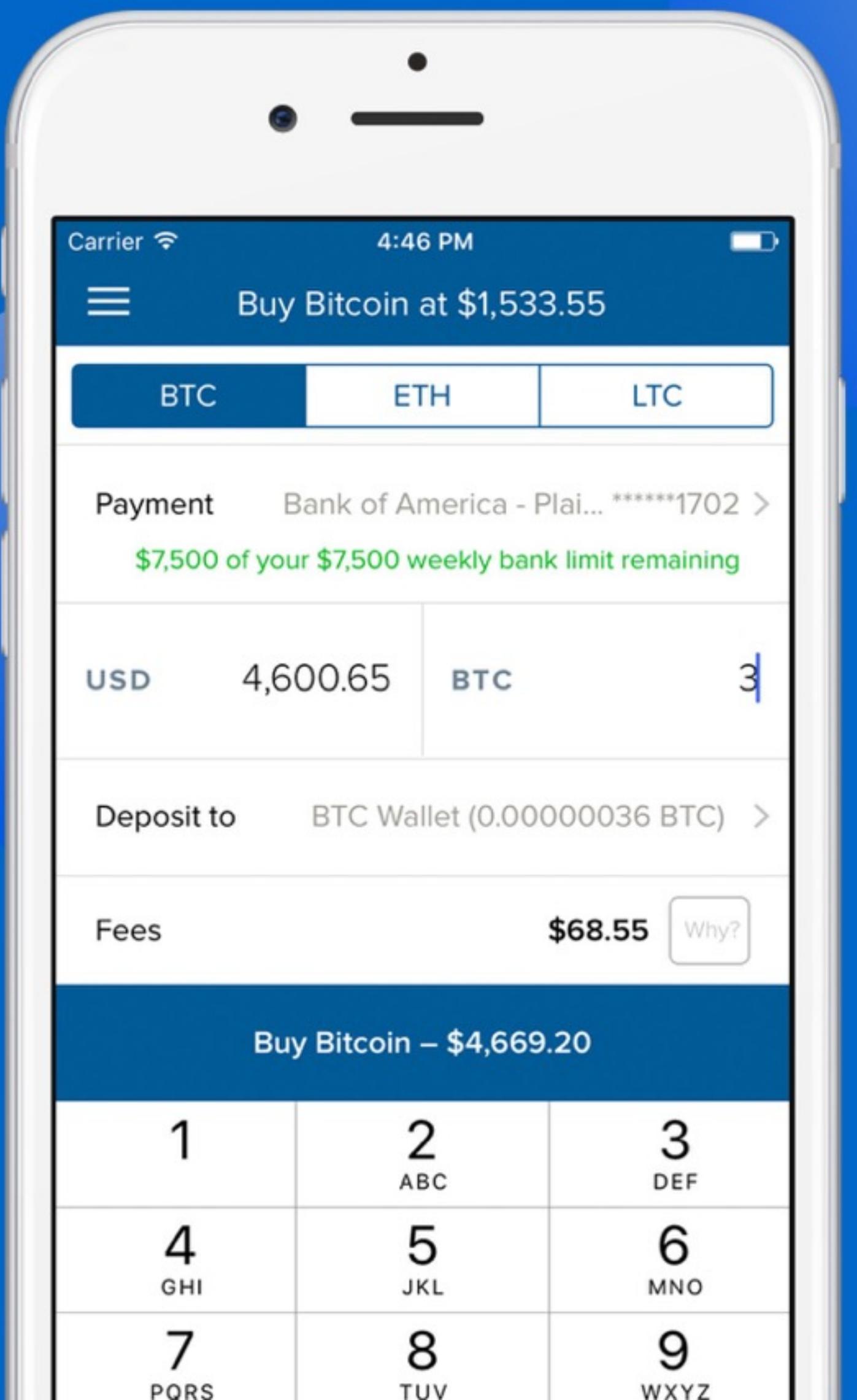
Price charts



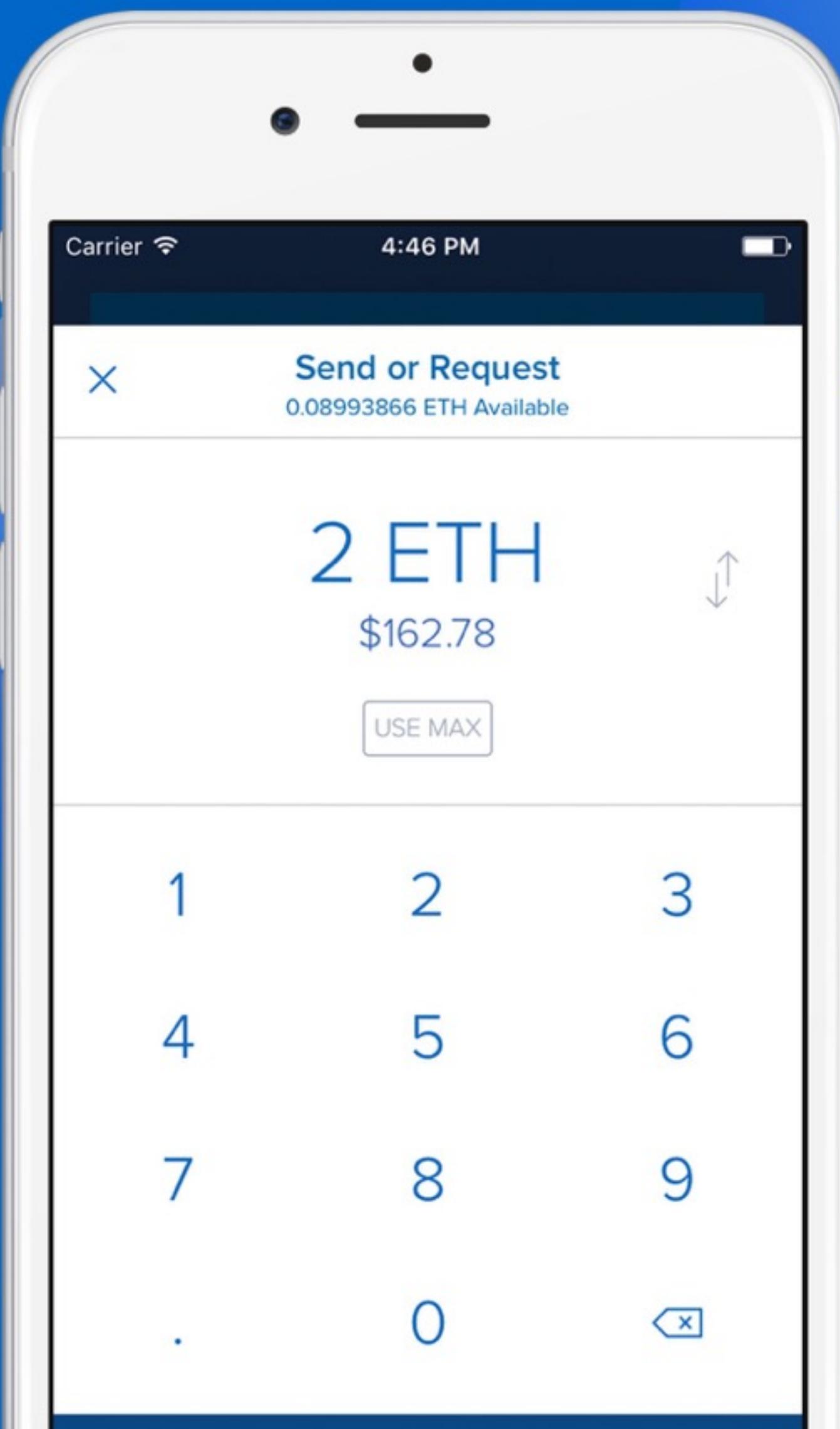
Create price alerts



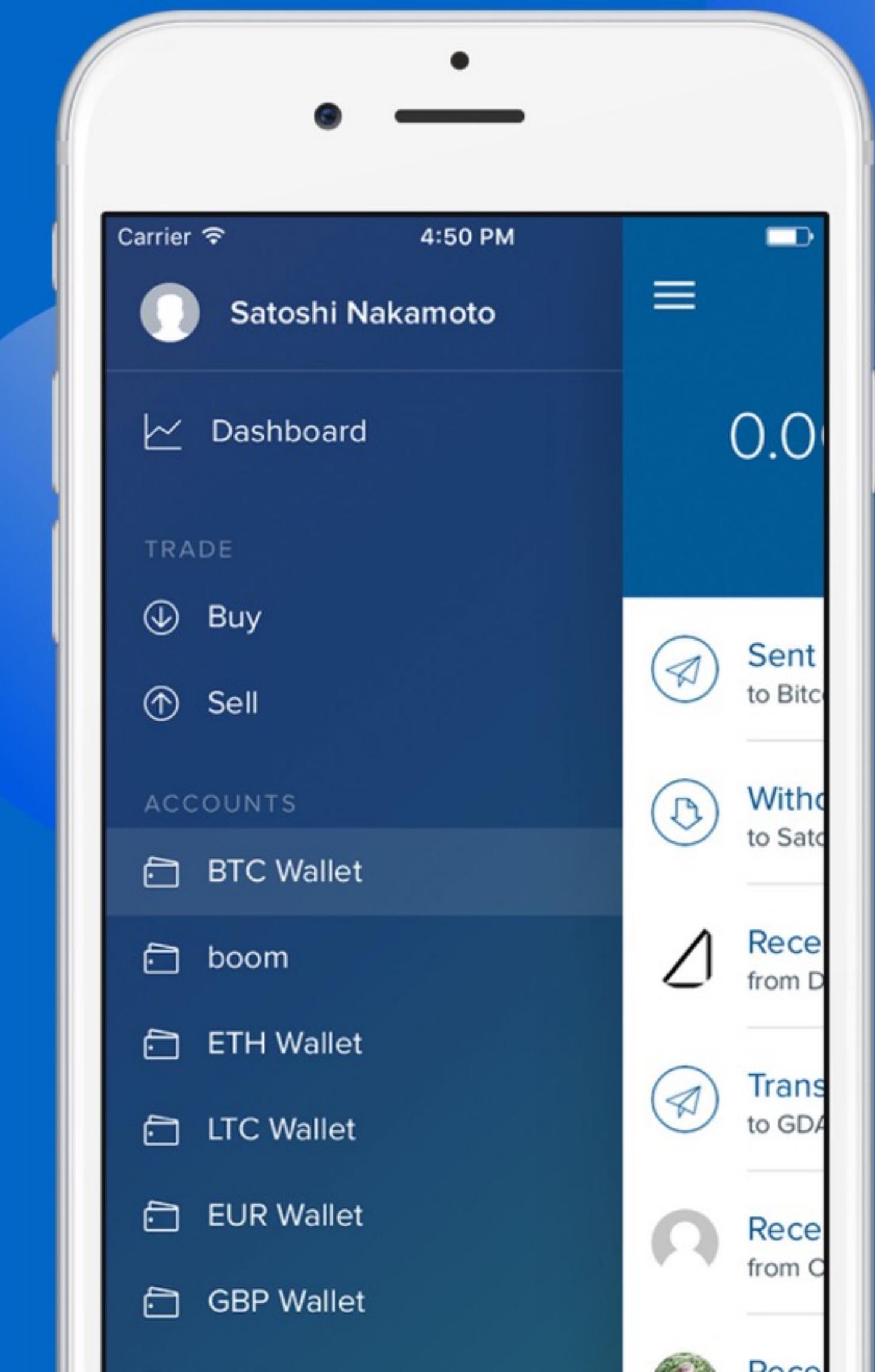
Buy and sell digital currency



Send or Request



Access your accounts



[INSIDE BITCOIN]

Inside Bitcoin

Tracking trends, news, and analysis around Bitcoin and cryptocurrencies



Your email

SUBSCRIBE

More at <https://cryptominded.com>

Business card scanner using Core
ML

Blur parts of the image which you
don't want anyone to see



Minimalist app to track daily water intake. See: WaterMinder

One random app idea using Product
Hunt API

One new book recommendation
using Kindle API

Safe mobile browser for kids

Книга жалоб для сервисов
Kazakhtelecom, Altel, Tele2.

Top 100 charts: top 100 cryptocurrencies,
top 100 private companies by valuation,
top 100 richest athletes, etc.

