Receive all Bitcoinist news in Telegram!

JOIN

BITCOIN POSTS LOWEST EVER 36% MARKET CAP SHARE AS ETHEREUM STEALS LIMELIGHT

IS NORTH KOREA BOOSTING BITCOIN?

BITCOIN AS GOOD AS GOLD. WELL, ACTUALLY BETTER

'IS CRYPTO MINING THE PUBLIC?' GOLDBUGS TELL MEDIA GOLD WILL BE GREAT AGAIN

NEWSLETTER SUBSCRIBE

For updates and exclusive offers
enter your email below.

SUBSCRIBE

BUY BITCOINS

BUY BITCOINS INSTANTLY
with a credit/debit card
VISA MasterCard
- NO IDENTITIY DOCUMENTS
- NO REGISTRATION
- FRIENDLY SUPPORT

USD EUR

$30 $40 $50 $60

YOU GET
≈ 0.0020 BTC

BUY NOW

JULIO GIL-PULGAR · DECEMBER 29, 2017 · 11:00 PM

BITCOIN | BITCOIN TECHNOLOGY | BLOCKCHAIN TECHNOLOGY | NEWS | NEWS TEASER

The Schnorr signatures algorithm promises to help to address one of the most pressing problems affecting Bitcoin today: scalability. Additionally, Schnorr signatures could help protect Bitcoin from certain types of spam attacks.

SCHNORR SIGNATURES COULD SOLVE BITCOIN'S SCALABILITY PROBLEM

An array of new technologies and schemes are being proposed that could help address Bitcoin's scalability problem, such as Segwit, Lightning

Network, and Schnorr signatures.

For example, many view the Schnorr signatures algorithm as a simple way of structuring digital signatures that could significantly improve the efficiency of validating a Bitcoin transaction, and it could offer new multi-signature (multisig) modes.

In this regard, Sam Wouters, Bitcoin and Blockchain speaker, wrote an article entitled *Why Schnorr Signatures Will Help Solve Two of Bitcoin's Biggest Problems Today.* In it, he explains how the Schnorr signatures protocol could help solve Bitcoin's scalability problem and how it could defend Bitcoin from certain types of spam attacks.

Wouters wrote this article in July 2017. Now, however, the article is gaining renewed traction on social media.

Valid Bitcoin transactions require signatures. These signatures occupy critical block space. This situation deteriorates when multiple addresses are involved in a transaction because each address needs its own signature. As a result, transaction size requirements increases, which in

turn pushes transaction fees higher.

A potential solution would be implementing the Schnorr signatures algorithm. Wouters writes:

> *At the end of the day, if it is just one person sending that transaction from multiple sources, there should be some way to do so with just one signature, right? This is what Schnorr signatures allow us to do.*

Wouters estimates that "this upgrade would reduce the use of storage and bandwidth by at least 25%. To point out the obvious: that is a huge efficiency gain."

SCHNORR SIGNATURES TO SHIELD BITCOIN AGAINST SPAM ATTACKERS

Schnorr signatures could also help prevent certain types spam attacks, such as those in which the attacker sends transactions that include multiple signatures. The attacker achieves this spam attack by repeatedly sending transactions from several sources. In this regard, Wouters writes:

> *Fortunately for us, Schnorr signatures would help combat this kind of spam attack. If we only have one signature per transaction, more transactions will fit into blocks and a spammer would need to send far more transactions in competition with more people, and thus likely spend more money to take up the same transaction space.*

ADVANTAGES OF SCHNORR SIGNATURES

The Schnorr signatures algorithm is compatible with multi-signatures (multsig). This functionality allows compiling several digital signatures into one signature. An article entitled *Technology Roadmap – Schnorr Signatures and Signature Aggregation*, points out some of the advantages of Schnorr signatures:

- Constant-size signatures irrespective of the number of participants in the multisig setup.
- The diminished size of data to be validated and transmitted across the network also translates into interesting capacity gains.
- From a privacy standpoint, Schnorr allows the entire policy of the multisig to be obscured and indistinguishable from a conventional single pubkey.
- The properties of Schnorr allowing for the combination of multiple signatures over a single input are also applicable to the aggregation of multiple inputs for all transactions.

