Vitalik Buterin Lays Roadmap for Ethereum Visa Levels Quadratic Sharding

() November 25, 2017 5:15 pm

> "The ethereum killer is ethereum, the ethereum of China is ethereum, the ethereum of Taiwan is ethereum… 2.0."

That was the opening statement (https://www.youtube.com/watch?v=9RtSod8EXn4&feature=youtu.be&t=11493) of Vitalik Buterin, Ethereum's inventor, at BeyondBlock in Taipei where he laid out a plan to reach Visa levels scalability within the next 3-5 years.

The main problems facing ethereum are privacy, safety and scalability, he said. With privacy being 3/4th solved, according to Buterin who was wearing a Byzantium t-shirt, referring to the latest ethereum hardfork.

That upgrade introduced some
fairly fancy new cryptographic algorithms, Buterin says, including zero-knowledge proofs and ring signatures which don't solve the privacy problem on their own but can give coders tools to build solutions.

From a base layer perspective, the privacy problem is three quarters of the way to being solved, he said. The one quarter that isn't solved… there's still leaks at the protocol level. If you use a mixer and pay for gas there may be privacy leaks, but most of the work from here is at layer 2 he says.

Suggesting base layer privacy has been solved, at least conceptually, by zk-Snarks which give you the ability to hide a transaction from all at the same time as allowing you to choose who you wish to show that transaction.

Ethereum main problems

Safety, of course, isn't a problem you solve, only minimize or maximize as may be the case. But one problem that could be solved is scalability.

However it's a hard problem due to the trilema of decentralization, security, and scalability. Having two out of three is easy he says, providing examples of current solutions that have made that two out of three trade-off:

Existing blockchains, like Ethereum and Bitcoin in their current state, sacrifice scalability, he says, while super big blocks, at the size of 10GB, would sacrifice decentralization, Buterin says.

But ethereum aims to have all three without sacrificing either. One such way is through second layer solutions, like Plasma, Raiden, or the Lightning Network, however ethereum also aims to achieve the trilemma of decentralization, safety and scalability, all on-chain.

He says ethereum aims to scale on-chain, to thousands of transactions, without masternodes, consortium nodes, or any other centralizing aspects.

"So, can we do this?" – he asks, "I believe we can," he says, presenting a first and somewhat basic conceptualized version of sharding.

"The way I generally describe sharding is… you can think of it as, in a fairly simple version, creating a blockchain where you have, lets say, a hundred different universes and each of these universes is a different account space," Buterin says before adding:

“So you can have an account in some universe or you can have a contract in some universe and you can send a transaction in some universe and if you send a transaction in some universe it only affects stuff in some universe.

You might have some protocol of transferring resources, transferring data, between these universes, but it could be more limited, it could be something asynchronous, it could have a two weeks delay, and generally it’s not as clean and convenient as doing stuff in one universe.

But these 100 universes are not just separate blockchains, they are systems that are also interconnected with each other. Particularly, they share consensus. So in order to break even one of them, you have to break the whole thing.

This doesn’t describe every possible sharding solution out there, and we can really ratchet things up on the margins and eventually make communications between these different universes really good and possibly even blur the distinction between going across universes and between universes, but this is one simple way of thinking about it.

How would an instantiation of this actually work on ethereum? We could try think about the very far end of what the optimal system would look like, or we can try think about what we can design fairly easily in the near term.

Here’s one example of something we can design fairly easily in the near term. Let’s imagine we keep the main blockchain and into the main blockchain we would publish a contract, and this contract would be called the validator manager contract [which] would maintain an internal Proof of Stake (PoS) system…

The validator manager contract also keeps track of a set of shards… the 100 universes. During each block or cycle the validator manager contract assigns a random validator the right to create the next block on each shard…

Each of these shards have blocks and transactions, but we are not going to put all of those blocks and transactions into the main chain. Instead, what we are going to do, we are going to take the same structure ethereum currently has,

where you have a big block that gets represented by a tiny header, and we're just going to replicated again one level down.

At the shard level we would have things called collations. A collation is basically just a group of transactions and the collation would have a collation header that would be basically a PoS signed block header, and these collation headers would be pushed into the validator manager contract, but all of the actual transactions in the shards, all of the shards states, all of the shards collations, that would go off-chain.

The only thing that goes on-chain is these collation headers and the validator manager contract would keep track of these headers and would keep track of the state roots of each shard.

So there is this kind of division of labor here where basically the validator manager contract just acts as a light client for each shard."

