

- Companies
- Exchanges
- Merchants
- Wallets
- Investors
- Funding
- Technology
- Mining
- Bitcoin Protocol
- Bitcoin ATMs
- Altcoins
- Cryptocurrency 2.0
- Regulation
- BitLicense
- Crime
- Silk Road
- Events
- Prices
- Features
- Opinion
- Data Analysis
- Reviews



Private Blockchains in 2016

Preston J. Byrne (@prestonjbyrne) | Published on December 29, 2015 at 15:15 GMT

OPINION

516

150

16

254

Preston Byrne is a co-founder and COO of Eris Industries and a fellow of the Adam Smith Institute. Previously, he was a securitisation and derivatives lawyer with Norton Rose Fulbright in London and he continues to "geek out" on high finance.

It’s been said the only way to win the game of life is for your obituary to run in *The Economist*.

By that measure, the blockchain (or rather, the idea of a blockchain as a distributed database, rather than merely a backbone for a cryptocurrency) is certainly doing well.

This year alone, the blockchain has chalked up dozens (if not hundreds) of articles in most financial periodicals of record and the cover, no less, of *The Economist*. Even liberal culture hero Lawrence Lessig [recently called](#) the technology "the most important innovation in fundamental architecture since the tubes of the Internet were first developed".

I agree with this assessment, albeit cautiously. I was there when bitcoin's earliest adopters were describing their technology in similarly high-flying terms (back in the heady days of Charlie Shrem and Mark Karpeles, before anyone noticed the [three transaction-per-second](#) throughput limits or before FinCEN got antsy about MSB licensing).

It’s the same now with blockchains.

Although the technology has considerable potential, given that so few people actually know how to build with it, there is a risk that failing to be sufficiently sober about its capabilities and straightforward about its drawbacks will lead us to apply it in ways that will not showcase this potential at its best.

I would therefore like to humbly offer a few sober and fairly boring predictions for 2016, in the hope that this puts everyone in a hype-free state of mind for the new year.

1. Nobody will own the stack

I’m often asked by journalists and VCs whether the blockchain game is a '[winner take all](#)' proposition.

To ask the question betrays a degree of ignorance about what blockchains actually do. Blockchains allow disparate groups to do things on a peer-to-peer basis that, to date, they have relied on third parties like IBM, Google or Amazon to do for them. They cut the data service provider, whomever that might be, out of the transaction and let the blockchain's pre-set transaction management rules do the heavy lifting.

DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Email Address

SUBSCRIBE



FEATURES



4 Trends That Will Shape Bitcoin Regulation in 2016



How '70s Cryptography Could Improve Bitcoin in 2016 and Beyond



Bitcoin Gives Back: The Biggest Charity Drives of 2015



Bitcoin's Big Challenge in 2016: Reaching 100 Million Users

INDUSTRY PRESS RELEASES

- Jan 4 | 12:00
- Uphold Becomes First Money Platform to List Voxels
- Dec 31 | 11:28
- Meet Decred: A Digital Currency by Bitcoin Developers
- Dec 26 | 12:14
- BTCC Deploys 100 Full Bitcoin Nodes Across Five Continents
- Dec 21 | 17:26
- New iOS Camera App, Uproov, Signals End of Fake Videos and Photos

VIEW MORE

SUBMIT RELEASE

Let’s take bitcoin as an example.

Most bitcoiners, when asked what problem bitcoin solves, will quickly respond with something like "trust" or "value" or "intermediaries." But if we reread the white paper from a teleological point of view, these aspects of the bitcoin solution were the means to achieving an objective, not the objective itself.

In the most abstract terms, the point of bitcoin is to provide verification and authentication for a particular type of transaction (cash payment) without the provision of personal information by either of the participants. In Satoshi’s own words, the problem bitcoin solves is privacy.

To do this with money, you need to create both new money (bitcoin) as well as a distributed network architecture that doesn’t depend on a central machine (the blockchain). To do this with most commercial data, however, you don’t need to create a new asset class. What you need is to wrest control of network infrastructure away from existing data service providers and allow people to run that infrastructure themselves.

Blockchains make sense because privacy and verifiability are not just problems in payments. Current free-to-use services, from search to email to social networking, are dependent on advertising revenue to fund their operations.

As a result, companies offering these services must – to paraphrase Satoshi Nakamoto – hassle their users for considerably more information than they would otherwise need. This necessity has skewed the Internet toward a more centralized infrastructure than was originally intended, with attendant consequences for personal liberty and data security.

Where bitcoin was designed to solve this centralisation problem in relation to point-of-sale and banking transactions, private blockchains hold the promise of distributing – if not fully decentralising – the logic of all manner of other apps. If we can prove who we are and enforce our relationships with cryptography, we don’t have to share as much data with each other.

