# Cypherpunks
# Blockchain
# Distributed Everything
# Disruption

Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)  Licence as described https://creativecommons.org/licenses/by-nc-nd/4.0/

# A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can remember what the others said and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their benevolence. It is to their advantage to speak of us, and we should expect that they will do so. To fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Eric Hughes <hughes@soda.berkeley.edu>

Right to Privacy

Privacy is Selective Self Determined Disclosure

Self Sovereign Authority

# Cypherpunks et al

## John Gilmore

Activist

John Gilmore is one of the fou
the Cypherpunks mailing list,
hierarchy in Usenet and is a r
Wikipedia

**Born:** 1955, York, Pennsylva

**Awards:** Award for Advancer

**Organizations founded:** Ele
Solutions

## Adam Back

British cryptographer

Adam Back is a British cryptographer and crypto-hacker. He i
inventor of hashcash, the proof-of-work system used by seve
spam systems. A similar system is used in bitcoin. Wikipedia

**Born:** July 1970, London, United Kingdom

**Residence:** Sliema, Malta

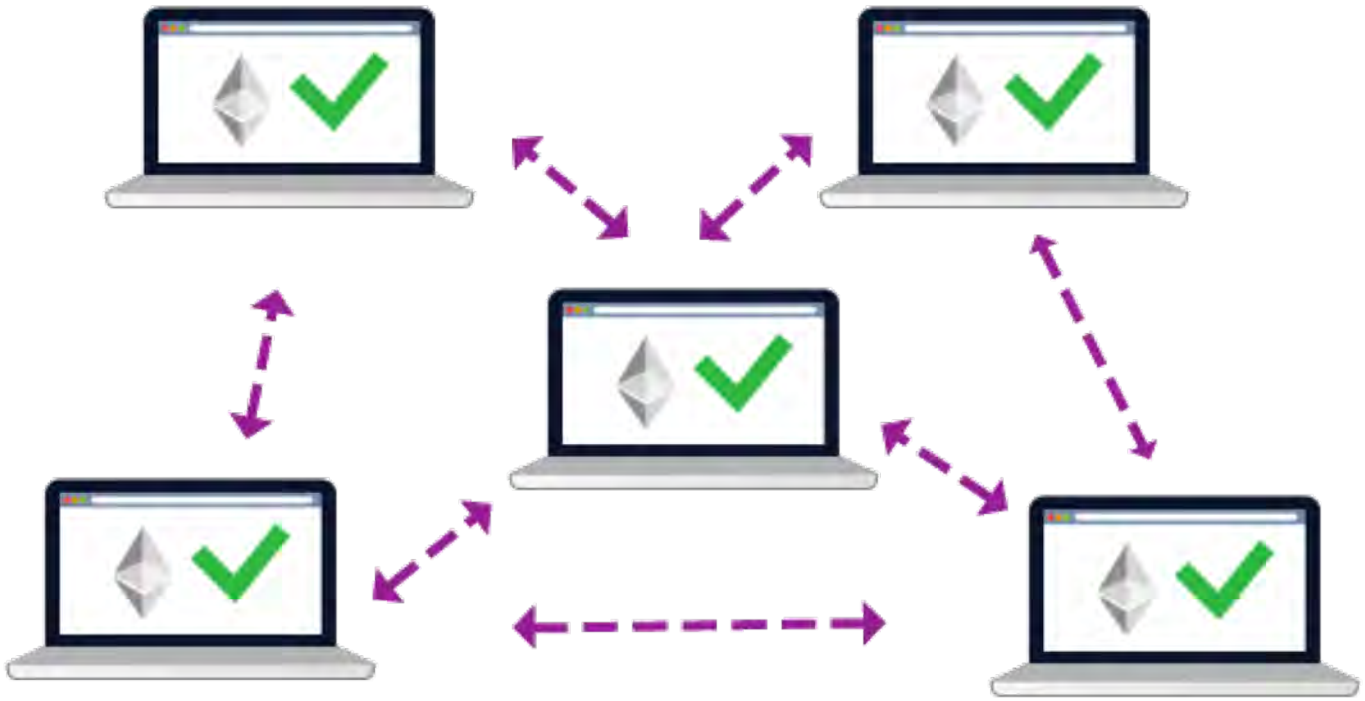
**Known for:** Hashcash, Blockstream

Bram Cohen, 2015

| | |
|---|---|
| **Born** | October 12, 1975 (age 41)<br>New York City, NY, U.S. |
| **Residence** | San Francisco Bay Area |
| **Nationality** | American |
| **Education** | Stuyvesant High School |
| **Alma mater** | University at Buffalo |
| **Occupation** | Chief Scientist, BitTorrent, Inc. |
| **Known for** | BitTorrent protocol |

# Blockchain

# Blockchain (Ethereum)



Ethereum Software on each machine creates a mesh and makes them all operate as a single machine