You'd have these two worlds, Buterin says. You'd have the old world that keeps operating with the same level of scalability which currently is limited as each transaction is replicated by each node that has to run on a laptop.

And this new world with its own rules which has quadratic scalability as nodes validate certain shards and act as light clients for other shards, with this new world potentially having even higher levels of scalability dependent on how sharding is implemented or incrementally improved.

This is all in the early stages of sharding, Buterin says, laying out the roadmap of how it would progress, with it eventually being incorporated at a protocol level through "tight coupling."

That being, the ethereum network upgrades so that clients enforce a rule which says if the blockchain contains a sharding header that is invalid then the entire blockchain is invalid.

“So basically tight coupling is where the validity of layer two becomes a condition for the validity of layer one,” Buterin says. At which stage the entire sharding system would have the same level of uniform security and it would all be governed by hardforks.

Initially there would be a two speeds ethereum with individuals running an eth node and a sharding node connected to the eth node. The two then eventually, once the network moves to tight coupling, are merged together.

The new shards create a new address space, he says, which means it doesn’t affect normal transactions and the current network.

Allowing devs to engage in important innovations, Buterin says, as they can operate more freely on the shards by turning on improvements only on the shards.

Eventually the main-chain will need to be upgraded, but we can do that later he says as there is no need to slow down by requiring constant on-chain backwards incompatible upgrades.

Those changes are increased parallelization, a faster ethereum virtual machine, binary Merkel trees and stateless clients.

Stateless clients being a sharding sorts of its own described by Buterin as “instead of requiring clients to have states, we would require transaction senders to provide a kind of merkle proofs of specific portions of states that they access.”

Stateless clients are very much at an early stage and there are many way to implement them, Buterin says, but it’s one example of what can be done on shards.

The sharding roadmap therefore appears to be the initial creation of a new “universe,” or 100 of them, that doesn’t quite affect the main-chain.

The reason for that, Buterin says, is because there would be quite a lot of backwards incompatible changes which may affect current states or projects, so they would rather start on a blank slate.

Ethereum, thus, is to transition into a two speeds lane until it eventually merges again into one road down the line.

With developers working on new shards, incrementally improving the code, adding zk-Snarks to shards and other features, increasing their ability to share data and communicate, and then continuously refining it through relatively minor improvements.

The time-line laid out is 3-5 years, thus around 2020. But one of the most difficult aspects, the architecture, seems to have reached a stable conceptual level, so we might perhaps see prototypes even by next year and potential first alpha versions in 2019 or earlier.

In the meantime there will be the transition to Proof of Stake/Proof of Work hybrid eth. That's a very major upgrade in itself and might, optimistically, be ready by summer.

The general approach eth therefore seems to be taking is prioritizing speed above perfection. Getting things out there and then improving them rather than refining it so fully that it is ready to be used by your grandma in first version.

That approach would be due to necessity. Ethereum now handles more transactions (http://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined) than all other decentralized public blockchains combined.

Demand for ethereum transactions has increased 10x since last year, with the network now able to handle only 4x more at best.

Time therefore isn't a luxury for the still young project, which is the only prominent one in this space to carry that Silicon Valley mantra of move fast and break things.

