CSUN | CALIFORNIA STATE UNIVERSITY NORTHRIDGE

DR JEFF SOFTWARE

Rev. 5-31-23

Cybersecurity & Cryptography

Blockchains

Dr Jeff Drobman

email → jeffrey.drobman@csun.edu

website → drjeffsoftware.com

Index

Section

Cryptography

Cryptography

- Encryption
  - □ Scrambles data
  - □ Makes data *unreadable*
- Hashing
  - □ Tags data with unique *hash* value
    - ➢ Completely *deterministic*
  - □ Makes data *immutable*
    - ➢ Any data corruption is detected

- Protects data:
  - □ in STORAGE
    - ▪ databases (PCI-DSS)
  - □ in TRANSIT
    - ▪ http**s** (uses *TLS*)

- Both use these:
  - □ Algorithms
  - □ Keys

Cryptography

❖Encryption

- Used to secure data in storage & *transit*
- Many standards (DES, 3DES, AES, RSA, etc.)
- algorithms use sequence of XOR operations
- Symmetric or Asymmetric
  - S uses single private key
  - A uses public-private key pairs
- replaces each character *in situ* with a code
- data retains same length
- does not detect tampering

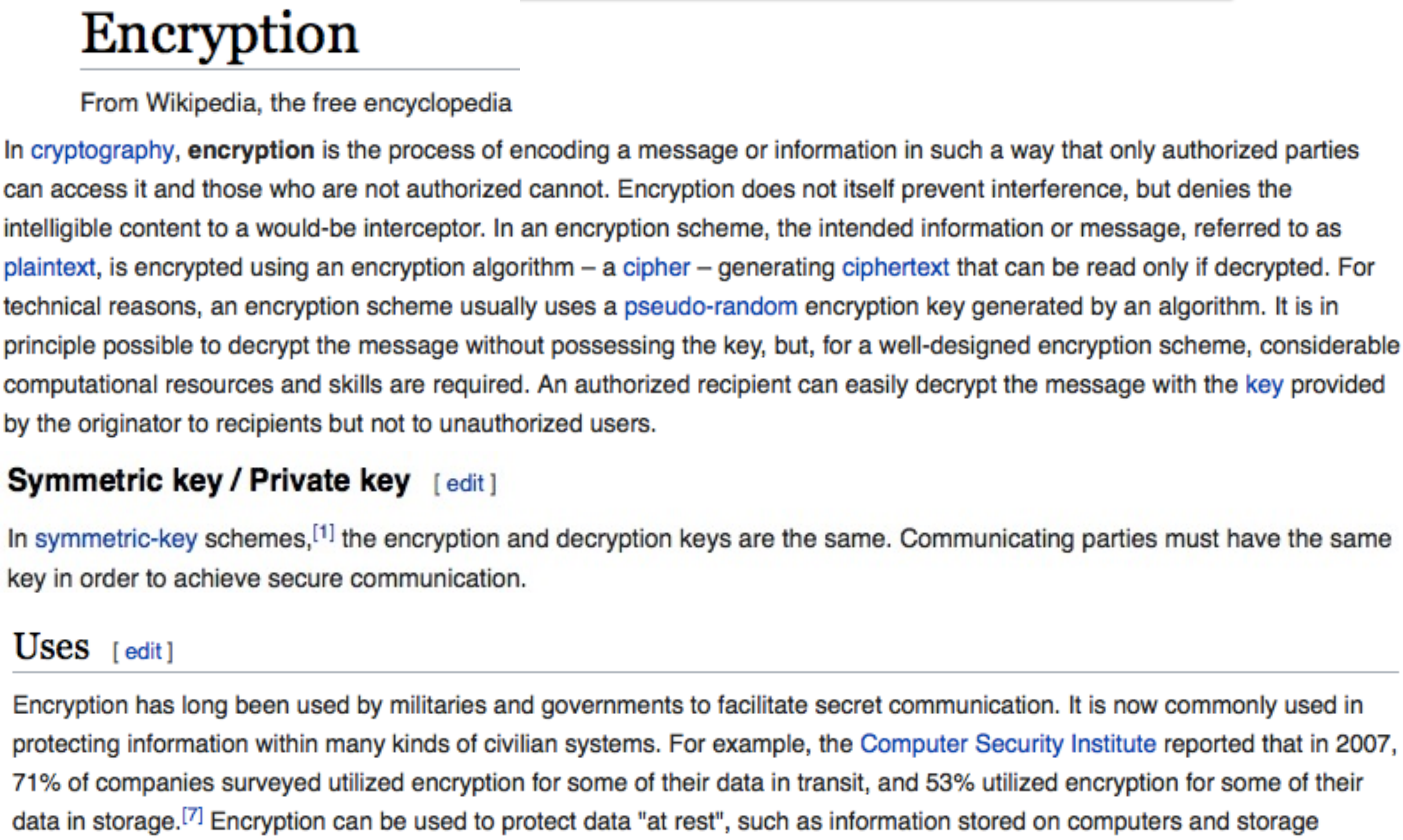
❖Hashing

- Used to secure data in storage (only)
- A few standards (MD, SHA)
- algorithms use complex sequence of math operations with key
- use private keys *derived* from random issued words
- does not replace data
- adds a “hash” value to each block of data
- hash value is a fixed 160 bits for SHA-1, 256 bits for SHA-2
- does detect tampering (*raison d’etre*)

Cryptography

Encryption

Encryption



Encryption

From Wikipedia, the free encyclopedia

In cryptography, **encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Symmetric key / Private key [edit]

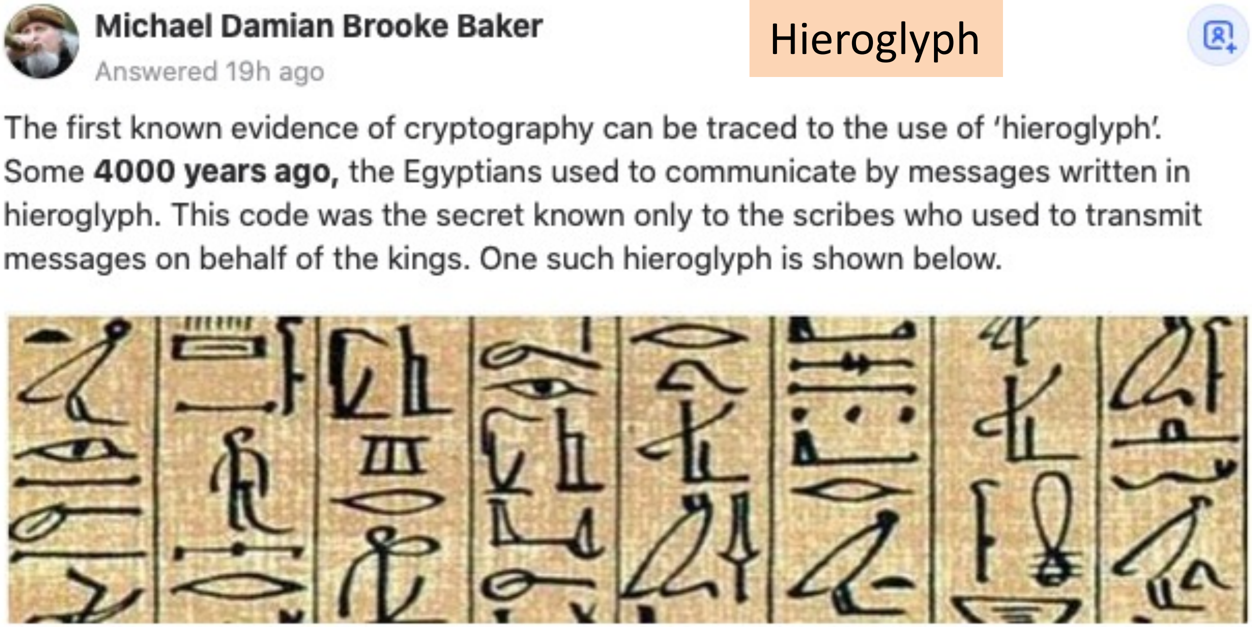
In symmetric-key schemes,[1] the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication.

Uses [edit]

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage.[7] Encryption can be used to protect data "at rest", such as information stored on computers and storage

Historic Encryption

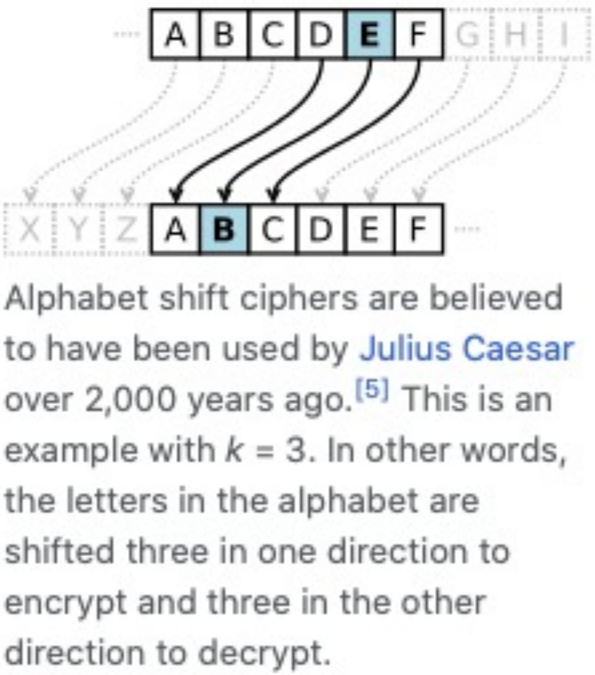
Hieroglyph



Michael Damian Brooke Baker
Answered 19h ago

The first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some **4000 years ago,** the Egyptians used to communicate by messages written in hieroglyph. This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such hieroglyph is shown below.

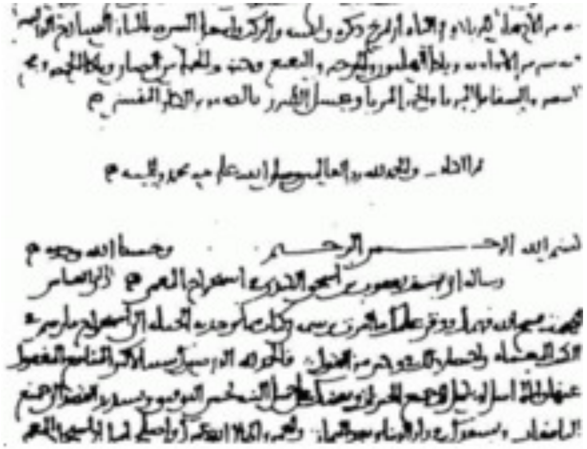
Caesarean



Alphabet shift ciphers are believed to have been used by Julius Caesar over 2,000 years ago.[5] This is an example with $k = 3$. In other words, the letters in the alphabet are shifted three in one direction to encrypt and three in the other direction to decrypt.

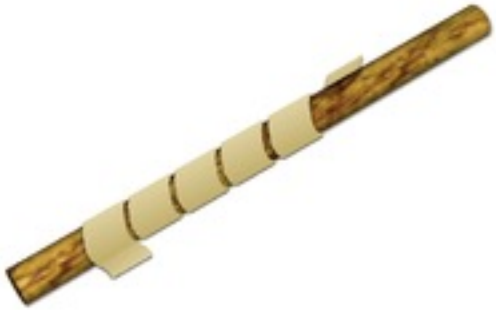
CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

Historic Encryption

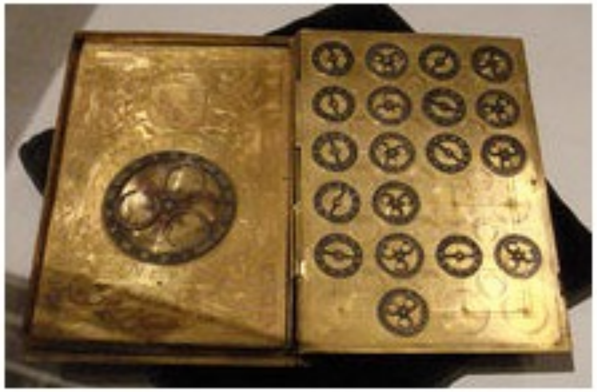


First page of a book by Al-Kindi which discusses encryption of messages

8th century (Arabic)



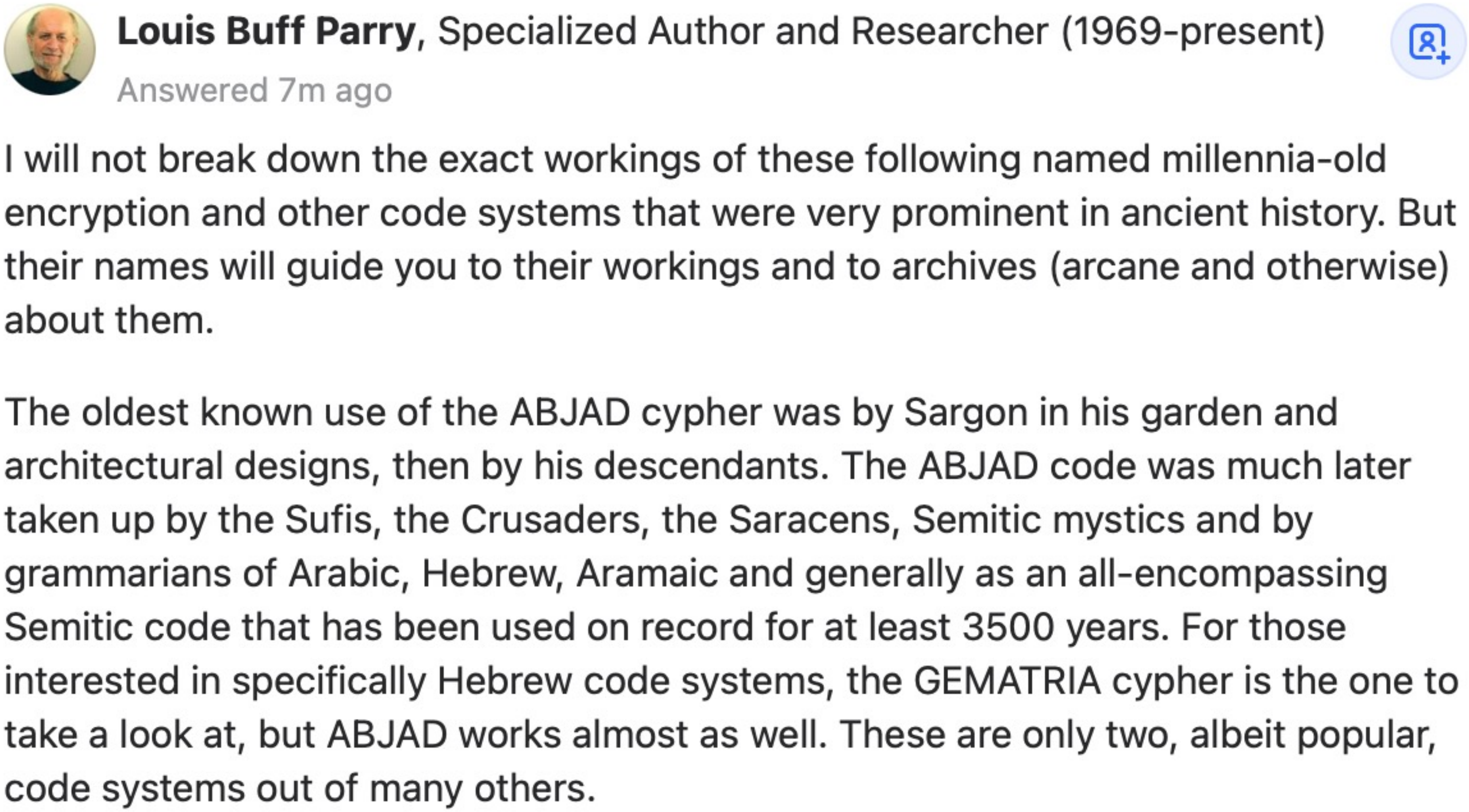
Reconstructed ancient Greek *scytale*, an early cipher device



16th-century book-shaped French cipher machine, with arms of Henri II of France

Enciphered letter from Gabriel de Luetz d'Aramon, French Ambassador to the Ottoman Empire, after 1546, with partial decipherment

Ancient Historic Encryption



Louis Buff Parry, Specialized Author and Researcher (1969-present)

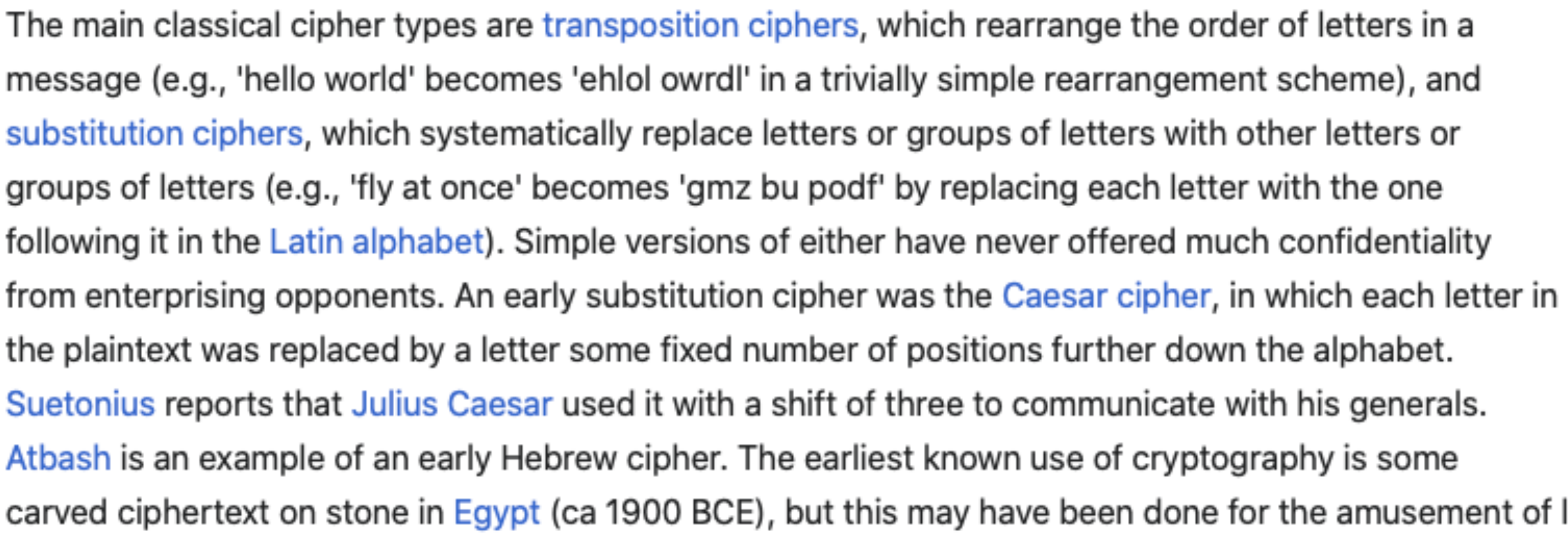
Answered 7m ago

I will not break down the exact workings of these following named millennia-old encryption and other code systems that were very prominent in ancient history. But their names will guide you to their workings and to archives (arcane and otherwise) about them.

The oldest known use of the ABJAD cypher was by Sargon in his garden and architectural designs, then by his descendants. The ABJAD code was much later taken up by the Sufis, the Crusaders, the Saracens, Semitic mystics and by grammarians of Arabic, Hebrew, Aramaic and generally as an all-encompassing Semitic code that has been used on record for at least 3500 years. For those interested in specifically Hebrew code systems, the GEMATRIA cypher is the one to take a look at, but ABJAD works almost as well. These are only two, albeit popular, code systems out of many others.

Classical Cyphers

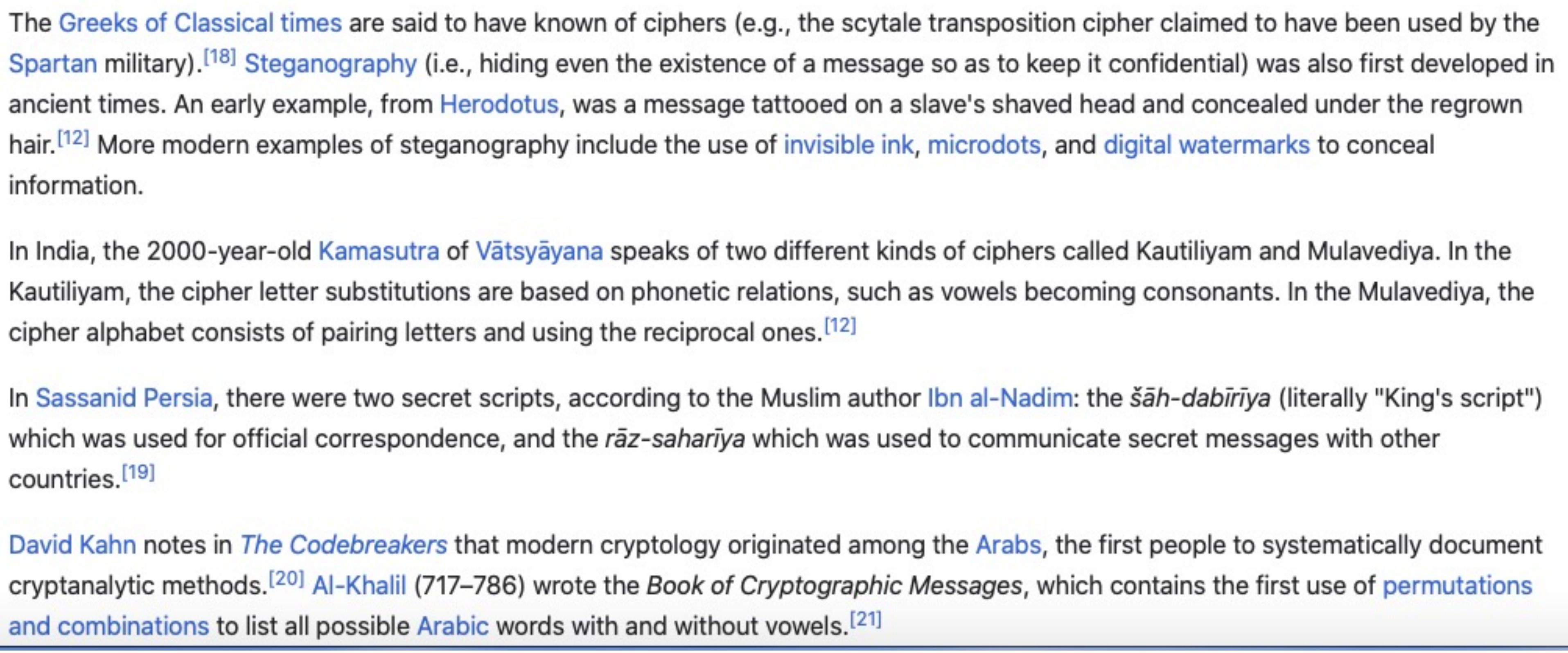
- Transposition
- Substitution



The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet). Simple versions of either have never offered much confidentiality from enterprising opponents. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. Suetonius reports that Julius Caesar used it with a shift of three to communicate with his generals. Atbash is an example of an early Hebrew cipher. The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BCE), but this may have been done for the amusement of

Classical Cyphers

❖ Steganography



The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cipher claimed to have been used by the Spartan military).[18] Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, was a message tattooed on a slave's shaved head and concealed under the regrown hair.[12] More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

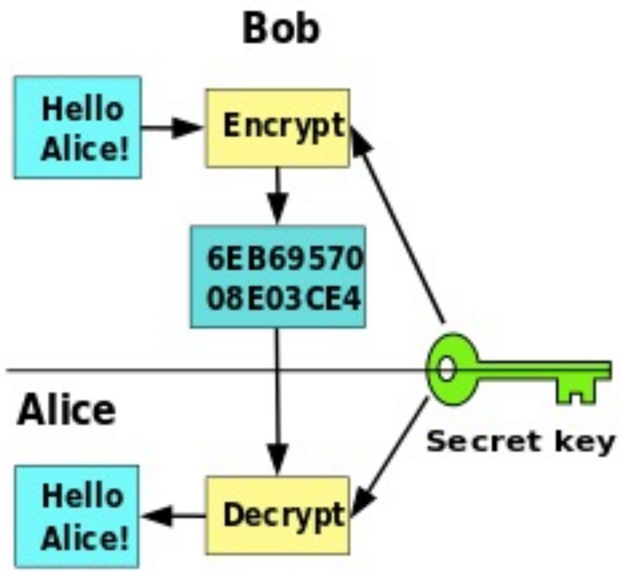
In India, the 2000-year-old Kamasutra of Vātsyāyana speaks of two different kinds of ciphers called Kautiliyam and Mulavediya. In the Kautiliyam, the cipher letter substitutions are based on phonetic relations, such as vowels becoming consonants. In the Mulavediya, the cipher alphabet consists of pairing letters and using the reciprocal ones.[12]

In Sassanid Persia, there were two secret scripts, according to the Muslim author Ibn al-Nadim: the *šāh-dabīrīya* (literally "King's script") which was used for official correspondence, and the *rāz-saharīya* which was used to communicate secret messages with other countries.[19]

David Kahn notes in *The Codebreakers* that modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods.[20] Al-Khalil (717–786) wrote the *Book of Cryptographic Messages*, which contains the first use of permutations and combinations to list all possible Arabic words with and without vowels.[21]

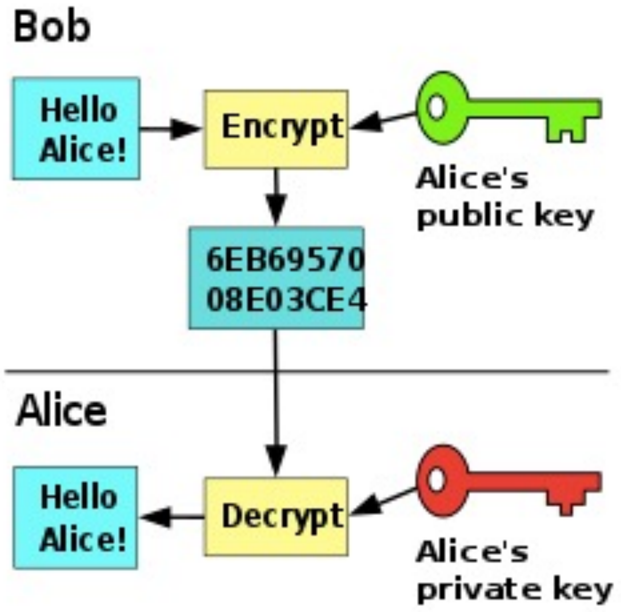
Encryption: (A)Symmetric

Symmetric



Symmetric-key cryptography, where a single key is used for encryption and decryption

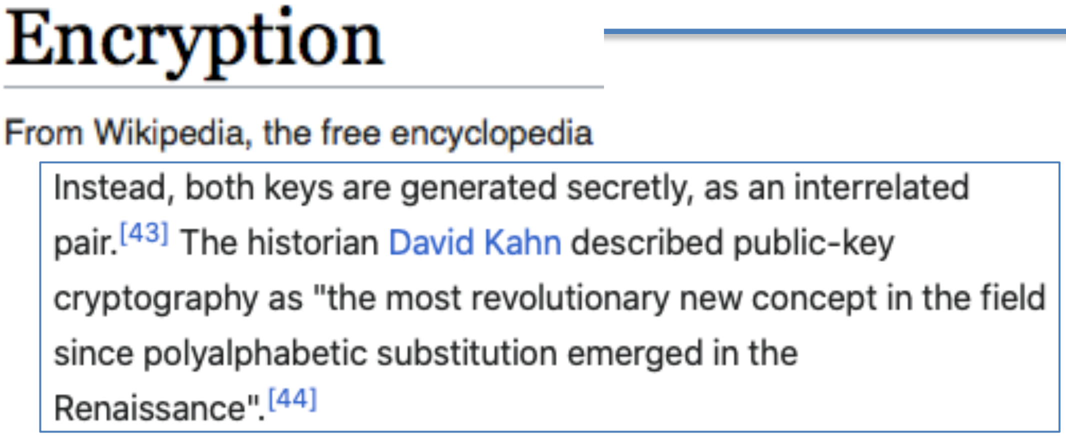
Asymmetric



Public-key cryptography, where different keys are used for encryption and decryption.

Examples of asymmetric systems include RSA (Rivest–Shamir–Adleman),

Encryption – Public Key



Encryption

From Wikipedia, the free encyclopedia

Instead, both keys are generated secretly, as an interrelated pair.[43] The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance".[44]

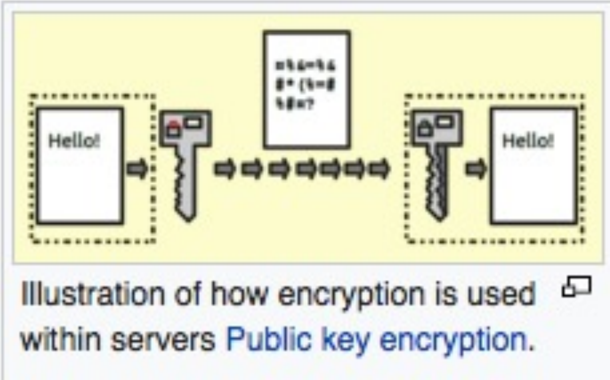
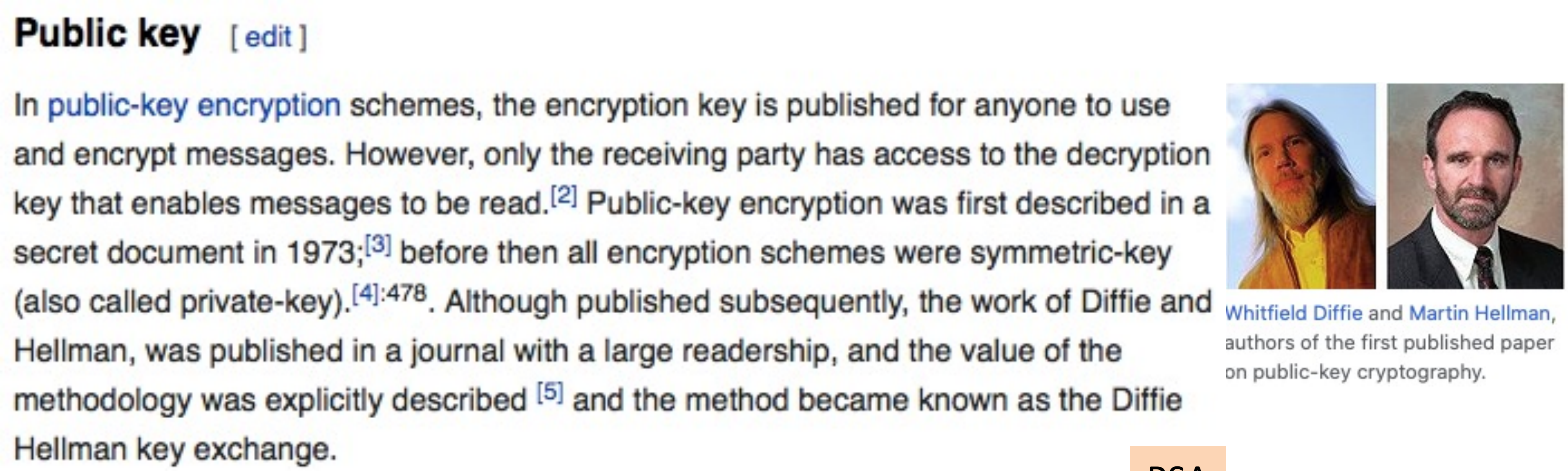


Illustration of how encryption is used within servers Public key encryption.

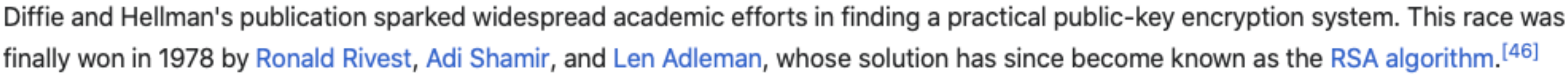


Public key [edit]

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read.[2] Public-key encryption was first described in a secret document in 1973;[3] before then all encryption schemes were symmetric-key (also called private-key).[4]:478. Although published subsequently, the work of Diffie and Hellman, was published in a journal with a large readership, and the value of the methodology was explicitly described [5] and the method became known as the Diffie Hellman key exchange.

Whitfield Diffie and Martin Hellman, authors of the first published paper on public-key cryptography.

RSA

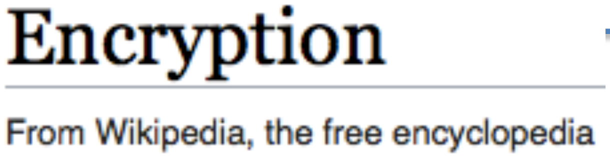


Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.[46]

CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

Encryption – Public Key

DR JEFF SOFTWARE



Encryption

From Wikipedia, the free encyclopedia

PGP

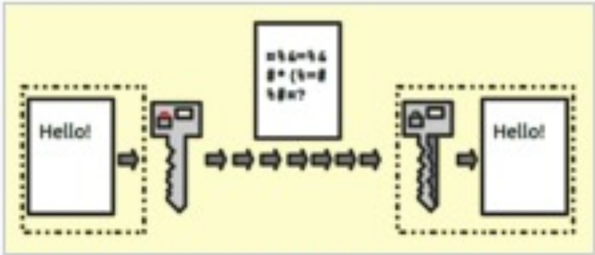
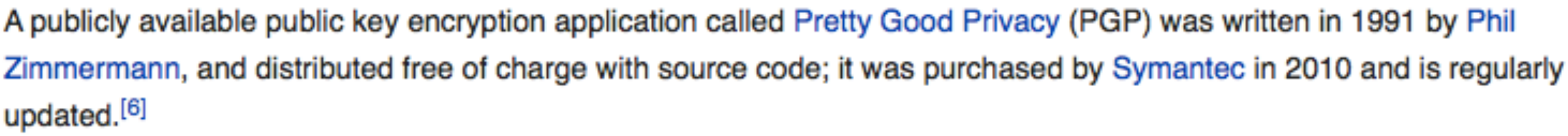
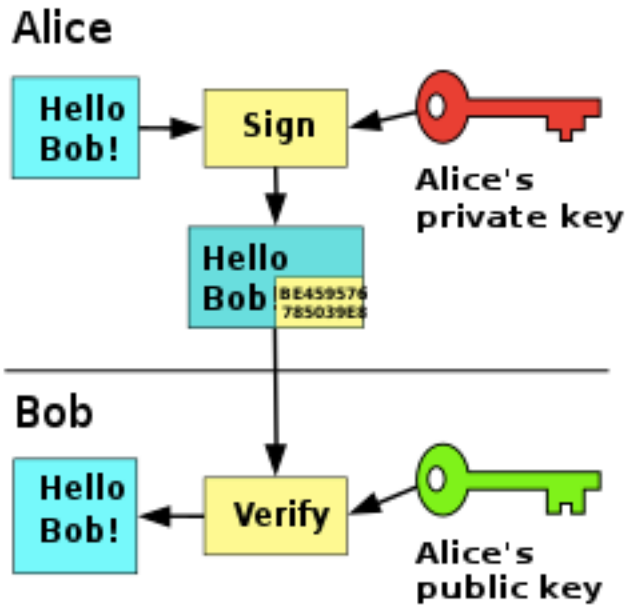


Illustration of how encryption is used within servers Public key encryption.



A publicly available public key encryption application called Pretty Good Privacy (PGP) was written in 1991 by Phil Zimmermann, and distributed free of charge with source code; it was purchased by Symantec in 2010 and is regularly updated.[6]

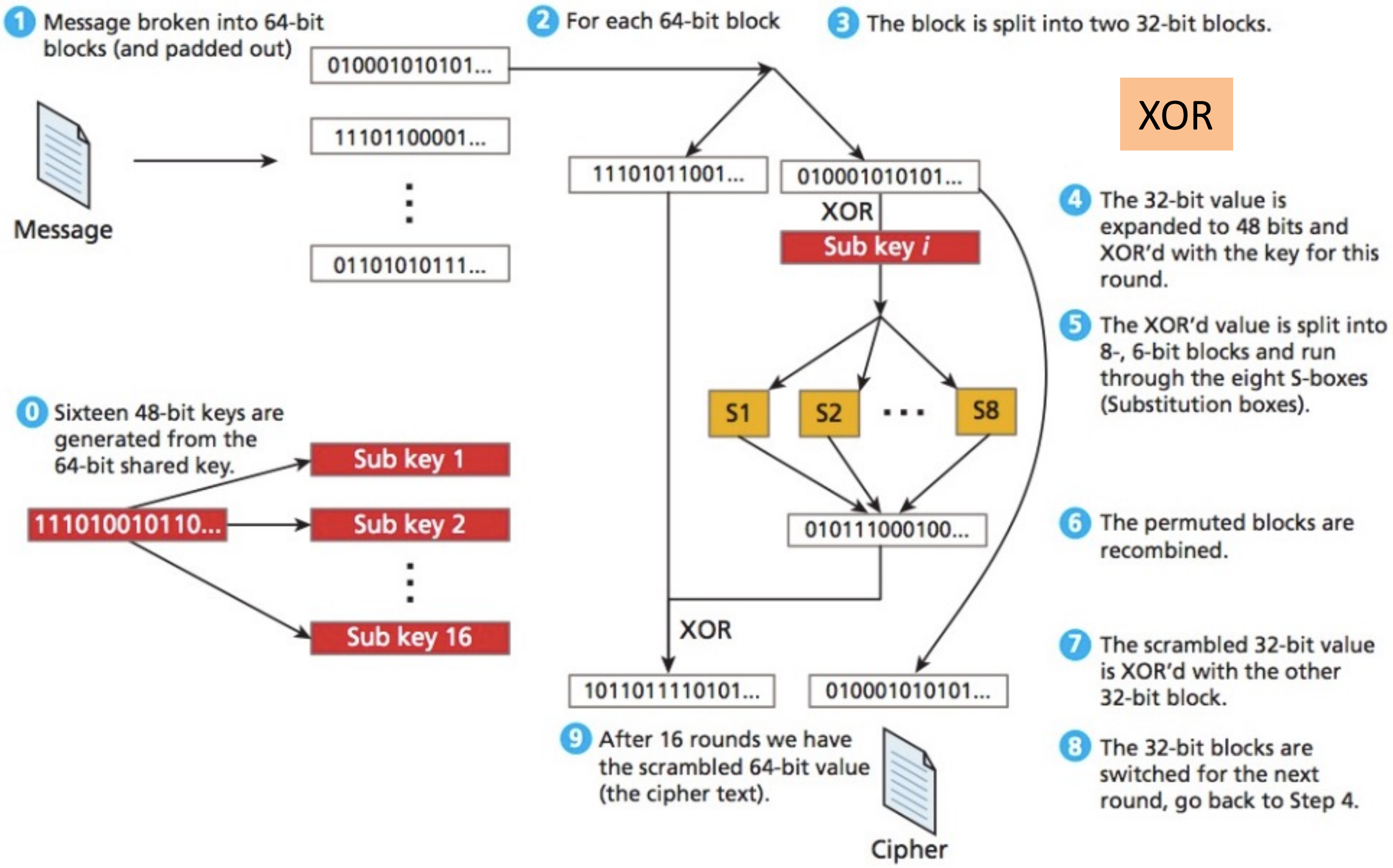
Encryption: Signing



In this example the message is only signed and not encrypted. 1) Alice signs a message with her private key. 2) Bob can verify that Alice sent the message and that the message has not been modified.