For our part, Eris has built a [distributed Reddit](#) and [distributed YouTube](#) (both open-source, so feel free to steal the code) all with a view to proving one thing: the blockchain, together with other new technologies such as [IPFS](#), is DIY Internet.

Nobody owns HTTP, and nobody’s going to own blockchain.

2. Blockchains will be accepted as general-purpose databases

Last week's news that IBM had developed a free, open-source blockchain and was [donating that code to the Linux Foundation](#) was greeted with widespread derision by the bitcoin community, including a number of [prominent VCs](#).

This lack of enthusiasm is extremely odd, keeping in mind the 'DIY Internet' that blockchain tech allows. Although bitcoin fans grate at the idea that permissioned databases should bear the name, it's clear from the [white paper](#) that bitcoin and the blockchain are clearly not the same thing.

After all, bitcoin is "a purely peer to peer version of electronic cash", while a blockchain is four pages of technical writing that follows the phrase “a purely peer to peer version of electronic cash” and describe the database back-end that runs that application.

If we were to summarise those four pages, we might come up with something like this: a shared datastore for peer-to-peer networks designed to "reliably (manage) a large amount of data in a multi-user environment so that many users can concurrently access the same data."

If the latter line sounds familiar, it's because it is. The part in quotation marks is Oracle [describing its own open-source database management systems](#).

Similarly, at Eris, our thesis is simple: what relational database management systems such as [MySQL](#) were in the 1990s and 2000s for computing silos, blockchains are in the 2010s and 2020s for distributed networks.

So how is a 'private blockchain' innovative vis-a-vis existing databases? As [Tim Swanson wrote](#) about bitcoin, "while all the individual elements that comprise the bitcoin blockchain have been around since 2001, it took until Satoshi's 2008 white paper to demonstrate how these individual pieces could be cobbled together to work as one."

No mining.
Just trading.

 Trade Bitcoins Now

 **NADEX** | Binary Options

Futures, options, and swaps trading involves risk
and may not be appropriate for all investors.

MUST READ

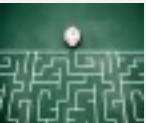
MOST POPULAR



Visa Europe: The Blockchain is 'No Longer a Choice'



Chain Issues Investor Shares on Nasdaq Blockchain Platform



Report: Blythe Masters' Blockchain Startup Struggles to Close Funding



Blockchain Land Title Project 'Stalls' in Honduras



Got a news tip or guest feature?

What is Bitcoin?

It's a decentralized digital currency



How Can I Buy Bitcoins?

From an exchange or an individual



No mining.
Just trading.

 Trade Bitcoins Now

 **NADEX** | Binary Options

Futures, options, and swaps trading involves risk
and may not be appropriate for all investors.

Private blockchains simply mix and match new components to better fit particular use cases. Where bitcoin needs (1) a timestamp server (which ‘chains the blocks’), (2) [hashcash](#)'s proof-of-work algorithm, and (3) a digital signature scheme ([ECDSA secp256k1](#)),

Most commercial chains with permissioning systems just keep what we need (the timestamping) and swap out what we don't with better components (eg: the Tendermint consensus algorithm plus [EdDSA ed22519](#) signature algorithm).

In 2016, this proposition will no longer be controversial.

3. Mining will be (mostly) relegated to irrelevance

Mining is not, and will likely not ever be, relevant to running a private blockchain.

The reasons for this are fairly straightforward: bitcoin mining isn't 'transaction processing' or 'transaction validation', as both of these are done on an ongoing basis by full nodes on the bitcoin network as they propagate valid transactions to one another (verifying digital signatures).

'Mining' is not about validation: [it is about fork choice](#). With a decentralised system like bitcoin's, anyone in the world can add a block to the end of the chain. As a result, a competitive mechanism is needed to penalise bad conduct.

A private blockchain, on the other hand, is designed to suit a very specific coordination and communication need for a very specific person or group of people, some (or all) of which will be known.

If you control those nodes or know who runs them, you can use the same digital signatures that secure a bitcoin balance (a write permission to spend bitcoin) to secure the chain (a write permission to add a block to the end of a chain).

Chain security thus becomes a question of sufficiently distributing your nodes and effective key management. These are difficult problems, but they are (if done well) as effective and significantly more flexible than bitcoin's approach.

For bitcoin itself, of course, mining is likely to remain relevant for some years to come until a better solution can be found.

4. Code, don't talk

Where 2015 was the year everyone talked about blockchain, 2016 is going to be the year everyone builds on it.

There's a lot of experimentation, improvement and optimisation left to do. In my personal opinion, we're two budget cycles away from the first production systems in finance, and I agree with [Chris Skinner](#), chair of the Financial Services Club, that we're probably 10 years away from mainstream use.

