


CoinDesk

TRENDING
 CoinDesk Research Poll: Will Blockchain Disrupt Venture Capital?

BITCOIN PRICE INDEX (24H)


USD 1.1% ▲ **CNY** 9.2% ▲
\$1,007.84 **¥6,738.87**
EUR €952.97 **GBP** £808.29

[NEWS](#) [PRICE & DATA](#) [GUIDES](#) [EVENTS](#) [RESEARCH](#) [PRESS RELEASES](#)

Search icon

[COMPANIES](#) • [FEATURES](#) • [INTERVIEWS](#) • [TECHNOLOGY](#)

Hardware Over Hard Forks: How Accenture Plans to End Blockchain's Security Debate

Michael del Castillo (@DelRayMan) | Published on February 14, 2017 at 12:00 GMT

FEATURE


The ethereal world of blockchain tech is increasingly being tethered to more tangible, saleable solutions.

As major institutions have sought software concepts that rethink or remove bitcoin's [proof-of-work mining](#) mechanism, so too have the firms involved with those products needed to seek hardware solutions that provide a similar level of security to their desired distributed ledgers.

Most recently, the \$75bn consulting firm [Accenture](#) unveiled a patent-pending security layer integrated with a hardware security module (HSM) made by Thales – a global security firm already protecting the passwords and encrypted data of some of the most high-value assets around the world.

While the distributed nature of the blockchain itself is designed to ensure the soundness of each transaction, applications *built on* the technology and distributed solutions with fewer nodes (and

Like CoinDesk? Send us a tip!


1GJ4F5zmu4BsffHSdq4Wb5ze26X3zCxEoUW

Contributions go towards 2017 investments in new bitcoin projects -- like testing how bitcoin micro-payments can replace paywalls and obtrusive ads.

BTW, you can do this automatically with [Brave](#) 😊

[DOWNLOAD BRAVE](#)
DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Email Address

[SUBSCRIBE](#)

Registration Is Open!
[REGISTER NOW](#)

(therefore less protection) remain vulnerable, according to Accenture's general manager, David Treat.

In conversation with CoinDesk, Treat said his firm's decision to integrate with existing, government-certified hardware is about more than just having a new product to sell to existing and future clients. Instead, it's about entering the fray by implementing real-world blockchain solutions.

Treat said:

"Our focus on building this HSM integration layer is part of a whole innovation campaign that we have right now to think about all the different facets of what it's going to take to bring blockchain systems out of the PoC and prototype phase and into production."

Eliminating debate

In Accenture's Thales integration, private keys essential for conducting transactions are stored within nShield hardware [certified](#) by the US National Institute for Standards and Technology (NIST) in conjunction with the Canadian Communications Security Establishment.



Image via Thales

Developed in London with support from Accenture's team in Rome, the security system is initially based on the Hyperledger Fabric platform and integrated with Thales' nShield HSM, already being used by the French company to protect UK tax payers, Samsung cellphones and [fighter jets](#).

The as-yet unbranded blockchain integration is expected to be formally named later this week, alongside the launch of a new website designed to integrate with any number of distributed ledgers, blockchains and competing HSMs.

Treat positions the hardware as part of blockchain's natural evolution, as regulators, existing financial infrastructure providers and banks move to capitalize on the faster settlement times and easier auditability of shared, trusted ledgers, but hesitate out of a number of security and privacy concerns.

Instead of storing private keys that are essential to confirming identity within the application layer of the protocol, the Accenture solution is designed to keep them in a physical HSM architecture.

"It's eliminating that part of the debate of how secure are the keys," Treat said. "It comes as a much simpler answer if you see we are adhering to the high level of standards associated with the current certification of security infrastructure."

Hardware competition

Exactly how Accenture will market this 'blockchain agnostic' integration layer has yet to be determined, or at least publicized. But, much can be learned by taking a closer look at the burgeoning blockchain hardware ecosystem.

SPONSORED FINANCIAL CONTENT



Motley Fool issues new "buy alert" on IPO stock
The Motley Fool



Stocks Are On The Cusp Of An Historic Surge..Never Been More Certain
Banyan Hill

dianomi

FEATURES



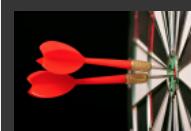
Deutsche Bank Analyst: Blockchain Could Have Prevented Soros Leaks



Blockchain Venture Test Will Have to Wait With Mainstreet Launch Delay



Forex Giants Trading Bitcoin? In Japan That Might Be Months Away



Blockchain Firms Aim For Hedge Funds, But is There a Better Target?