DES Encryption

XOR



1 Message broken into 64-bit blocks (and padded out)

2 For each 64-bit block

3 The block is split into two 32-bit blocks.

4 The 32-bit value is expanded to 48 bits and XOR'd with the key for this round.

5 The XOR'd value is split into 8-, 6-bit blocks and run through the eight S-boxes (Substitution boxes).

6 The permuted blocks are recombined.

7 The scrambled 32-bit value is XOR'd with the other 32-bit block.

8 The 32-bit blocks are switched for the next round, go back to Step 4.

0 Sixteen 48-bit keys are generated from the 64-bit shared key.

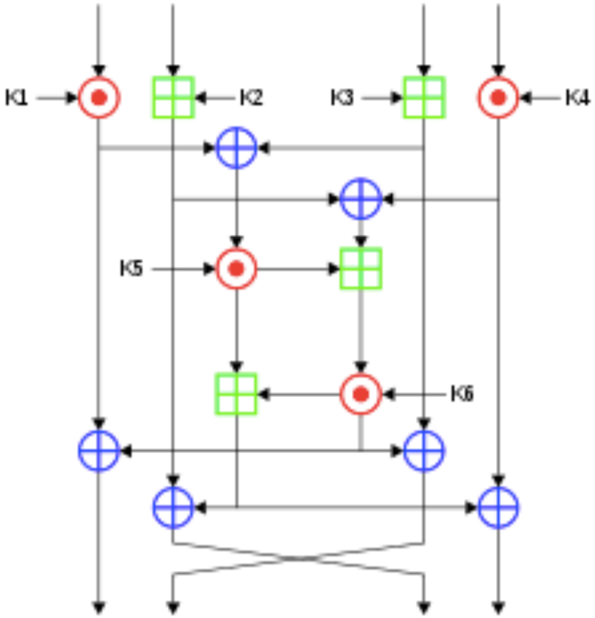
9 After 16 rounds we have the scrambled 64-bit value (the cipher text).

FIGURE 16.10 High-level illustration of the DES cipher

Algorithms + Keys

PGP: Pretty Good Encr.

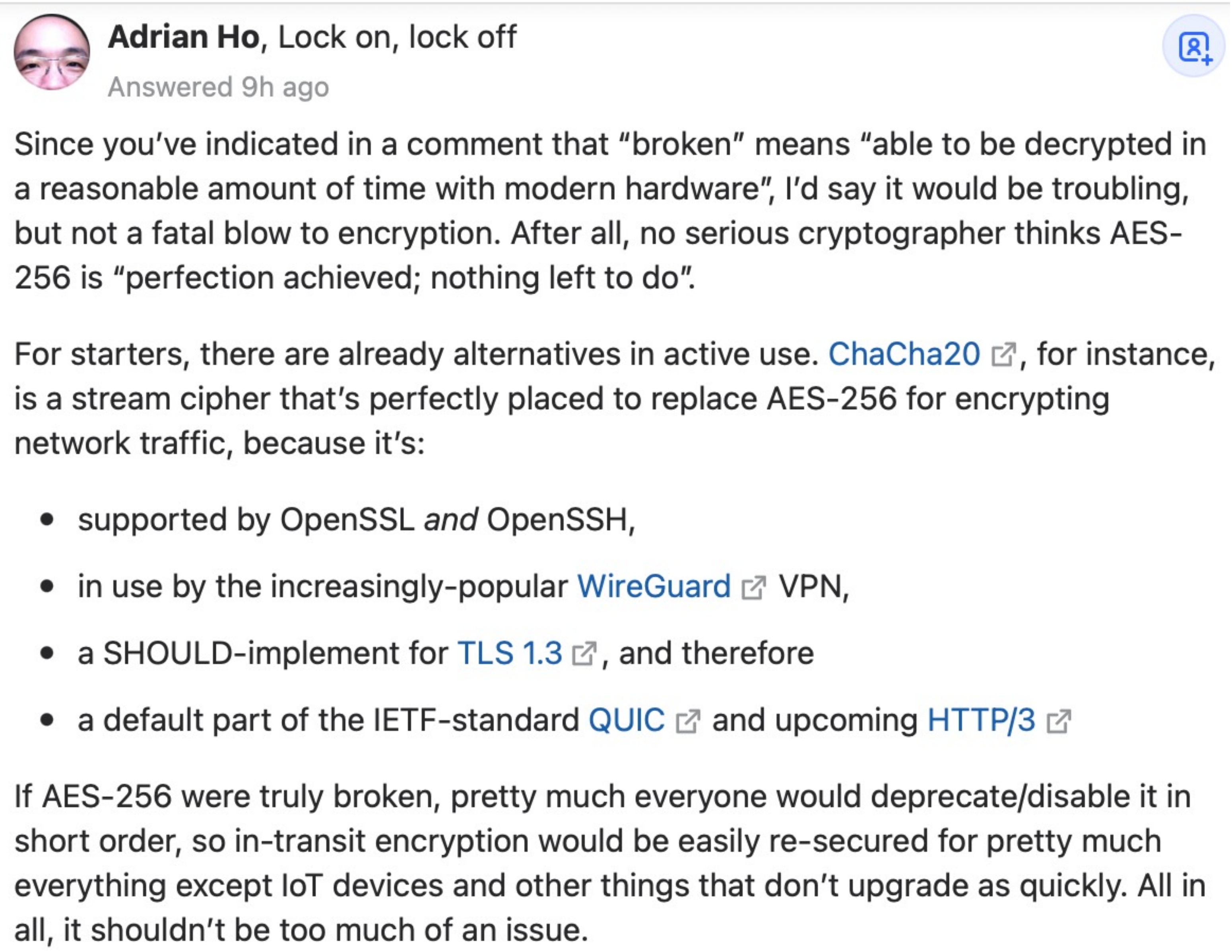
Open Standard Software



One round (out of 8.5) of the IDEA cipher, used in most versions of PGP and OpenPGP compatible software for time-efficient encryption of messages

AES

Quora



Adrian Ho, Lock on, lock off
Answered 9h ago

Since you've indicated in a comment that "broken" means "able to be decrypted in a reasonable amount of time with modern hardware", I'd say it would be troubling, but not a fatal blow to encryption. After all, no serious cryptographer thinks AES-256 is "perfection achieved; nothing left to do".

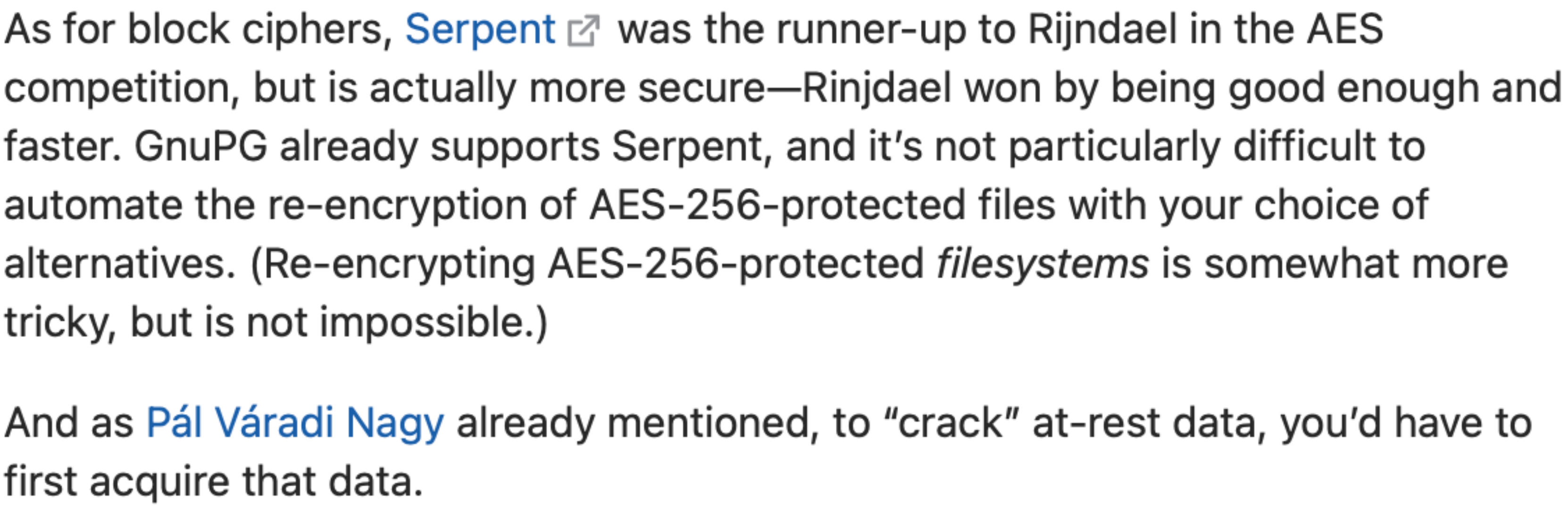
For starters, there are already alternatives in active use. ChaCha20, for instance, is a stream cipher that's perfectly placed to replace AES-256 for encrypting network traffic, because it's:

- supported by OpenSSL *and* OpenSSH,
- in use by the increasingly-popular WireGuard VPN,
- a SHOULD-implement for TLS 1.3, and therefore
- a default part of the IETF-standard QUIC and upcoming HTTP/3

If AES-256 were truly broken, pretty much everyone would deprecate/disable it in short order, so in-transit encryption would be easily re-secured for pretty much everything except IoT devices and other things that don't upgrade as quickly. All in all, it shouldn't be too much of an issue.

AES-256

Quora



As for block ciphers, Serpent was the runner-up to Rijndael in the AES competition, but is actually more secure—Rinjdael won by being good enough and faster. GnuPG already supports Serpent, and it's not particularly difficult to automate the re-encryption of AES-256-protected files with your choice of alternatives. (Re-encrypting AES-256-protected *filesystems* is somewhat more tricky, but is not impossible.)

And as Pál Váradi Nagy already mentioned, to "crack" at-rest data, you'd have to first acquire that data.

Encryption – *Elliptic* PKE

Encryption

From Wikipedia, the free encyclopedia

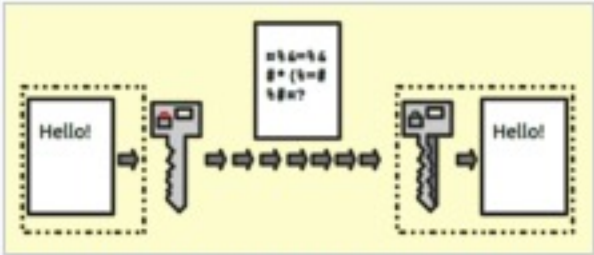
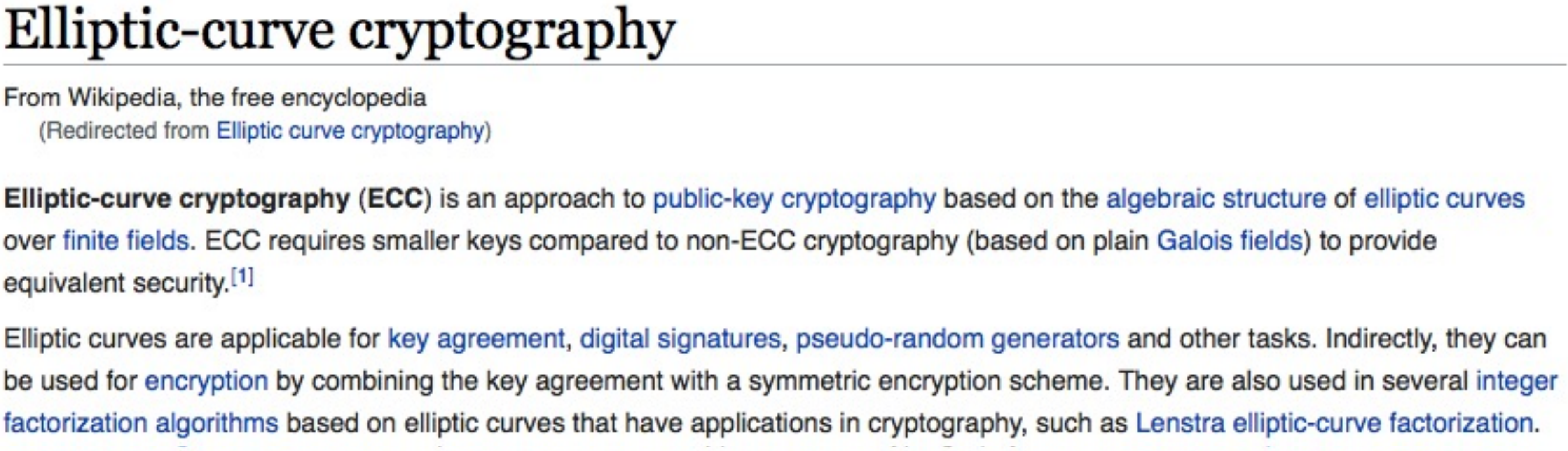


Illustration of how encryption is used within servers Public key encryption.



Elliptic-curve cryptography

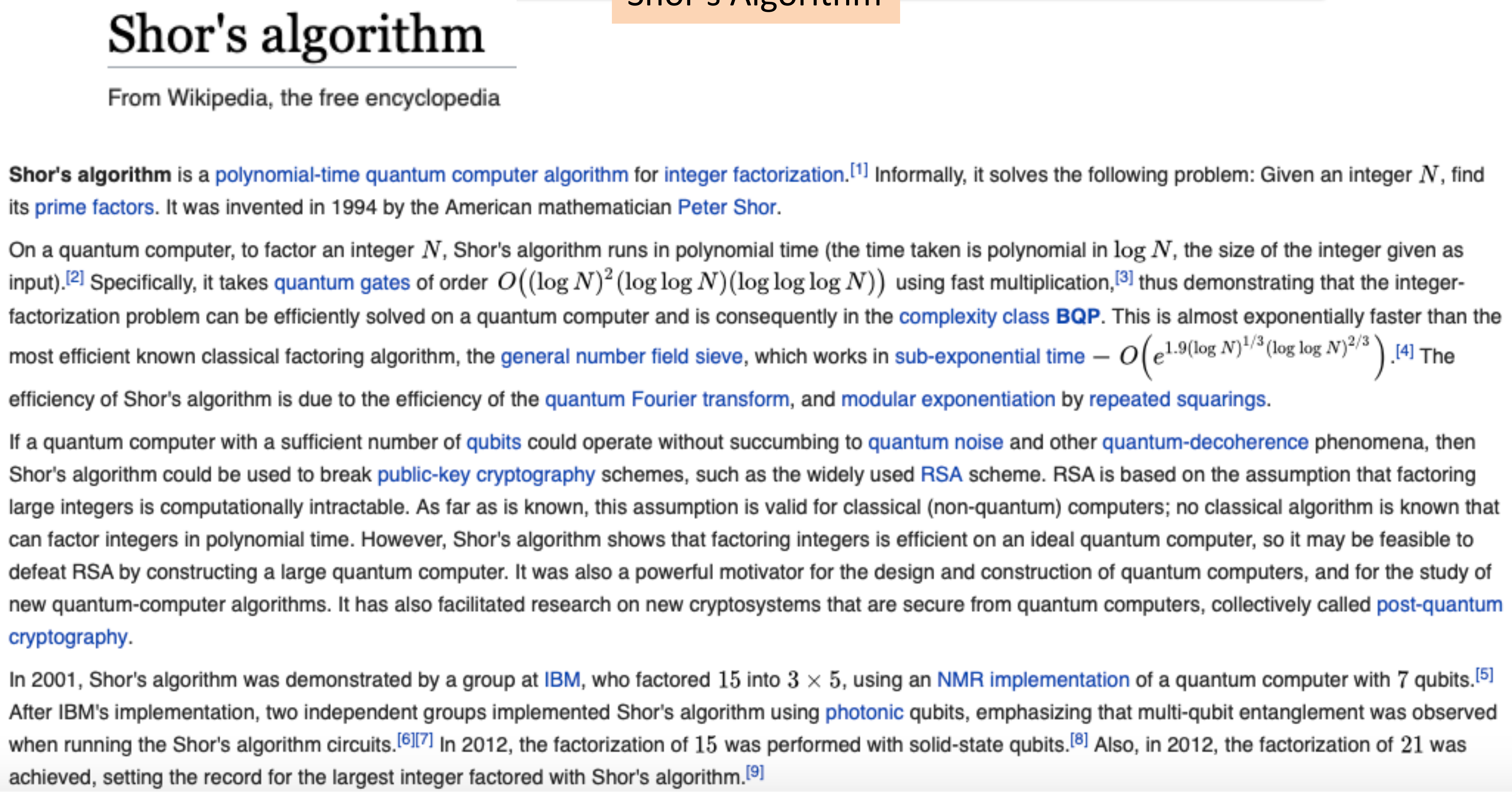
From Wikipedia, the free encyclopedia
(Redirected from Elliptic curve cryptography)

Elliptic-curve cryptography (**ECC**) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security.[1]

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization.

Asymmetric Encryption

Shor's Algorithm



Shor's algorithm

From Wikipedia, the free encyclopedia

Shor's algorithm is a polynomial-time quantum computer algorithm for integer factorization.[1] Informally, it solves the following problem: Given an integer N, find its prime factors. It was invented in 1994 by the American mathematician Peter Shor.

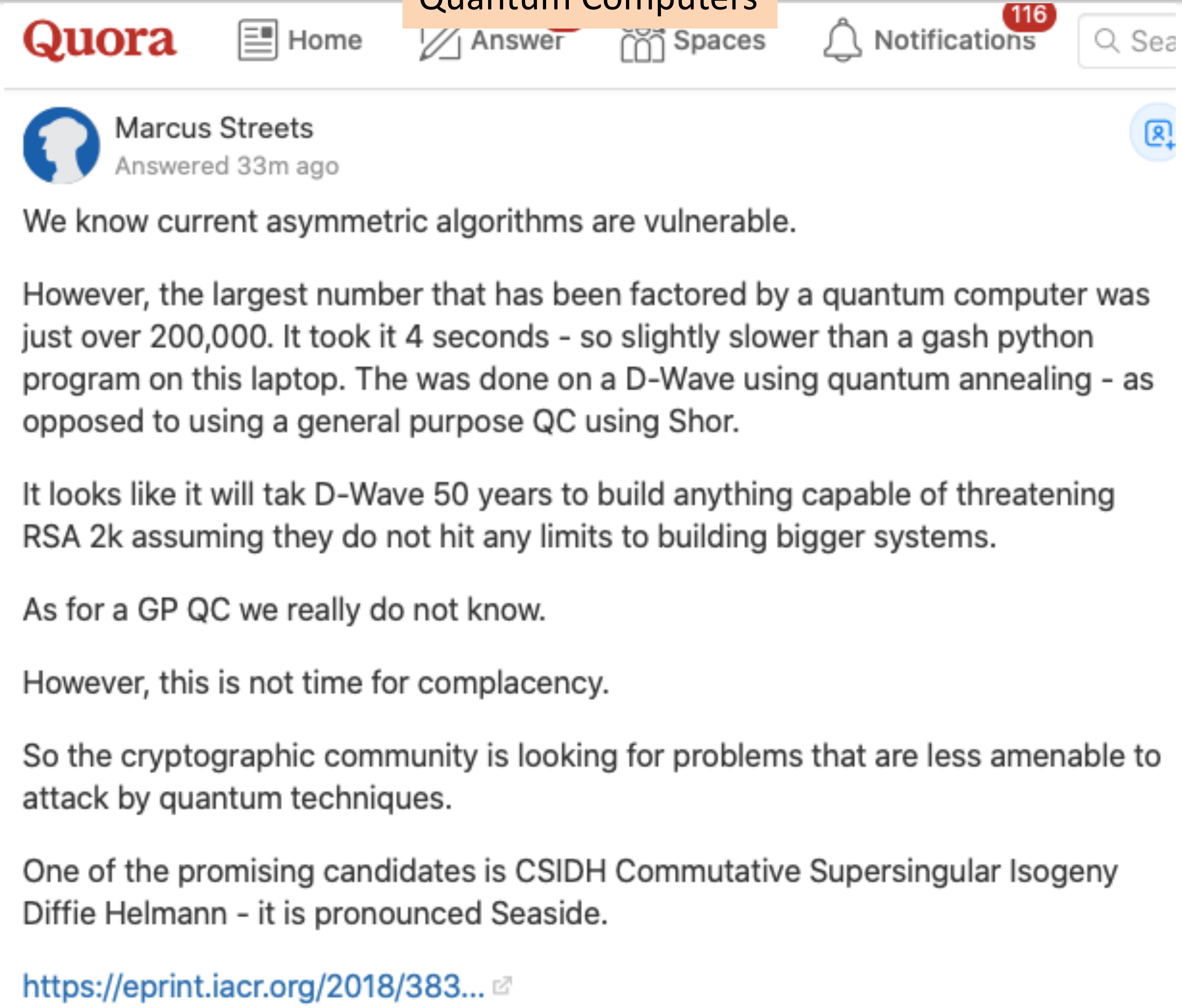
On a quantum computer, to factor an integer N, Shor's algorithm runs in polynomial time (the time taken is polynomial in $\log N$, the size of the integer given as input).[2] Specifically, it takes quantum gates of order $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$ using fast multiplication,[3] thus demonstrating that the integer-factorization problem can be efficiently solved on a quantum computer and is consequently in the complexity class **BQP**. This is almost exponentially faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time – $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$.[4] The efficiency of Shor's algorithm is due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squarings.

If a quantum computer with a sufficient number of qubits could operate without succumbing to quantum noise and other quantum-decoherence phenomena, then Shor's algorithm could be used to break public-key cryptography schemes, such as the widely used RSA scheme. RSA is based on the assumption that factoring large integers is computationally intractable. As far as is known, this assumption is valid for classical (non-quantum) computers; no classical algorithm is known that can factor integers in polynomial time. However, Shor's algorithm shows that factoring integers is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by constructing a large quantum computer. It was also a powerful motivator for the design and construction of quantum computers, and for the study of new quantum-computer algorithms. It has also facilitated research on new cryptosystems that are secure from quantum computers, collectively called post-quantum cryptography.

In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3×5, using an NMR implementation of a quantum computer with 7 qubits.[5] After IBM's implementation, two independent groups implemented Shor's algorithm using photonic qubits, emphasizing that multi-qubit entanglement was observed when running the Shor's algorithm circuits.[6][7] In 2012, the factorization of 15 was performed with solid-state qubits.[8] Also, in 2012, the factorization of 21 was achieved, setting the record for the largest integer factored with Shor's algorithm.[9]

QC Vulnerability

Quantum Computers



Marcus Streets
Answered 33m ago

We know current asymmetric algorithms are vulnerable.

However, the largest number that has been factored by a quantum computer was just over 200,000. It took it 4 seconds - so slightly slower than a gash python program on this laptop. The was done on a D-Wave using quantum annealing - as opposed to using a general purpose QC using Shor.

It looks like it will tak D-Wave 50 years to build anything capable of threatening RSA 2k assuming they do not hit any limits to building bigger systems.

As for a GP QC we really do not know.

However, this is not time for complacency.

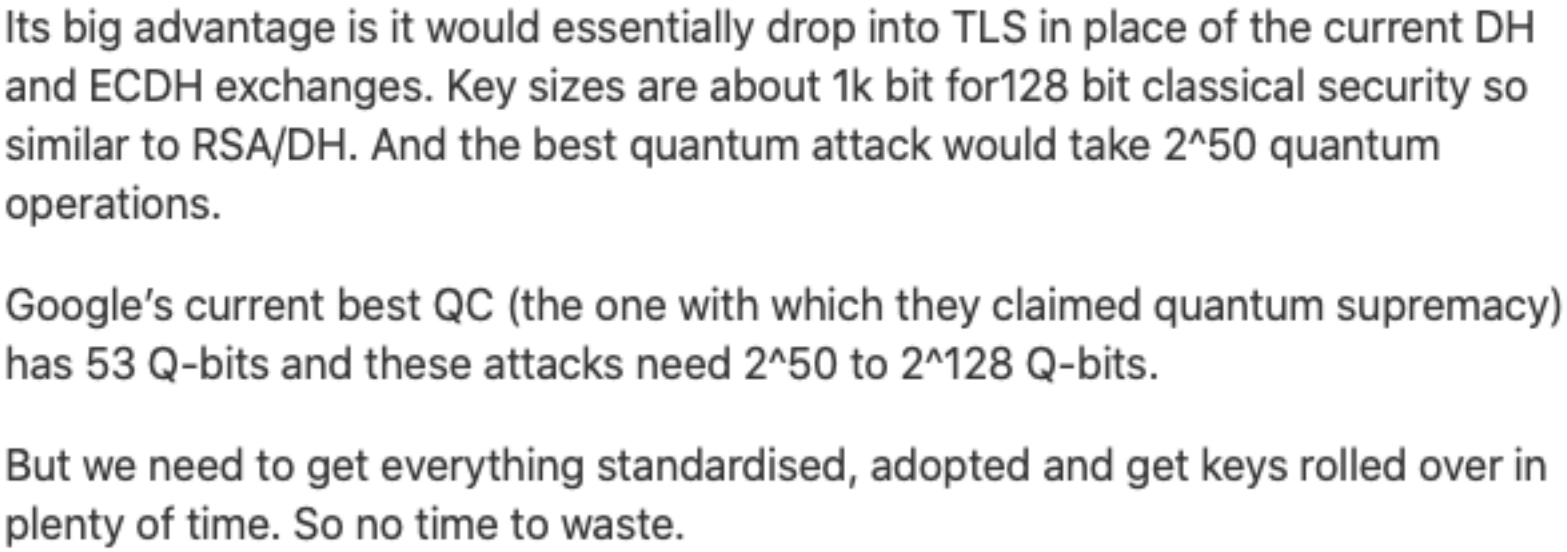
So the cryptographic community is looking for problems that are less amenable to attack by quantum techniques.

One of the promising candidates is CSIDH Commutative Supersingular Isogeny Diffie Helmann - it is pronounced Seaside.

https://eprint.iacr.org/2018/383...

QC Vulnerability

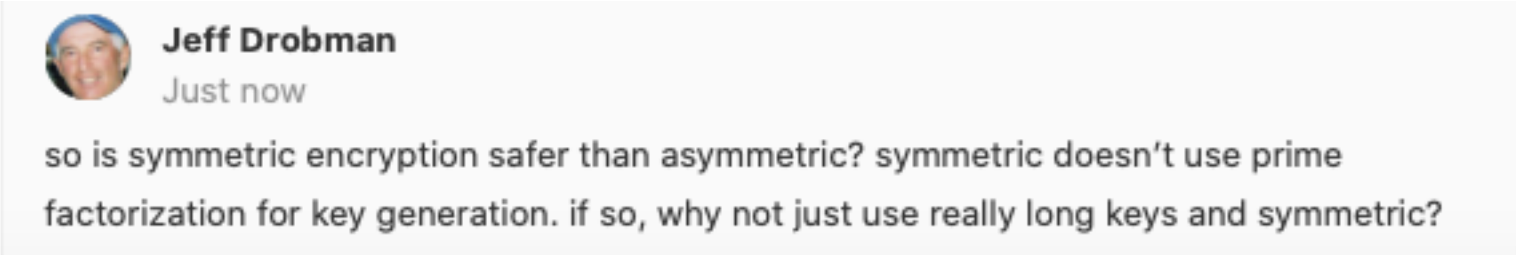
Quantum Computers



Its big advantage is it would essentially drop into TLS in place of the current DH and ECDH exchanges. Key sizes are about 1k bit for128 bit classical security so similar to RSA/DH. And the best quantum attack would take 2^50 quantum operations.

Google's current best QC (the one with which they claimed quantum supremacy) has 53 Q-bits and these attacks need 2^50 to 2^128 Q-bits.

But we need to get everything standardised, adopted and get keys rolled over in plenty of time. So no time to waste.



Jeff Drobman

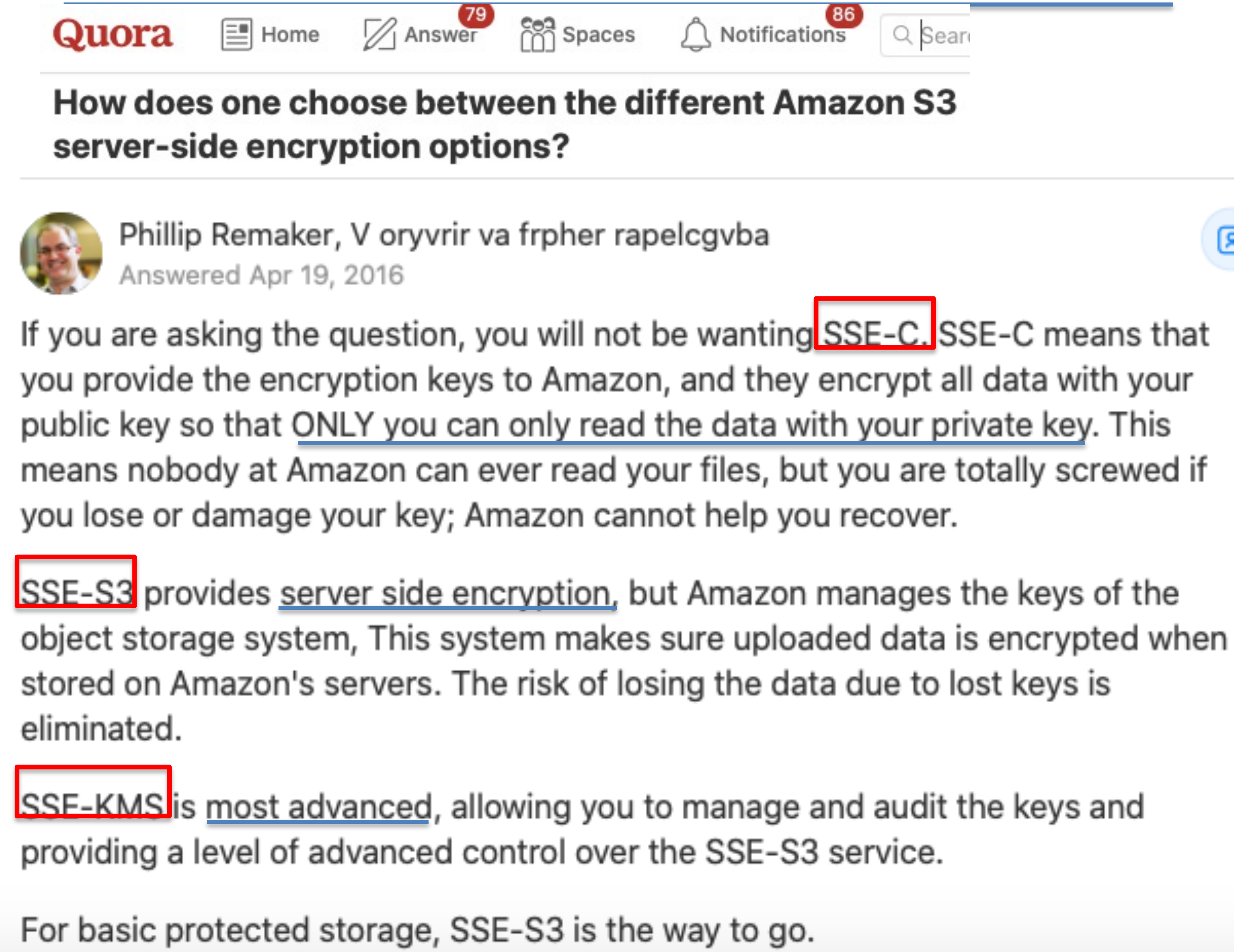
Just now

so is symmetric encryption safer than asymmetric? symmetric doesn't use prime factorization for key generation. if so, why not just use really long keys and symmetric?

CSUN
CALIFORNIA STATE UNIVERSITY NORTHRIDGE

Amazon S3 Encryption

DR JEFF SOFTWARE



How does one choose between the different Amazon S3 server-side encryption options?

Phillip Remaker, V oryvrir va frpher rapelcgvba
Answered Apr 19, 2016

If you are asking the question, you will not be wanting SSE-C. SSE-C means that you provide the encryption keys to Amazon, and they encrypt all data with your public key so that ONLY you can only read the data with your private key. This means nobody at Amazon can ever read your files, but you are totally screwed if you lose or damage your key; Amazon cannot help you recover.

SSE-S3 provides server side encryption, but Amazon manages the keys of the object storage system, This system makes sure uploaded data is encrypted when stored on Amazon's servers. The risk of losing the data due to lost keys is eliminated.

SSE-KMS is most advanced, allowing you to manage and audit the keys and providing a level of advanced control over the SSE-S3 service.

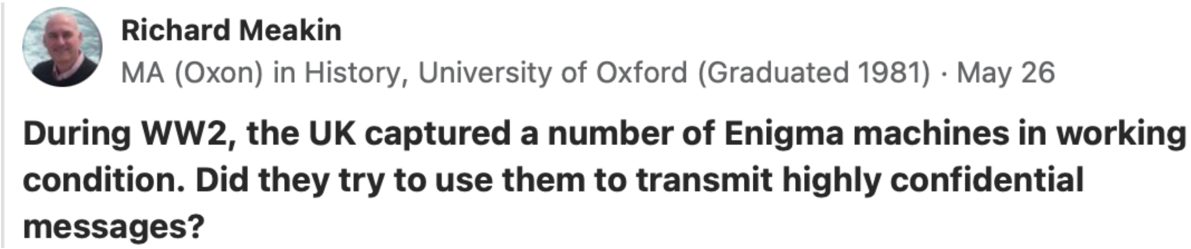
For basic protected storage, SSE-S3 is the way to go.

Cryptography

Enigma

Encrypt: Enigma

Quora



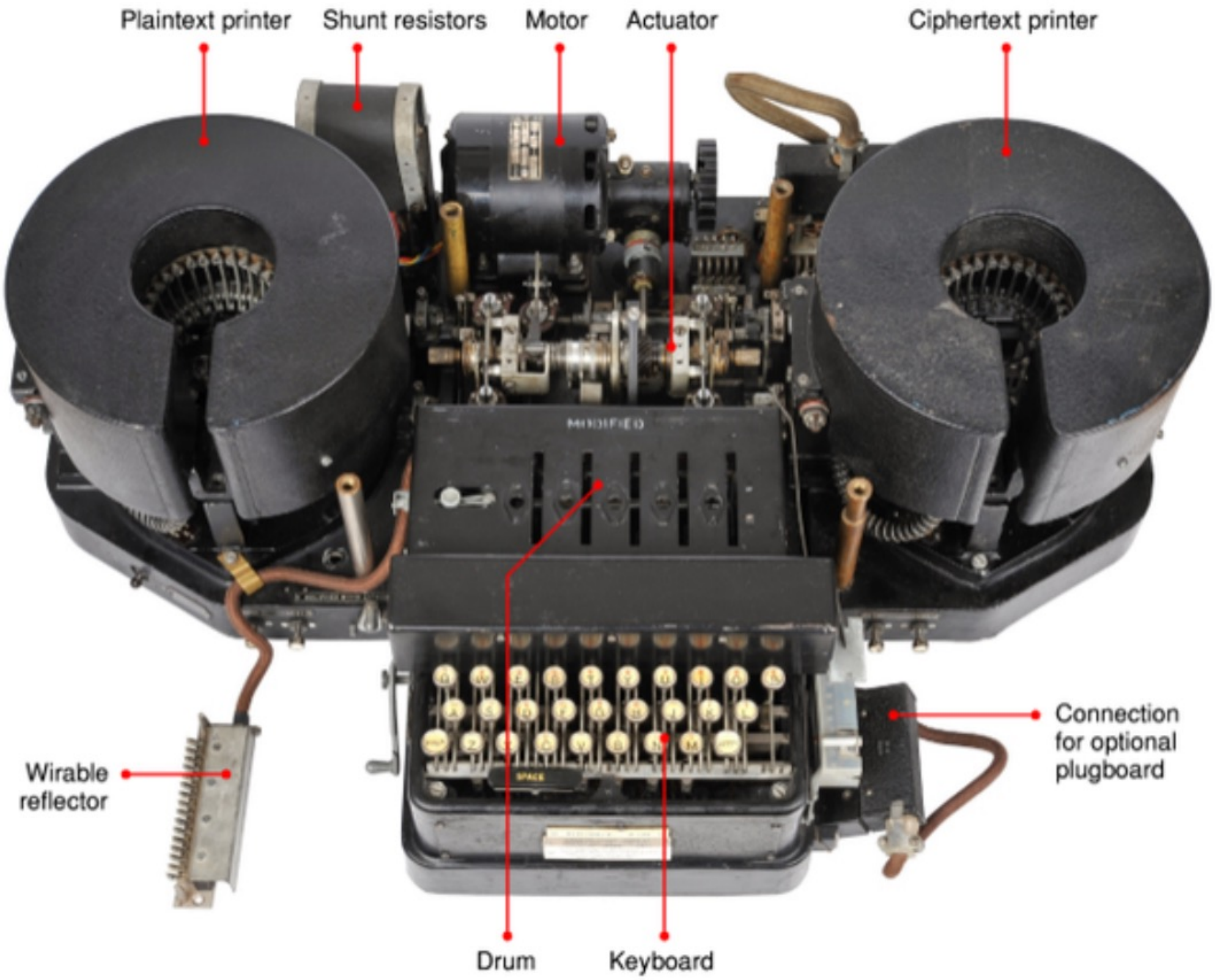
Richard Meakin
MA (Oxon) in History, University of Oxford (Graduated 1981) · May 26

During WW2, the UK captured a number of Enigma machines in working condition. Did they try to use them to transmit highly confidential messages?