The mesh is called The Ethereum Virtual Machine = The World Computer

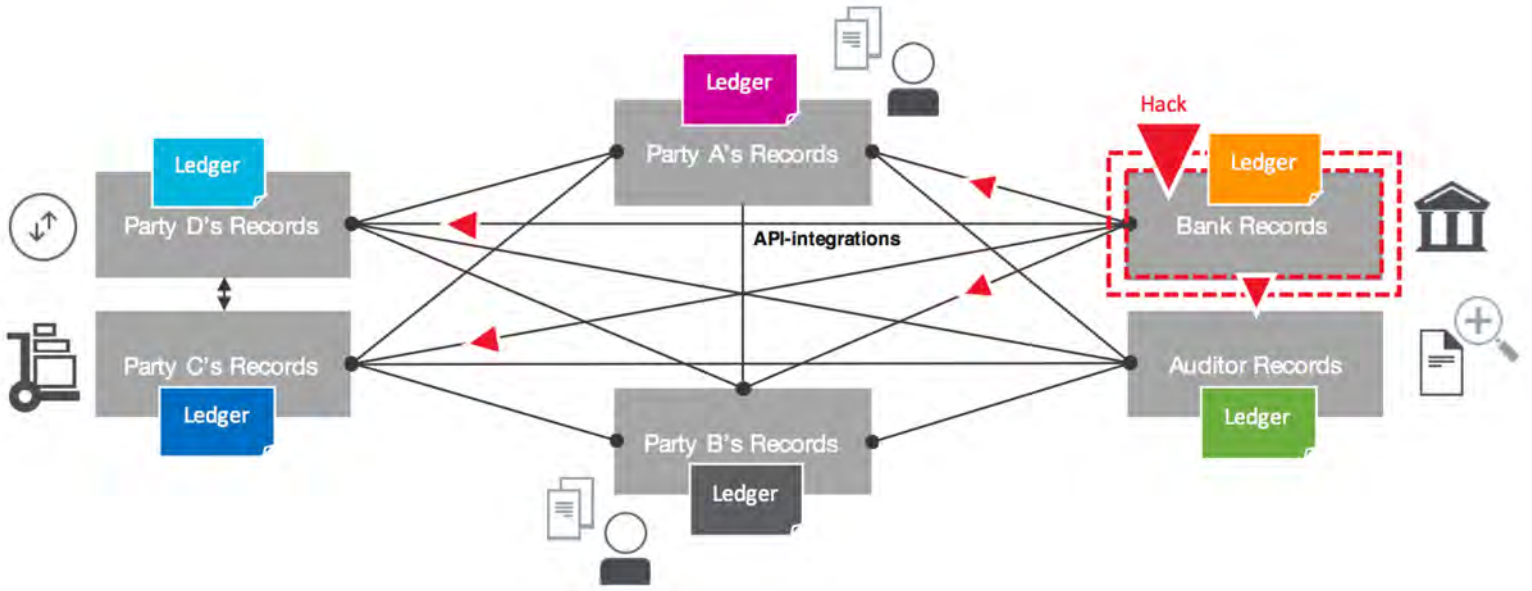
Every machine processes every transaction, keeps a “ledger” and maintains consensus of the truth