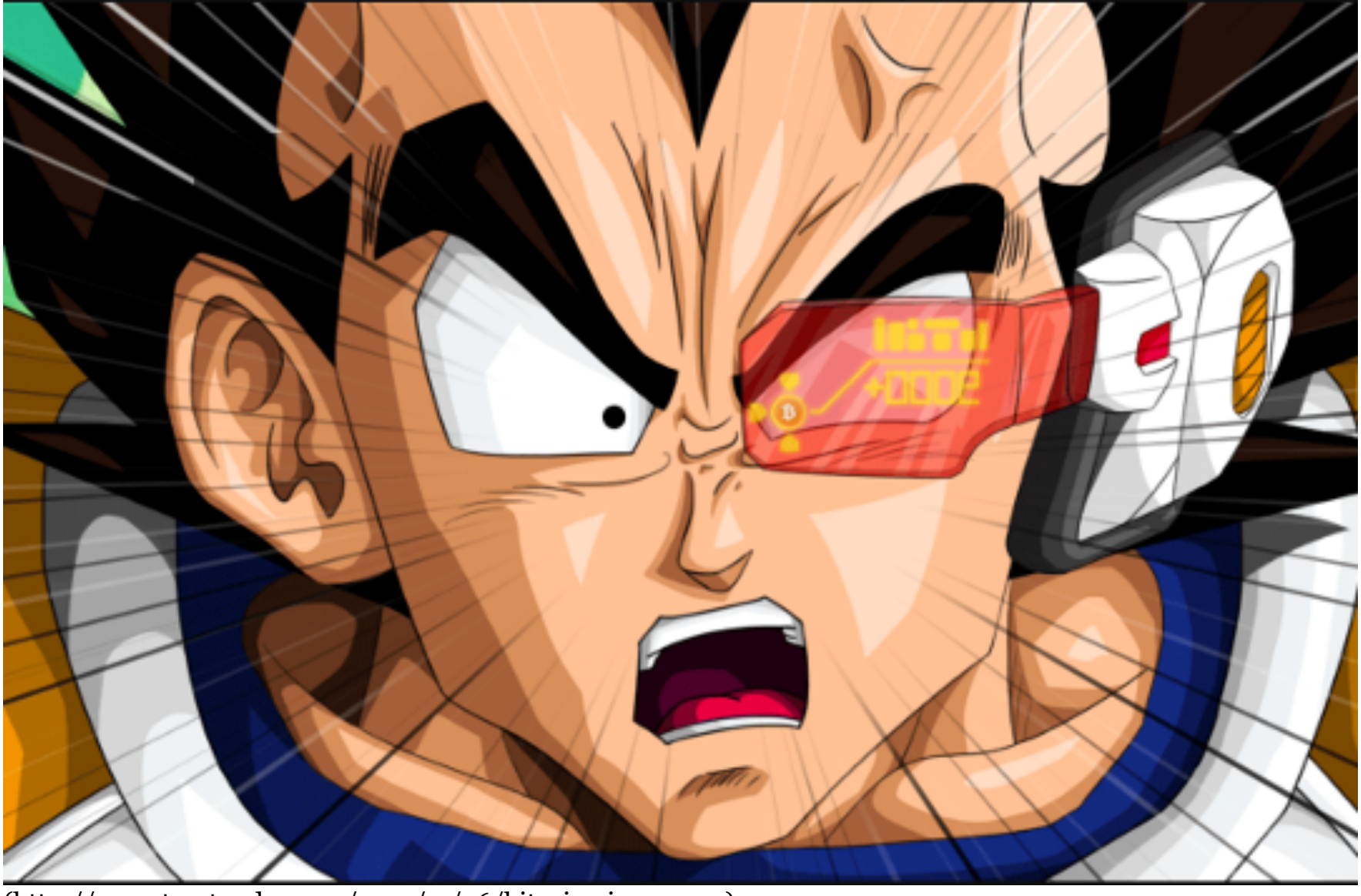
(http://www.trustnodes.com?bsa_pro_id=23&bsa_pro_url=1)

RELATED POSTS

(http://www.trustnodes.com/2017/11/26/bitcoin-gold-instantly-gains-market-cap-6-billion)

Bitcoin Gold Instantly Gains a Market Cap of $6 Billion (http://www.trustnodes.com/2017/11/26/bitcoin-gold-instantly-gains-market-cap-6-billion)

November 26, 2017 4:19 pm



(http://www.trustnodes.com/2017/11/26/bitcoin-rises-9000)

Bitcoin Rises to Over $9,000 (http://www.trustnodes.com/2017/11/26/bitcoin-rises-9000)

November 26, 2017 2:58 pm

(http://www.trustnodes.com/2017/11/24/bitcoin-cash-new-religion)

Bitcoin Cash, The New Religion (http://www.trustnodes.com/2017/11/24/bitcoin-cash-new-religion)

November 24, 2017 5:12 pm

(http://www.trustnodes.com/2017/11/24/ethereum-444s-market-cap-rises-40-billion)

Ethereum $444s, Market Cap Rises Above $40 Billion (http://www.trustnodes.com/2017/11/24/ethereum-444s-market-cap-rises-40-billion)

November 24, 2017 2:08 pm

(http://www.trustnodes.com/2017/11/23/can-now-buy-three-million-products-bitcoin-black-friday)

You Can Now Buy Three Million Products with Bitcoin This Black Friday (http://www.trustnodes.com/2017/11/23/can-now-buy-three-million-products-bitcoin-black-friday)

November 23, 2017 6:42 pm

(http://www.trustnodes.com/2017/11/23/millennials-ditching-savings-accounts-cryptocurrencies-new-survey-says)

Millennials Ditching Savings Accounts for Cryptocurrencies New Survey Says (http://www.trustnodes.com/2017/11/23/millennials-ditching-savings-accounts-cryptocurrencies-new-survey-says)