They didn't need to. The Enigma machine itself was not in any way secret as it was commercially available in various forms and sold by the German firm Scherbius & Ritter from 1923 onwards.
The British developed the Typex machine from commercial enigma and used it from 1937 onwards, in fact the machine was originally called the "RAF Enigma with Type X attachments".
Typex was similar to Enigma but contained five two part rotors (rotor and slug), each of which had multiple notches that would turn the next rotor.
Initially Typex machines had no plugboard but one (and in some cases two) were introduced later.

Encrypt: Enigma

Richard Meakin
MA (Oxon) in History, University of Oxford



British/Commonwealth Typex Mark 23 machine (courtesy of the Crypto Museum)

Quora

Richard Meakin
MA (Oxon) in History, University of Oxford

Encrypt: Enigma

Enigma messages were typed, enciphered, transmitted, received, deciphered, and written again, while Type messages were typed and then automatically enciphered and transmitted all in one step, with the reverse also true. Messages were also automatically printed onto paper tape in both clear text and cipher.

Although ***Typex*** was vulnerable to some of the same cryptanalytic attacks that were used on the Enigma, the German naval cipher group Beobachtungsdienst (B-Dienst or observation service) apparently spent only around six weeks trying to crack the code before concluding that the extra wheel made the system "unbreakable".

Typex machines remained in use into the 1950s with apparently the last ones being used by the New Zealand military up to 1973.

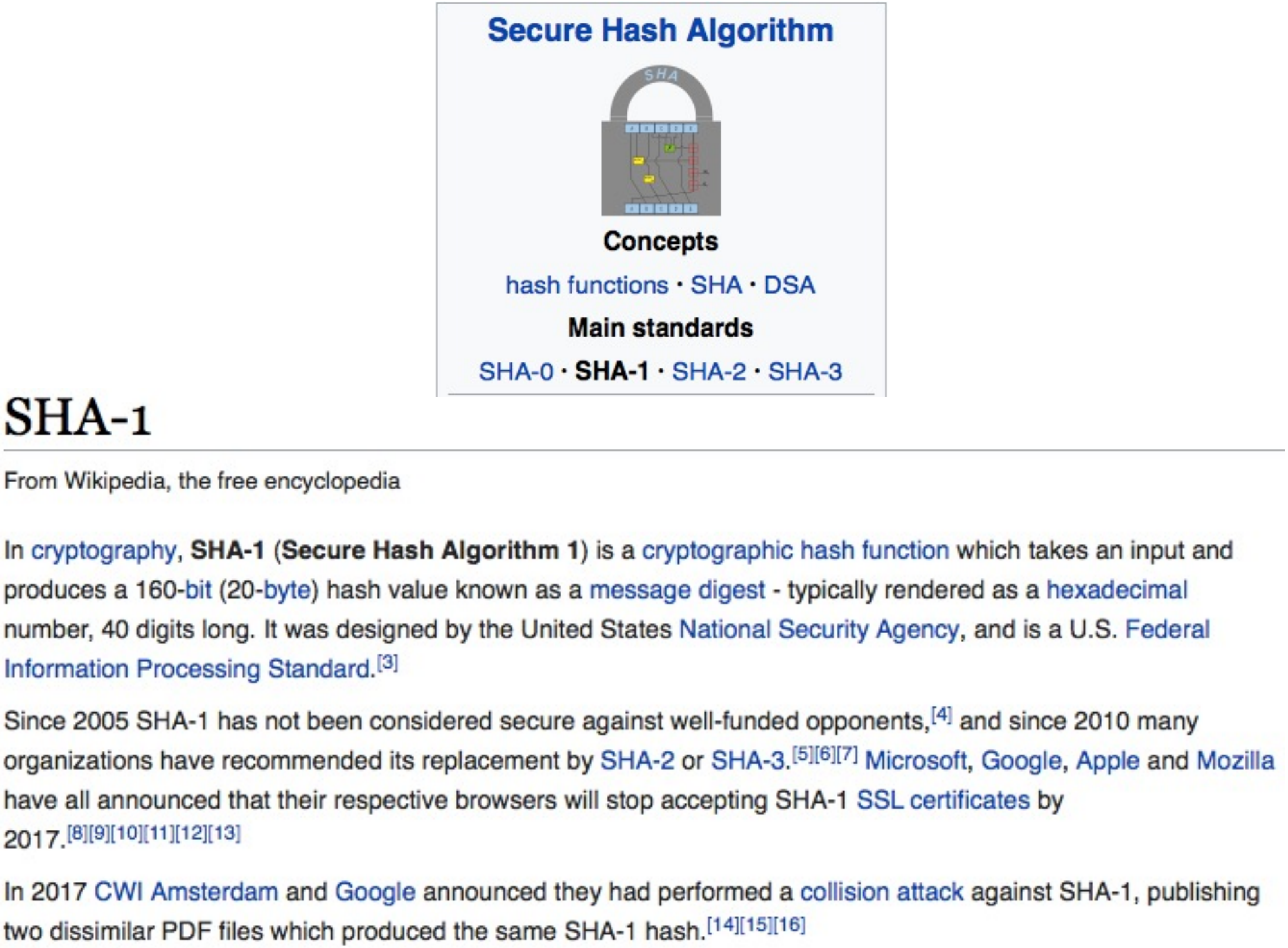
Cryptography

Hashing

CSUN CALIFORNIA STATE UNIVERSITY NORTHRIDGE

SHA Hashing

DR JEFF SOFTWARE
©Jeff Drobman
2017-23



Secure Hash Algorithm

Concepts

hash functions · SHA · DSA

Main standards

SHA-0 · **SHA-1** · SHA-2 · SHA-3

SHA-1

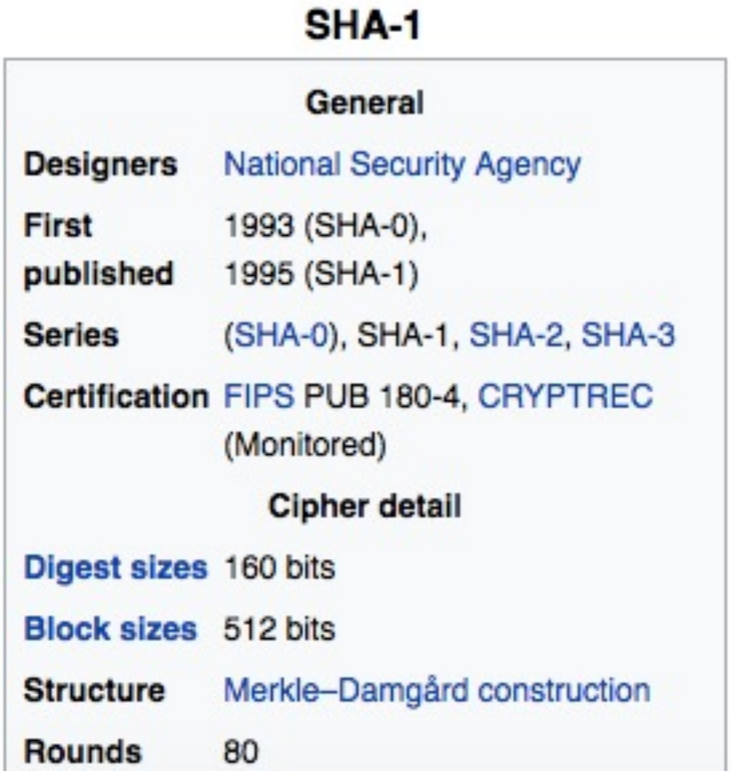
From Wikipedia, the free encyclopedia

In cryptography, **SHA-1** (**Secure Hash Algorithm 1**) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest - typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.[3]

Since 2005 SHA-1 has not been considered secure against well-funded opponents,[4] and since 2010 many organizations have recommended its replacement by SHA-2 or SHA-3.[5][6][7] Microsoft, Google, Apple and Mozilla have all announced that their respective browsers will stop accepting SHA-1 SSL certificates by 2017.[8][9][10][11][12][13]

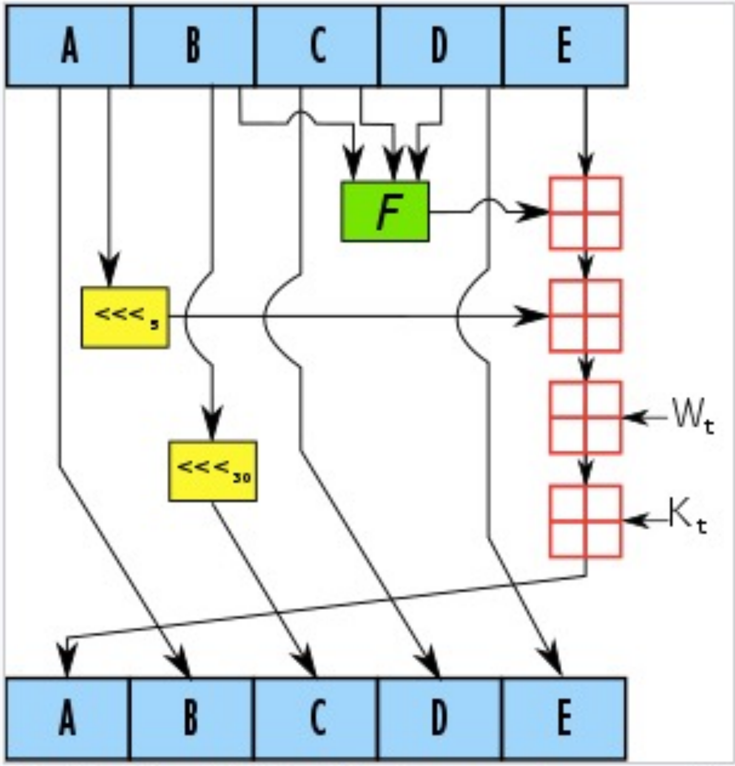
In 2017 CWI Amsterdam and Google announced they had performed a collision attack against SHA-1, publishing two dissimilar PDF files which produced the same SHA-1 hash.[14][15][16]

SHA Hashing



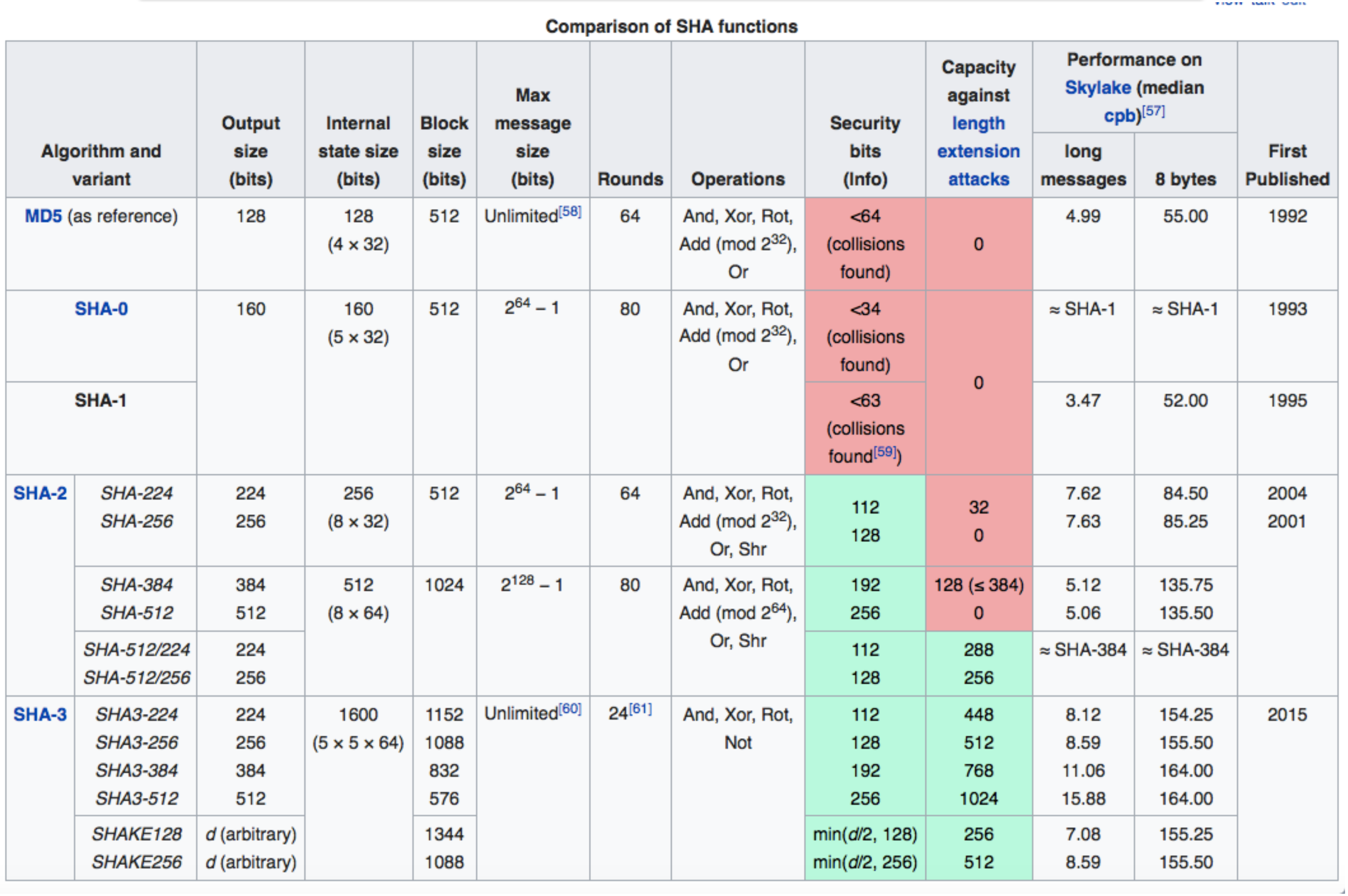
SHA-1

General	
Designers	National Security Agency
First published	1993 (SHA-0), 1995 (SHA-1)
Series	(SHA-0), SHA-1, SHA-2, SHA-3
Certification	FIPS PUB 180-4, CRYPTREC (Monitored)
Cipher detail	
Digest sizes	160 bits
Block sizes	512 bits
Structure	Merkle–Damgård construction
Rounds	80



One iteration within the SHA-1 compression function:
A, B, C, D and E are 32-bit words of the state;
F is a nonlinear function that varies;
$\lll_n$ denotes a left bit rotation by *n* places;
n varies for each operation;
W_t is the expanded message word of round t;
K_t is the round constant of round t;
⊞ denotes addition modulo 2^{32}.

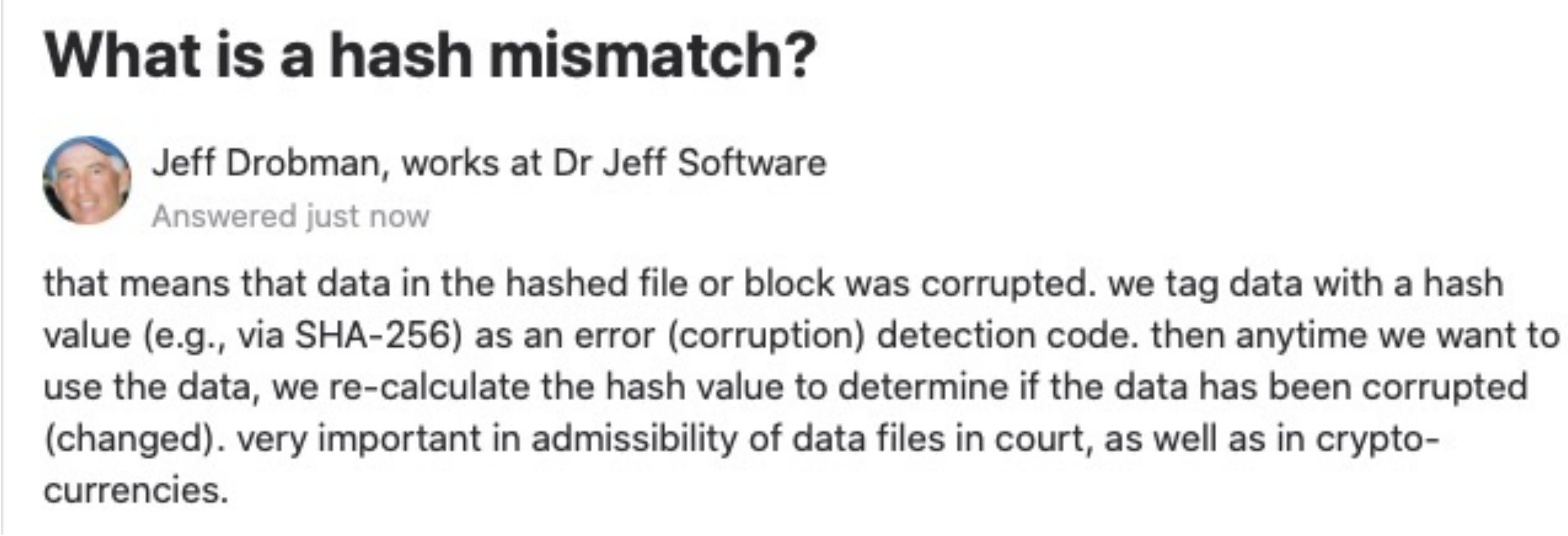
SHA Hashing



Comparison of SHA functions

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security bits (Info)	Capacity against length extension attacks	Performance on Skylake (median cpb)[57]		First Published
										long messages	8 bytes	
MD5 (as reference)		128	128 (4 × 32)	512	Unlimited[58]	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	0	4.99	55.00	1992
SHA-0		160	160 (5 × 32)	512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<34 (collisions found)	0	≈ SHA-1	≈ SHA-1	1993
SHA-1								<63 (collisions found[59])		3.47	52.00	1995
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	32 0	7.62 7.63	84.50 85.25	2004 2001
	SHA-384 *SHA-512*	384 512	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256	128 (≤ 384) 0	5.12 5.06	135.75 135.50	
	SHA-512/224 *SHA-512/256*	224 256						112 128	288 256	≈ SHA-384	≈ SHA-384	
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	Unlimited[60]	24[61]	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024	8.12 8.59 11.06 15.88	154.25 155.50 164.00 164.00	2015
	SHAKE128 *SHAKE256*	*d* (arbitrary) *d* (arbitrary)		1344 1088				min(*d*/2, 128) min(*d*/2, 256)	256 512	7.08 8.59	155.25 155.50	

Hash Mismatch



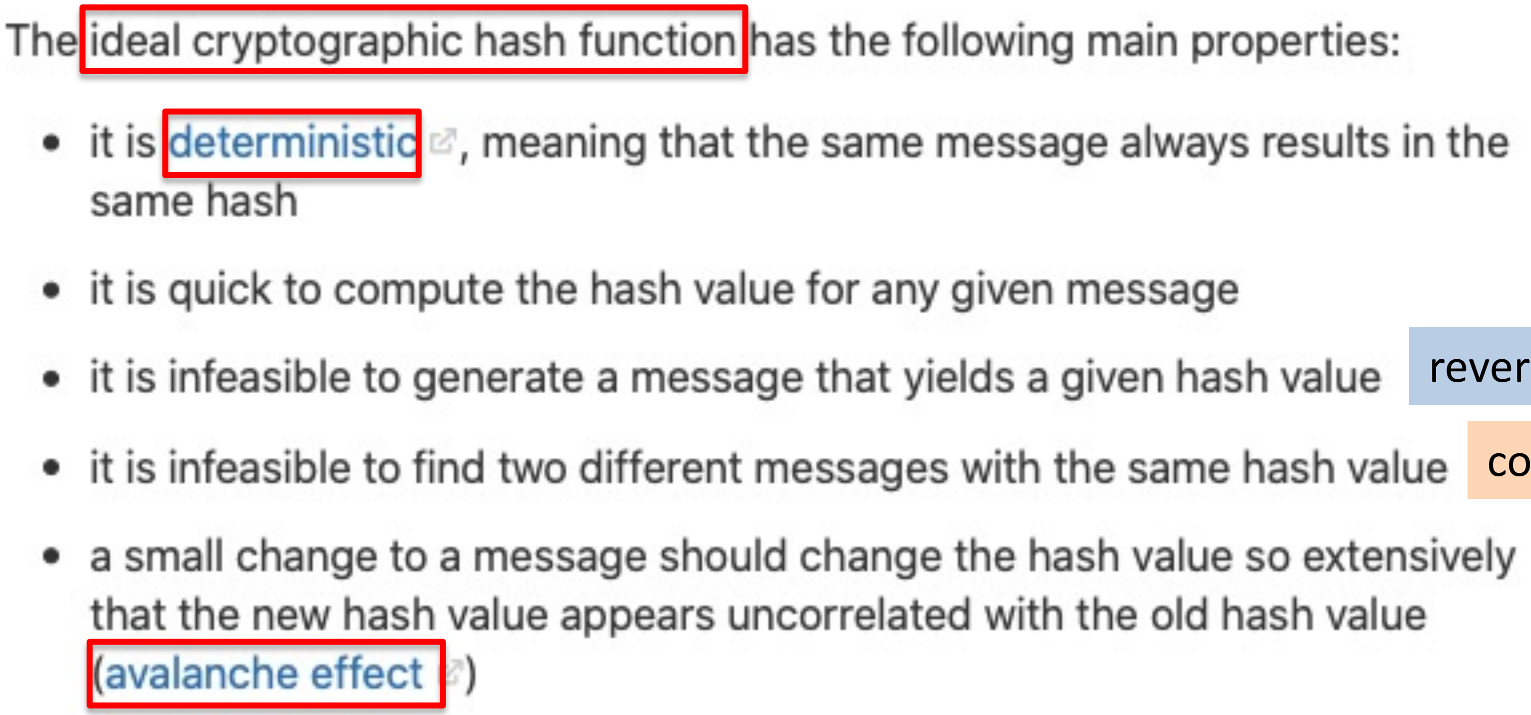
What is a hash mismatch?

Jeff Drobman, works at Dr Jeff Software

Answered just now

that means that data in the hashed file or block was corrupted. we tag data with a hash value (e.g., via SHA-256) as an error (corruption) detection code. then anytime we want to use the data, we re-calculate the hash value to determine if the data has been corrupted (changed). very important in admissibility of data files in court, as well as in crypto-currencies.

Re-Hash



The ideal cryptographic hash function has the following main properties:

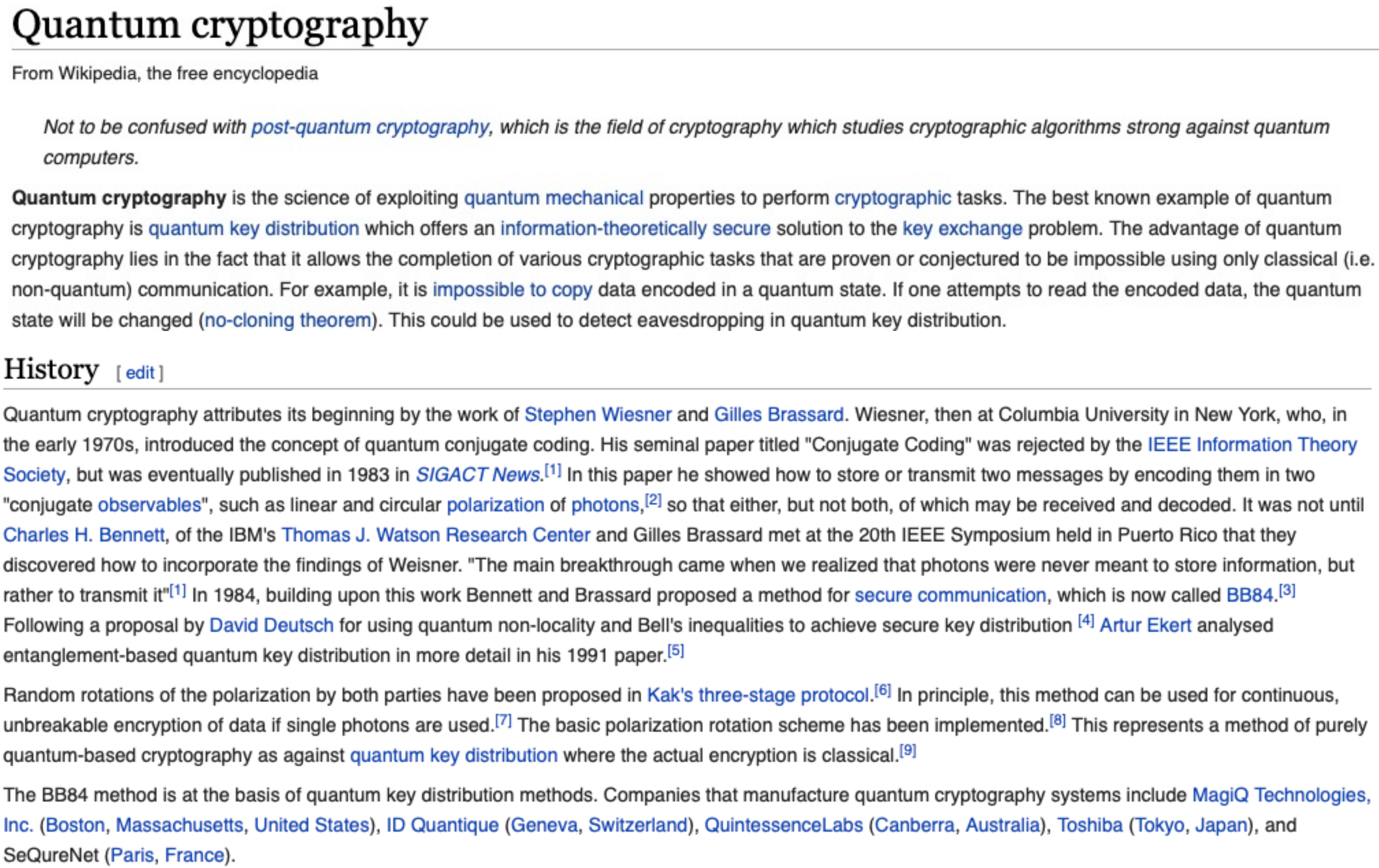
- it is deterministic, meaning that the same message always results in the same hash
- it is quick to compute the hash value for any given message
- it is infeasible to generate a message that yields a given hash value
- it is infeasible to find two different messages with the same hash value
- a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value (avalanche effect)

reversal

collision

CSUN Layer 8 Club

Quantum Crypto



Quantum cryptography

From Wikipedia, the free encyclopedia

Not to be confused with post-quantum cryptography, which is the field of cryptography which studies cryptographic algorithms strong against quantum computers.

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution.

History [edit]

Quantum cryptography attributes its beginning by the work of Stephen Wiesner and Gilles Brassard. Wiesner, then at Columbia University in New York, who, in the early 1970s, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by the IEEE Information Theory Society, but was eventually published in 1983 in *SIGACT News*.[1] In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of photons,[2] so that either, but not both, of which may be received and decoded. It was not until Charles H. Bennett, of the IBM's Thomas J. Watson Research Center and Gilles Brassard met at the 20th IEEE Symposium held in Puerto Rico that they discovered how to incorporate the findings of Weisner. "The main breakthrough came when we realized that photons were never meant to store information, but rather to transmit it"[1] In 1984, building upon this work Bennett and Brassard proposed a method for secure communication, which is now called BB84.[3] Following a proposal by David Deutsch for using quantum non-locality and Bell's inequalities to achieve secure key distribution [4] Artur Ekert analysed entanglement-based quantum key distribution in more detail in his 1991 paper.[5]

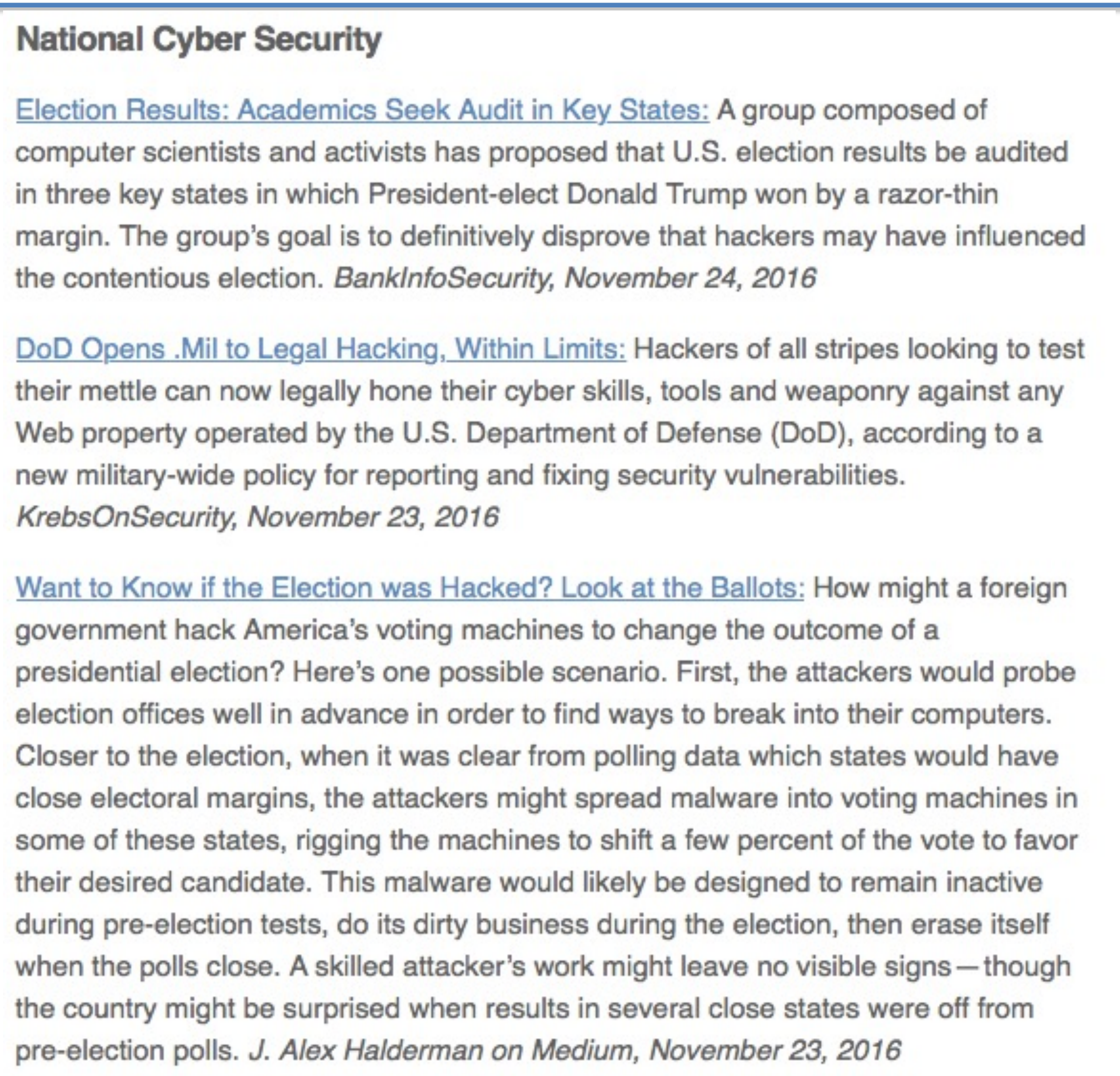
Random rotations of the polarization by both parties have been proposed in Kak's three-stage protocol.[6] In principle, this method can be used for continuous, unbreakable encryption of data if single photons are used.[7] The basic polarization rotation scheme has been implemented.[8] This represents a method of purely quantum-based cryptography as against quantum key distribution where the actual encryption is classical.[9]

The BB84 method is at the basis of quantum key distribution methods. Companies that manufacture quantum cryptography systems include MagiQ Technologies, Inc. (Boston, Massachusetts, United States), ID Quantique (Geneva, Switzerland), QuintessenceLabs (Canberra, Australia), Toshiba (Tokyo, Japan), and SeQureNet (Paris, France).

Cryptography

Cybersecurity

Cybersecurity



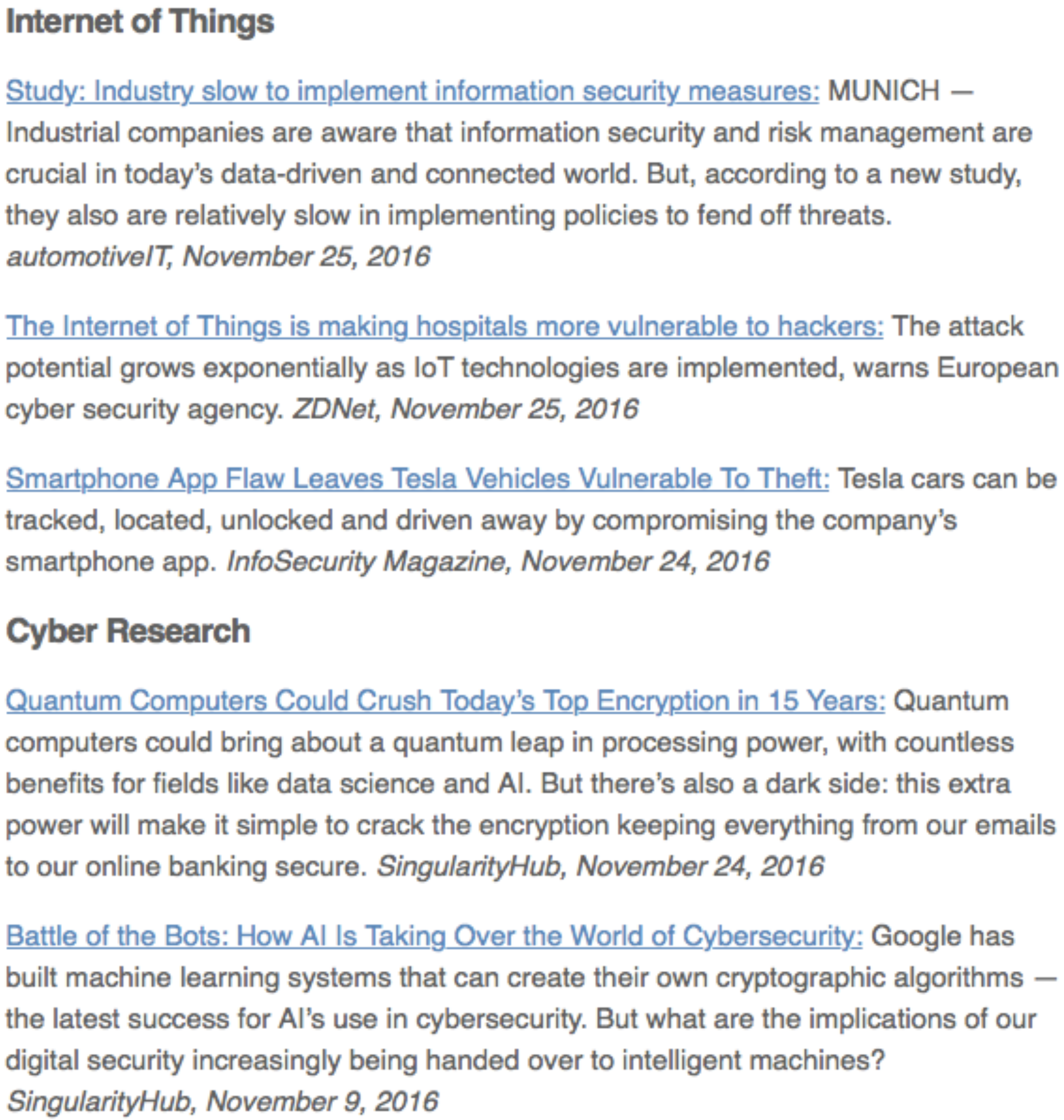
National Cyber Security

Election Results: Academics Seek Audit in Key States: A group composed of computer scientists and activists has proposed that U.S. election results be audited in three key states in which President-elect Donald Trump won by a razor-thin margin. The group's goal is to definitively disprove that hackers may have influenced the contentious election. *BankInfoSecurity, November 24, 2016*

DoD Opens .Mil to Legal Hacking, Within Limits: Hackers of all stripes looking to test their mettle can now legally hone their cyber skills, tools and weaponry against any Web property operated by the U.S. Department of Defense (DoD), according to a new military-wide policy for reporting and fixing security vulnerabilities. *KrebsOnSecurity, November 23, 2016*

Want to Know if the Election was Hacked? Look at the Ballots: How might a foreign government hack America's voting machines to change the outcome of a presidential election? Here's one possible scenario. First, the attackers would probe election offices well in advance in order to find ways to break into their computers. Closer to the election, when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines in some of these states, rigging the machines to shift a few percent of the vote to favor their desired candidate. This malware would likely be designed to remain inactive during pre-election tests, do its dirty business during the election, then erase itself when the polls close. A skilled attacker's work might leave no visible signs — though the country might be surprised when results in several close states were off from pre-election polls. *J. Alex Halderman on Medium, November 23, 2016*

Cybersecurity



Internet of Things

Study: Industry slow to implement information security measures: MUNICH — Industrial companies are aware that information security and risk management are crucial in today's data-driven and connected world. But, according to a new study, they also are relatively slow in implementing policies to fend off threats. *automotiveIT, November 25, 2016*

The Internet of Things is making hospitals more vulnerable to hackers: The attack potential grows exponentially as IoT technologies are implemented, warns European cyber security agency. *ZDNet, November 25, 2016*

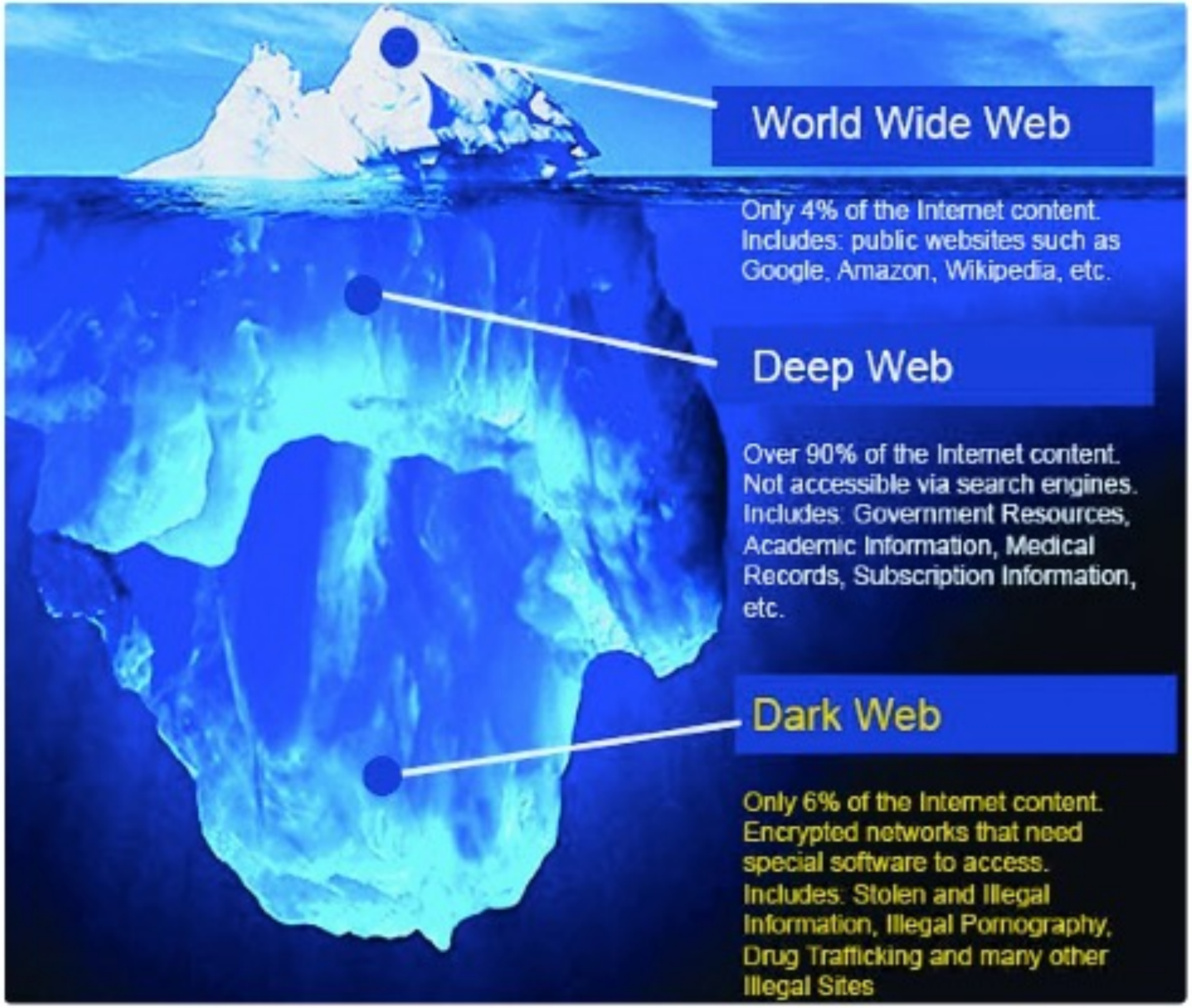
Smartphone App Flaw Leaves Tesla Vehicles Vulnerable To Theft: Tesla cars can be tracked, located, unlocked and driven away by compromising the company's smartphone app. *InfoSecurity Magazine, November 24, 2016*

Cyber Research

Quantum Computers Could Crush Today's Top Encryption in 15 Years: Quantum computers could bring about a quantum leap in processing power, with countless benefits for fields like data science and AI. But there's also a dark side: this extra power will make it simple to crack the encryption keeping everything from our emails to our online banking secure. *SingularityHub, November 24, 2016*

Battle of the Bots: How AI Is Taking Over the World of Cybersecurity: Google has built machine learning systems that can create their own cryptographic algorithms — the latest success for AI's use in cybersecurity. But what are the implications of our digital security increasingly being handed over to intelligent machines? *SingularityHub, November 9, 2016*

Deep & Dark Web



World Wide Web

Only 4% of the Internet content. Includes: public websites such as Google, Amazon, Wikipedia, etc.