INDUSTRY PRESS RELEASES

- Feb 13 | 22:57 [Press Release: Whaleclub, the Etrade of Bitcoin, Crosses \\$1 Billion in Volume Traded](#)
- Feb 6 | 13:21 [Press ReleaseThe Blockchain Academy London – A 2-day event on Bitcoin and Blockchain Technology](#)
- Feb 6 | 13:16 [Press Release: The Bitcoin Users Group Welcomes Edward NG as Executive Director for Asia](#)
- Jan 30 | 16:57 [Press Release: CoinDesk Acquires Lawnmower, Accelerating Growth in Research Offerings](#)

[VIEW MORE](#)

[SUBMIT RELEASE](#)

Got a news tip or guest feature?

DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Among the unknowns at Accenture, are whether the integration layer will be sold through a subscription model or flat rate offering. However, the customers Accenture will be marketing to are more certain.

Treat told CoinDesk that customers who already have their own HSM solution will be able to hire Accenture to integrate it to their blockchain, or blockchains, of choice. New customers, on the other hand, or those with a "heightened need for security" would go to Thales or another HSM provider to buy their hardware stack "and come to us to install our integration layer on top of it".

Accenture distinguishes itself from the recent [proliferation](#) of consulting firms offering blockchain services by being among the first to also join the rapidly growing blockchain hardware industry.

So far, blockchain infrastructure providers have tended to lease services for periodic fees, while cryptocurrency companies charge based on transaction size.

For example, IBM currently [charges](#) \$10,000 a month to give blockchain users high-security access to its HSM network, whereas venture-backed Xapo offers its customers free access to its 'vaults' stored offline and "deep underground in geographically dispersed locations", in exchange for charging [various fees](#) to move the funds associated with an account.

But perhaps the most informative example of the young industry is Intel's software guard extensions (SGX) – hardware designed to isolate keys and other valuable information. SGX has been proposed for use in both more general blockchain applications and a cryptocurrency-specific use case.

In each case, concerns over using hardware quickly became apparent.

Last year, when Intel proposed using SGX at the core of its [Sawtooth Lake](#) blockchain implementation, it sparked a [heated debate](#) over using trusted hardware to run a network with the potential to run without a trust. Then, weeks later, the Initiative For CryptoCurrencies & Contracts (IC3) proposed using SGX to help scale bitcoin, [setting off](#) similar disputes.

Pushing the limits

Accenture's David Treat is joined by Thales CTO Jon Geater in arguing that the limits of blockchain aren't in the technology itself, but in the way it is implemented.

In interview, Treat highlighted exchanges such as Mt Gox and Bitfinex, which were hacked through poor key management practices, as evidence of such concerns.

But Geater, who helped integrate Accenture's software into his company's hardware, focused more on potential limitations of smaller private networks when creating more sophisticated assets than cryptocurrency.

Further, for private networks that have fewer nodes than the 5,800 nodes [live](#) at any given time on the public bitcoin network, Geater argues the ability to protect each node from a wide variety of potential attack vectors is exponentially more important.

"When you've got a very small population," he told CoinDesk, "some of these threats become much more real, and so having trustworthy hardware underpinning is clearly more valuable for peace of mind, for speed of adoption and for business agility."

Couple that with concerns Geater has over highly regulated digital assets, and certified hardware becomes essential to widespread industry adoption, he said.

Not everyone agrees, however. The movement to push blockchain security into hardware owned by third parties is part of Accenture's broader, and controversial, push to make distributed ledgers more appetizing to legacy financial infrastructure providers and other organizations held accountable to regulators.

The 'redactable blockchain'

In December, Accenture published an article in the *New York Times* relaying its vision for '[redactable blockchains](#)' that, instead of relying on a consensus-driven hard fork like the one

Email Address

SUBSCRIBE

experienced by ethereum to undo transactions, relies on the ability to edit their history using highly protected private keys.

While critics have [jumped](#) on the idea as [contrary](#) to the underlying benefits of a distributed network, Geater argued that blockchain redaction accompanied by certified, secure hardware is the only way to get the current financial leaders to truly buy into the technology.

"In the real world, you have overrides and you have lawyers. You have disputes, and you need to code all of that kind of process and authority into the system," he said.