Moreover, during a presentation at Scaling Bitcoin 2016 Milan, Pieter Wuille summarized several of Schnorr signatures advantages, as shown in the slide below:

Cryptocurrency enthusiasts agree that Bitcoin must soon solve its problems with scalability and high transaction fees. Therefore, proposals that could address these issues, such as Schnorr signatures, should undergo careful review. Promising proposals should then receive support from all stakeholders to move forward.

What do you think would be the impact on Bitcoin if Schnorr signatures replace Bitcoins' signature digital algorithm, ECDSA?

Images courtesy of Pixabay, Sam Wouters

BITCOIN BITCOIN SCALING PIETER WUILLE SAM WOUTERS

SCHNORR SIGNATURES

SHOW COMMENTS

FEATURED COMPANIES

PAYMENT GATEWAY

COINGATE

FOREX

$IMPLEFX

EXCHANGES

Indacoin

Changelly

BITKAN

CASINOS

bitStarz
DREAM BIG WIN BIGGER

VEGAS CASINO

BETKING

ADVERTISING

FOLLOW US

18.7K	31.0K	223
LIKE	FOLLOWER	FOLLOWER

ADVERTISING

PRESS RELEASES

INTERVIEW WITH COINTED EXECUTIVES

TRAVELFLEX ICO ROUND CONTINUE UNTIL 12TH JAN 2018

EDTECH PIONEERS OFFER 10% BONUS TOKENS IN ICO FOR PEER-TO-PEER TUTORING PLATFORM

NEW PERFECT BITCOIN SEGWIT2X: WHO IS AFRAID AND WHY?

TRADE.IO PARTNERS WITH BANCOR PROTOCOL TO PROVIDE CONTINUOUS LIQUIDITY TO TOKEN HOLDERS

SUBMIT A PRESS RELEASE

BITCOIN POSTS LOWEST EVER 36% MARKET CAP SHARE AS ETHEREUM STEALS LIMELIGHT

IS NORTH KOREA BOOSTING BITCOIN?

BITCOIN AS GOOD AS GOLD. WELL, ACTUALLY BETTER

'IS CRYPTO MINING THE PUBLIC?' GOLDBUGS TELL MEDIA GOLD WILL BE GREAT AGAIN

NEWSLETTER SUBSCRIBE

For updates and exclusive offers
enter your email below.

SUBSCRIBE

BUY BITCOINS

BUY BITCOINS INSTANTLY
with a credit/debit card
VISA MasterCard
- NO IDENTITIY DOCUMENTS
- NO REGISTRATION
- FRIENDLY SUPPORT

USD EUR

$30 $40 $50 $60

YOU GET
≈ 0.0020 BTC

BUY NOW

JEFF FRANCIS · DECEMBER 29, 2017 · 8:00 PM

BITCOIN | BITCOIN ACCEPTANCE | NEWS | NEWS TEASER

Legendary tech investor Roger McNamee believes that 2018 could be a decisive year for Bitcoin, allowing it to become fully legitimate in the eyes of the financial world.

While a number of financial analysts are bullish on Bitcoin, many others are still quite hesitant on the eventual fate of the cryptocurrency. Such doubters point to the crypto's ongoing volatility and the number of major drops in value over the last year. However, tech investor Roger McNamee believes that the upcoming year could be a turning point for Bitcoin. In fact, he believes it's quite possible that Bitcoin could become fully

legitimate in the eyes of the business world.

2018 COULD MAKE OR BREAK BITCOIN

In an interview on CNBC, McNamee said that Bitcoin could be considered legit if is withstands a crash and sees enough gains in 2018. He elaborated by saying:

> *[Bitcoin is] still a very small market in the context of the larger financial world, but it has had a huge year. We've done it around a speculative mania. If a mania goes on long enough, it becomes self-fulfilling. Even after a crash, what follows is a legitimate industry.*

McNamee goes on to say that the cryptocurrency needs to keep investors on their toes and has to stick around long enough to become accepted.

He adds:

> *With the amount of activity going on around it, there are people willing to invest the kind of dollars it takes to make a thing like bitcoin into a long-term part of the financial market.*

A PROVEN TRACK RECORD

Roger McNamee has proven to have great instincts. He was an early investor in Facebook and told Mark Zuckerberg that he should not sell the company back when it received a major offer of $750 million. Bill Gates considers McNamee a “great sounding board” for many of the Microsoft co-founder’s ideas. Then there’s the fact that he made venture capital investments in a small game company by the name of Electronic Arts, which is now the second-largest game company in Europe and the Americas.