It  is Decentralized + Immutable + Eliminates the need for trust

# Starts to get coverage in 2015

# Blockchain in 3 slides

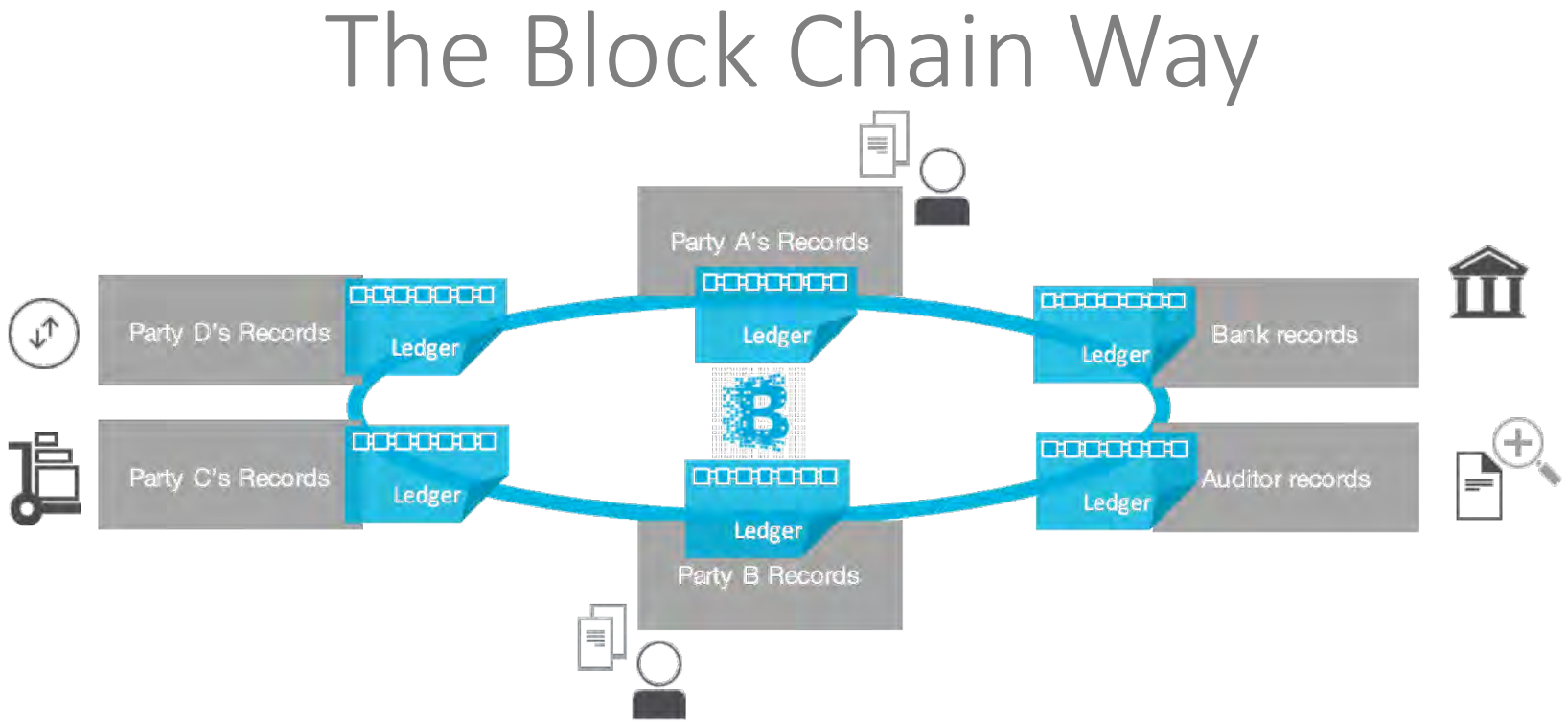
## The Old Way




Inefficient, expensive, error sensitive and vulnerable

http://www-05.ibm.com/be/businessconnect/assets/files/Blockchain-A-new-disruption-in-financial-servies.pdf

# Blockchain in 3 slides




Consistency, efficiency, security and resilience

http://www-05.ibm.com/be/businessconnect/assets/files/Blockchain-A-new-disruption-in-financial-servies.pdf

# Blockchain in 3 slides

## The 4 Key Concepts

### Distributed shared ledger

### Cryptography

### Consensus

### Smart contracts

http://www-05.ibm.com/be/businessconnect/assets/files/Blockchain-A-new-disruption-in-financial-servies.pdf

| | | |
|---|---|---|
| Web 1.0 | – Read Only | – Ideas |
| Web 2.0 | – Read Write | – Ideas |
| Web 3.0 | – Transactions | – eCommerce |
| Web 4.0 | – Distributed Ledger | – Ownership |

# Tokenisation of Ownership

# Not New

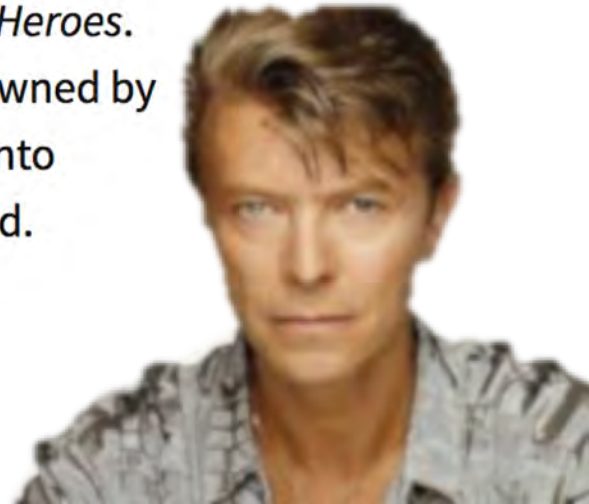
## Bowie Bond

### DEFINITION of 'Bowie Bond'

A Bowie bond is an asset-backed security which uses the current and future revenue from albums recorded by musician David Bowie as collateral.

### BREAKING DOWN 'Bowie Bond'

Bowie bonds were first issued in 1997 when David Bowie partnered with Prudential Insurance Company and raised $55 million by promising investors income generated by his back catalog of 25 albums. The 25 albums, which were used as the underlying assets for Bowie bonds, were recorded prior to 1990 and included classics such as *The Man Who Sold The World*, *Ziggy Stardust*, and *Heroes*. David Bowie used the proceeds from the bond sale to purchase old recordings of his music owned by his former manager. His rights to royalties from wholesale sales in the U.S. were securitized into bonds. In effect, by creating the bonds, he ultimately forfeited royalties for the life of the bond.



# Tokenisation of Currency

CryptoCurrency

# BitCoin

## History [ edit ]

*Main article: History of bitcoin*

Bitcoin was created[15] by Satoshi Nakamoto,[14] who published the invention[15] on 31 October 2008 to a cryptography mailing list[23] in a research paper called "Bitcoin: A Peer-to-Peer Electronic Cash System".[22] Nakamoto implemented bitcoin as open source code and released in January 2009.[15] The identity of Nakamoto remains unknown, though many have claimed to know it.[14]