November 23, 2017 5:07 pm

(http://www.trustnodes.com/2017/11/23/bitcoin-cash-rises-1500)

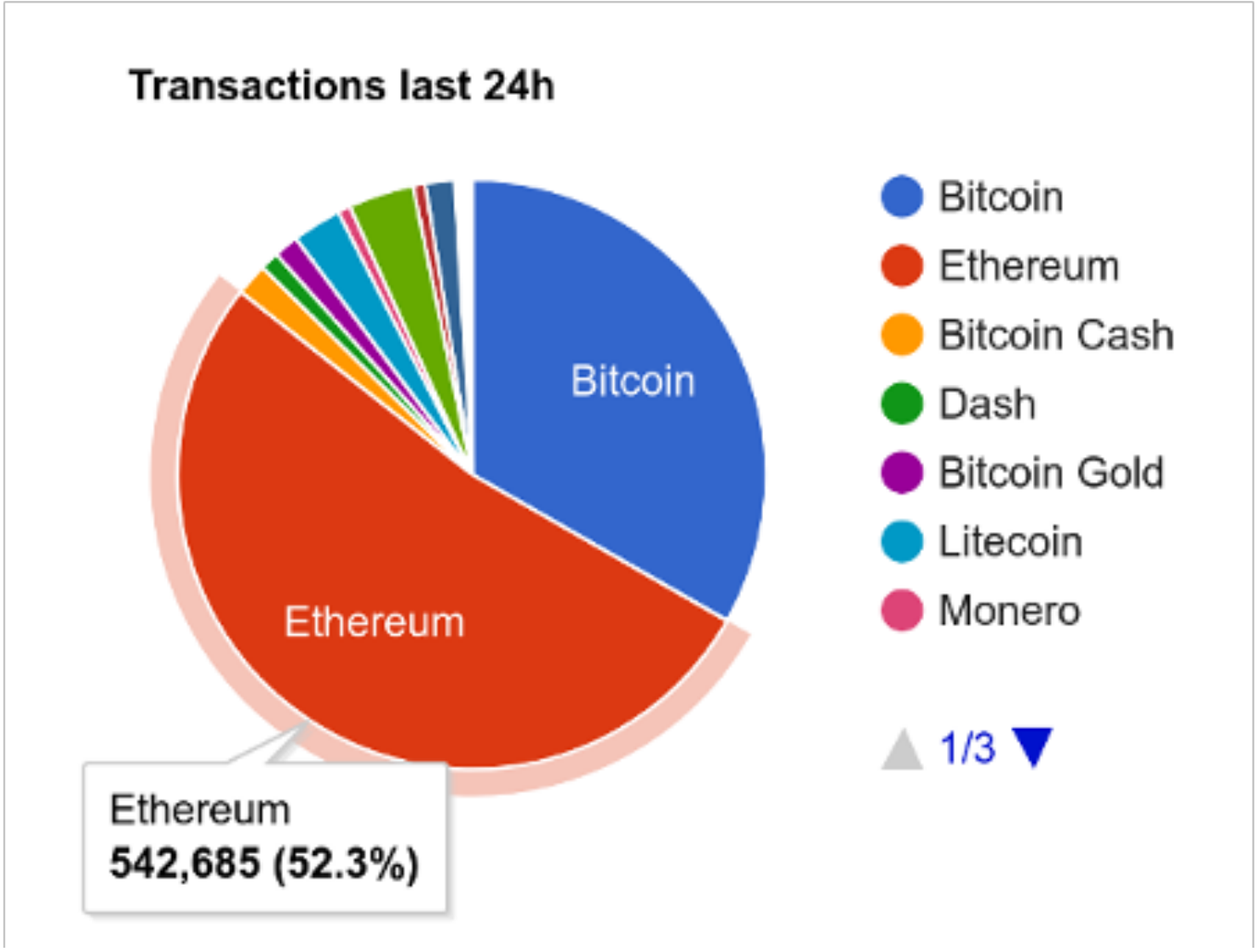
Bitcoin Cash Rises to $1,500 (http://www.trustnodes.com/2017/11/23/bitcoin-cash-rises-1500)

November 23, 2017 3:10 pm

(http://www.trustnodes.com/2017/11/23/ethereums-market-cap-reaches-time-high-price-rises-400)

Ethereum's Market Cap Reaches All-Time High, Price Rises to $400 (http://www.trustnodes.com/2017/11/23/ethereums-market-cap-reaches-time-high-price-rises-400)