"Whereas bitcoin is almost entirely anti-authority and anti-centralization, what Accenture is doing is bringing most of the benefits of that technology, but applying it to cases where businesses do actually have some authority of legal override."

The debate over whether hardware, hard fork or another solution is more desirable remains unresolved, with [pre-emptive](#) solutions around standards also [springing](#) up.

But, according to Treat, the ability to edit a blockchain and the hardware to protect the keys to those crucial editing rights are inevitable.

"A part of our answer in designing solutions," he said. "we would absolutely store the sharded copies of those keys in HSMs as a further ability to allow people to trust that system."

Geater concluded that more sophisticated implementations of blockchain than cryptocurrency require more imaginative solutions:

"That doesn't translate at all to other use cases; it doesn't translate as soon as you're trying to do things like regulatory compliance or multi-way asset trading, rather than coin trading. It doesn't apply when you're trying to overlay a real business relationship, and implement it in terms of blockchain, rather than using blockchain itself."

Featured [servers](#) image via Shutterstock

[Accenture](#) [Blockchain Technology](#) [hardware](#)



PREVIOUS ARTICLE



[Arizona's Proposed Blockchain Gun Tracking Ban Pushes...](#)

NEXT ARTICLE



[Banking Giant Mizuho Invests in Japan's Biggest Bitcoin...](#)

Don't miss a single story

Subscribe to our free newsletter and follow us

Email Address

SUBSCRIBE

SPONSORED FINANCIAL CONTENT

dianomi™

If you don't invest in marijuana right now, you'll regret it forever.

Money Map Press

He made 21,078% buying Amazon. Here's his new stock pick...

The Motley Fool

\$500,000 Term Life Coverage For Less Than \$0.54/Day

AIG Direct

Before Applying For A Citi Card, Check If You Pre-Qualify

Citi

A massive stock market rally is at our doorsteps, according to ...

Banyan Hill

Why the Next Depression is Already Underway

Money and Markets

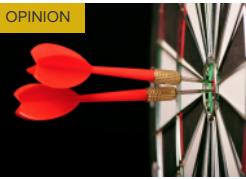
Homeowners Must Claim Their \$4272 Early in 2017

Innovative Metrics

Consider future dividend stocks instead of looking at past ones.

Fidelity Investments

RELATED STORIES



Feb 14, 2017 at 11:00 | Stan Higgins

Arizona's Proposed Blockchain Gun Tracking Ban Pushes Ahead

An effort to prohibit the tracking of firearms with distributed ledgers has progressed to the state's Senate.

Feb 13, 2017 at 13:30 | Stan Higgins

Blockchain is 5 Years From Mainstream, Post-Trade Consortium Members Say

Members of the Post-Trade Distributed Ledger Group see a multi-year adoption timeline for the technology, according to a new survey.

Feb 13, 2017 at 13:00 | Michael del Castillo

Deutsche Bank Analyst: Blockchain Could Have Prevented Soros Leaks

One Deutsche Bank analyst believes a recent, unwanted financial disclosure could have been prevented with blockchain tech.

Feb 13, 2017 at 11:00 | Noelle Acheson

Blockchain Firms Aim For Hedge Funds, But is There a Better Target?

While blockchain startups are targeting the hedge fund industry, venture capital may be a better place to focus efforts, says Noelle Acheson.

0 Comments CoinDesk Login ▾ Recommend Share

Sort by Best ▾



Start the discussion...

Be the first to comment.

ALSO ON COINDESK

JP Morgan, Santander Said to Join 'Enterprise Ethereum' Blockchain Group

32 comments • a day ago*

jtnichol — WOW. Just incredible. Keep up the good work everyone!

Lawyer Arrested in Attempt to Sell Confidential Complaint for Bitcoin

6 comments • 5 days ago*

sukramko — Next time, encrypt your documents.

China's Bitcoin Traders Are Losing Confidence in Exchange Prices

2 comments • 7 hours ago*

Tracer289 — I was unfamiliar with Bitcoinworld and Bitpie. I presumed localbitcoins.com would fill the gap ...

Arizona's Proposed Blockchain Gun Tracking Ban Pushes Ahead

2 comments • 10 hours ago*

DougNJ — Database or Spreadsheet is information in formation.

 Subscribe  Add Disqus to your site Add Disqus Add  Privacy**DISQUS**