By "mainstream use," of course, I mean that applications with blockchain back-ends are ubiquitous and the end-users don't even know they're using a blockchain.

For the time being, however, there are numerous distributed networking platforms – including our own, OpenChain, Tendermint, MultiChain, and IPFS – which exist, work, and are free to use, and which some of the world's largest corporations are already testing to solve difficult commercial problems, particularly in terms of business process efficiency.

What this means for any financial institution or other business looking to use the tech is that the ball is entirely in your court.

It's cheap as chips to get started and there's much to be learned, so there's simply no excuse not to allocate budget and let your developers loose on this for a year – especially considering that your competitors already are.

Want to share your opinion on bitcoin or blockchain in 2015, or a prediction for the year ahead? Send ideas to news@coindesk.com to learn how you can join the conversation.

[Paperclip chain](#) image via Shutterstock

Disclaimer: *The views expressed in this article are those of the author and do not necessarily represent the views of, and should not be attributed to, CoinDesk.*

516

150


16

254





FROM THE WEB

Sponsored Links by Taboola 

Warren Buffett Just Gave Americans a Big Warning

The Motley Fool

This Father and Son Took the Same Photo 28 Years in a Row, and the Last One Is Absolutely Amazing

Your Daily Dish

Is The 2-Step Credit Card Payoff Method Really That Powerful? [Review]

LendingTree

A Clever Way to Pay Down Credit Card Debt at a Swift Pace

CreditDonkey.com

7 Hacks To Learn Any Language In 7 Days From Crazy 9-Language Twins

Babbel

The longest 21-month 0% APR card has hit the market

NextAdvisor

6 Reasons Why Glasses Should be Bought Online

GlassesUSA.com

This "Universal Fuel" Could End Big Oil

Money Morning Subscription


Worst Exercise For Middle Age -- Ages You Faster

MAX Workouts Fitness Guide

10 Methods For Arthritis Pain Reduction - Without Medication...

ArthritisLiving.Today

FROM THE WEB

Sponsored Links by Taboola 

A Clever Way to Pay Down Credit Card Debt at a Swift Pace

CreditDonkey.com

The longest 21-month 0% APR card has hit the market

NextAdvisor

6 Reasons Why Glasses Should be Bought Online

GlassesUSA.com

This "Universal Fuel" Could End Big Oil

Money Morning Subscription

Worst Exercise For Middle Age -- Ages You Faster

MAX Workouts Fitness Guide

10 Methods For Arthritis Pain Reduction - Without Medication...

ArthritisLiving.Today

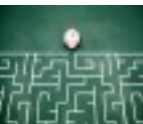
"Brightest Flashlight Ever" is Selling Like Crazy
G700 Tactical Flashlight

Nicholas Cage's Net Worth Will Shock You
AccessTheStars

The World Was Not Ready For The Outfit She Wore
StyleBistro

What to Know Before Dating An Athletic Woman
Lifescrypt

PREVIOUS ARTICLE

 Report: Blythe Masters' Blockchain Startup Struggles to...

NEXT ARTICLE

 From Worst to First: Bitcoin's Price Ends 2015 on Top

RELATED STORIES

OPINION

Jan 3, 2016 at 17:45 | Kristov Atlas

How ’70s Cryptography Could Improve Bitcoin in 2016 and Beyond

Security and privacy researcher Kristov Atlas discusses how cryptography research from the 1970s could help bitcoin addresses become user-friendly.

OPINION

Jan 2, 2016 at 16:45 | Victoria van Eyk, Connie Gallippi & Elizabeth McCauley

Bitcoin Gives Back: The Biggest Charity Drives of 2015

ChangeTip community director Victoria van Eyk details the charitable efforts of the bitcoin community in 2015.

OPINION

Jan 1, 2016 at 16:34 | Michael Jackson

Bitcoin's Big Challenge in 2016: Reaching 100 Million Users

CoinDesk explores the importance of creating bitcoin products and services that will delight users globally and prove the technology's worth in 2016.

FEATURE

Dec 31, 2015 at 15:50 | Daniel Palmer

14 Headlines That Rocked Bitcoin and the Blockchain in 2015

In this year-end special, we look back at the 14 bitcoin and blockchain news stories that made the most impact during 2015.

No mining. Just trading.

Futures, options, and swaps trading involves risk and may not be appropriate for all investors.

Trade Bitcoins Now

NADEX

Binary Options

SPONSORED

FISHER INVESTMENTS

Want To Retire Comfortably?

If you have a \$500,000 portfolio, download The Definitive Guide to Retirement Income by Forbes columnist Ken Fisher’s firm.

Learn More