ARKit app where you collect
characters of the upcoming movie



Teach Kazakh
through
emojis: 🍑



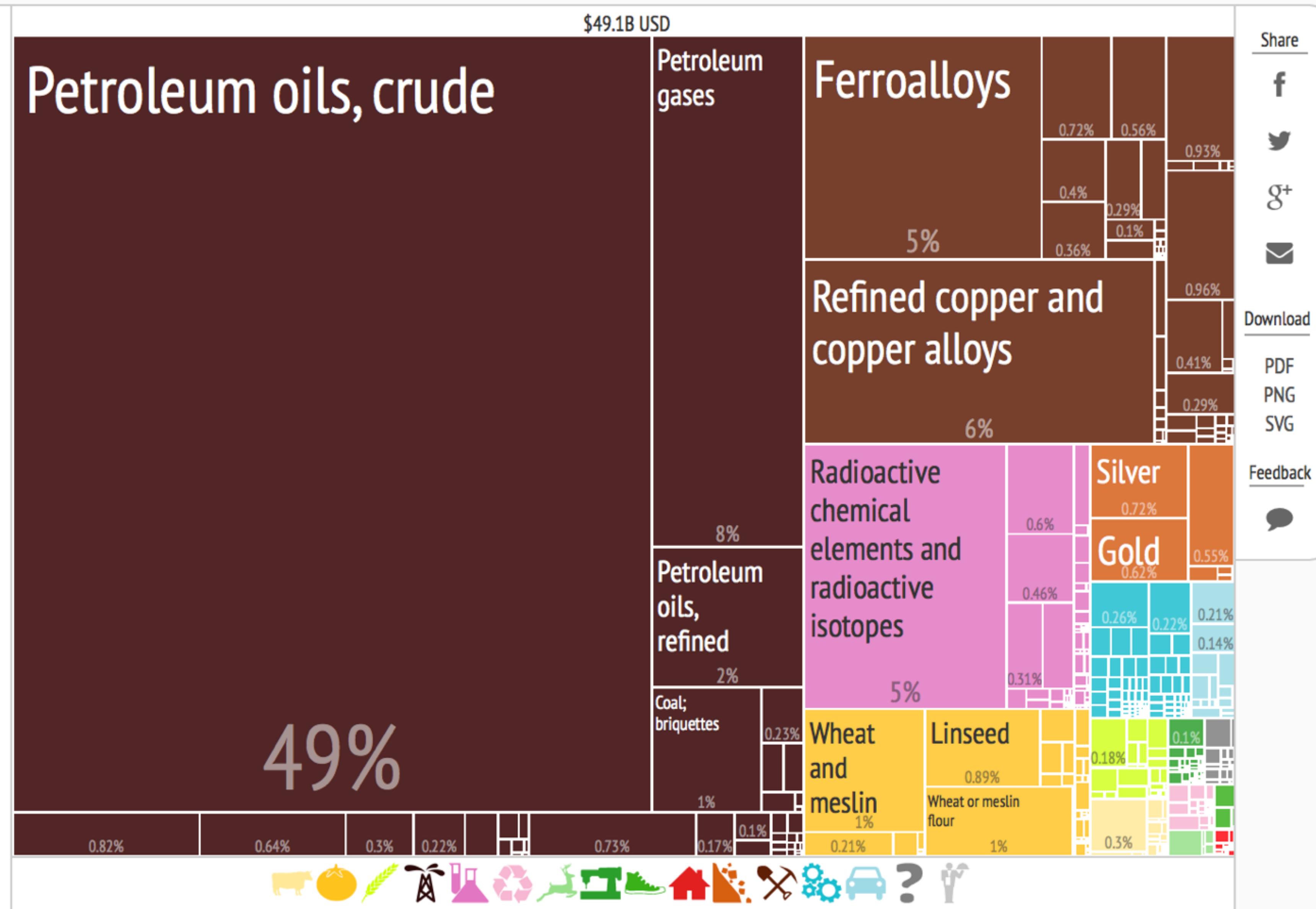
Presentation discovery app using
slideshare.net API

Online order tracker using Kazpost
API

Most favorited/trending libraries
using Github API

The Atlas of Economic Complexity

What did Kazakhstan export in 2015?



Complete multiple tasks with one app

Switch between channels to tune the description of what's in front of the camera.



Short Text

Speaks text as soon as it appears in front of the camera



Documents

Provides audio guidance to capture a printed page, and recognizes the text, along with its original formatting



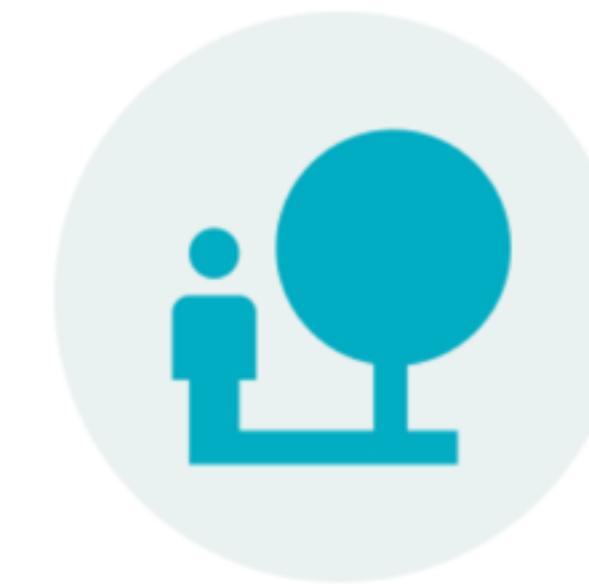
Products

Gives audio beeps to help locate barcodes and then scans them to identify products