Deep Web

Over 90% of the Internet content. Not accessible via search engines. Includes: Government Resources, Academic Information, Medical Records, Subscription Information, etc.

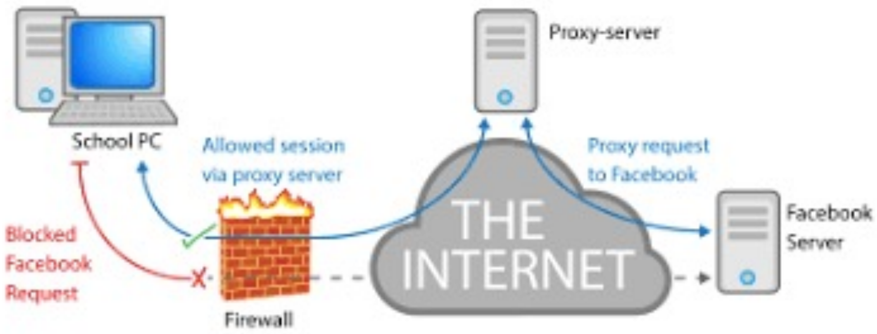
Dark Web

Only 6% of the Internet content. Encrypted networks that need special software to access. Includes: Stolen and Illegal Information, Illegal Pornography, Drug Trafficking and many other Illegal Sites

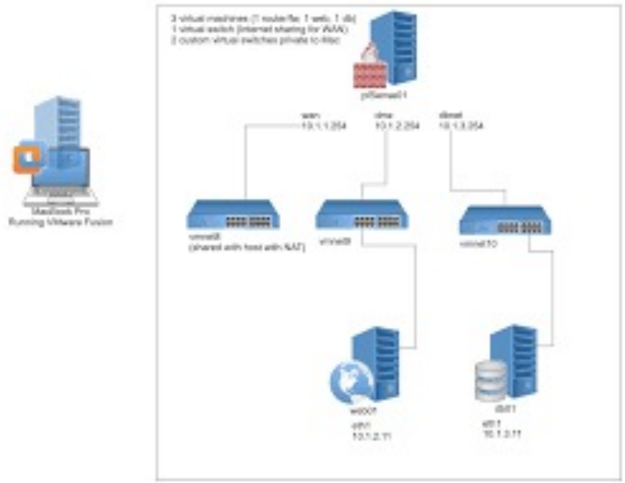
IP Spoofing

Quora Home Answer 66 Sp

Proxy server

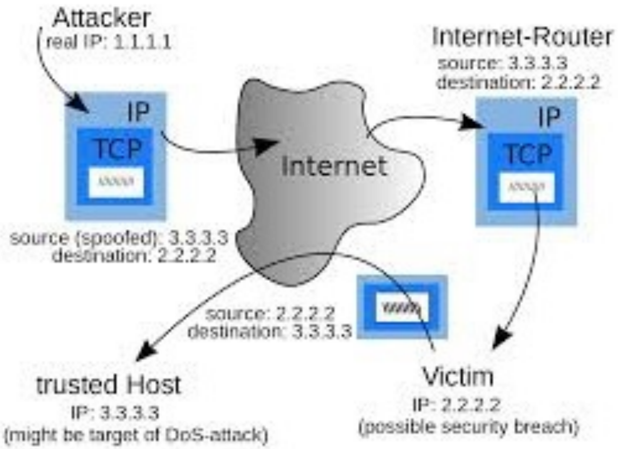


Virtual machines



Quora Home Answer 66

Spoofing the ip address



Geo spoofing with VPNs

Web Vulnerability

LOG4J

ABOUT LOG4J

Cybersecurity exploit

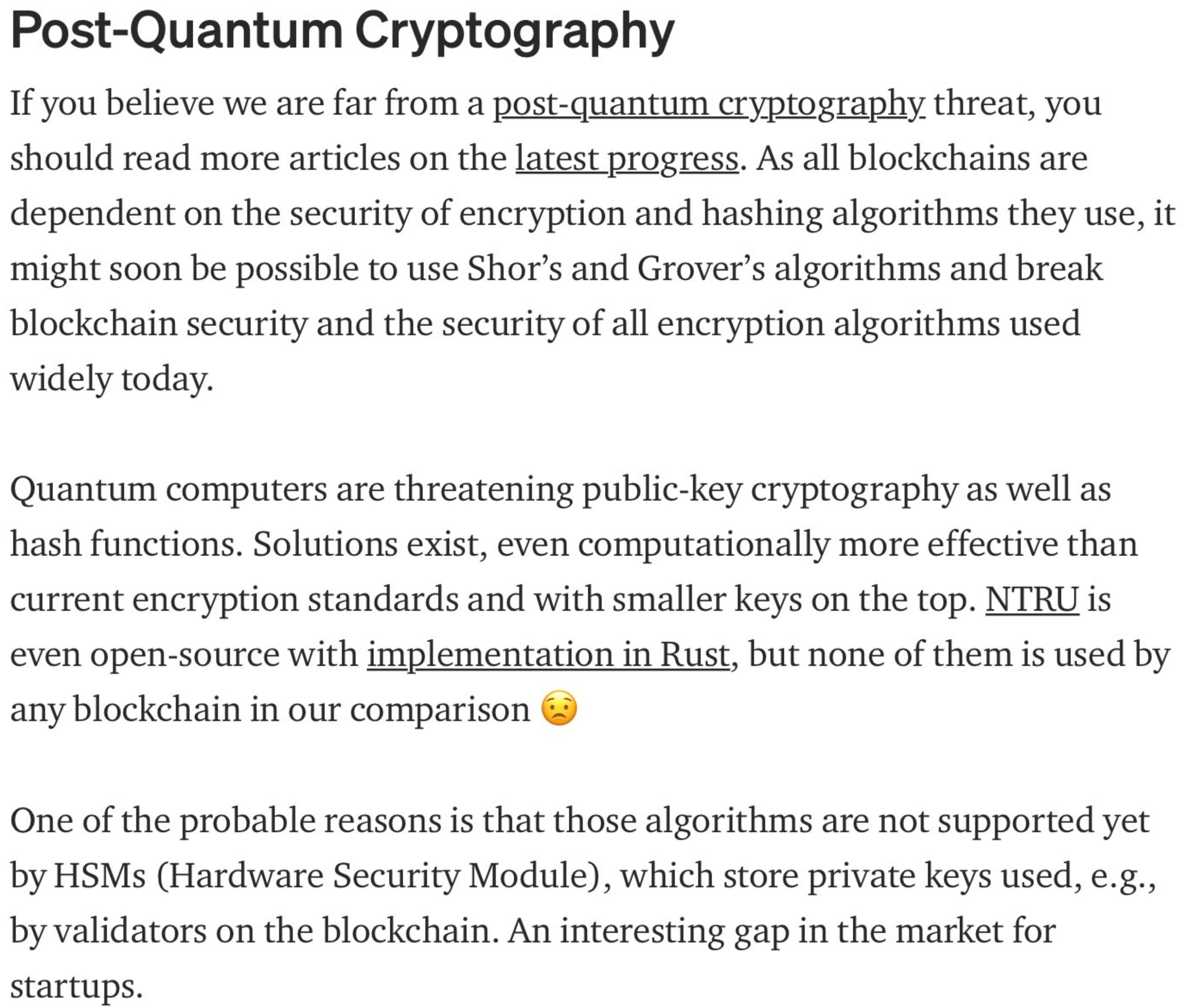
Open-source code, embedded in every Java based product or web service

A CYBER PANDEMIC?

CHECK POINT CEO ON TECH VULNERABILITIES

2-YR YIELD	0.705%
10-YR YIELD	1.482%
30-YR YIELD	1.885%

Quantum



Post-Quantum Cryptography

If you believe we are far from a post-quantum cryptography threat, you should read more articles on the latest progress. As all blockchains are dependent on the security of encryption and hashing algorithms they use, it might soon be possible to use Shor's and Grover's algorithms and break blockchain security and the security of all encryption algorithms used widely today.

Quantum computers are threatening public-key cryptography as well as hash functions. Solutions exist, even computationally more effective than current encryption standards and with smaller keys on the top. NTRU is even open-source with implementation in Rust, but none of them is used by any blockchain in our comparison 😟

One of the probable reasons is that those algorithms are not supported yet by HSMs (Hardware Security Module), which store private keys used, e.g., by validators on the blockchain. An interesting gap in the market for startups.

Cryptography

Blockchains

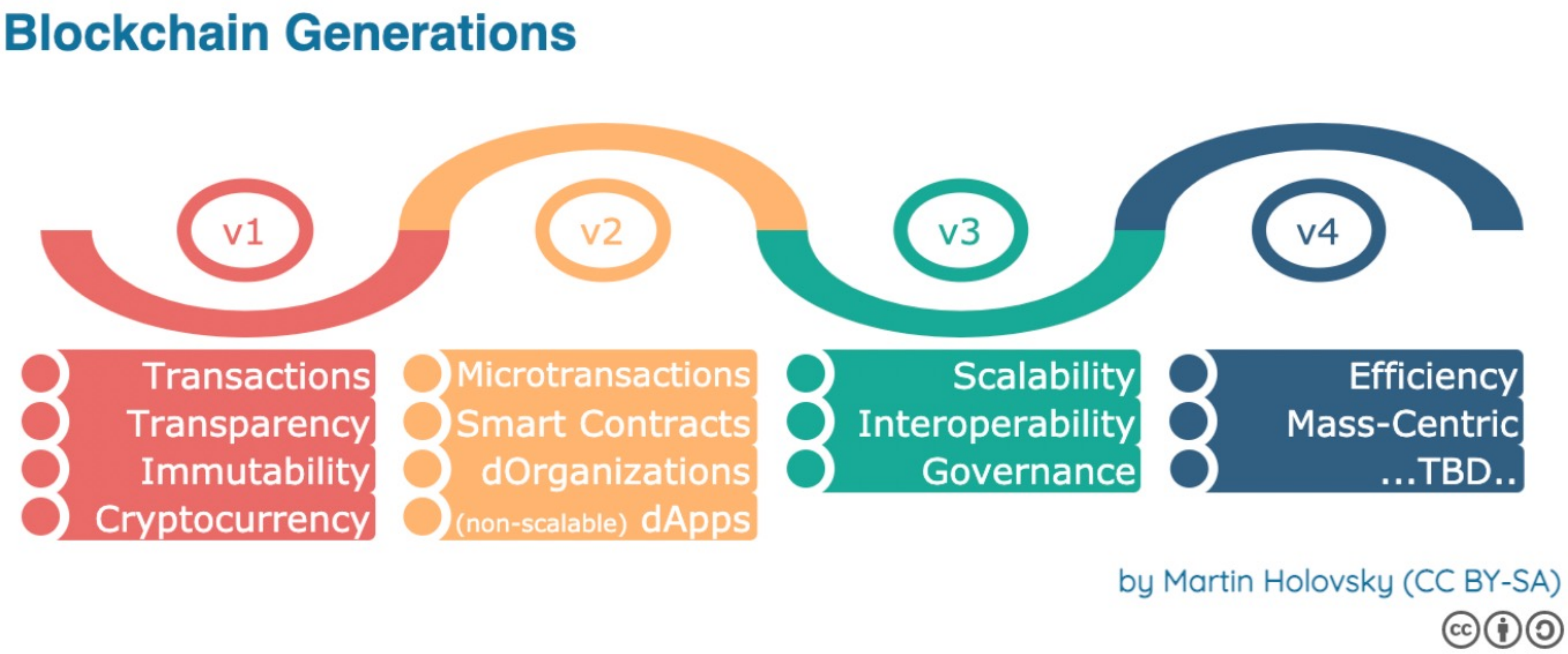
Blockchain Overview

- ❖Blockchain properties
  - ❑ Public vs. Private
  - ❑ Centralized vs. De-centralized
  - ❑ Forks, Shards

- ❖Blockchain applications
  - ❑ Crypto-currency
  - ❑ Financial
    - ▪ FinTech
    - ▪ DeFi
  - ❑ Smart contracts
    - ▪ NFT
  - ❑ Online voting

Generations

Blockchain Generations

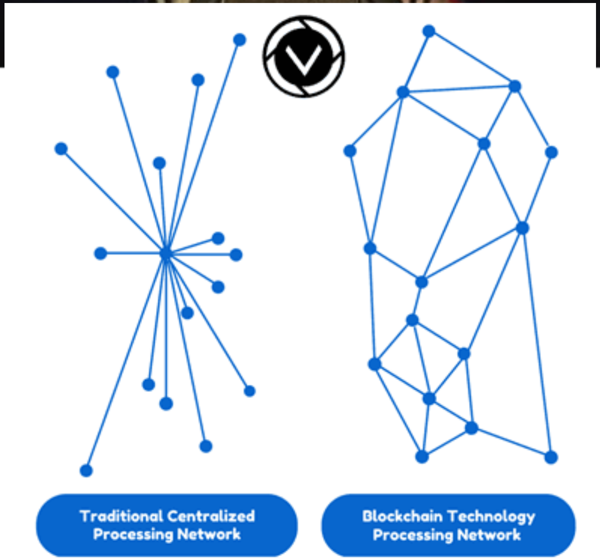


Blockchain Generations

v1	v2	v3	v4
Transactions	Microtransactions	Scalability	Efficiency
Transparency	Smart Contracts	Interoperability	Mass-Centric
Immutability	dOrganizations	Governance	...TBD..
Cryptocurrency	(non-scalable) dApps		

by Martin Holovsky (CC BY-SA)

Blockchains


Traditional Centralized Processing Network
Blockchain Technology Processing Network

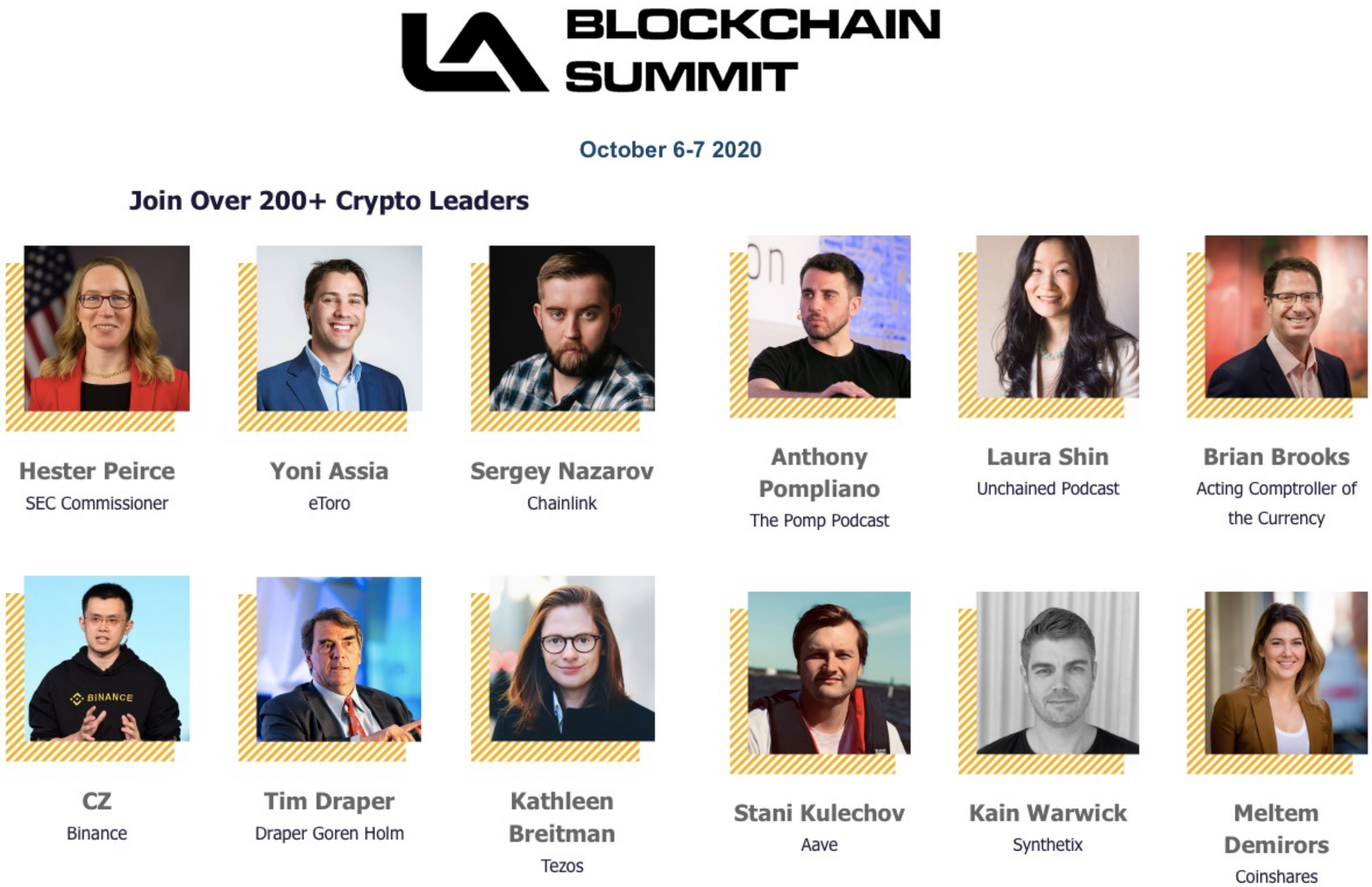
Blockchain for Business:

IBM/CSUN symposium on Blockchain skills, use-cases and the workforce of future

Feb 14th, 2018

CSUN DAVID NAZARIAN COLLEGE OF BUSINESS AND ECONOMICS IBM

CIS 2020



LA BLOCKCHAIN SUMMIT

October 6-7 2020

Join Over 200+ Crypto Leaders

Hester Peirce
SEC Commissioner

Yoni Assia
eToro

Sergey Nazarov
Chainlink

Anthony Pompliano
The Pomp Podcast

Laura Shin
Unchained Podcast

Brian Brooks
Acting Comptroller of the Currency

CZ
Binance

Tim Draper
Draper Goren Holm

Kathleen Breitman
Tezos

Stani Kulechov
Aave

Kain Warwick
Synthetix

Meltem Demirors
Coinshares

CIS 2021

8TH ANNUAL

LA BLOCKCHAIN SUMMIT

November 2-3, 2021

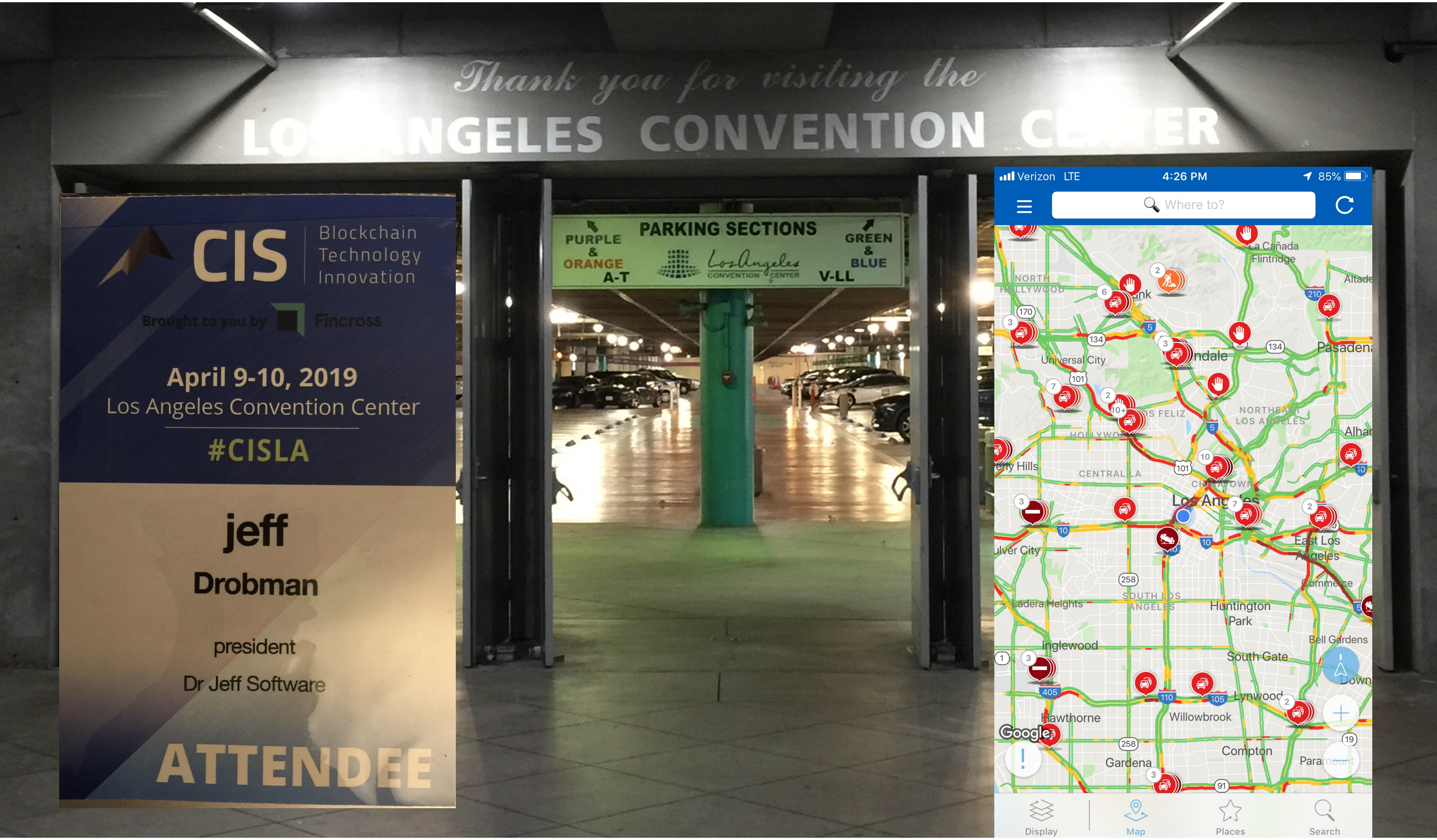
LA Convention Center & Online

LABlockchainSummit.com

PRODUCED BY

DRAPER GOREN HOLM

CIS 2019



CIS Blockchain Technology Innovation

Brought to you by Fincross

April 9-10, 2019
Los Angeles Convention Center

#CISLA

jeff
Drobman
president
Dr Jeff Software

ATTENDEE

CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

CIS 2019

DR JEFF
SOFTWARE

CSUN Blockchain Club (Biz School)

Blockchain Clubs & IEEE

Santiago Cuevas
Executive Advisor | Spring 2019
CSUN Blockchain Society | California State University, Northridge
Santiago.cuevas.480@my.csun.edu|
(818) 231-3409
==
UCLA
https://www.blockchainatucla.com/about

BLOCKCHAIN
ACCELERATION FOUNDATION

blockchain
at ucla

itute of Electrical and Electronics Engineers (IEEE)
California State University, Northridge
sites.ieee.org/sb-csun

CSUN Student Branch

BAF

BAF Membership: https://thebafnetwork.typeform.com/to/jes7CS
BAF Twitter: https://twitter.com/TheBAFNetwork
Next BAF Event: https://live.remo.co/e/the-path-to-mass-adoption

Become a member of BAF if you're interested in participating in BAF's weekly events, Discord, recruiting program, and research opportunities. It's free to join and it only takes five minutes
👉https://thebafnetwork.typeform.com/to/jes7CS

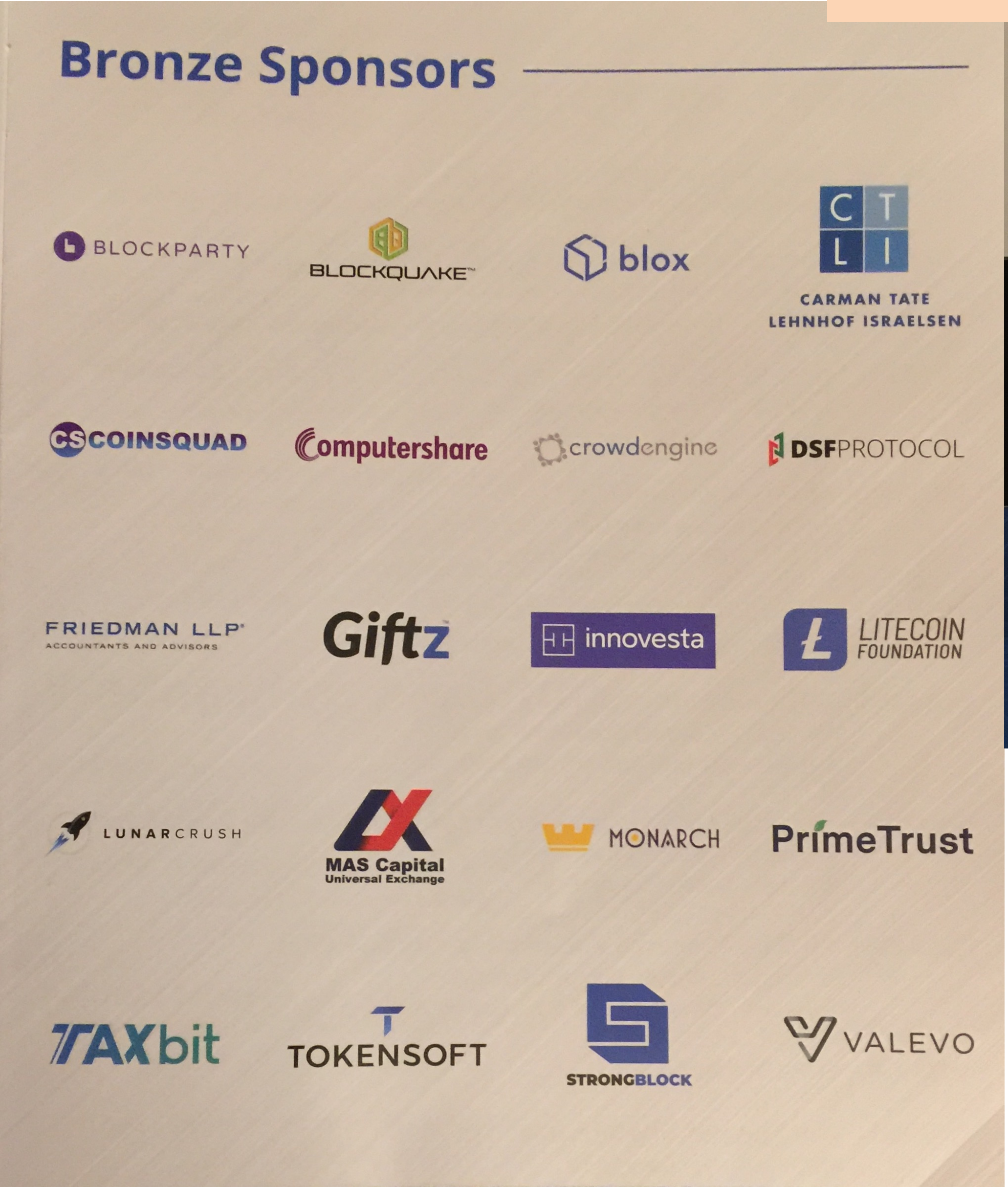
BLOCKCHAIN
ACCELERATION FOUNDATION

Newsletter: https://tinyurl.com/yyz7va94
Twitter: https://twitter.com/FindoraOrg

ALSO! BAF is co-organizing a virtual conference with the top zero-knowledge researchers on October 19th and we would love for you to attend :D It's 100% free and this some of the very best ZK education out there! - https://zkp-privacy-summit.dystopialabs.com/

CIS

Exhibitors



Bronze Sponsors

BLOCKPARTY
BLOCKQUAKE™
blox
CTLI CARMAN TATE LEHNHOF ISRAELSEN
COINSQUAD
Computershare
crowdengine
DSFPROTOCOL
FRIEDMAN LLP® ACCOUNTANTS AND ADVISORS
Giftz
innovesta
LITECOIN FOUNDATION
LUNARCRUSH
MAS Capital Universal Exchange
MONARCH
PrimeTrust
TAXbit
TOKENSOFT
STRONGBLOCK
VALEVO

DSFPROTOCOL
https://dsfprotocol.com • @dsfprotocol

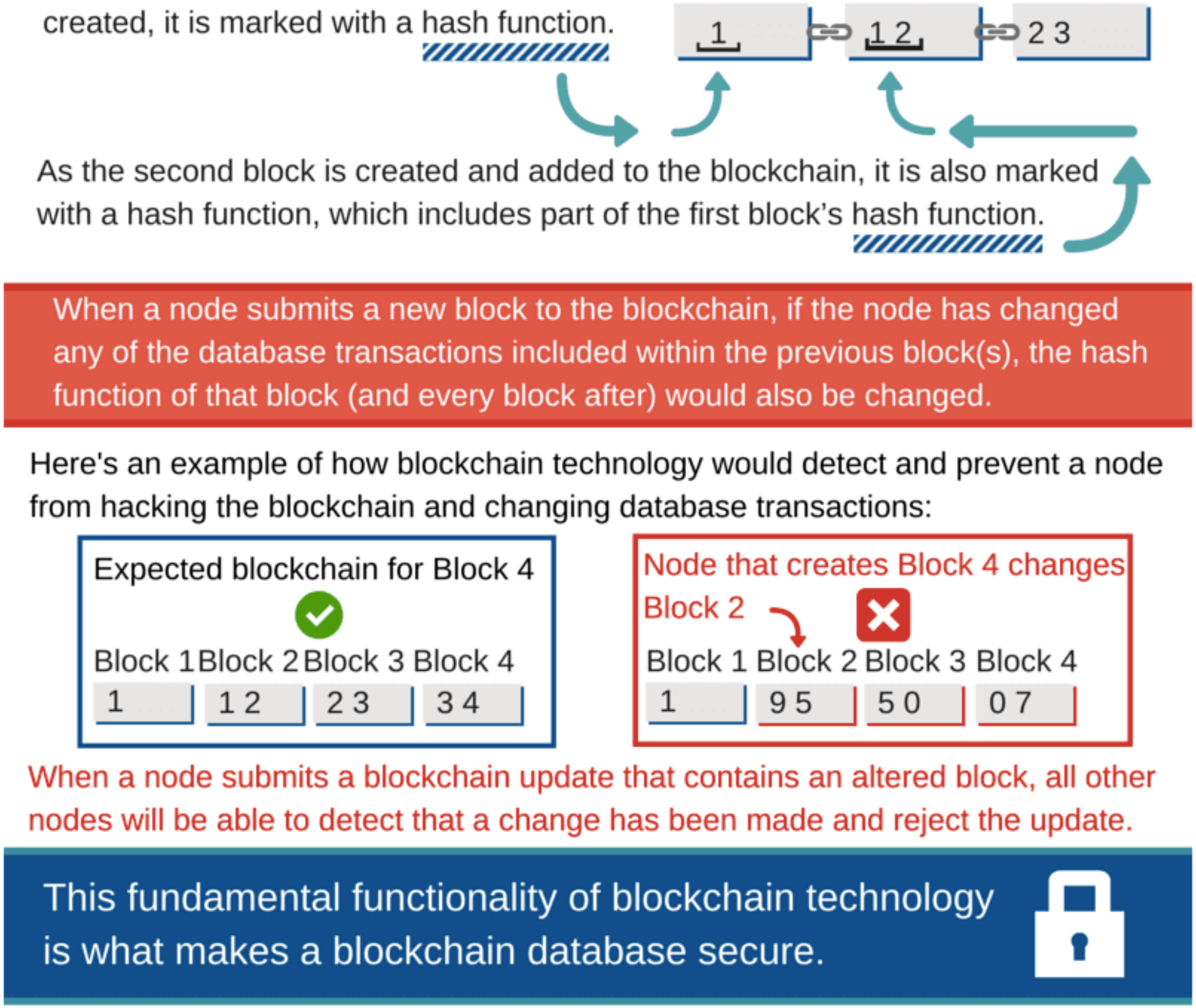
edge

BLOCKCHAIN ACCELERATION FOUNDATION

cyzen℠
Powered by Friedman
Your security, enlightened.
A Friedman LLP Company

COINGENIUS
TRADE SMARTER

Blockchain Hashing



created, it is marked with a hash function.

As the second block is created and added to the blockchain, it is also marked with a hash function, which includes part of the first block's hash function.

When a node submits a new block to the blockchain, if the node has changed any of the database transactions included within the previous block(s), the hash function of that block (and every block after) would also be changed.

Here's an example of how blockchain technology would detect and prevent a node from hacking the blockchain and changing database transactions:

Expected blockchain for Block 4 ✓

Block 1	Block 2	Block 3	Block 4
1	1 2	2 3	3 4

Node that creates Block 4 changes Block 2 ☒

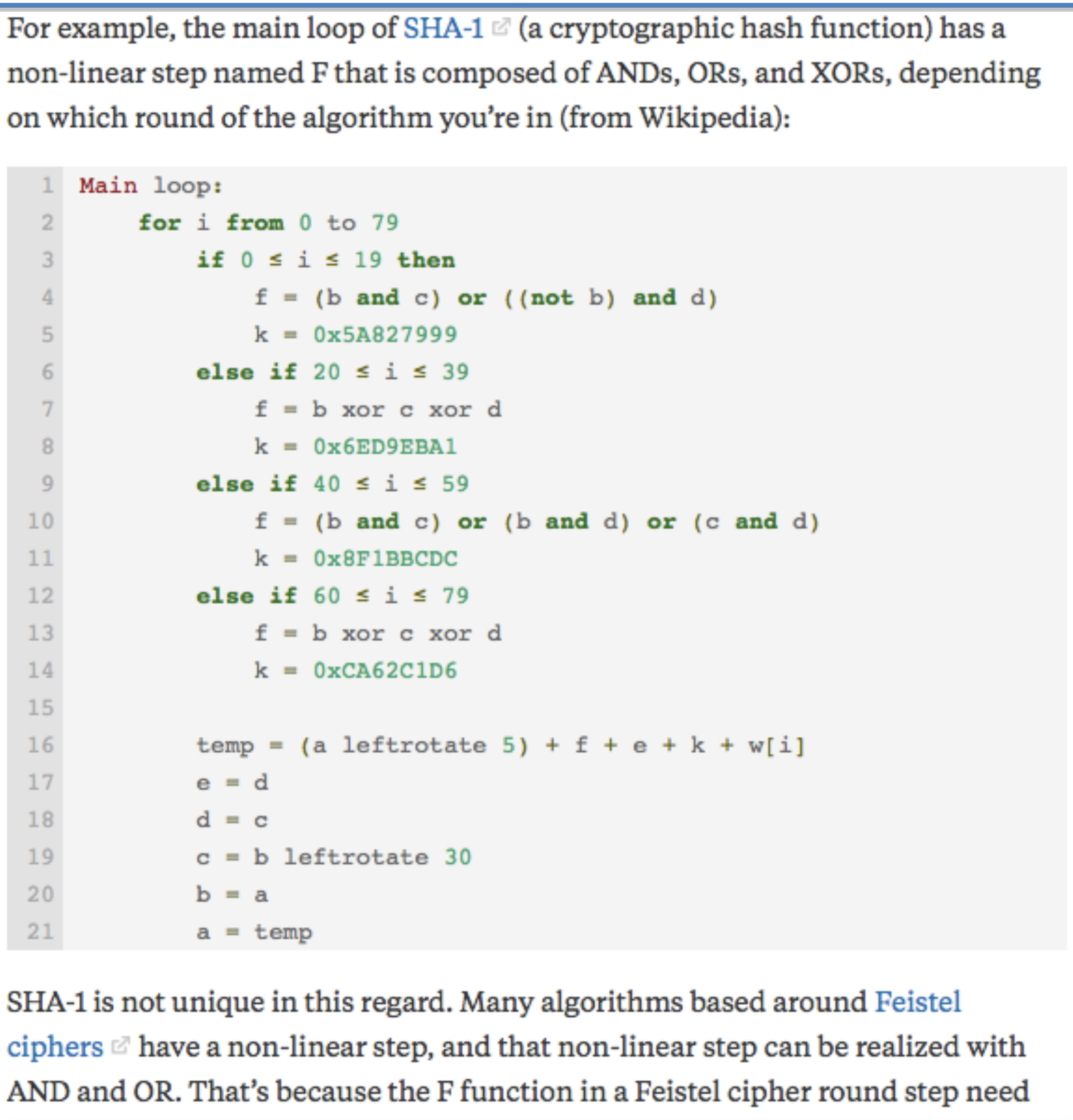
Block 1	Block 2	Block 3	Block 4
1	9 5	5 0	0 7

When a node submits a blockchain update that contains an altered block, all other nodes will be able to detect that a change has been made and reject the update.