Roger McNamee is also a musician in addition to being a tech investor.

As for Bitcoin, McNamee thinks that the cryptocurrency is still too new for many investors to understand. However, he thinks 2018 will open some eyes on how Bitcoin could play a role in the financial markets. Looking ahead to the new year and Bitcoin, he says:

> *You’ll have these big swings, up and presumably down, as well. And, you know, wherever that settles out I think will tell us a lot about the role of bitcoin long-term.*

Overall, McNamee also thinks that, no matter how the year treats Bitcoin, it won’t be the end of the story for the virtual currency. It is refreshing to

hear someone express pragmatic optimism on how Bitcoin could break through those final trust barriers that the financial world has erected. He fully understands that there are going to be ups and downs, but what is important is that Bitcoin continues to stick around and shows staying power.

Do you agree with Roger McNamee that 2018 could be a decisive year for Bitcoin? Let us know in the comments below.

Images courtesy of Wikimedia Commons, Pixabay, and Bitcoinist archives.

BITCOIN BITCOIN ACCEPTANCE BITCOIN PRICE ROGER MCNAMEE

SHOW COMMENTS

FEATURED COMPANIES

PAYMENT GATEWAY

COINGATE

FOREX

$IMPLEFX

EXCHANGES

Indacoin

CASINOS

bitStarz

DREAM BIG WIN BIGGER

Changelly

VEGAS CASINO

BITKAN

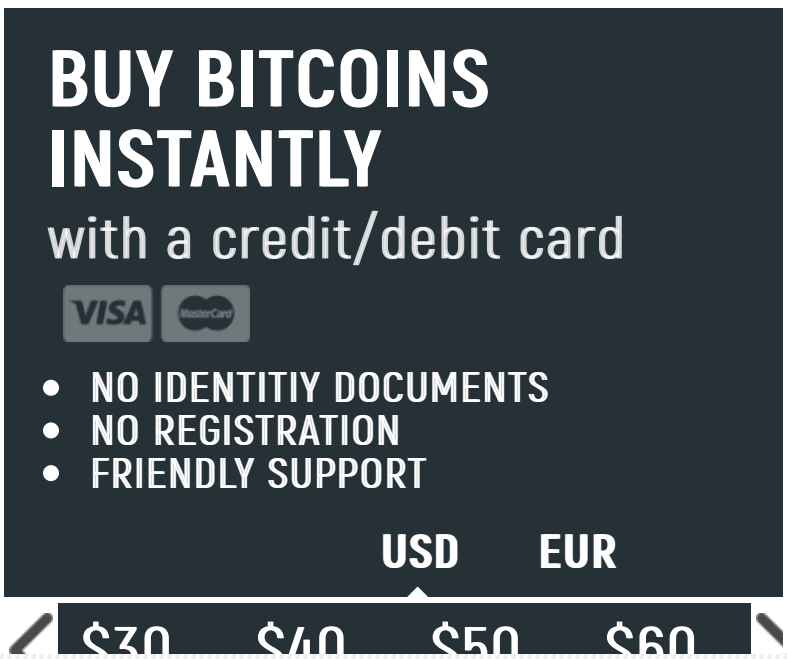
BETKING

ADVERTISING

FOLLOW US

18.7K	31.0K	223
LIKE	FOLLOWER	FOLLOWER

ADVERTISING



PRESS RELEASES

INTERVIEW WITH COINTED EXECUTIVES

TRAVELFLEX ICO ROUND CONTINUE UNTIL 12TH JAN 2018

EDTECH PIONEERS OFFER 10% BONUS TOKENS IN ICO FOR PEER-TO-PEER TUTORING PLATFORM

NEW PERFECT BITCOIN SEGWIT2X: WHO IS AFRAID AND WHY?

TRADE.IO PARTNERS WITH BANCOR PROTOCOL TO PROVIDE CONTINUOUS LIQUIDITY TO TOKEN HOLDERS

SUBMIT A PRESS RELEASE

ADVERTISING

BITCOINIST.COM
CRYPTOCURRENCY REVIEWS AND TECHNOLOGY

© 2018 Bitcoinist.com. All Rights Reserved.