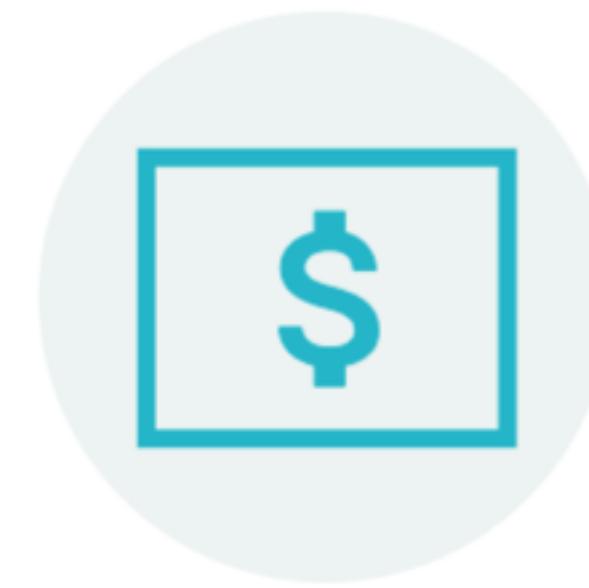
Person

Recognizes friends and describes people around you, including their emotions



Scene

An experimental feature to describe the scene around you



Currency

Identify currency bills when paying with cash. (Coming soon)

FEATURED A MONTH AGO

Estimapp 2.0

How much does it really cost to make an app?

ANDROID

IPHONE

SALES

+ 3

GET IT

▲ 1395



≡

SHARE

***** Voda NZ 4G 5:31 PM 37%

Estimation

hours per hour tax
483 + \$50 × 10%

\$23,908.50

~20 weeks, starting in a week

Static website
Web app
Signing and logging
Both, email & social
Maps
Yes, definitely need a map in my app
Analytics
I need to know all about my users
Integration
Yes, but my team handle that

***** Voda NZ 4G 5:31 PM 37%

Step 10

Complexity: Low, Medium, High

Timeline: Relaxed, Normal, Rush

Starting: Now, In a week, Later

Energize!

***** Voda NZ 4G 5:30 PM 36%

***** Voda NZ 4G

Get detailed estimation

Each line explained and estimated in hours of development time

Show me the money

...



STARTUPSTASH

A curated directory of resources & tools to help you build your Startup



Search for the right tool

Search by **Algolia**

Idea generation

Naming

Domain names

Hosting

Market research

Forms & Surveys

Mockups &
Wireframing

Design

Development

Deployment

Market research

Dying of dysentery.

 Cards Against Humanity

Coming to Broadway this season,
_____;
The Musical.

 Cards Against Humanity

Dead parents.

 Cards Against Humanity

_____.
That's how I want to die.

 Cards Against Humanity

TSA guidelines now prohibit _____ on airplanes.

 Cards Against Humanity

Repression.

 Cards Against Humanity

Maybe she's born with it. Maybe it's _____.

 Cards Against Humanity

Being marginalized.

 Cards Against Humanity

What's a girl's best friend?

 Cards Against Humanity

I'm sorry, Professor, but I couldn't complete my homework because of _____.

 Cards Against Humanity

I drink to forget _____

 Cards Against Humanity

A bag of magic beans.

 Cards Against Humanity

The art of seduction.

 Cards Against Humanity

Estrogen.

 Cards Against Humanity

Sexual tension.

 Cards Against Humanity

Today on Maury:
"Help! My son is _____!"

 Cards Against Humanity

It's a pity that kids these days are all getting involved with _____.

 Cards Against Humanity

What's that smell?

 Cards Against Humanity

The new Chevy Tahoe. With the power and space to take _____ everywhere you go.

 Cards Against Humanity

The class field trip was completely ruined by _____

 Cards Against Humanity

What gives me uncontrollable gas?

 Cards Against Humanity

Powerful thighs.

 Cards Against Humanity

Next on ESPN2, the World Series of _____.

 Cards Against Humanity

The invisible hand.

 Cards Against Humanity

API list: <http://apilist.fun>