This fundamental functionality of blockchain technology is what makes a blockchain database secure.

Blockchains: SHA-1

Main Loop



For example, the main loop of SHA-1 (a cryptographic hash function) has a non-linear step named F that is composed of ANDs, ORs, and XORs, depending on which round of the algorithm you're in (from Wikipedia):

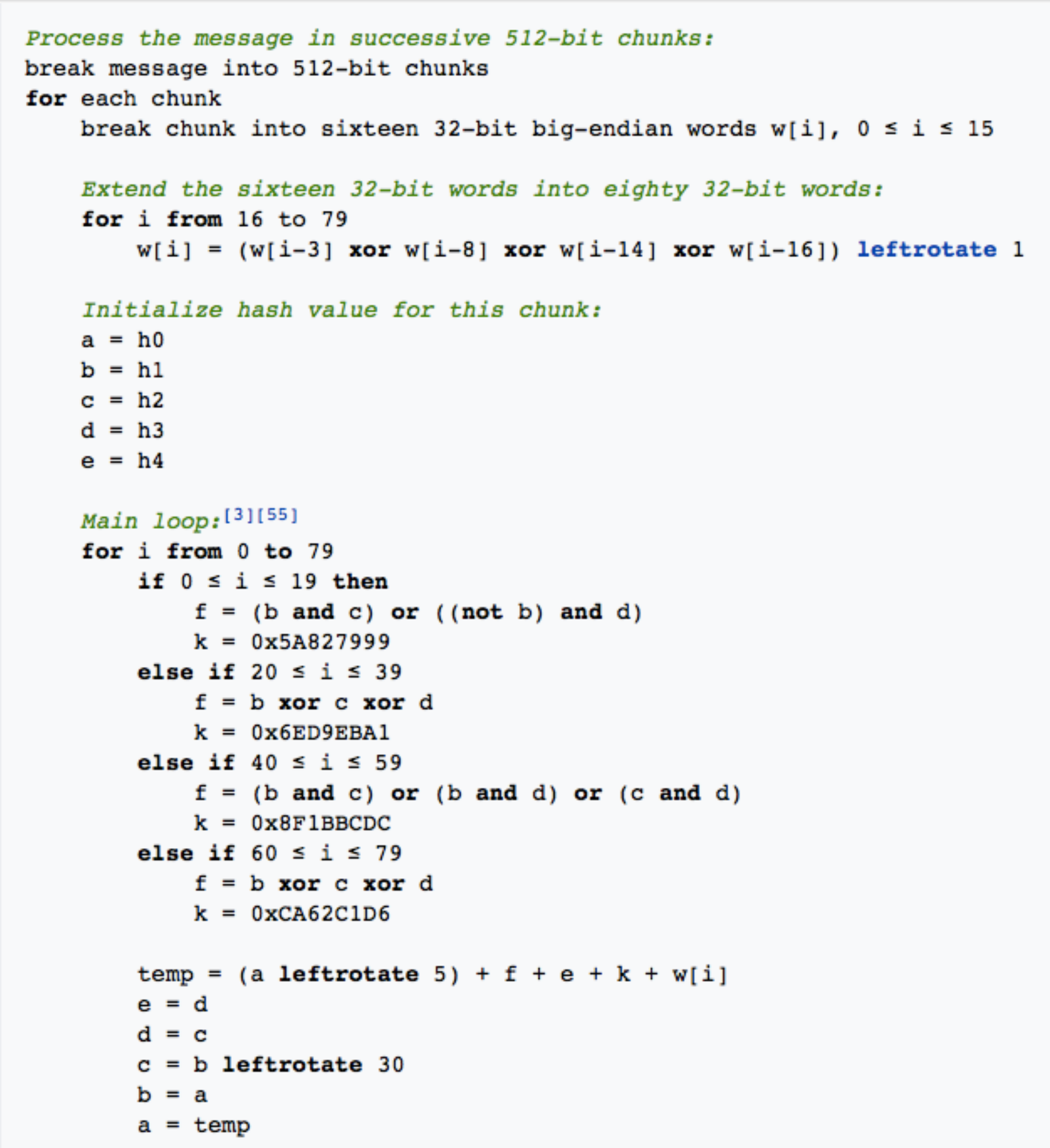
```
Main loop:
    for i from 0 to 79
        if 0 ≤ i ≤ 19 then
            f = (b and c) or ((not b) and d)
            k = 0x5A827999
        else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = 0x6ED9EBA1
        else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d) or (c and d)
            k = 0x8F1BBCDC
        else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6

        temp = (a leftrotate 5) + f + e + k + w[i]
        e = d
        d = c
        c = b leftrotate 30
        b = a
        a = temp
```

SHA-1 is not unique in this regard. Many algorithms based around Feistel ciphers have a non-linear step, and that non-linear step can be realized with AND and OR. That's because the F function in a Feistel cipher round step need

Blockchains: SHA-1

Body



```
Process the message in successive 512-bit chunks:
break message into 512-bit chunks
for each chunk
    break chunk into sixteen 32-bit big-endian words w[i], 0 ≤ i ≤ 15

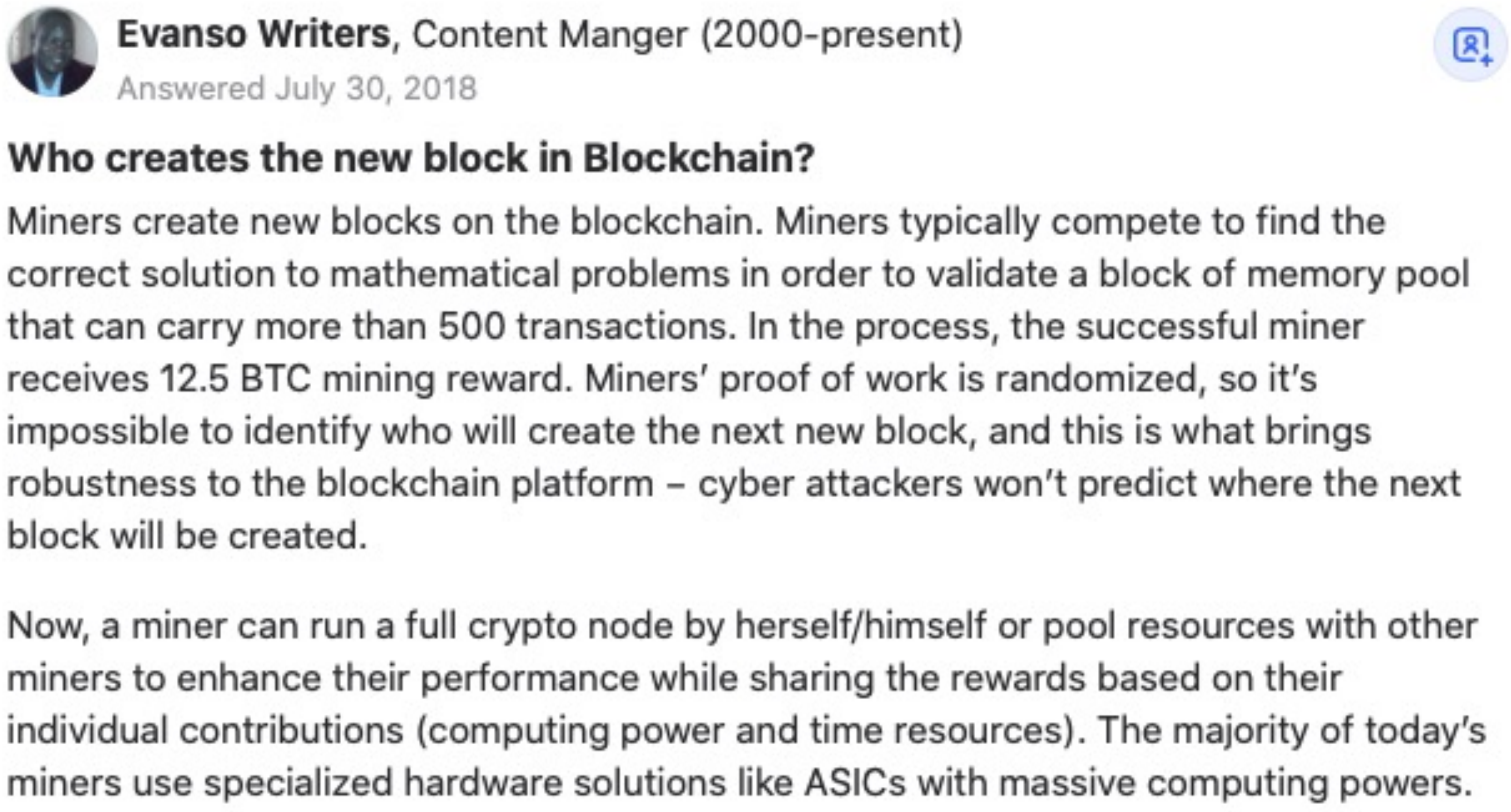
    Extend the sixteen 32-bit words into eighty 32-bit words:
    for i from 16 to 79
        w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) leftrotate 1

    Initialize hash value for this chunk:
    a = h0
    b = h1
    c = h2
    d = h3
    e = h4

    Main loop:[3][55]
    for i from 0 to 79
        if 0 ≤ i ≤ 19 then
            f = (b and c) or ((not b) and d)
            k = 0x5A827999
        else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = 0x6ED9EBA1
        else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d) or (c and d)
            k = 0x8F1BBCDC
        else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6

        temp = (a leftrotate 5) + f + e + k + w[i]
        e = d
        d = c
        c = b leftrotate 30
        b = a
        a = temp
```

Blockchains



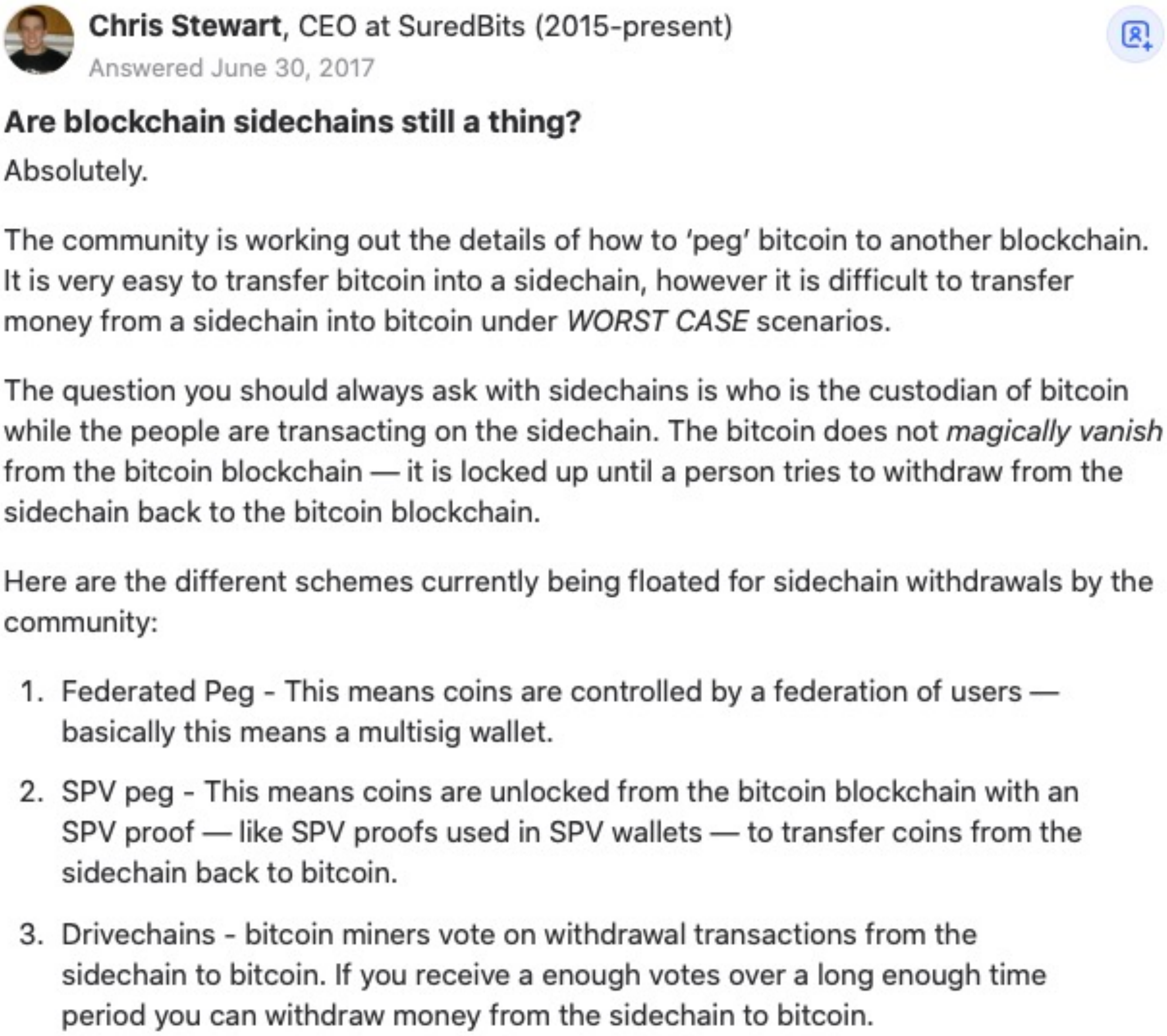
Evanso Writers, Content Manger (2000-present)
Answered July 30, 2018

Who creates the new block in Blockchain?

Miners create new blocks on the blockchain. Miners typically compete to find the correct solution to mathematical problems in order to validate a block of memory pool that can carry more than 500 transactions. In the process, the successful miner receives 12.5 BTC mining reward. Miners' proof of work is randomized, so it's impossible to identify who will create the next new block, and this is what brings robustness to the blockchain platform – cyber attackers won't predict where the next block will be created.

Now, a miner can run a full crypto node by herself/himself or pool resources with other miners to enhance their performance while sharing the rewards based on their individual contributions (computing power and time resources). The majority of today's miners use specialized hardware solutions like ASICs with massive computing powers.

Blockchains



Chris Stewart, CEO at SuredBits (2015-present)

Answered June 30, 2017

Are blockchain sidechains still a thing?

Absolutely.

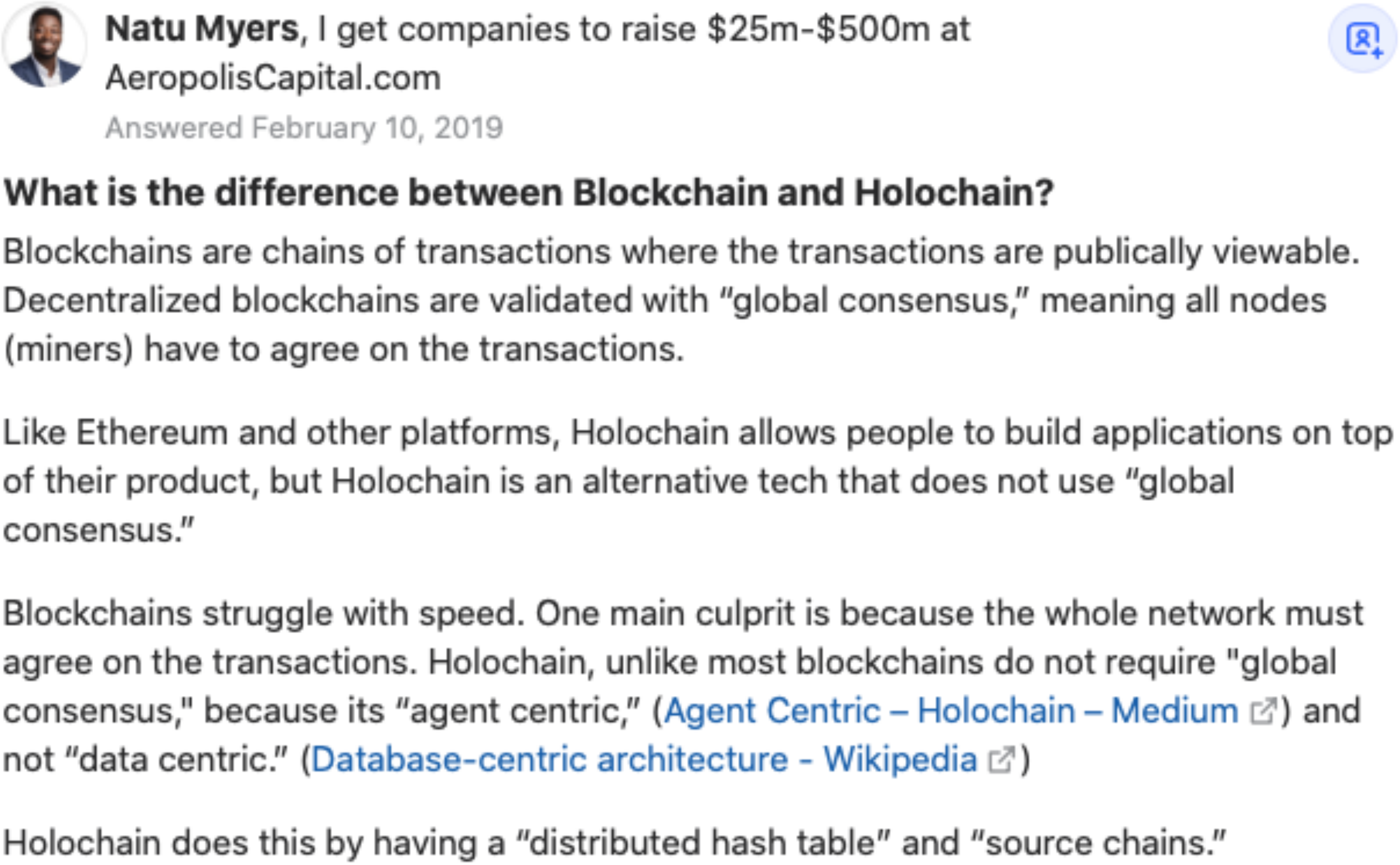
The community is working out the details of how to 'peg' bitcoin to another blockchain. It is very easy to transfer bitcoin into a sidechain, however it is difficult to transfer money from a sidechain into bitcoin under *WORST CASE* scenarios.

The question you should always ask with sidechains is who is the custodian of bitcoin while the people are transacting on the sidechain. The bitcoin does not *magically vanish* from the bitcoin blockchain — it is locked up until a person tries to withdraw from the sidechain back to the bitcoin blockchain.

Here are the different schemes currently being floated for sidechain withdrawals by the community:

1. Federated Peg - This means coins are controlled by a federation of users — basically this means a multisig wallet.
2. SPV peg - This means coins are unlocked from the bitcoin blockchain with an SPV proof — like SPV proofs used in SPV wallets — to transfer coins from the sidechain back to bitcoin.
3. Drivechains - bitcoin miners vote on withdrawal transactions from the sidechain to bitcoin. If you receive a enough votes over a long enough time period you can withdraw money from the sidechain to bitcoin.

Holochain



Natu Myers, I get companies to raise $25m-$500m at AeropolisCapital.com

Answered February 10, 2019

What is the difference between Blockchain and Holochain?

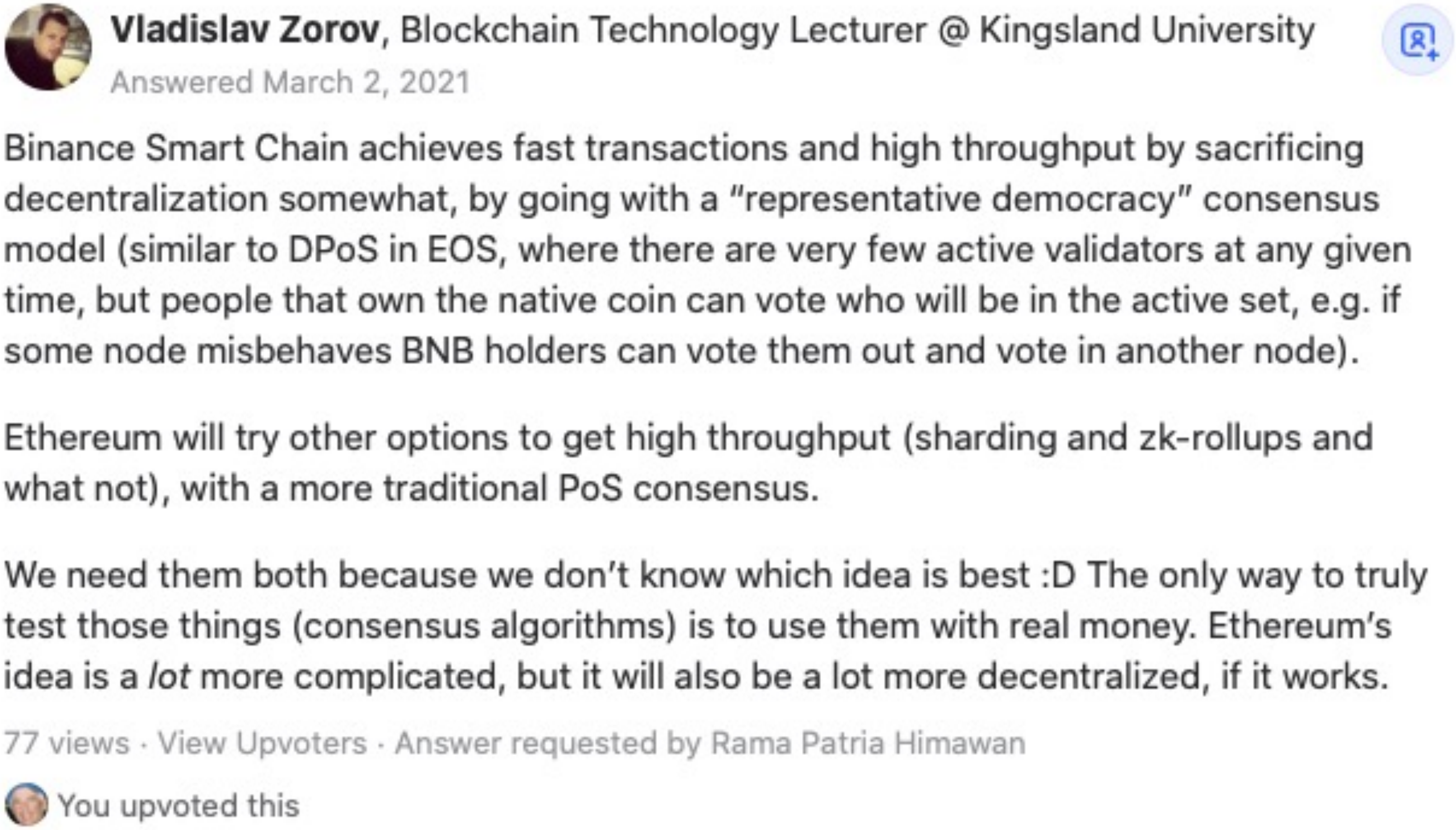
Blockchains are chains of transactions where the transactions are publically viewable. Decentralized blockchains are validated with "global consensus," meaning all nodes (miners) have to agree on the transactions.

Like Ethereum and other platforms, Holochain allows people to build applications on top of their product, but Holochain is an alternative tech that does not use "global consensus."

Blockchains struggle with speed. One main culprit is because the whole network must agree on the transactions. Holochain, unlike most blockchains do not require "global consensus," because its "agent centric," (Agent Centric – Holochain – Medium ↗) and not "data centric." (Database-centric architecture - Wikipedia ↗)

Holochain does this by having a "distributed hash table" and "source chains."

BSC



Vladislav Zorov, Blockchain Technology Lecturer @ Kingsland University
Answered March 2, 2021

Binance Smart Chain achieves fast transactions and high throughput by sacrificing decentralization somewhat, by going with a "representative democracy" consensus model (similar to DPoS in EOS, where there are very few active validators at any given time, but people that own the native coin can vote who will be in the active set, e.g. if some node misbehaves BNB holders can vote them out and vote in another node).

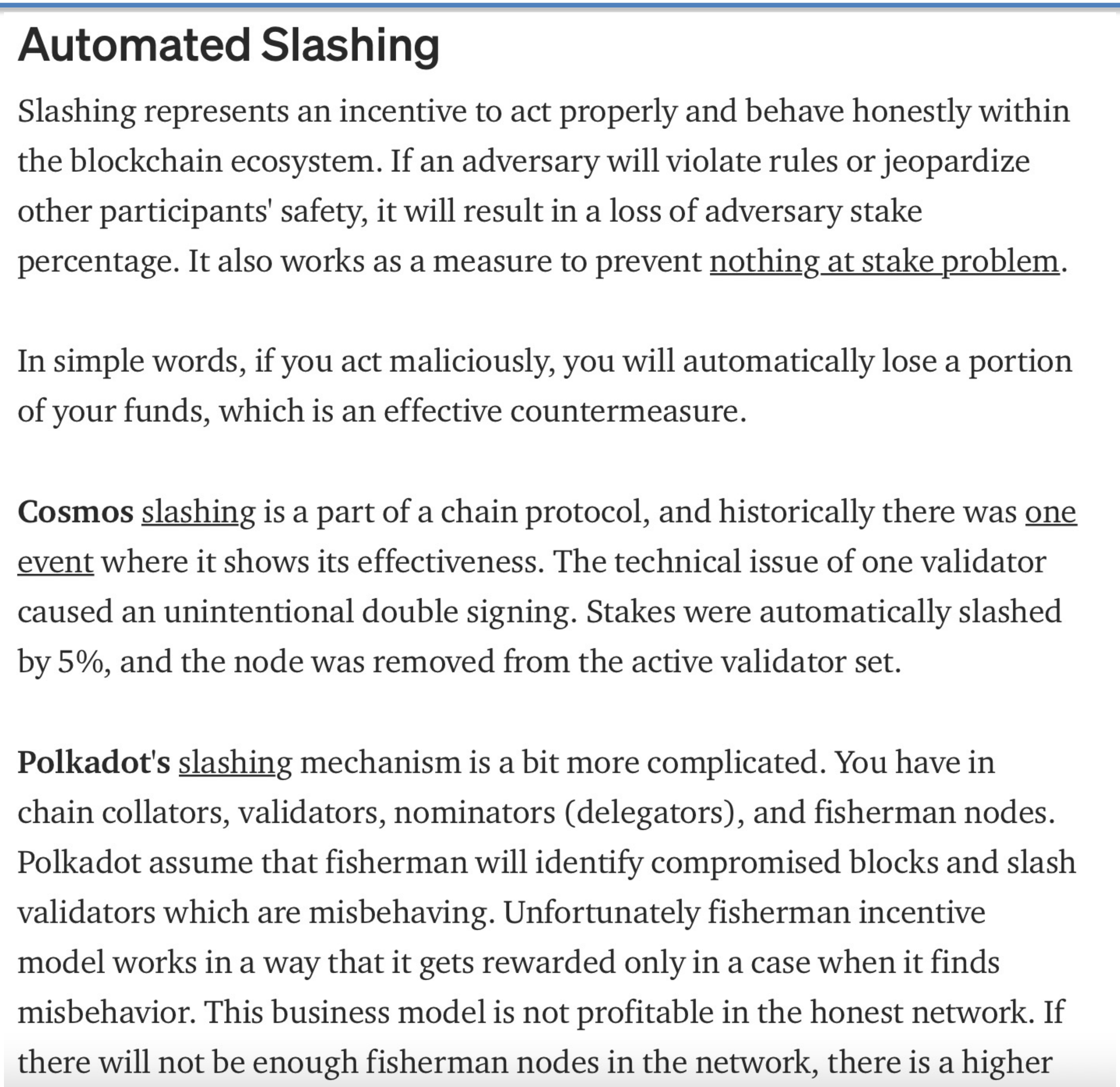
Ethereum will try other options to get high throughput (sharding and zk-rollups and what not), with a more traditional PoS consensus.

We need them both because we don't know which idea is best :D The only way to truly test those things (consensus algorithms) is to use them with real money. Ethereum's idea is a *lot* more complicated, but it will also be a lot more decentralized, if it works.

77 views · View Upvoters · Answer requested by Rama Patria Himawan

You upvoted this

Slashing



Automated Slashing

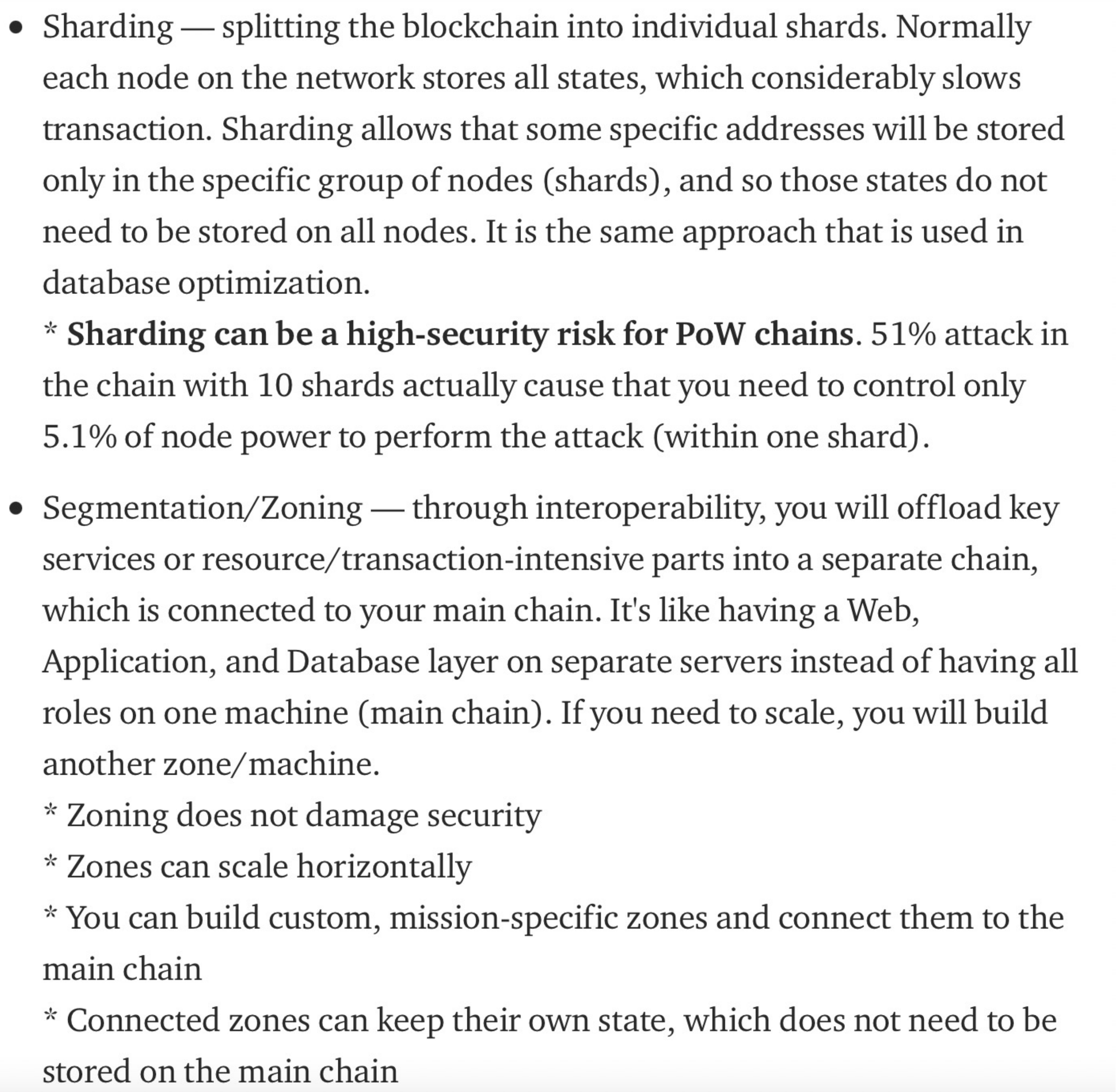
Slashing represents an incentive to act properly and behave honestly within the blockchain ecosystem. If an adversary will violate rules or jeopardize other participants' safety, it will result in a loss of adversary stake percentage. It also works as a measure to prevent nothing at stake problem.

In simple words, if you act maliciously, you will automatically lose a portion of your funds, which is an effective countermeasure.

Cosmos slashing is a part of a chain protocol, and historically there was one event where it shows its effectiveness. The technical issue of one validator caused an unintentional double signing. Stakes were automatically slashed by 5%, and the node was removed from the active validator set.

Polkadot's slashing mechanism is a bit more complicated. You have in chain collators, validators, nominators (delegators), and fisherman nodes. Polkadot assume that fisherman will identify compromised blocks and slash validators which are misbehaving. Unfortunately fisherman incentive model works in a way that it gets rewarded only in a case when it finds misbehavior. This business model is not profitable in the honest network. If there will not be enough fisherman nodes in the network, there is a higher

Sharding, Segmentation

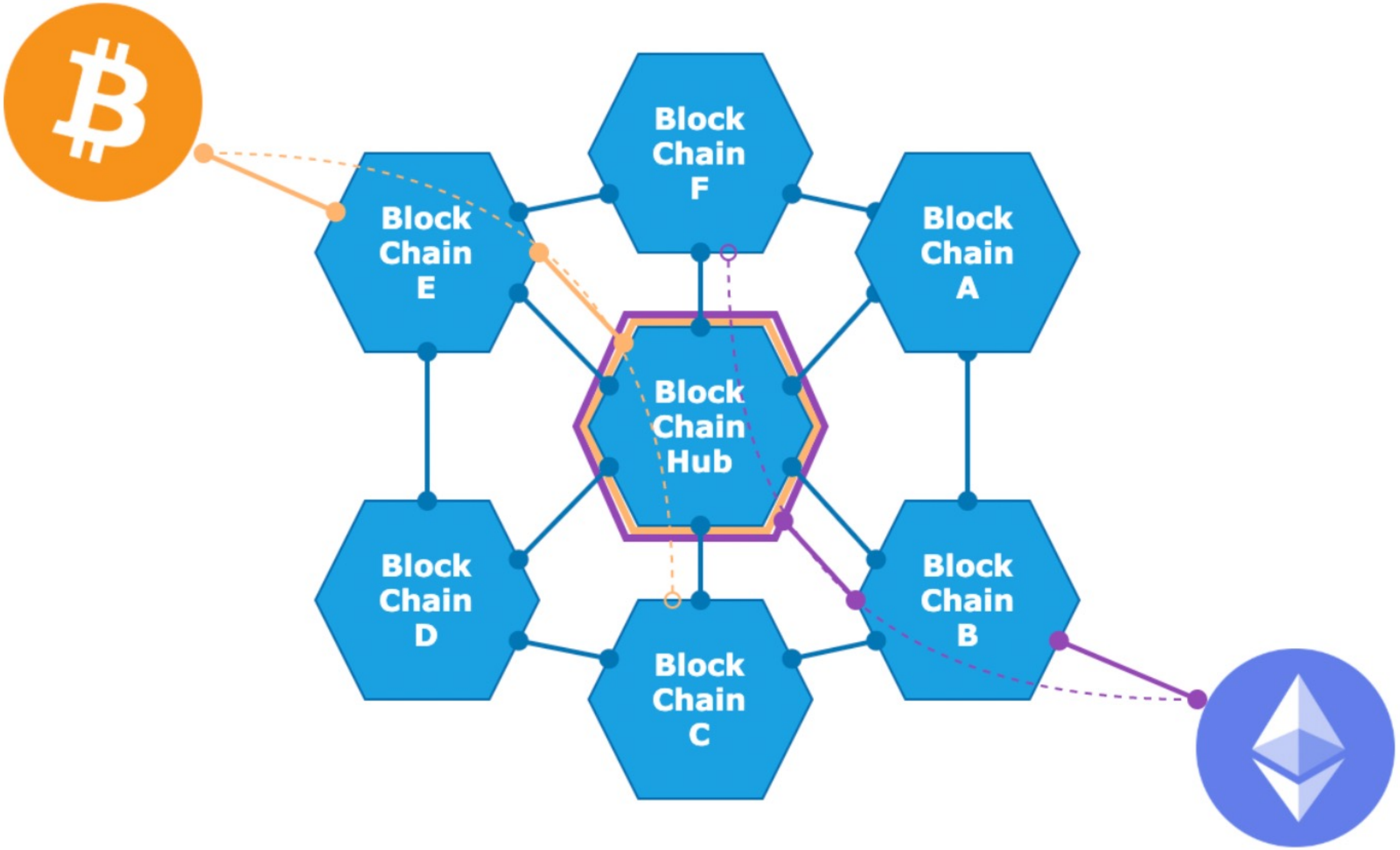


- Sharding — splitting the blockchain into individual shards. Normally each node on the network stores all states, which considerably slows transaction. Sharding allows that some specific addresses will be stored only in the specific group of nodes (shards), and so those states do not need to be stored on all nodes. It is the same approach that is used in database optimization.
  * **Sharding can be a high-security risk for PoW chains**. 51% attack in the chain with 10 shards actually cause that you need to control only 5.1% of node power to perform the attack (within one shard).