# Ethereum

## Ethereum

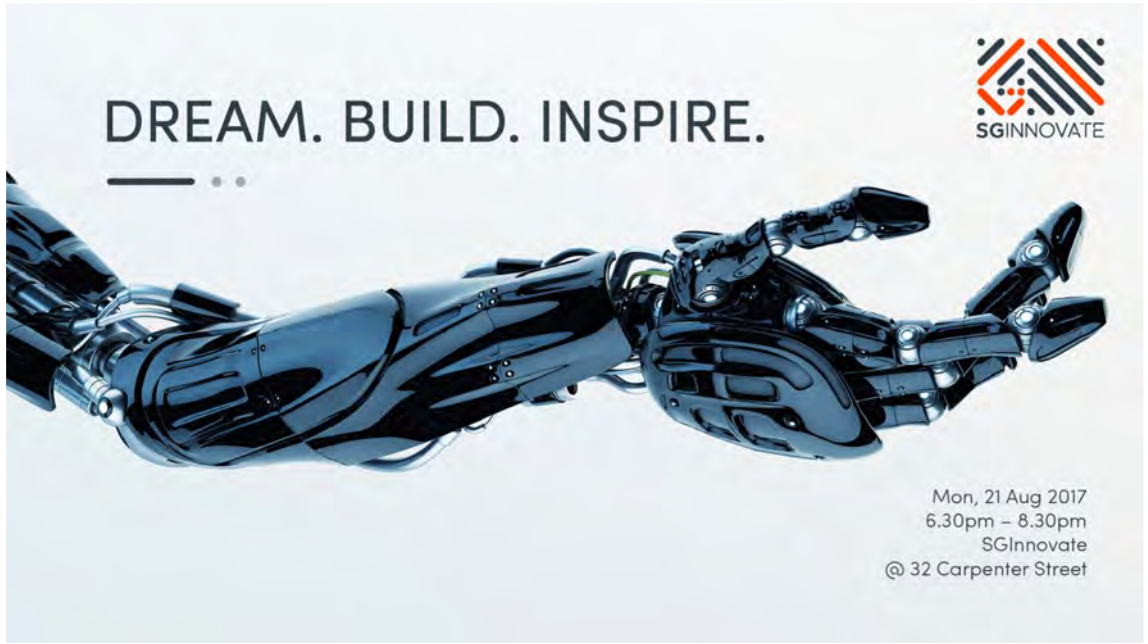
From Wikipedia, the free encyclopedia

**Ethereum** is an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality.[2] It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. Ethereum also provides a cryptocurrency token called "ether", which can be transferred between accounts and used to compensate participant nodes for computations performed. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network.[2][3]

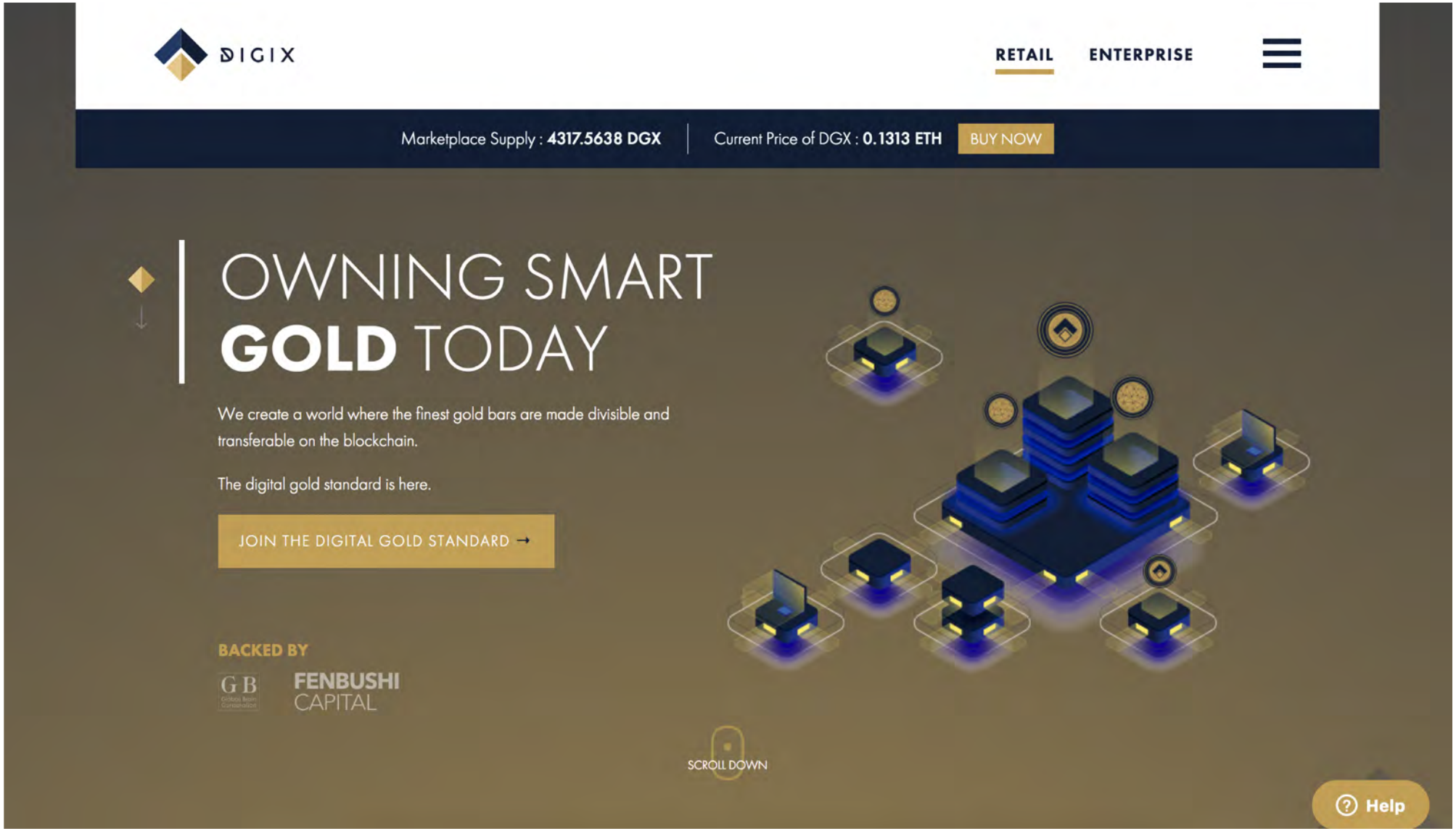
Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer. Development was funded by an online crowdsale during July–August 2014.[4] The system went live on 30 July 2015.[5]