November 23, 2017 2:03 pm



(http://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined)

Ethereum Now Handles More Transactions Than All Digital Currencies Combined (http://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined)

November 22, 2017 5:23 pm

Leave a Reply

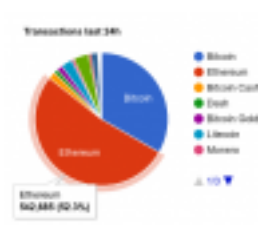
4 Comments on "Vitalik Buterin Lays Roadmap for Ethereum Visa Levels Quadratic Sharding"

Notify of new follow-up comments Email ›

Join the discussion

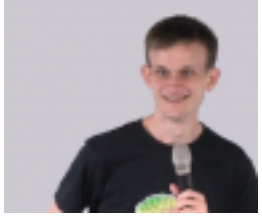
Sort by: newest|oldest|most voted

POPULAR



Ethereum Now Handles More Transactions Than All Digital Currencies Combined (http://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined)

(http://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined)



Vitalik Buterin Lays Roadmap for Ethereum Visa Levels Quadratic Sharding (http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding)

(http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding)

Bitfinex Reveals a New Polish Bank Account Under a Panama Registered Company (http://www.trustnodes.com/2017/11/22/bitfinex-reveals-new-polish-bank-account-panama-registered-company)

(http://www.trustnodes.com/2017/11/22/bitfinex-reveals-new-polish-bank-account-panama-registered-company)

Confido ICO Vanishes Days After Raising Nearly Half a Million Dollars (http://www.trustnodes.com/2017/11/20/confido-ico-vanishes-days-raising-nearly-half-million-dollars)

(http://www.trustnodes.com/2017/11/20/conf

ido-ico-vanishes-days-raising-nearly-half-million-dollars)

(http://tradingview.go2cloud.org/aff_c?offer_id=2&aff_id=4145)

LATEST

The Ideal Digital Currency Needs Clear Regulations (http://www.trustnodes.com/2017/11/26/ideal-digital-currency-needs-clear-regulations)

November 26, 2017 5:28 pm

(http://www.trustnodes.com/2017/11/26/ideal-digital-currency-

needs-clear-regulations)

Bitcoin Gold Instantly Gains a Market Cap of $6 Billion (http://www.trustnodes.com/2017/11/26/bitcoin-gold-instantly-gains-market-cap-6-billion)

November 26, 2017 4:19 pm

(http://www.trustnodes.com/2017/11/26/bitcoin-gold-instantly-gains-market-cap-6-billion)

Bitcoin Rises to Over $9,000 (http://www.trustnodes.com/2017/11/26/bitcoin-rises-9000)

November 26, 2017 2:58 pm

(http://www.trustnodes.com/2017/11/26/bitcoin-rises-9000)

Press Release: DMarket and DreamTeam Become Partners, Announce Special Token Sale Offers (http://www.trustnodes.com/2017/11/25/press-release-dmarket-dreamteam-become-partners-announce-special-token-sale-offers)

November 25, 2017 6:01 pm

(http://www.trustnodes.com/2017/11/25/press-release-

dmarket-
dreamteam-
become-
partners-
announce-
special-
token-sale-
offers)

(htt ps://www.facebook.com/trustnodes/) (htt ps://twitter.com/trustnodes) (htt ps://plus.google.com/+Trustnodes/)

(http://www.trustnodes.com?bsa_pro_id=13&bsa_pro_url=1)

LATEST NEWS

The Ideal Digital Currency Needs Clear Regulations (http://www.trustnodes.com/2017/11/26/ideal-digital-currency-needs-clear-regulations)

Bitcoin Gold Instantly Gains a Market Cap of $6 Billion (http://www.trustnodes.com/2017/11/26/bitcoin-gold-instantly-gains-market-cap-6-billion)

Bitcoin Rises to Over $9,000 (http://www.trustnodes.com/2017/11/26/bitcoin-rises-9000)

TRUSTNODES SERVICES

Press Releases (http://www.trustnodes.com/2017/08/15/trustnodes-opens-a-press-releases-section)

Advertising (http://www.trustnodes.com/2017/06/14/advertise-on-trustnodes)

News Tips (http://www.trustnodes.com)

Positions (http://www.trustnodes.com)

SUBSCRIBE TO THE MOST TRUSTED NEWS

THE TRUSTNODES NEWSMAIL

Your email address

☐ **Daily** ☐ **Weekly** ☐ **Monthly** Sign up