- Segmentation/Zoning — through interoperability, you will offload key services or resource/transaction-intensive parts into a separate chain, which is connected to your main chain. It's like having a Web, Application, and Database layer on separate servers instead of having all roles on one machine (main chain). If you need to scale, you will build another zone/machine.
  * Zoning does not damage security
  * Zones can scale horizontally
  * You can build custom, mission-specific zones and connect them to the main chain
  * Connected zones can keep their own state, which does not need to be stored on the main chain

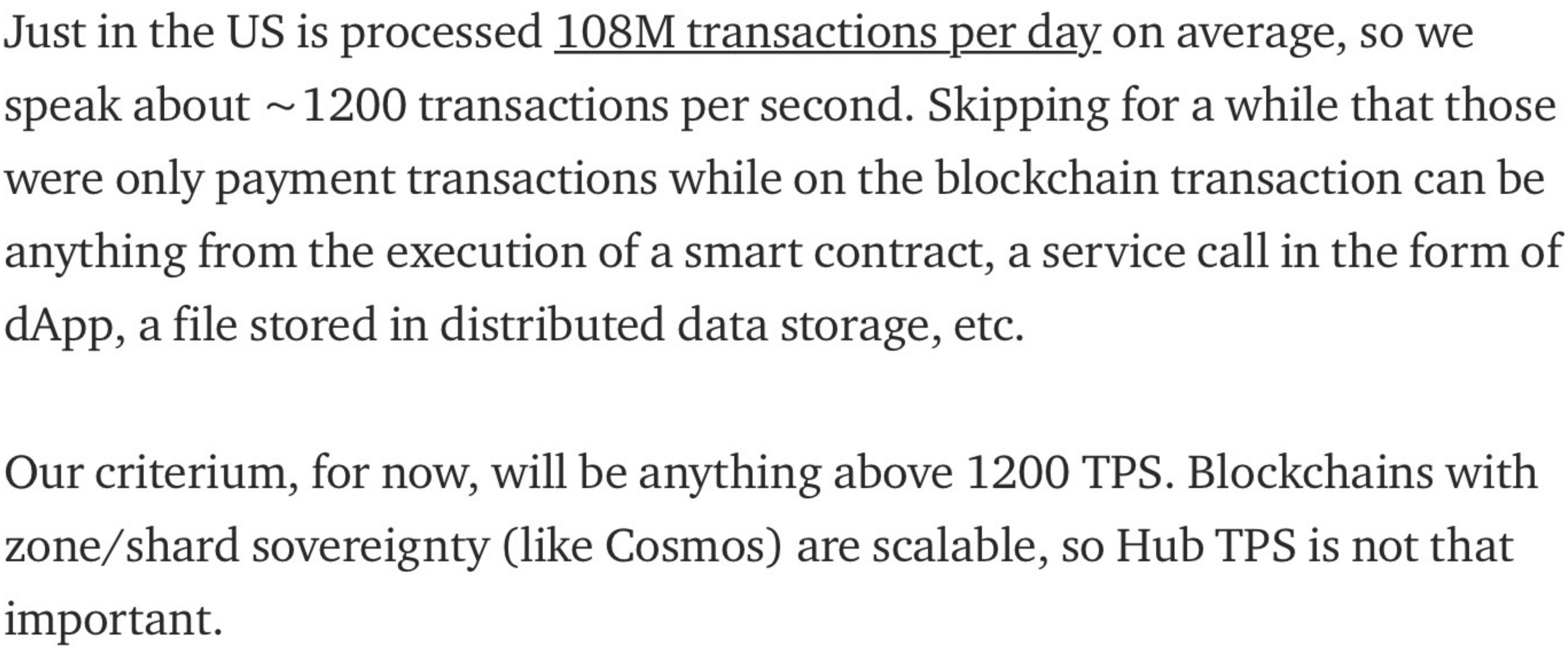
Blockchains

Cross-chain communication capability



Cross-chain capability can connect different blockchains, by author.

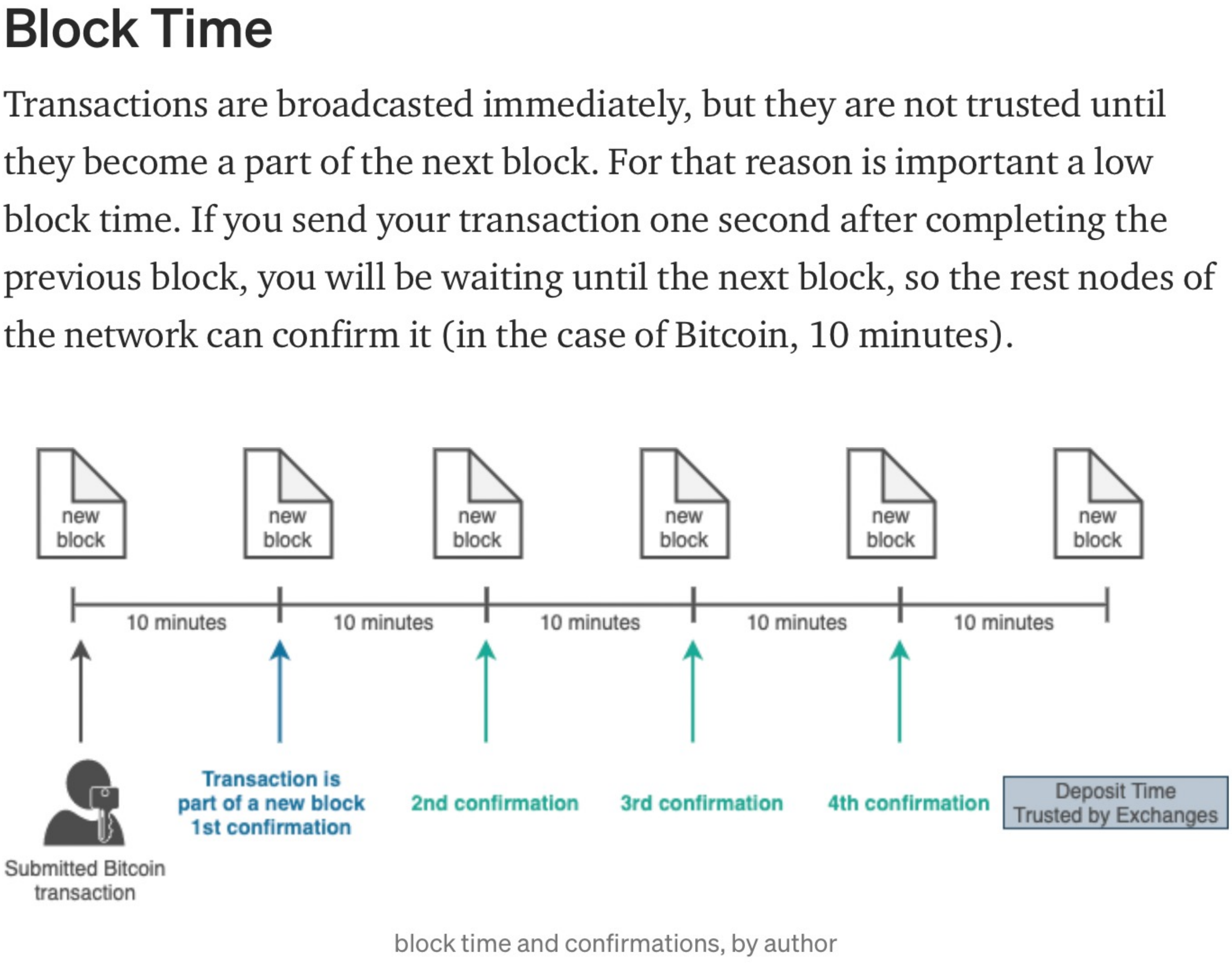
Transaction Rate



Just in the US is processed 108M transactions per day on average, so we speak about ~1200 transactions per second. Skipping for a while that those were only payment transactions while on the blockchain transaction can be anything from the execution of a smart contract, a service call in the form of dApp, a file stored in distributed data storage, etc.

Our criterium, for now, will be anything above 1200 TPS. Blockchains with zone/shard sovereignty (like Cosmos) are scalable, so Hub TPS is not that important.

Block Rate



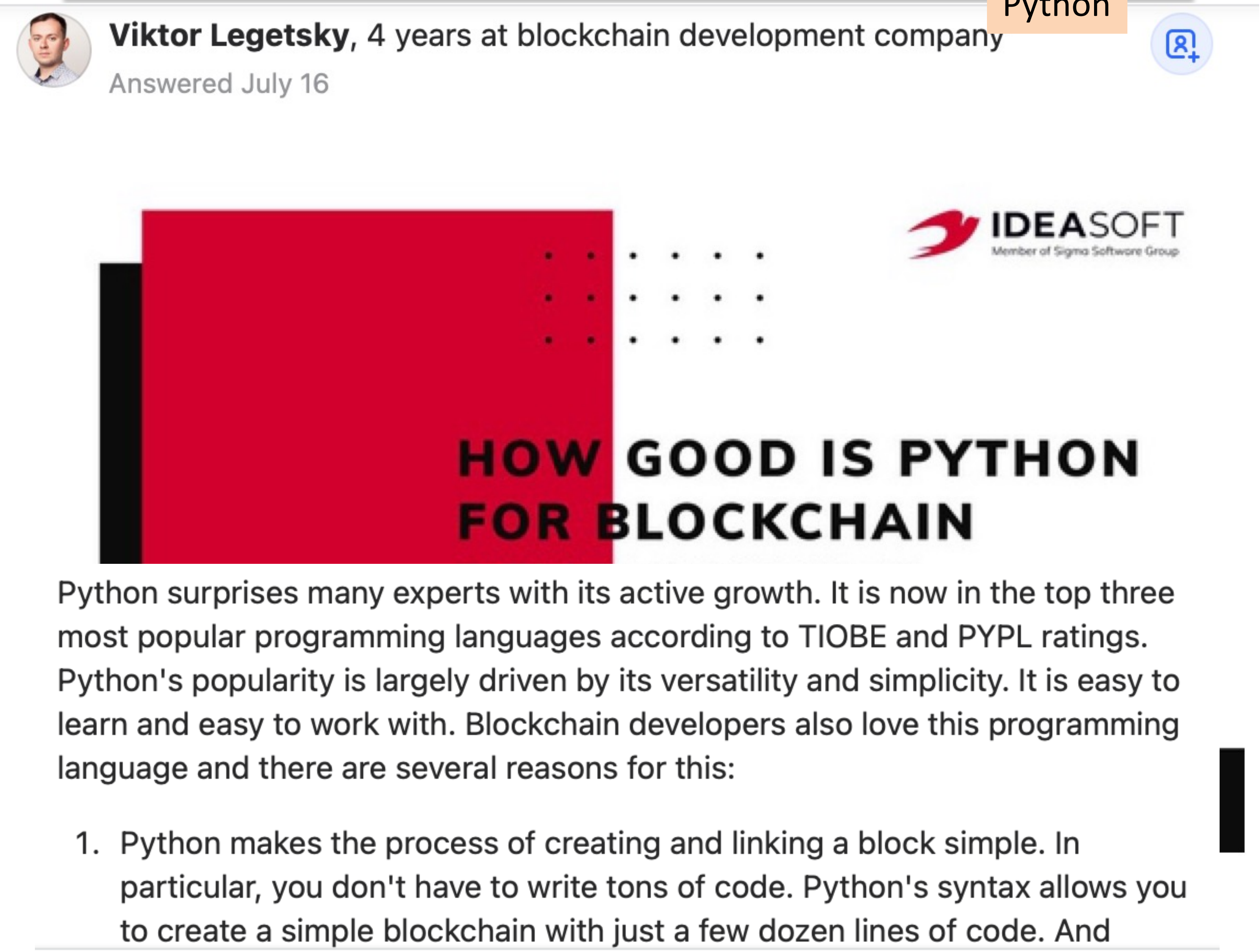
Block Time

Transactions are broadcasted immediately, but they are not trusted until they become a part of the next block. For that reason is important a low block time. If you send your transaction one second after completing the previous block, you will be waiting until the next block, so the rest nodes of the network can confirm it (in the case of Bitcoin, 10 minutes).

block time and confirmations, by author

Blockchain Programming

Python



Viktor Legetsky, 4 years at blockchain development company

Answered July 16

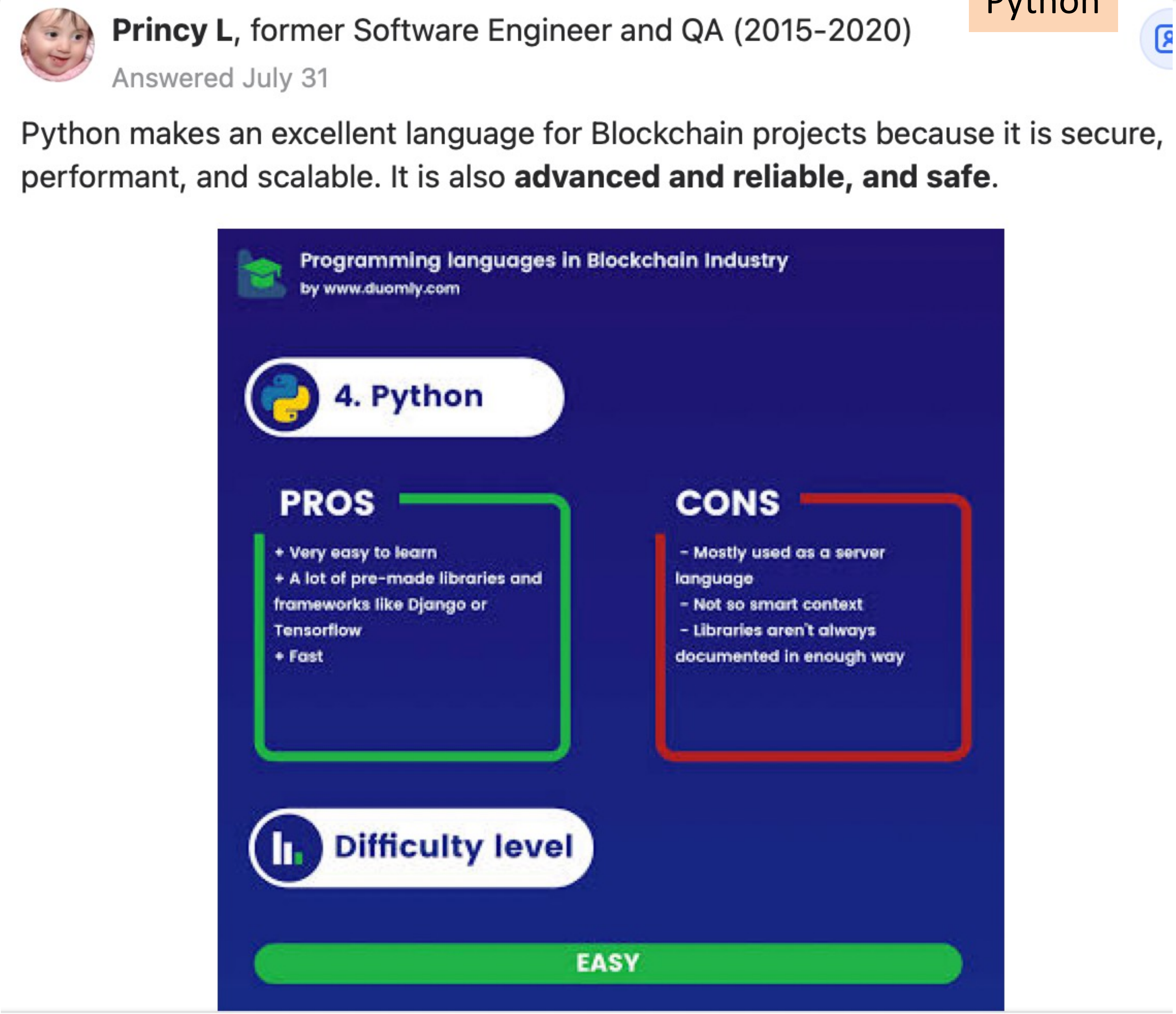
IDEASOFT
Member of Sigma Software Group
HOW GOOD IS PYTHON FOR BLOCKCHAIN

Python surprises many experts with its active growth. It is now in the top three most popular programming languages according to TIOBE and PYPL ratings. Python's popularity is largely driven by its versatility and simplicity. It is easy to learn and easy to work with. Blockchain developers also love this programming language and there are several reasons for this:

1. Python makes the process of creating and linking a block simple. In particular, you don't have to write tons of code. Python's syntax allows you to create a simple blockchain with just a few dozen lines of code. And

Blockchain Programming

Python



Princy L, former Software Engineer and QA (2015-2020)

Answered July 31

Python makes an excellent language for Blockchain projects because it is secure, performant, and scalable. It is also **advanced and reliable, and safe.**

Programming languages in Blockchain Industry
by www.duomly.com

4. Python

PROS

+ Very easy to learn
+ A lot of pre-made libraries and frameworks like Django or Tensorflow
+ Fast

CONS

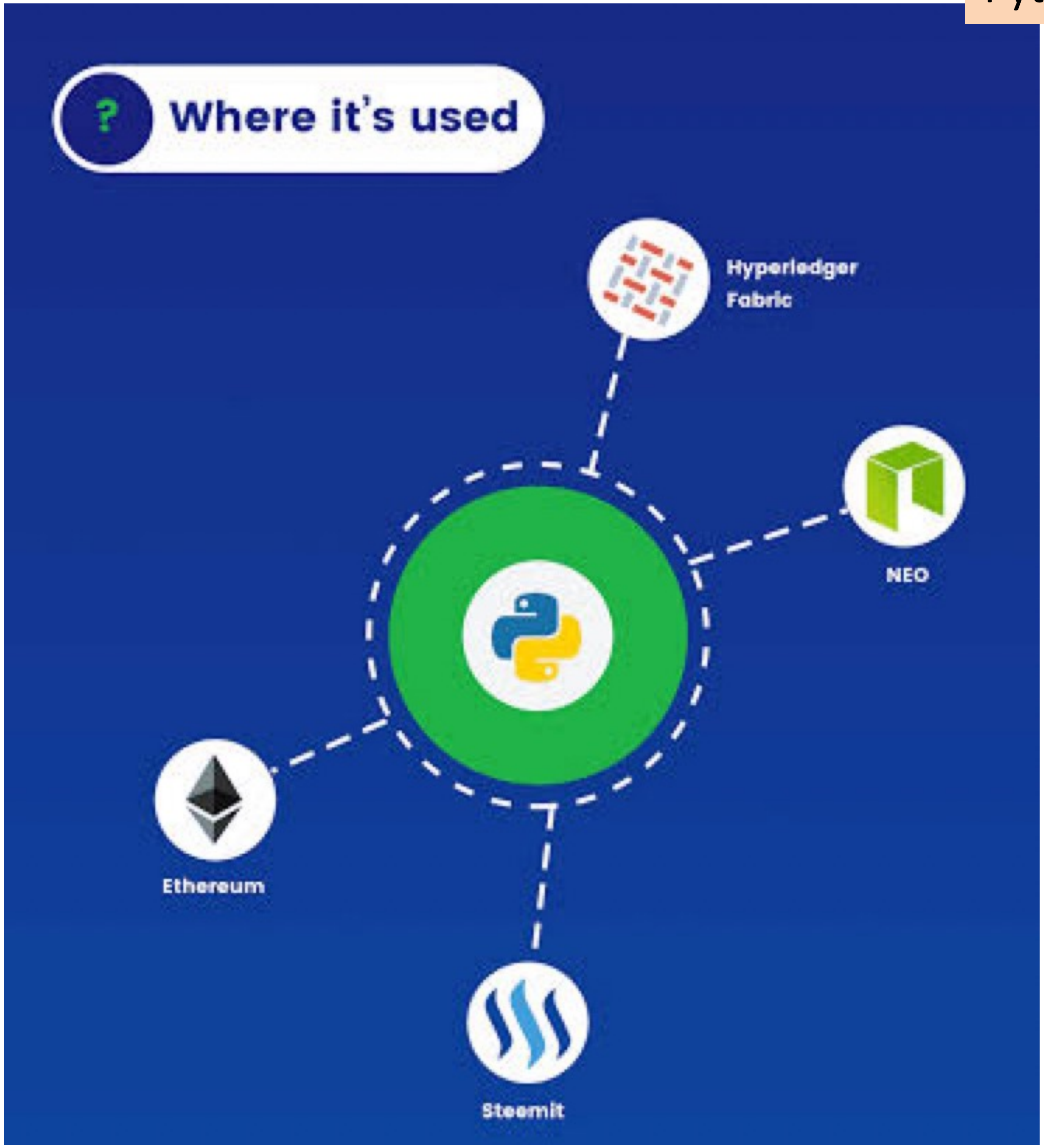
- Mostly used as a server language
- Not so smart context
- Libraries aren't always documented in enough way

Difficulty level

EASY

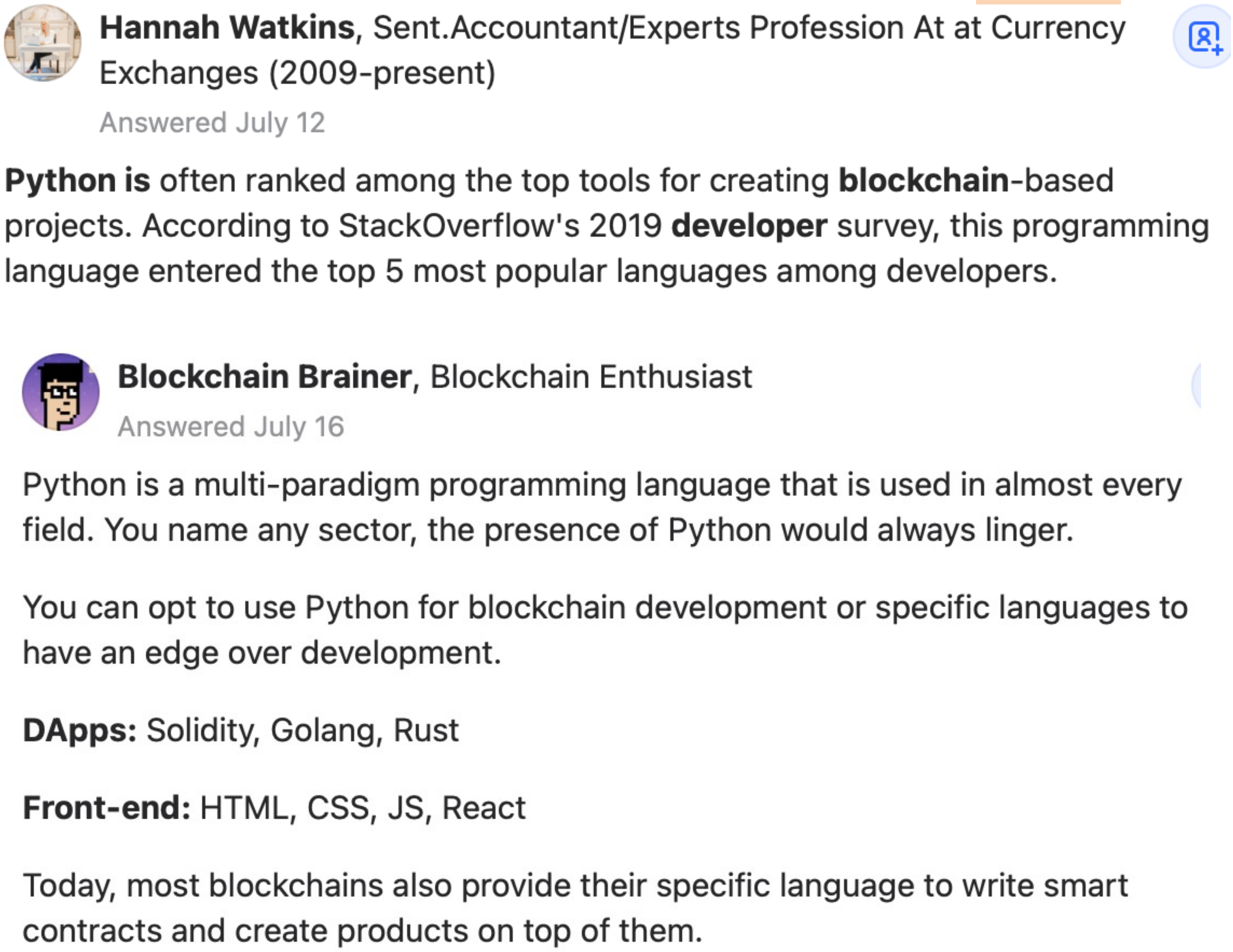
Blockchain Programming

Python



Blockchain Programming

Python



Hannah Watkins, Sent.Accountant/Experts Profession At at Currency Exchanges (2009-present)

Answered July 12

Python is often ranked among the top tools for creating **blockchain**-based projects. According to StackOverflow's 2019 **developer** survey, this programming language entered the top 5 most popular languages among developers.

Blockchain Brainer, Blockchain Enthusiast

Answered July 16

Python is a multi-paradigm programming language that is used in almost every field. You name any sector, the presence of Python would always linger.

You can opt to use Python for blockchain development or specific languages to have an edge over development.

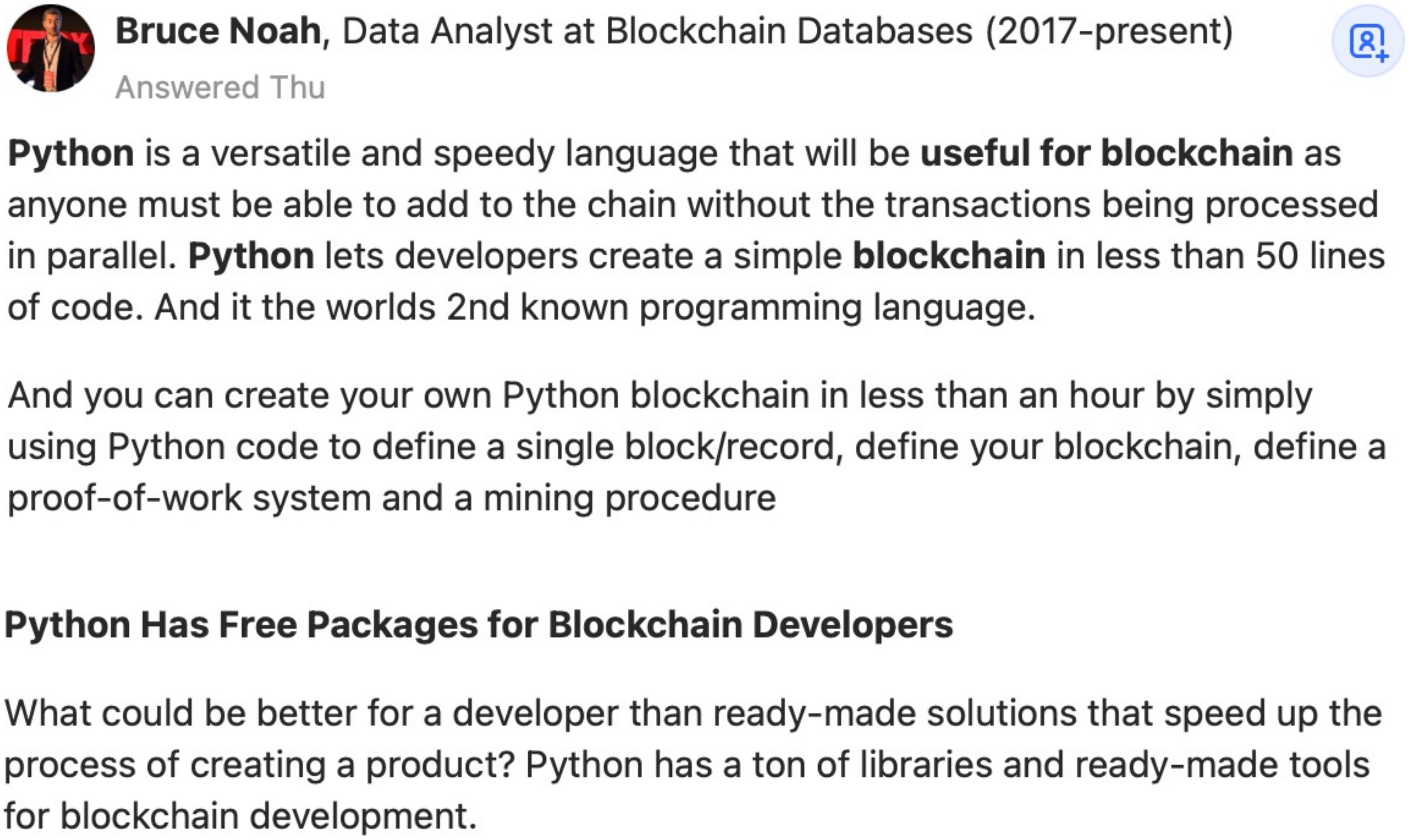
DApps: Solidity, Golang, Rust

Front-end: HTML, CSS, JS, React

Today, most blockchains also provide their specific language to write smart contracts and create products on top of them.

Blockchain Programming

Python



Bruce Noah, Data Analyst at Blockchain Databases (2017-present)

Answered Thu

Python is a versatile and speedy language that will be **useful for blockchain** as anyone must be able to add to the chain without the transactions being processed in parallel. **Python** lets developers create a simple **blockchain** in less than 50 lines of code. And it the worlds 2nd known programming language.

And you can create your own Python blockchain in less than an hour by simply using Python code to define a single block/record, define your blockchain, define a proof-of-work system and a mining procedure

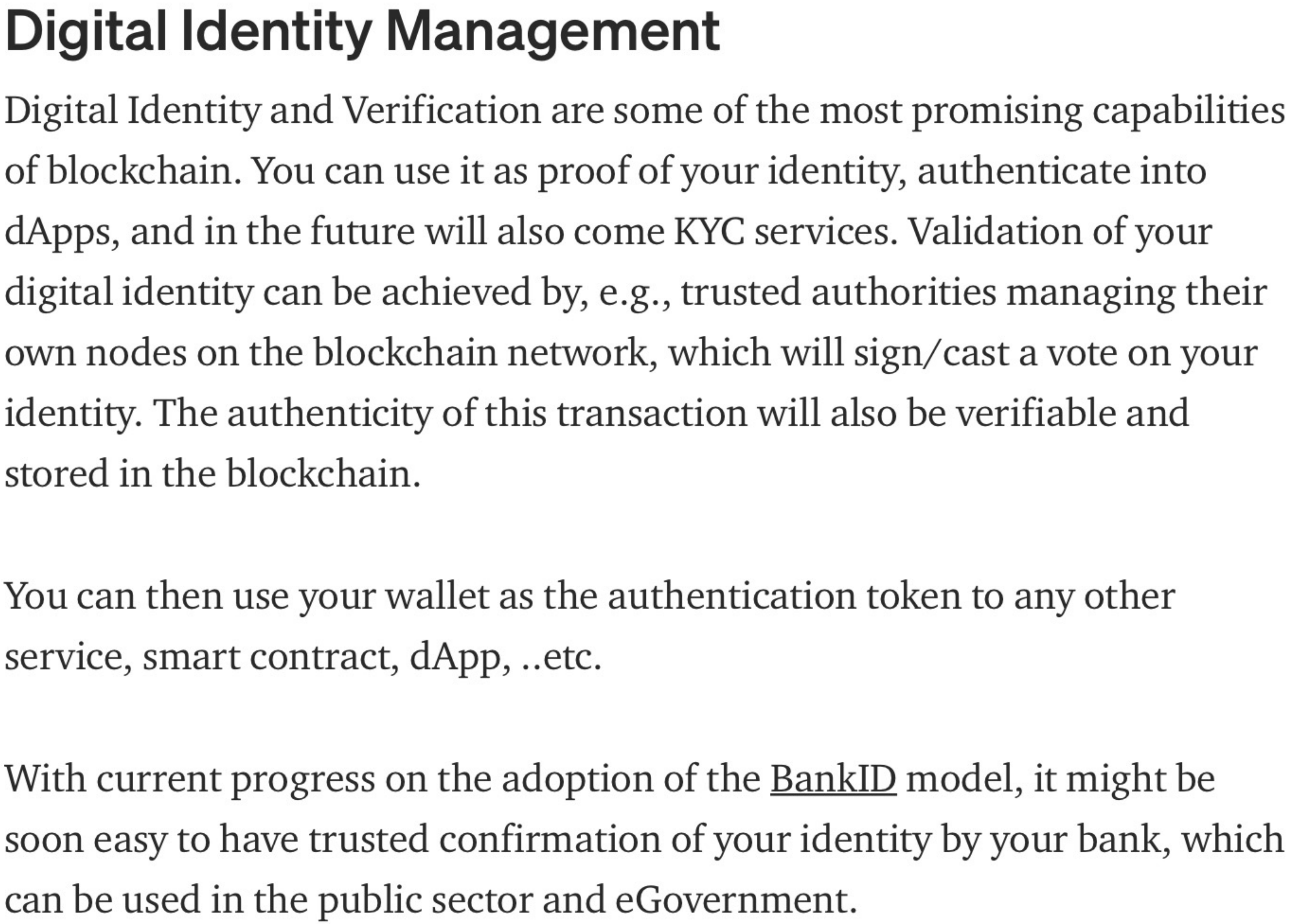
Python Has Free Packages for Blockchain Developers

What could be better for a developer than ready-made solutions that speed up the process of creating a product? Python has a ton of libraries and ready-made tools for blockchain development.

Blockchain Applications

- Digital ID
- dApps
- DeFi
- DEX
- Online Voting
- **Cryptocurrency**

Digital ID & Authentication



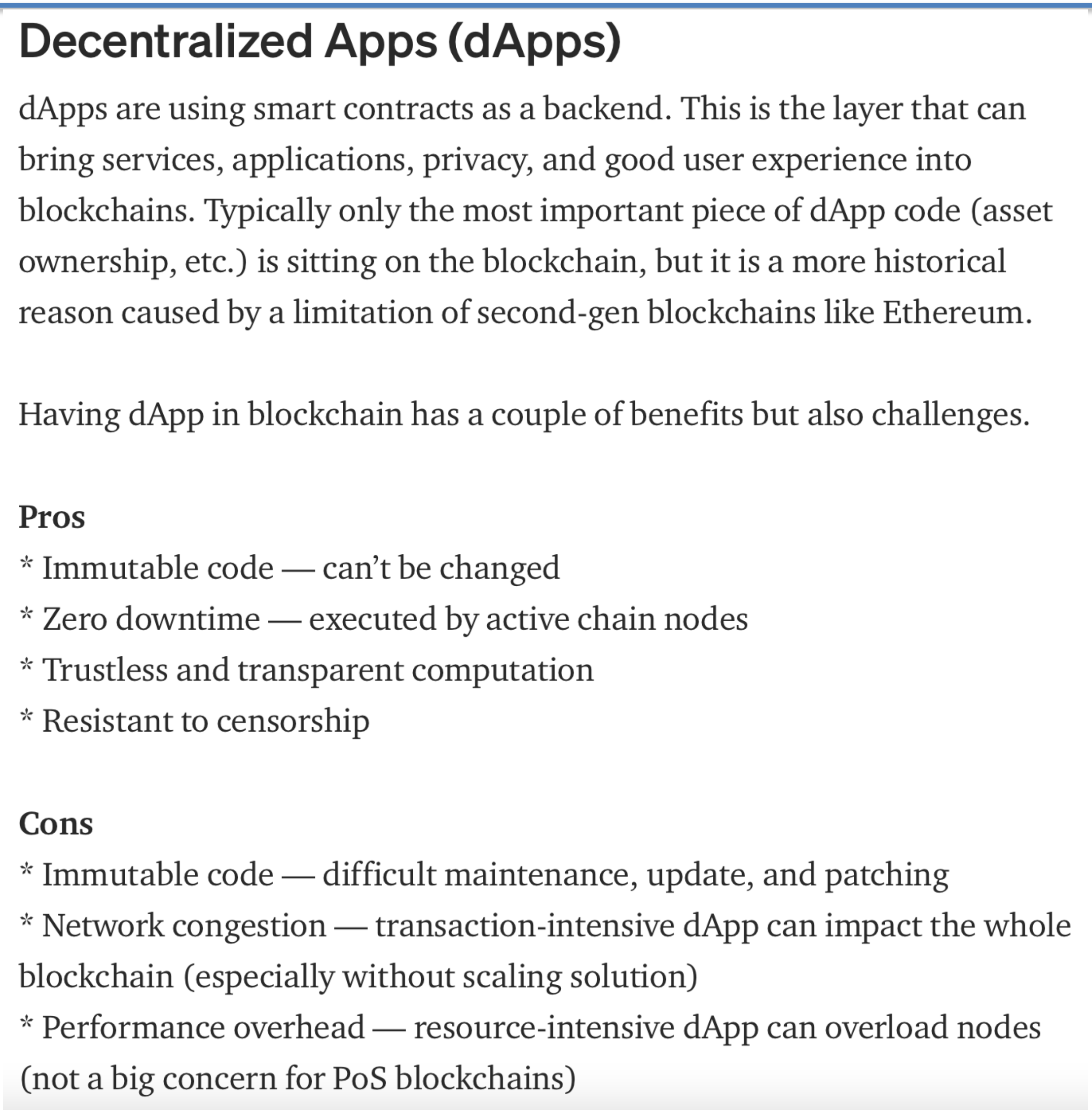
Digital Identity Management

Digital Identity and Verification are some of the most promising capabilities of blockchain. You can use it as proof of your identity, authenticate into dApps, and in the future will also come KYC services. Validation of your digital identity can be achieved by, e.g., trusted authorities managing their own nodes on the blockchain network, which will sign/cast a vote on your identity. The authenticity of this transaction will also be verifiable and stored in the blockchain.

You can then use your wallet as the authentication token to any other service, smart contract, dApp, ..etc.