# Ethereum

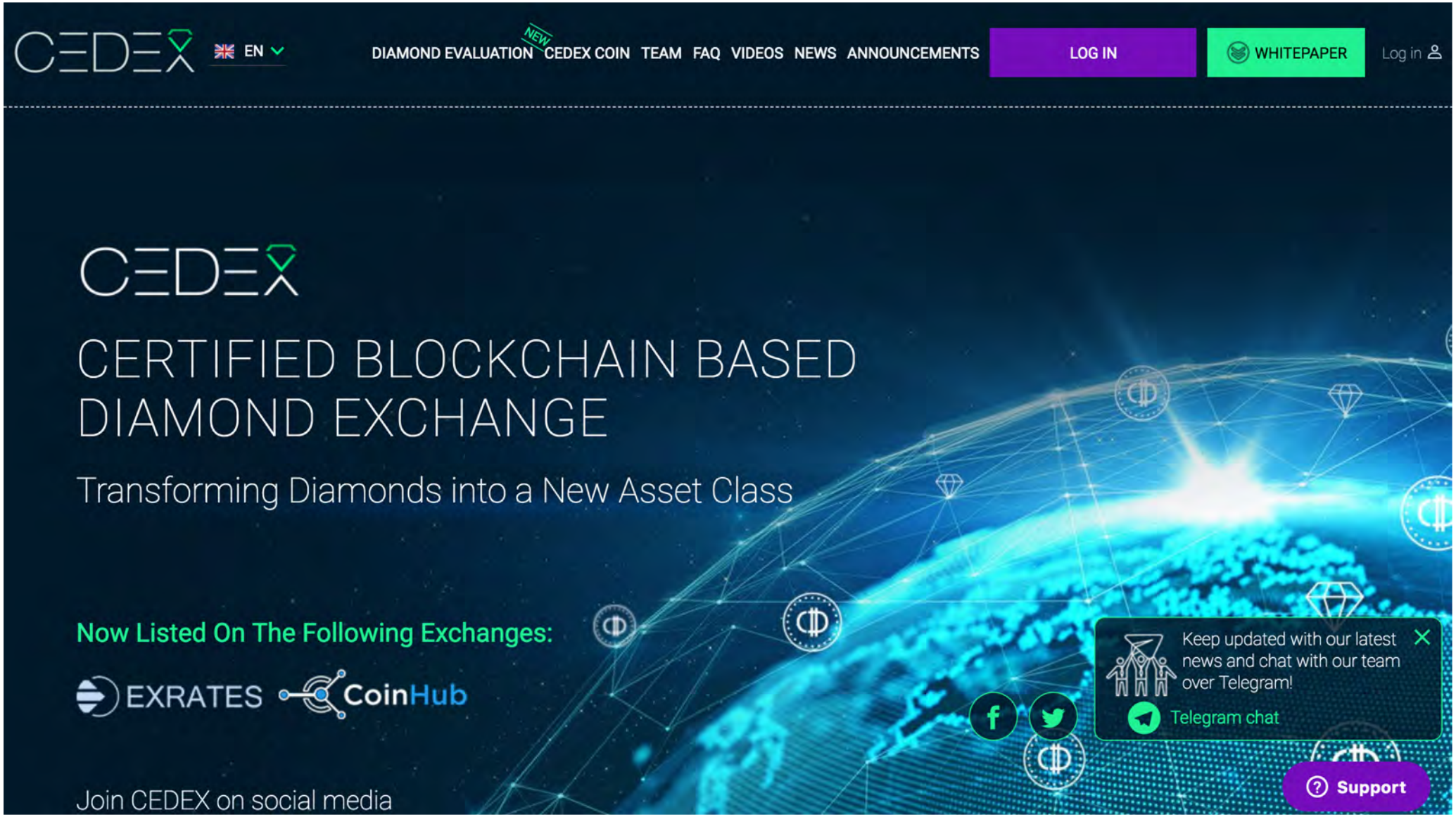
1 Ether equals
403.81 Singapore Dollar
3 Sep, 12:34 AM UTC · Disclaimer
1
Ether
403.81
Singapore Dollar
1D
5D
1 M
1 Y
5 Y
Max
600
400
200
393.17 Wed, Aug 29
19 Aug
2 Sep


DREAM. BUILD. INSPIRE.
SGINNOVATE
Mon, 21 Aug 2017
6.30pm – 8.30pm
SGInnovate
@ 32 Carpenter Street

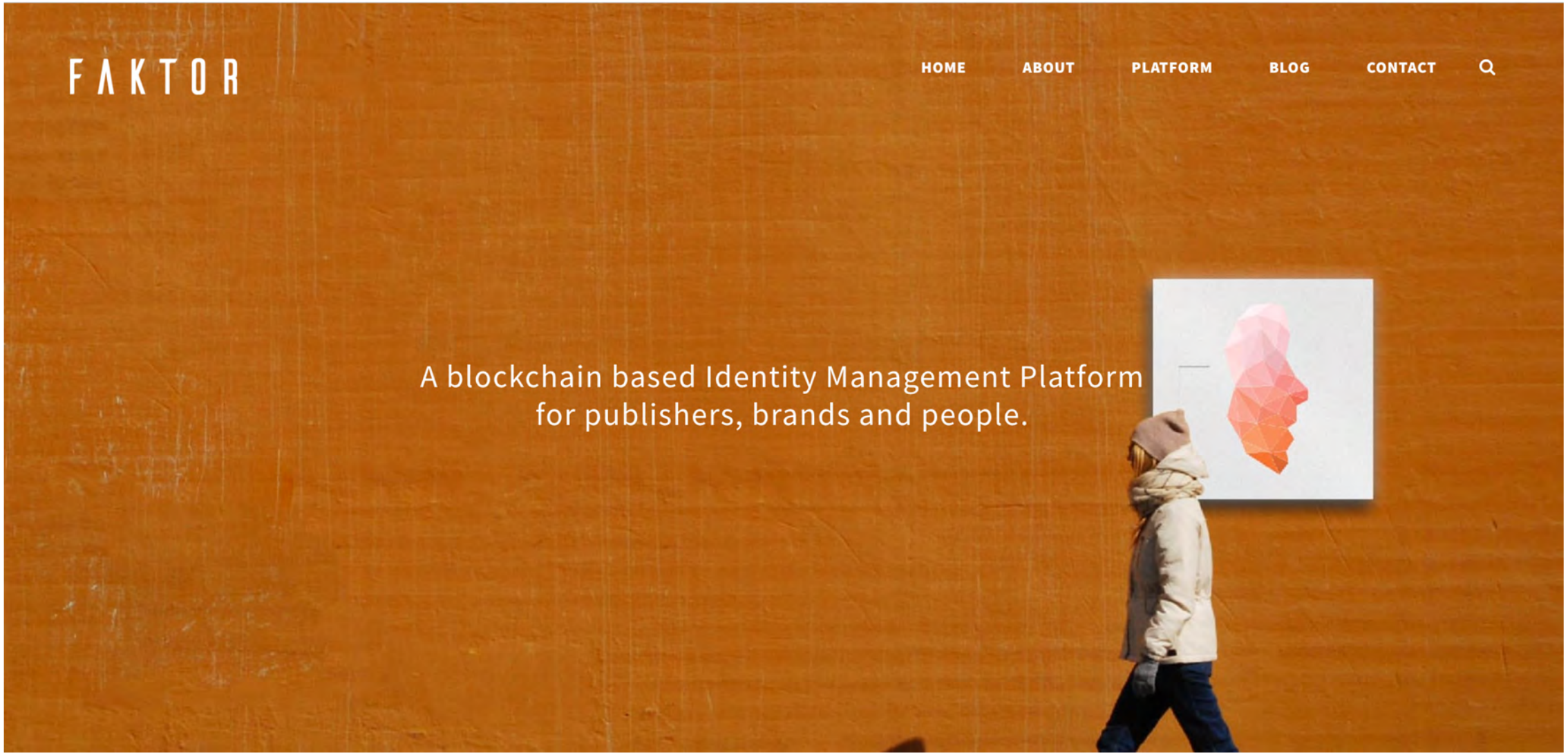
# Tokenisation of Commodities



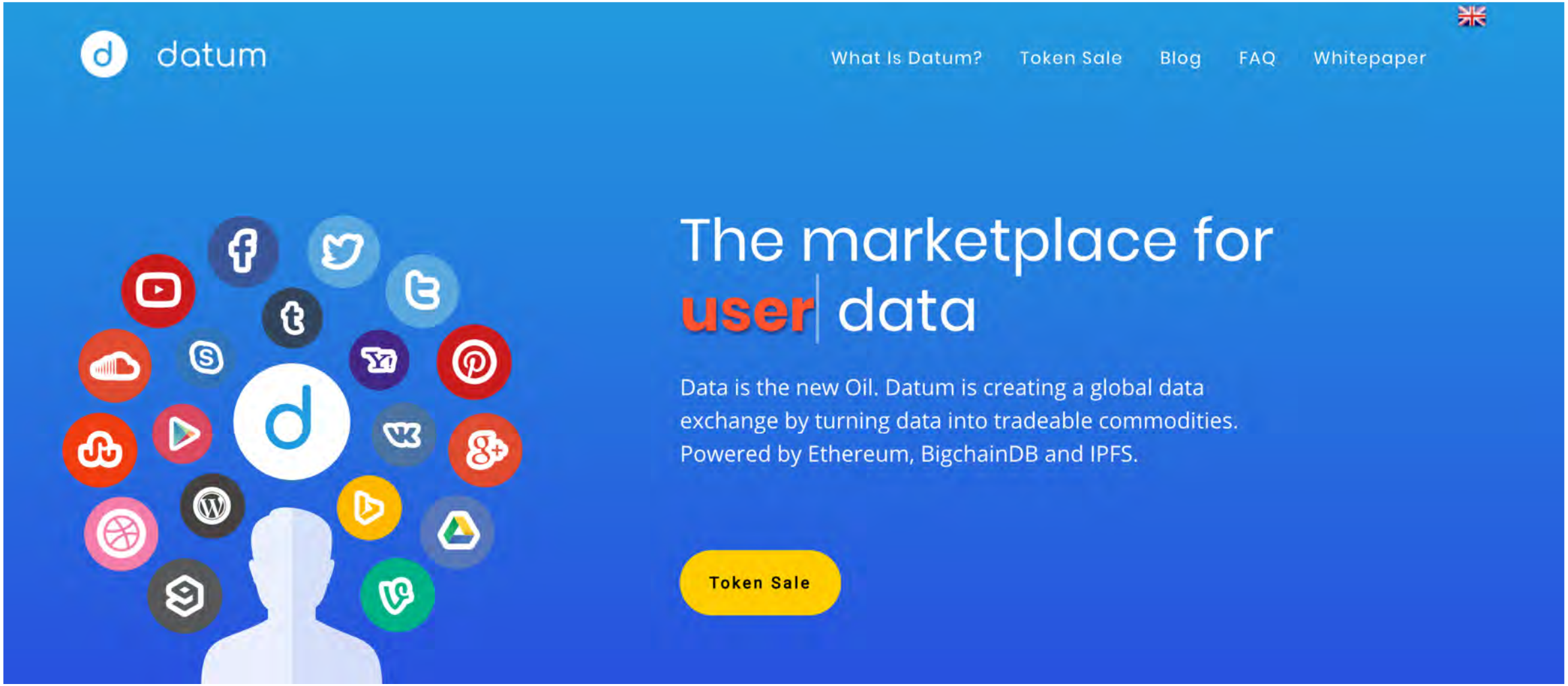