With current progress on the adoption of the BankID model, it might be soon easy to have trusted confirmation of your identity by your bank, which can be used in the public sector and eGovernment.

dApps



Decentralized Apps (dApps)

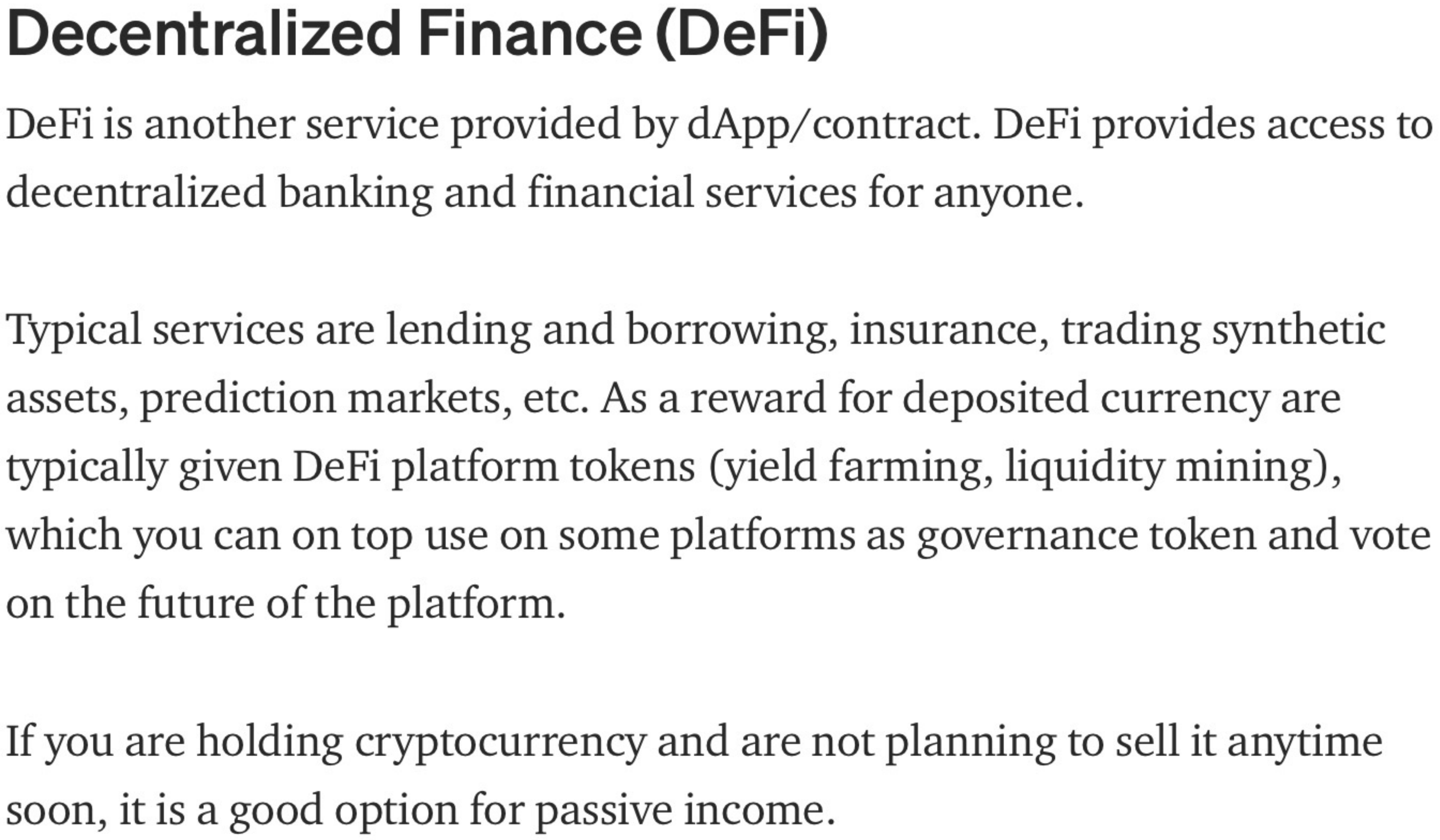
dApps are using smart contracts as a backend. This is the layer that can bring services, applications, privacy, and good user experience into blockchains. Typically only the most important piece of dApp code (asset ownership, etc.) is sitting on the blockchain, but it is a more historical reason caused by a limitation of second-gen blockchains like Ethereum.

Having dApp in blockchain has a couple of benefits but also challenges.

Pros
* Immutable code — can’t be changed
* Zero downtime — executed by active chain nodes
* Trustless and transparent computation
* Resistant to censorship

Cons
* Immutable code — difficult maintenance, update, and patching
* Network congestion — transaction-intensive dApp can impact the whole blockchain (especially without scaling solution)
* Performance overhead — resource-intensive dApp can overload nodes (not a big concern for PoS blockchains)

DeFi



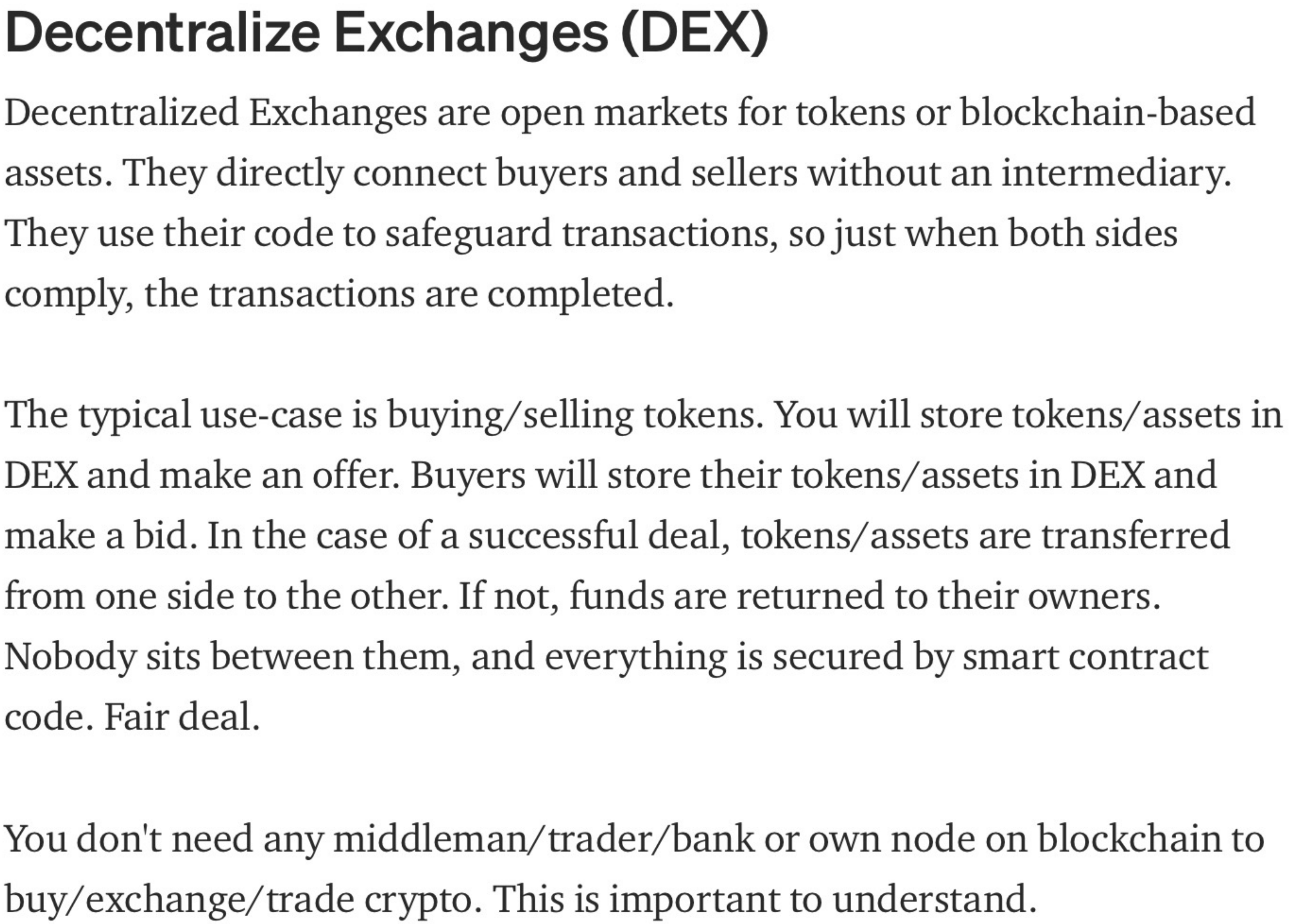
Decentralized Finance (DeFi)

DeFi is another service provided by dApp/contract. DeFi provides access to decentralized banking and financial services for anyone.

Typical services are lending and borrowing, insurance, trading synthetic assets, prediction markets, etc. As a reward for deposited currency are typically given DeFi platform tokens (yield farming, liquidity mining), which you can on top use on some platforms as governance token and vote on the future of the platform.

If you are holding cryptocurrency and are not planning to sell it anytime soon, it is a good option for passive income.

DEX



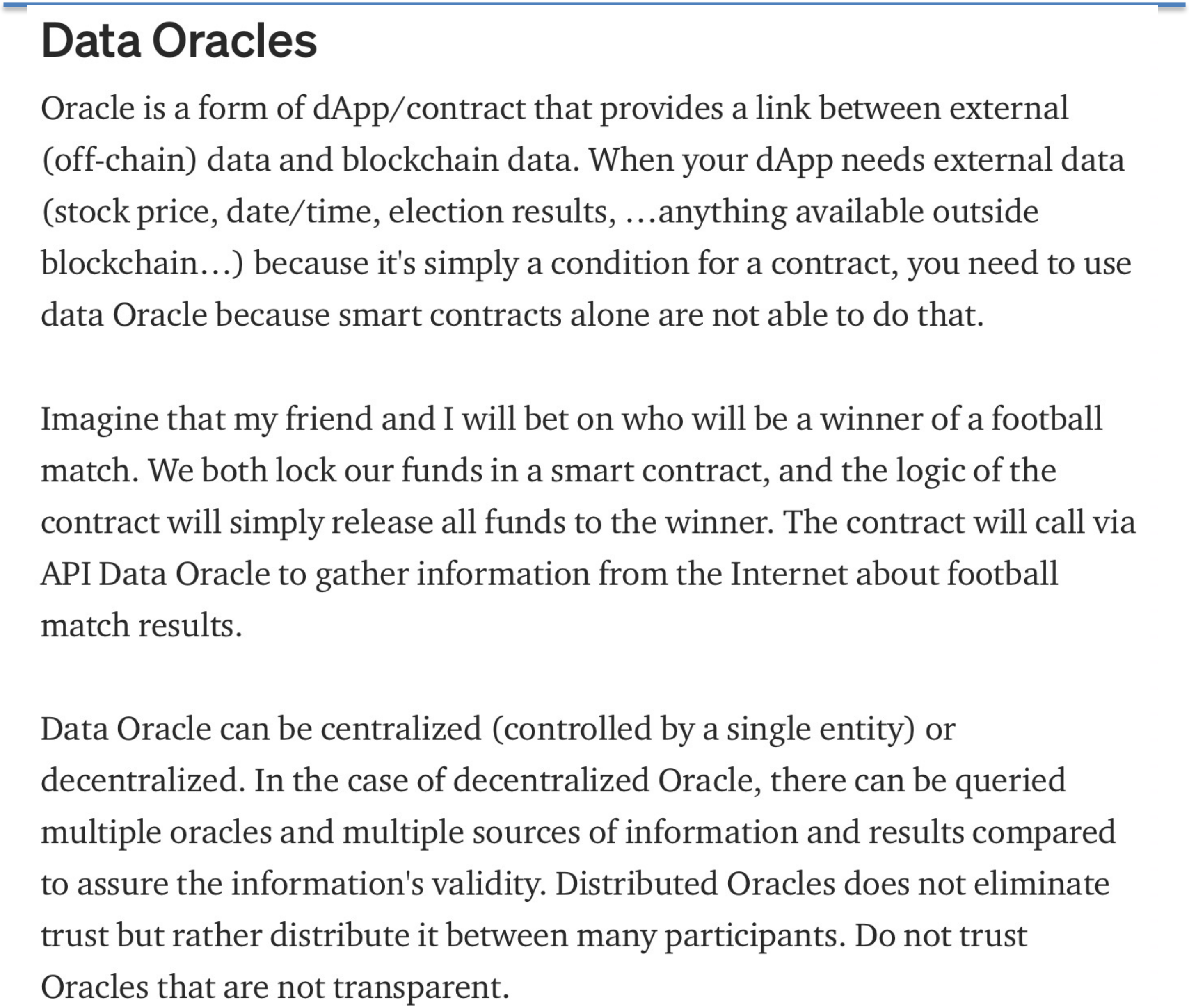
Decentralize Exchanges (DEX)

Decentralized Exchanges are open markets for tokens or blockchain-based assets. They directly connect buyers and sellers without an intermediary. They use their code to safeguard transactions, so just when both sides comply, the transactions are completed.

The typical use-case is buying/selling tokens. You will store tokens/assets in DEX and make an offer. Buyers will store their tokens/assets in DEX and make a bid. In the case of a successful deal, tokens/assets are transferred from one side to the other. If not, funds are returned to their owners. Nobody sits between them, and everything is secured by smart contract code. Fair deal.

You don't need any middleman/trader/bank or own node on blockchain to buy/exchange/trade crypto. This is important to understand.

Data Oracles



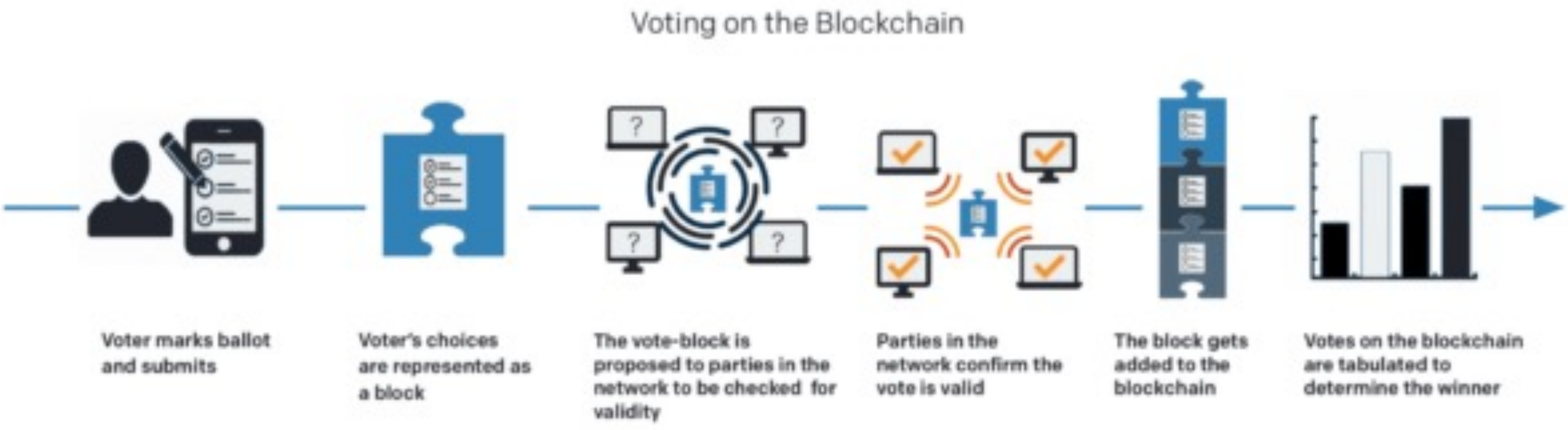
Data Oracles

Oracle is a form of dApp/contract that provides a link between external (off-chain) data and blockchain data. When your dApp needs external data (stock price, date/time, election results, …anything available outside blockchain…) because it's simply a condition for a contract, you need to use data Oracle because smart contracts alone are not able to do that.

Imagine that my friend and I will bet on who will be a winner of a football match. We both lock our funds in a smart contract, and the logic of the contract will simply release all funds to the winner. The contract will call via API Data Oracle to gather information from the Internet about football match results.

Data Oracle can be centralized (controlled by a single entity) or decentralized. In the case of decentralized Oracle, there can be queried multiple oracles and multiple sources of information and results compared to assure the information's validity. Distributed Oracles does not eliminate trust but rather distribute it between many participants. Do not trust Oracles that are not transparent.

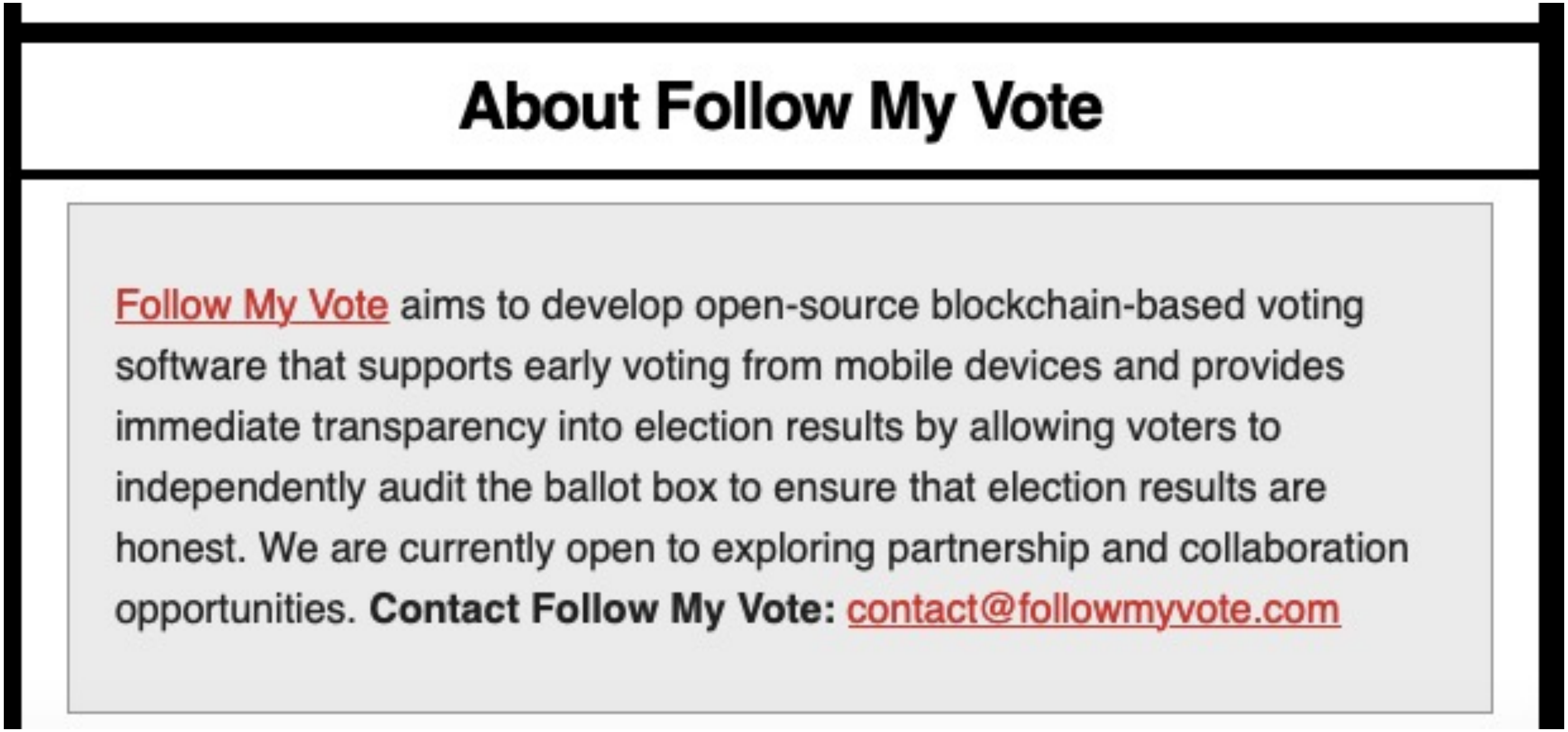
Blockchain App: Voting


Voting on the Blockchain
Voter marks ballot and submits
Voter's choices are represented as a block
The vote-block is proposed to parties in the network to be checked for validity
Parties in the network confirm the vote is valid
The block gets added to the blockchain
Votes on the blockchain are tabulated to determine the winner

- ❖ Everyone who uses a blockchain (e.g. Bitcoin) stores the complete blockchain
- ❖ On their own server (so there are *millions* of copies)

Online Voting Companies

Follow My Vote

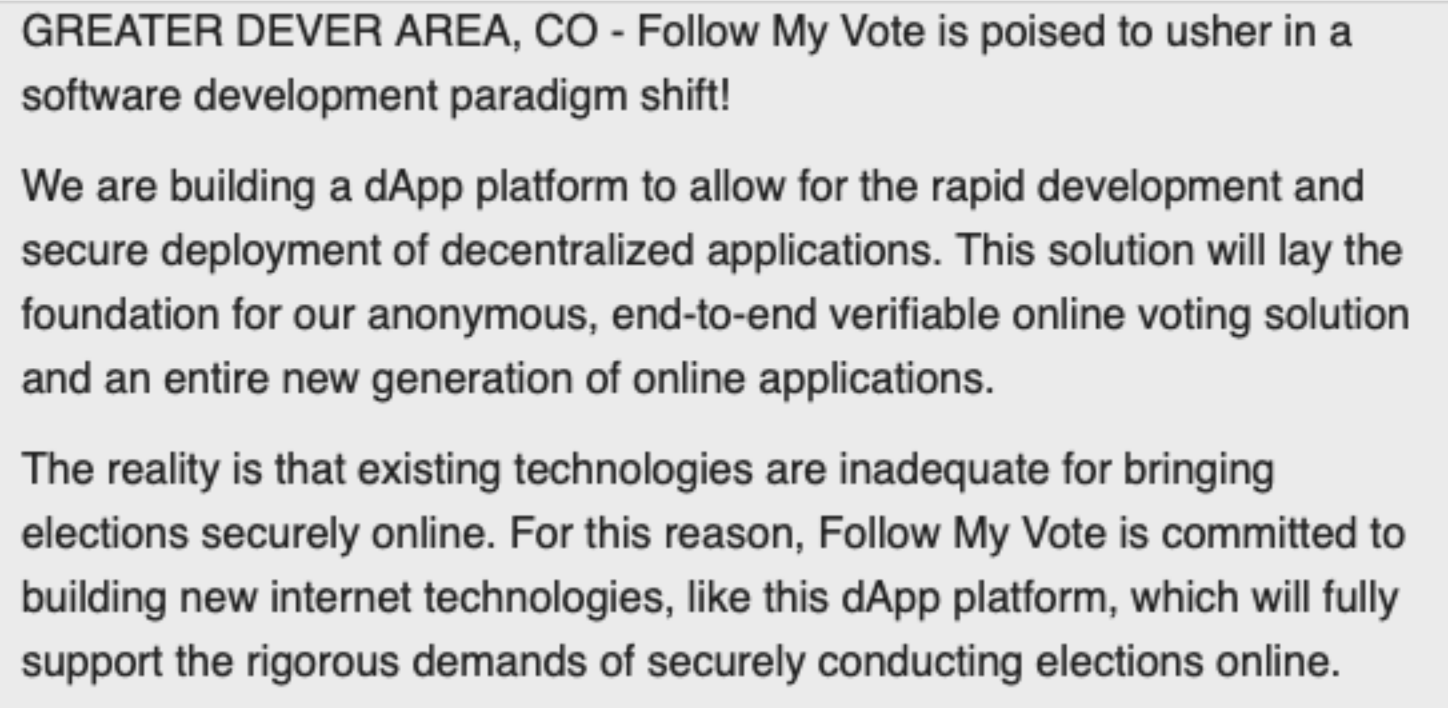


About Follow My Vote

Follow My Vote aims to develop open-source blockchain-based voting software that supports early voting from mobile devices and provides immediate transparency into election results by allowing voters to independently audit the ballot box to ensure that election results are honest. We are currently open to exploring partnership and collaboration opportunities. **Contact Follow My Vote:** contact@followmyvote.com

Online Voting Companies

Follow My Vote



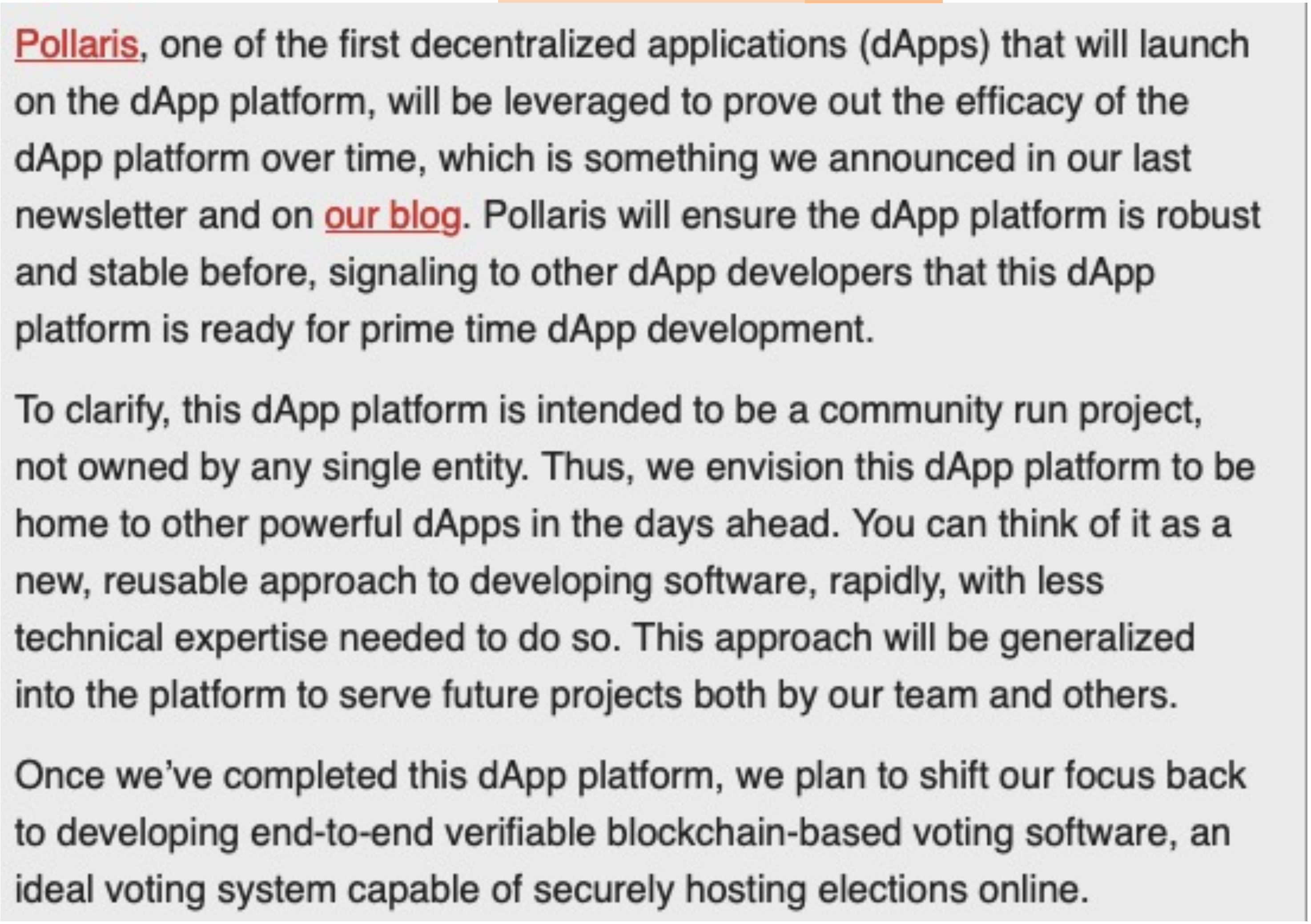
GREATER DEVER AREA, CO - Follow My Vote is poised to usher in a software development paradigm shift!

We are building a dApp platform to allow for the rapid development and secure deployment of decentralized applications. This solution will lay the foundation for our anonymous, end-to-end verifiable online voting solution and an entire new generation of online applications.

The reality is that existing technologies are inadequate for bringing elections securely online. For this reason, Follow My Vote is committed to building new internet technologies, like this dApp platform, which will fully support the rigorous demands of securely conducting elections online.

Online Voting Companies

Follow My Vote | dApp



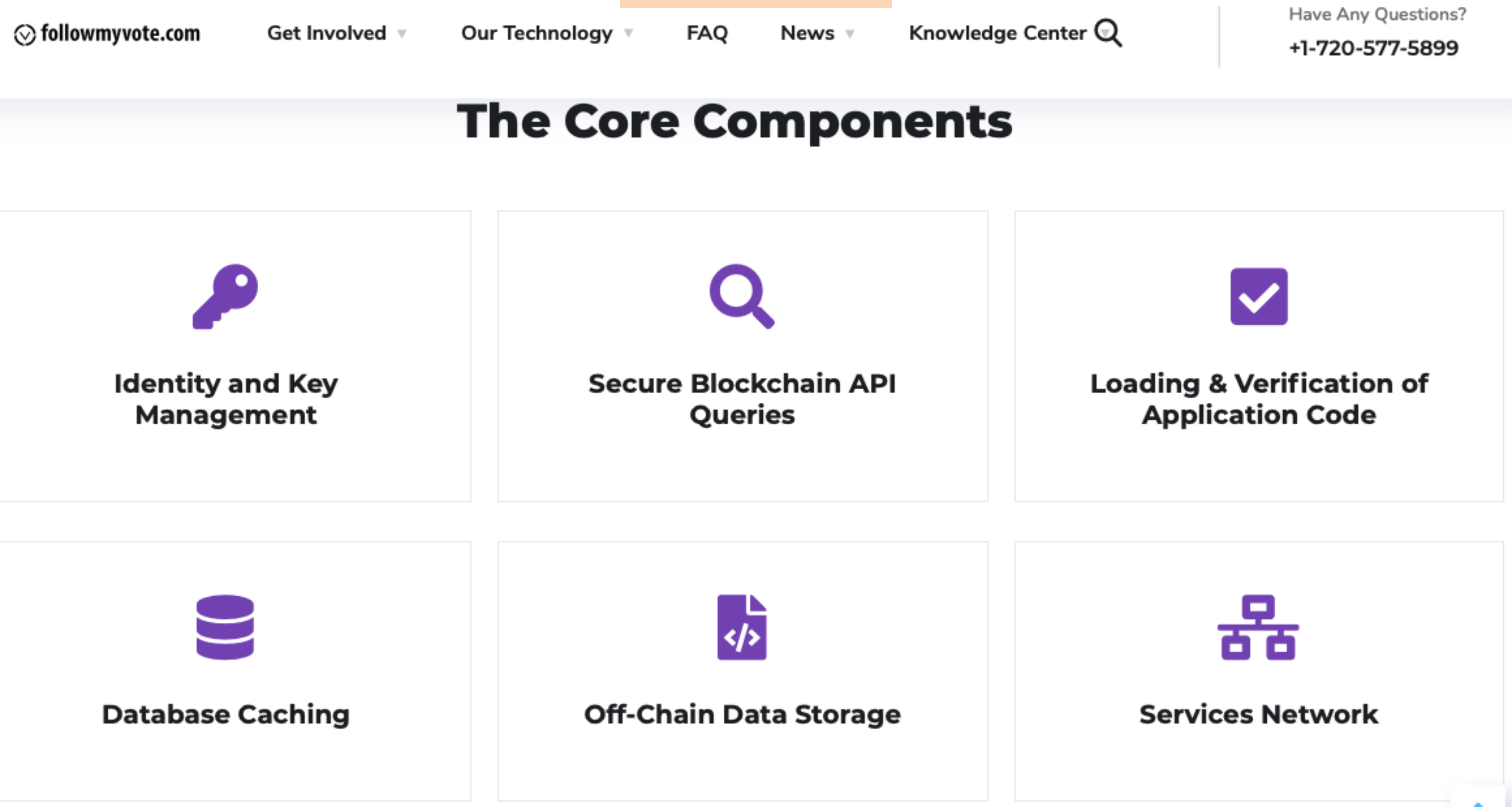
Pollaris, one of the first decentralized applications (dApps) that will launch on the dApp platform, will be leveraged to prove out the efficacy of the dApp platform over time, which is something we announced in our last newsletter and on our blog. Pollaris will ensure the dApp platform is robust and stable before, signaling to other dApp developers that this dApp platform is ready for prime time dApp development.

To clarify, this dApp platform is intended to be a community run project, not owned by any single entity. Thus, we envision this dApp platform to be home to other powerful dApps in the days ahead. You can think of it as a new, reusable approach to developing software, rapidly, with less technical expertise needed to do so. This approach will be generalized into the platform to serve future projects both by our team and others.

Once we've completed this dApp platform, we plan to shift our focus back to developing end-to-end verifiable blockchain-based voting software, an ideal voting system capable of securely hosting elections online.

Online Voting Companies

Follow My Vote



followmyvote.com Get Involved ▾ Our Technology ▾ FAQ News ▾ Knowledge Center

Have Any Questions?
+1-720-577-5899

The Core Components

Identity and Key Management

Secure Blockchain API Queries

Loading & Verification of Application Code

Database Caching

Off-Chain Data Storage

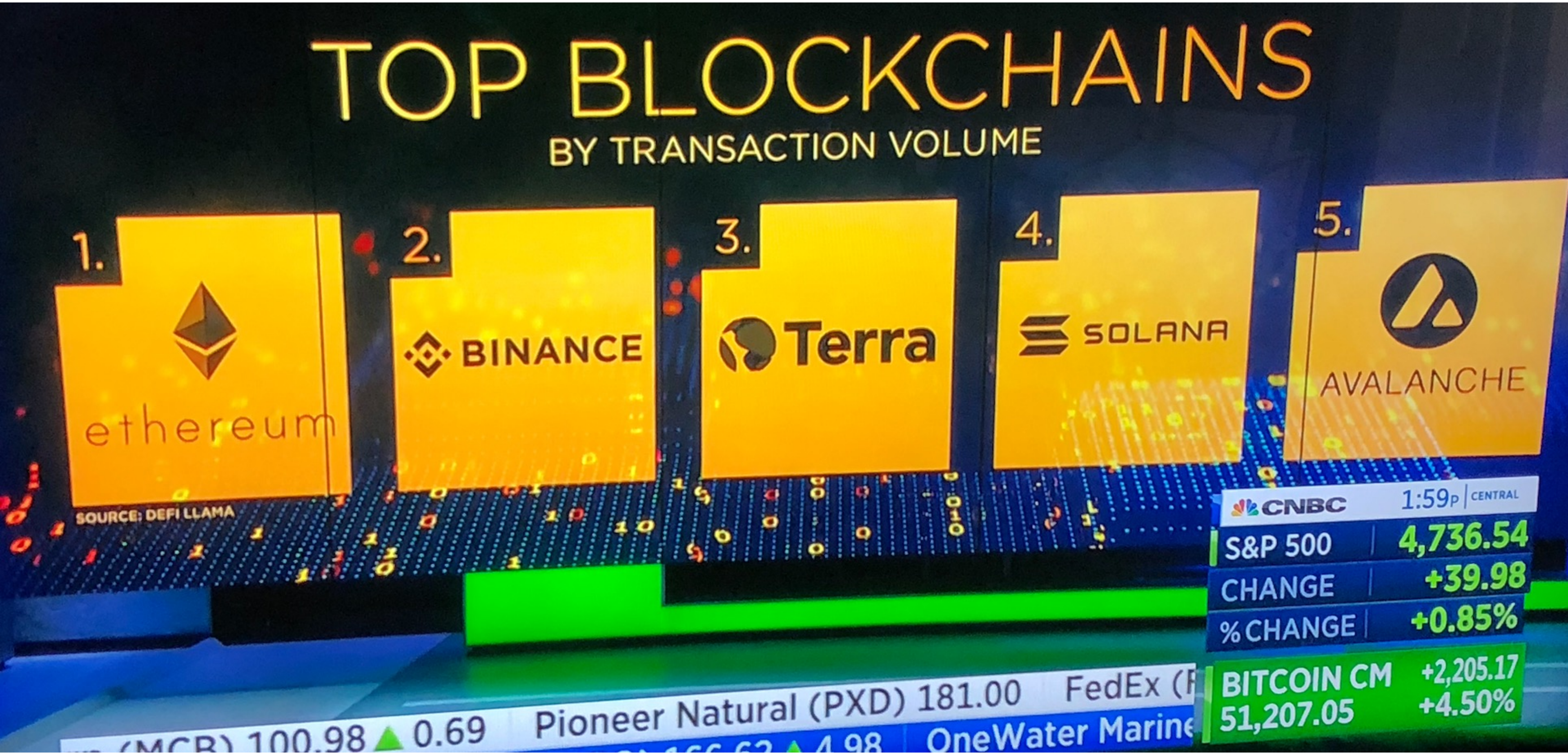
Services Network

Crypto Currencies

- ❖Bitcoin
- ❖Ethereum
- ❖Digital Wallets
- ❖Central Banks (CBDC)

Top Cryptos

Dec 2021



TOP BLOCKCHAINS
BY TRANSACTION VOLUME

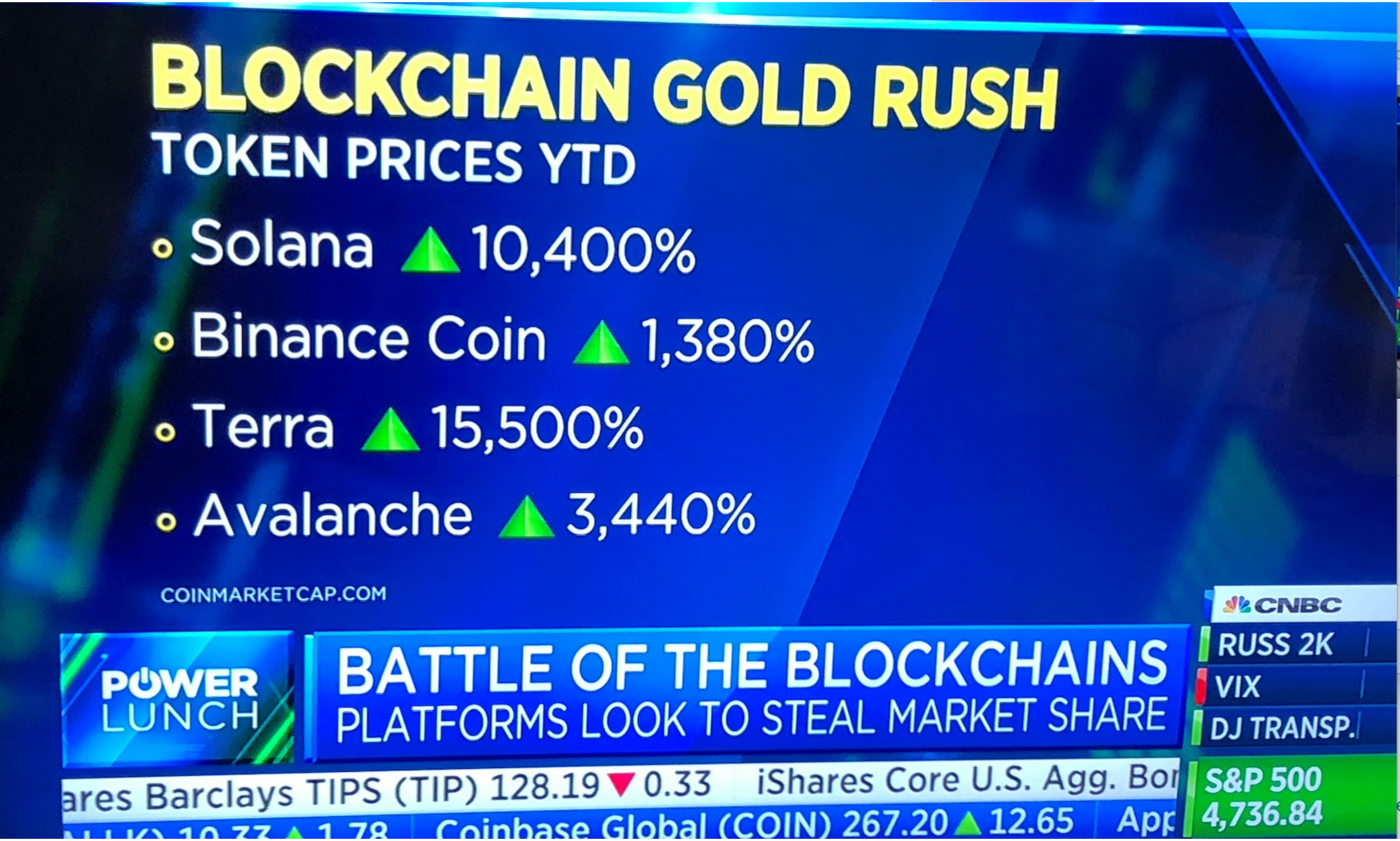
1. ethereum
2. BINANCE
3. Terra
4. SOLANA
5. AVALANCHE