# Tokenisation of Commodities



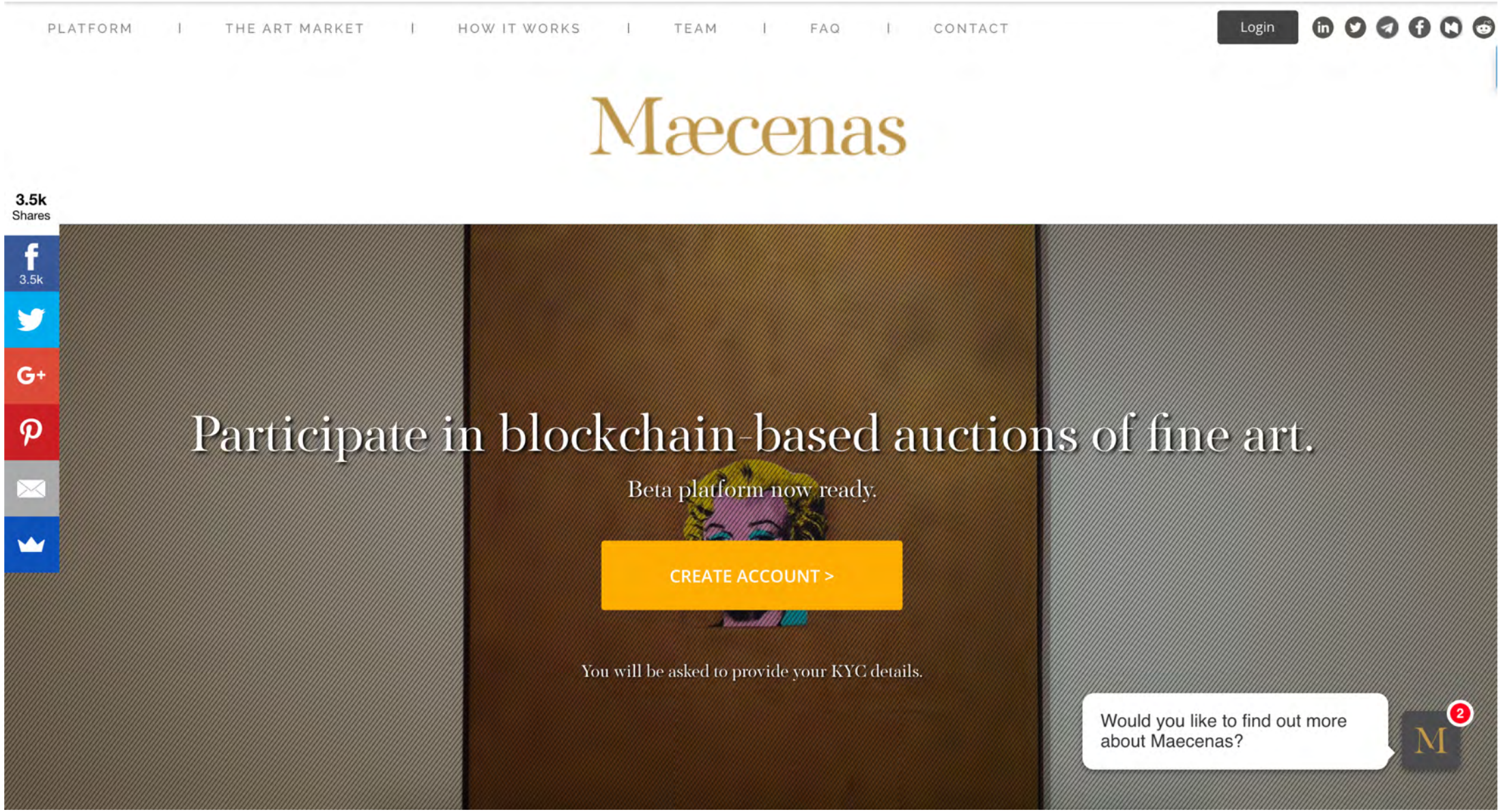
# Tokenisation of Identity



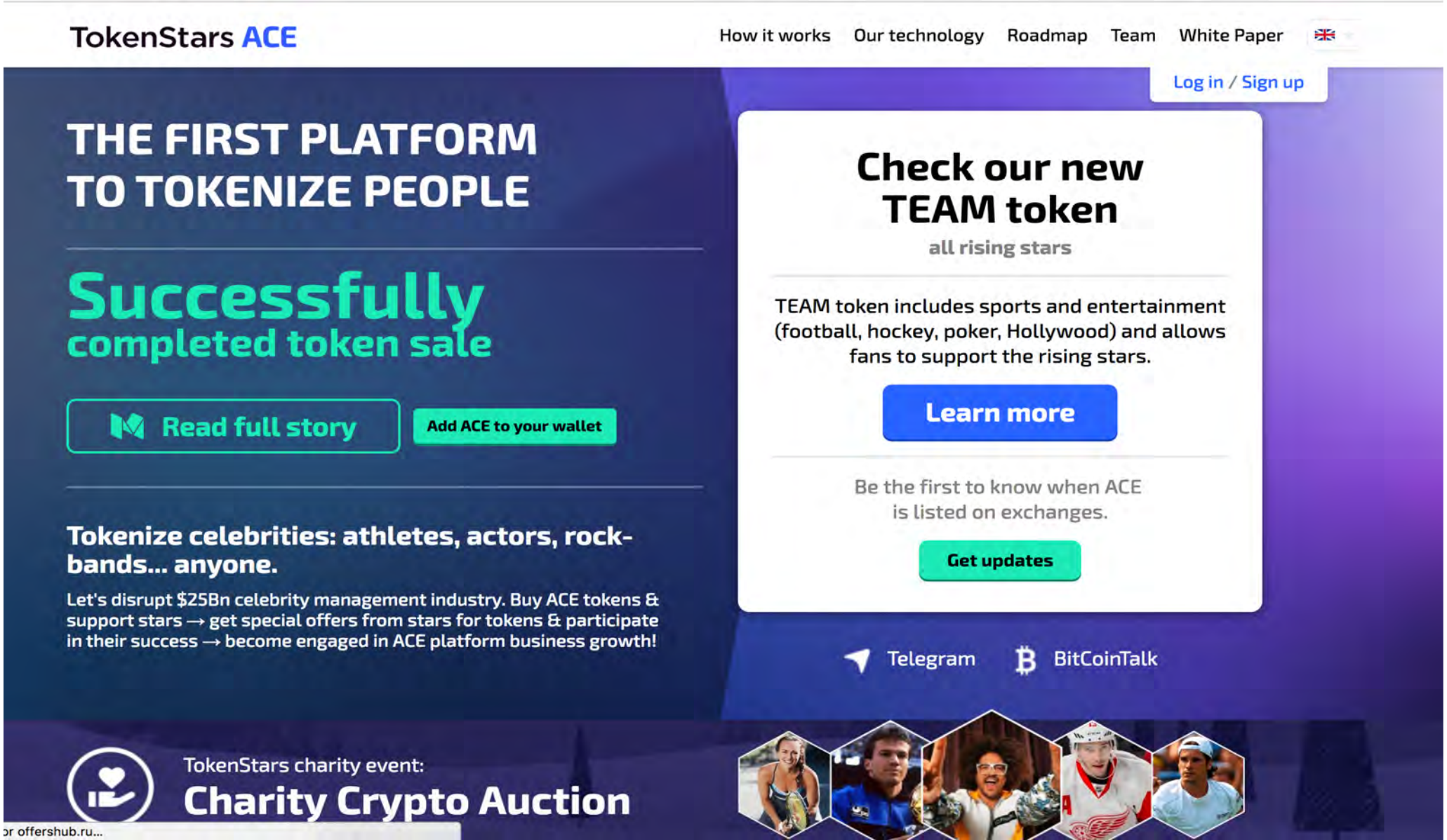
# Tokenisation of Personal Data



# Tokenisation of Fine Art



# Tokenisation of People



# Summary

Cypherpunks
Blockchain
Distributed Everything
Disruption

# What's Next?

Ian McKee
+65 96840019
ian.mckee@vuulr.com