SOURCE: DEFI LLAMA

CNBC 1:59P CENTRAL
S&P 500 4,736.54
CHANGE +39.98
% CHANGE +0.85%
BITCOIN CM 51,207.05 +2,205.17 +4.50%
(MCB) 100.98 ▲ 0.69 Pioneer Natural (PXD) 181.00 FedEx (F
166.63 ▲ 4.98 OneWater Marine

Top Cryptos

Dec 2021



BLOCKCHAIN GOLD RUSH

TOKEN PRICES YTD

- Solana ▲ 10,400%
- Binance Coin ▲ 1,380%
- Terra ▲ 15,500%
- Avalanche ▲ 3,440%

COINMARKETCAP.COM

POWER LUNCH

BATTLE OF THE BLOCKCHAINS
PLATFORMS LOOK TO STEAL MARKET SHARE

CNBC
RUSS 2K
VIX
DJ TRANSP.
S&P 500
4,736.84

ares Barclays TIPS (TIP) 128.19 ▼ 0.33 iShares Core U.S. Agg. Bor
10.33 ▲ 1.78 Coinbase Global (COIN) 267.20 ▲ 12.65 App

My Comments on Crypto

- **Bitcoin**
  - has about **10,000 nodes** now? each node stores at least one ***fork*** of the blockchain? (“hard fork”?)
  - not all **Bitcoin** owners (clients) serve as "nodes". there are **~10,000,000** owners? but only ~10,000 nodes.
  - compare ZKP to Satoshi Nakamoto’s ***Proof of Work***

- **Ethereum** is now the preferred protocol for "smart contracts" (programmed in "Unity/Solidity")

- **Online Voting:** privacy manifests as "anonymity" – an essential

Bitcoin Price

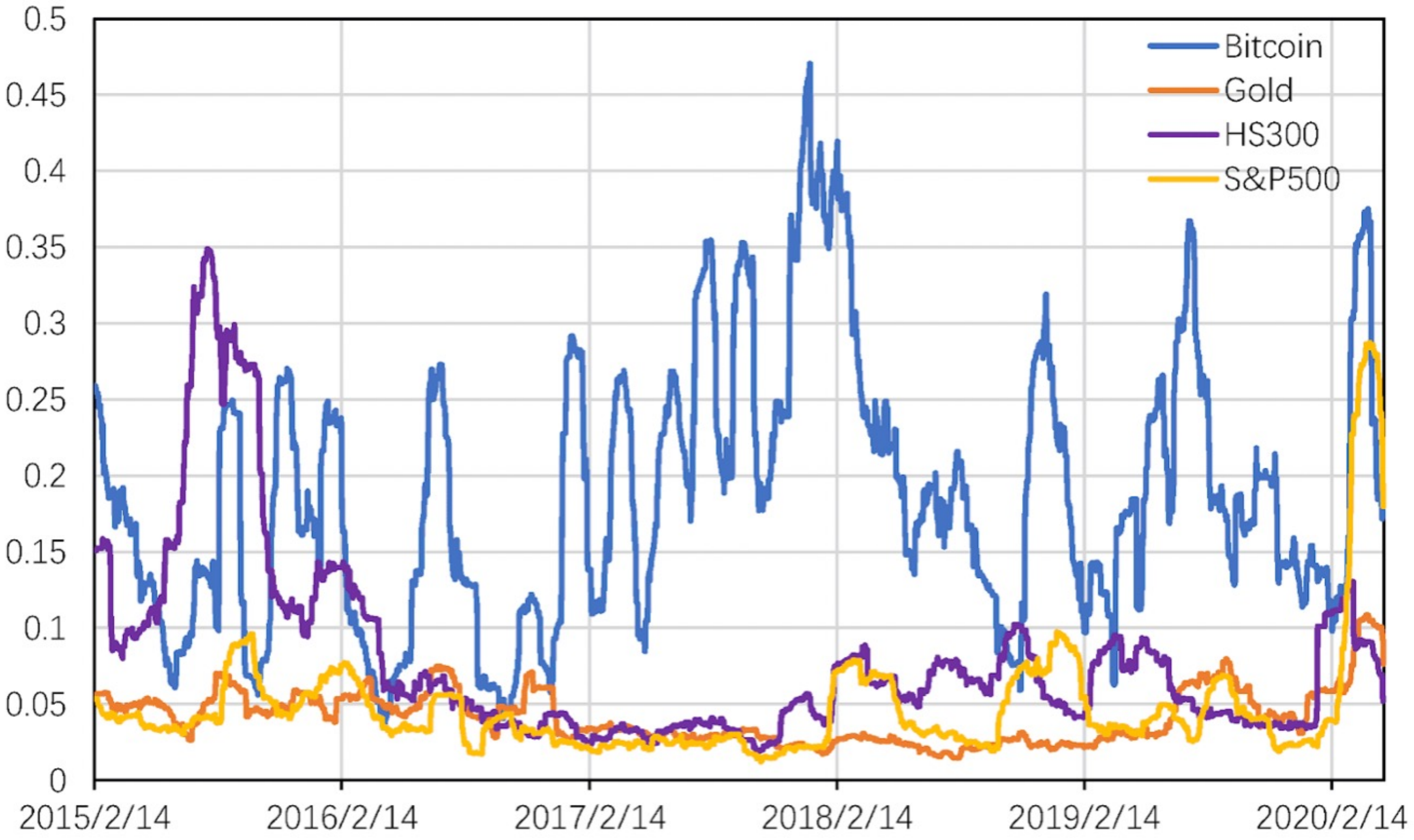
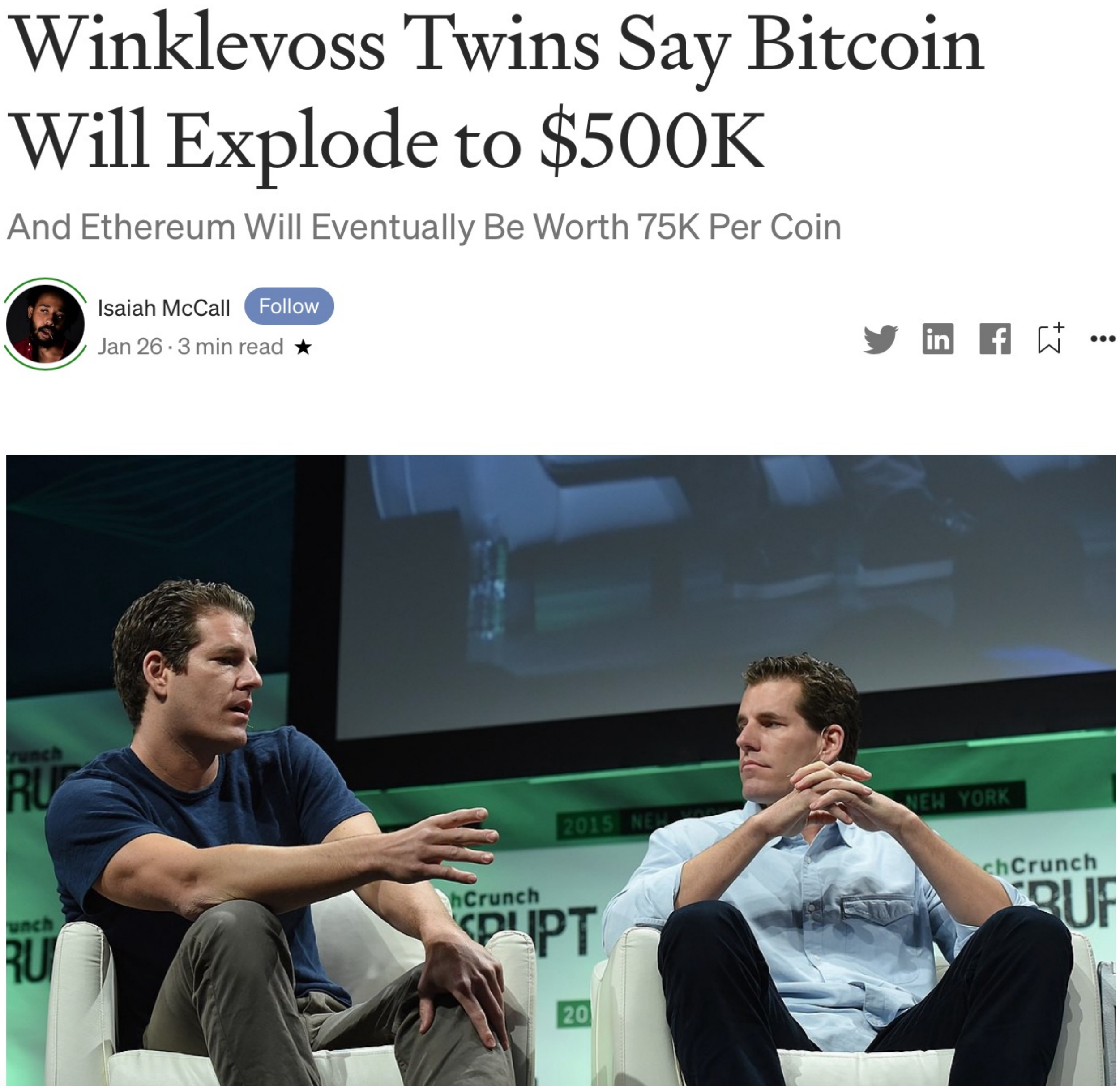


Figure 1: Historical Volatility of Bitcoin, Gold, HS300, and SP500 over 30 Days [1]

CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

Bitcoin

DR JEFF
SOFTWARE
©Jeff Drobman
2017-23



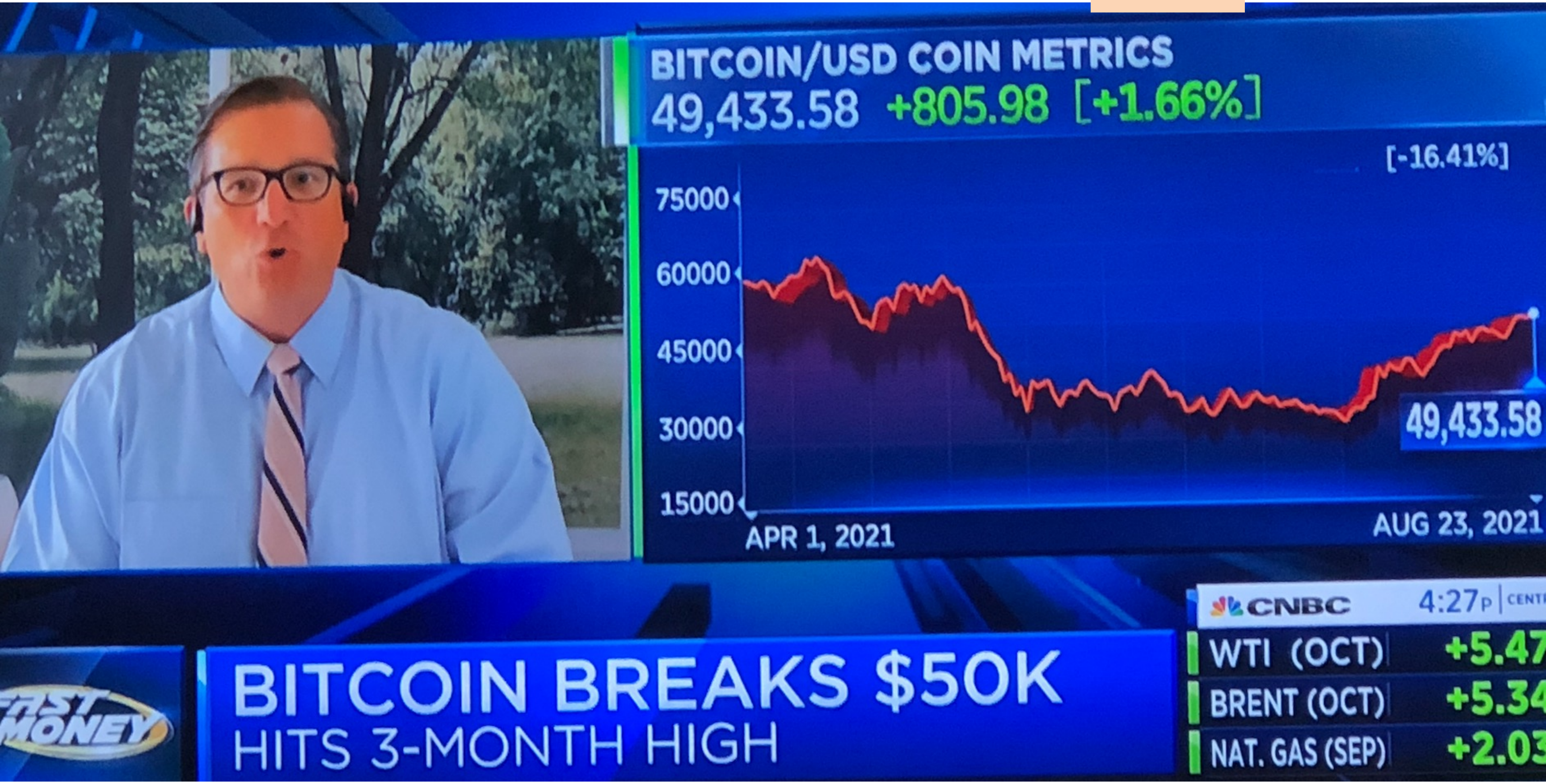
Winklevoss Twins Say Bitcoin Will Explode to $500K

And Ethereum Will Eventually Be Worth 75K Per Coin

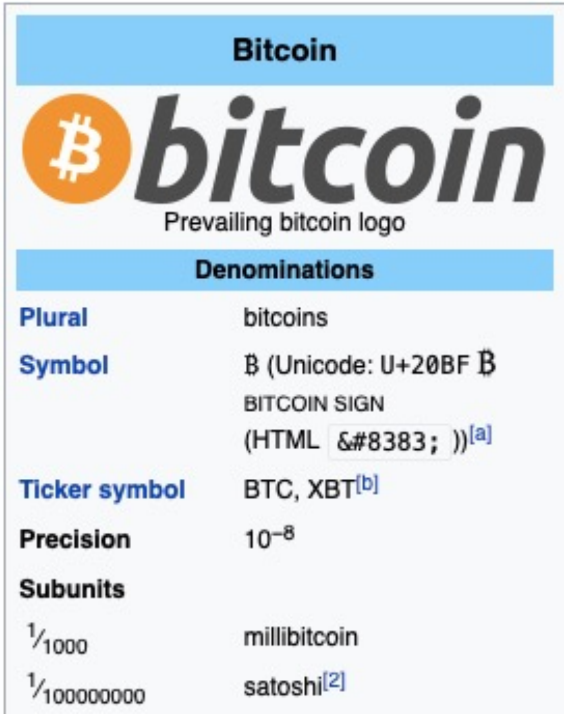
Isaiah McCall Follow
Jan 26 · 3 min read ★

Bitcoin Price

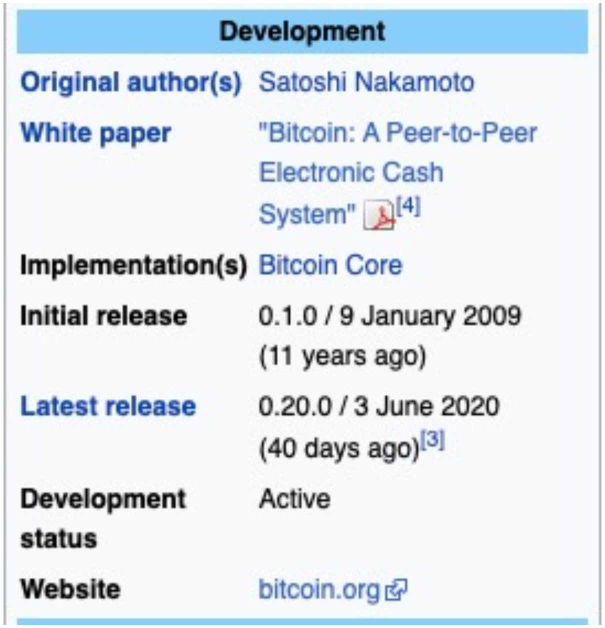
8-23-21



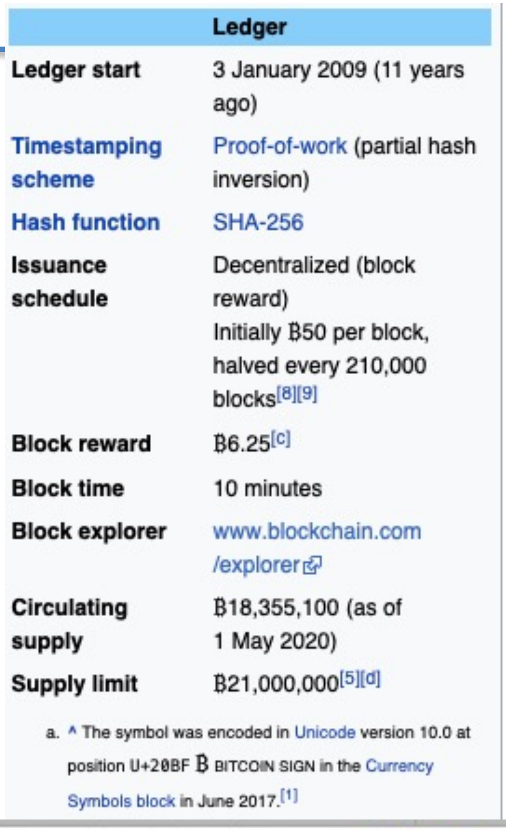
Bitcoin



Bitcoin	
Prevailing bitcoin logo	
Denominations	
Plural	bitcoins
Symbol	₿ (Unicode: U+20BF ₿ BITCOIN SIGN (HTML `&#8383;`))[a]
Ticker symbol	BTC, XBT[b]
Precision	10^{-8}
Subunits	
1/1000	millibitcoin
1/100000000	satoshi[2]

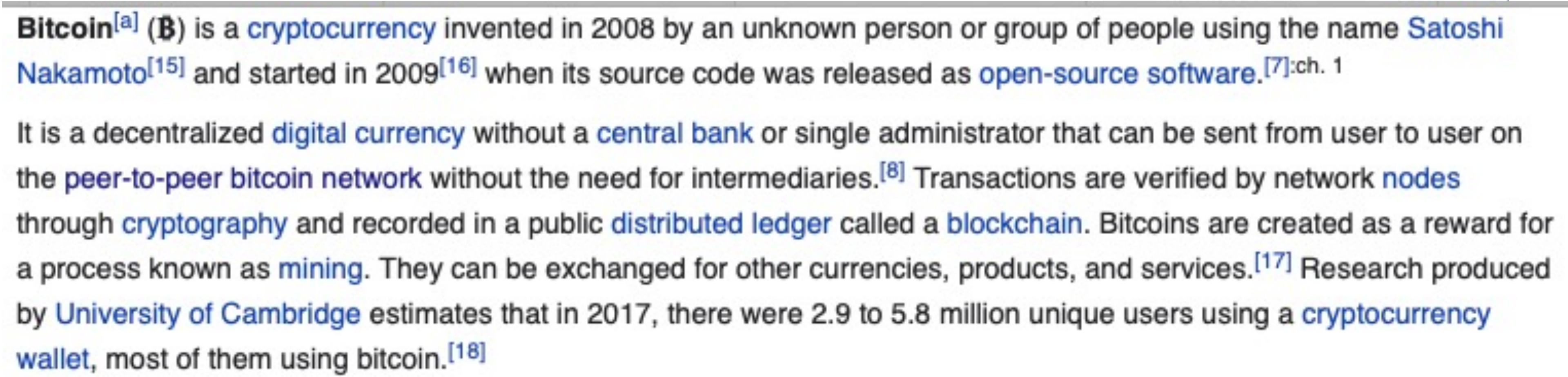


Development	
Original author(s)	Satoshi Nakamoto
White paper	"Bitcoin: A Peer-to-Peer Electronic Cash System"[4]
Implementation(s)	Bitcoin Core
Initial release	0.1.0 / 9 January 2009 (11 years ago)
Latest release	0.20.0 / 3 June 2020 (40 days ago)[3]
Development status	Active
Website	bitcoin.org



Ledger	
Ledger start	3 January 2009 (11 years ago)
Timestamping scheme	Proof-of-work (partial hash inversion)
Hash function	SHA-256
Issuance schedule	Decentralized (block reward) Initially ₿50 per block, halved every 210,000 blocks[8][9]
Block reward	₿6.25[c]
Block time	10 minutes
Block explorer	www.blockchain.com/explorer
Circulating supply	₿18,355,100 (as of 1 May 2020)
Supply limit	₿21,000,000[5][d]

a. ^ The symbol was encoded in Unicode version 10.0 at position U+20BF ₿ BITCOIN SIGN in the Currency Symbols block in June 2017.[1]

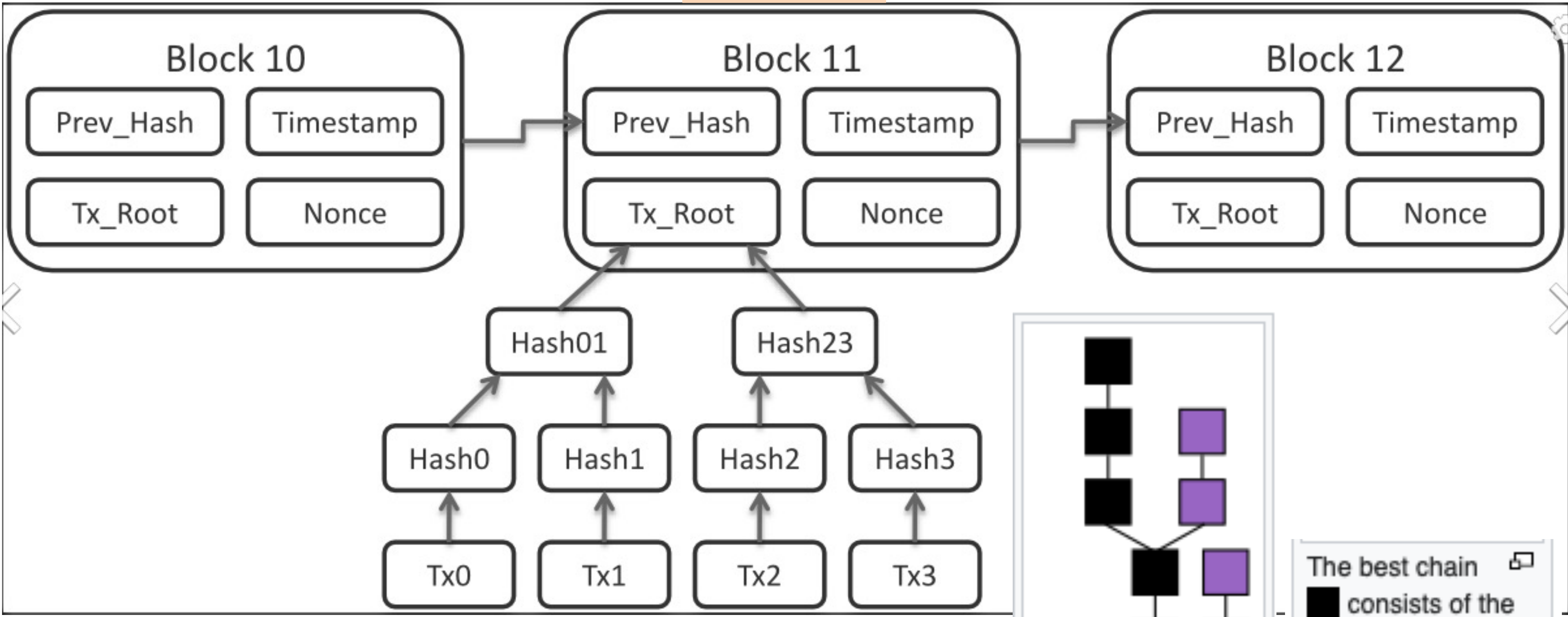


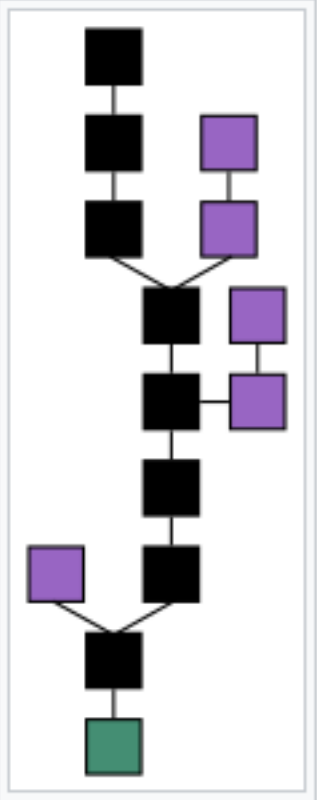
Bitcoin[a] (₿) is a cryptocurrency invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto[15] and started in 2009[16] when its source code was released as open-source software.[7]:ch. 1

It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.[8] Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services.[17] Research produced by University of Cambridge estimates that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin.[18]

Bitcoin

Blockchain

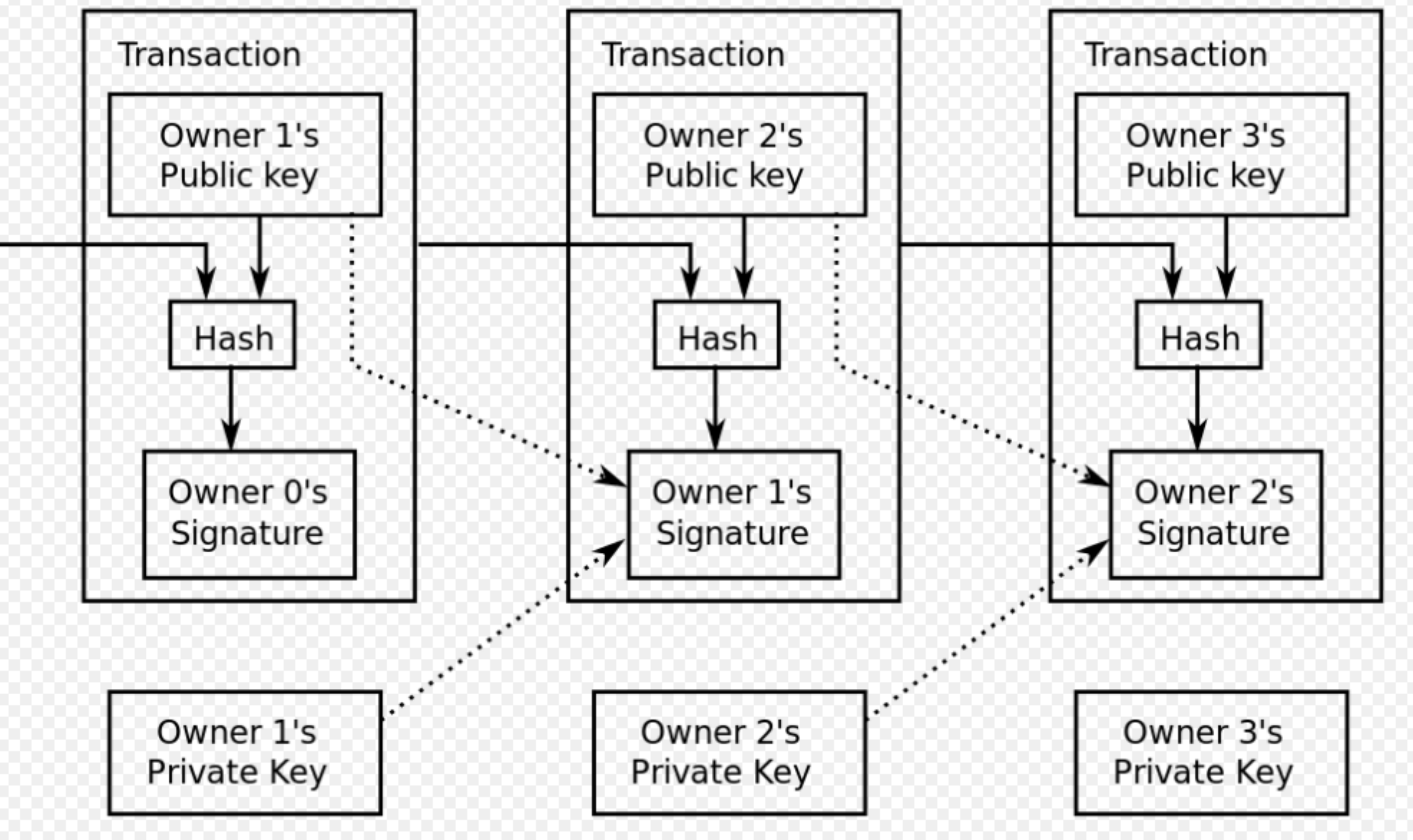




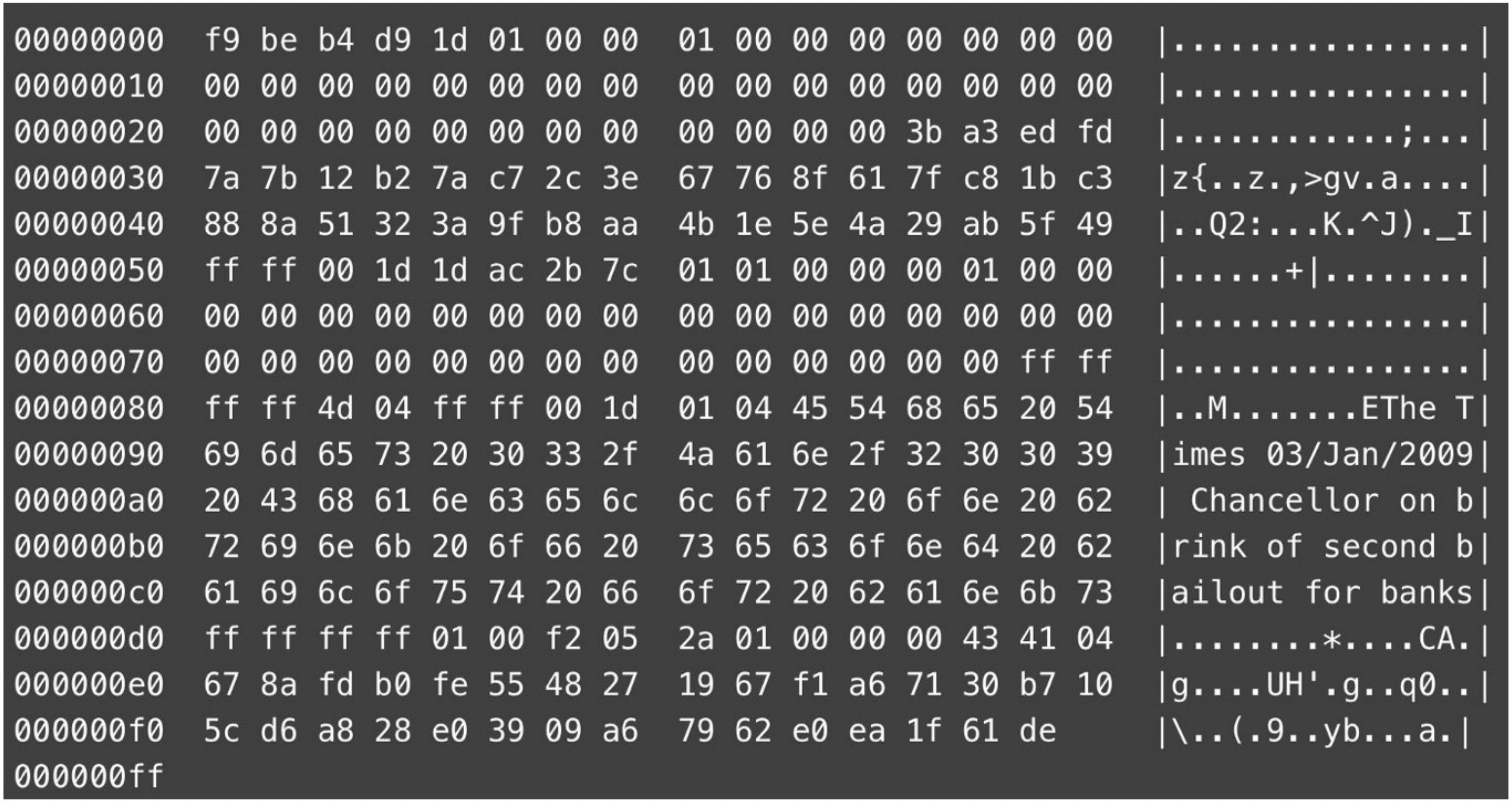
The best chain ■ consists of the longest series of transaction records from the genesis block 🟩 to the current block or record. Orphaned records 🟪 exist outside of the best chain.

Bitcoin

A diagram of a bitcoin transfer



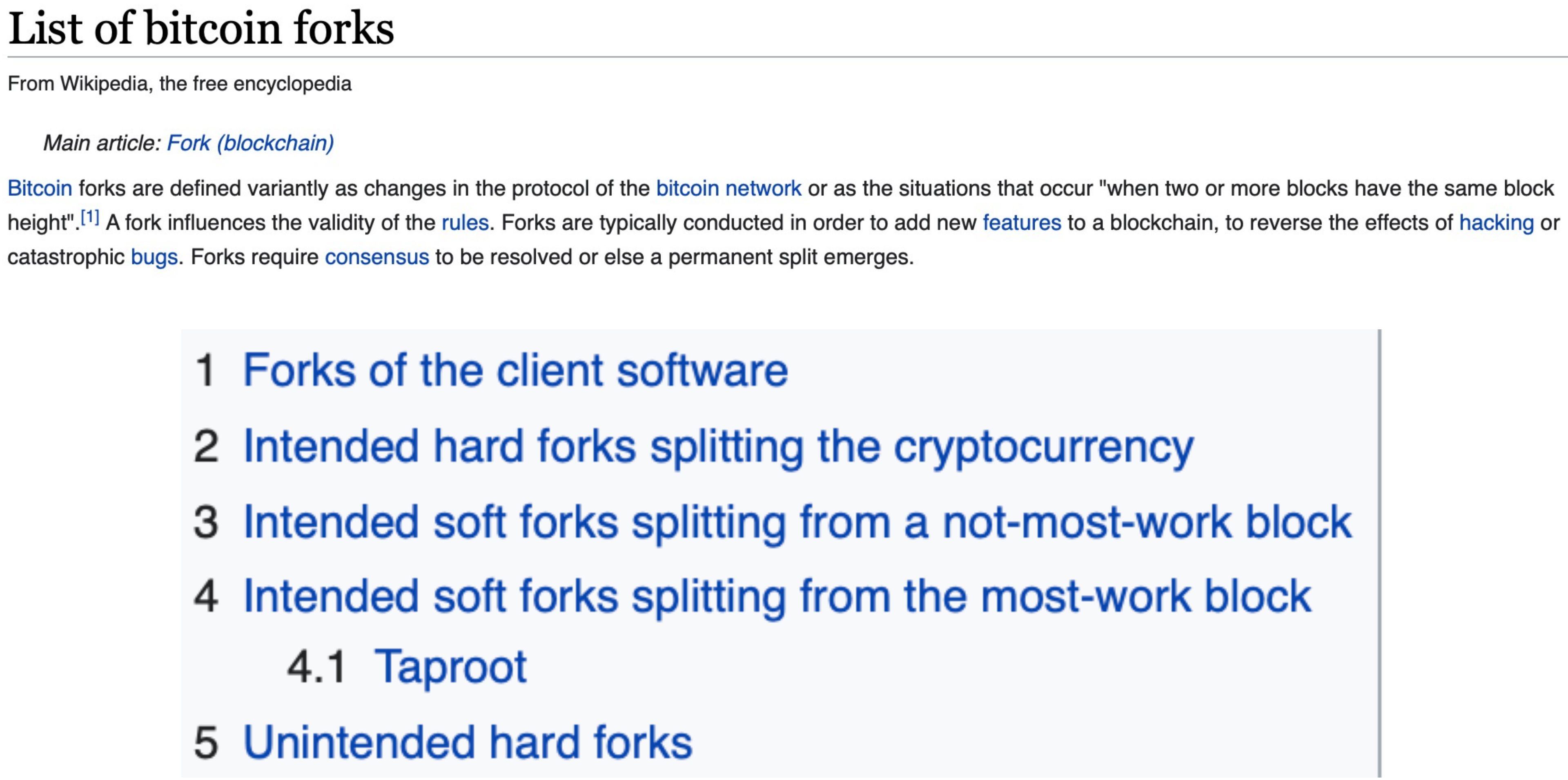
Bitcoin Genesis Block



```
00000000  f9 be b4 d9 1d 01 00 00  01 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 3b a3 ed fd  |............;...|
00000030  7a 7b 12 b2 7a c7 2c 3e  67 76 8f 61 7f c8 1b c3  |z{..z.,>gv.a....|
00000040  88 8a 51 32 3a 9f b8 aa  4b 1e 5e 4a 29 ab 5f 49  |..Q2:...K.^J)._I|
00000050  ff ff 00 1d 1d ac 2b 7c  01 01 00 00 00 01 00 00  |......+|........|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff  |................|
00000080  ff ff 4d 04 ff ff 00 1d  01 04 45 54 68 65 20 54  |..M.......EThe T|
00000090  69 6d 65 73 20 30 33 2f  4a 61 6e 2f 32 30 30 39  |imes 03/Jan/2009|
000000a0  20 43 68 61 6e 63 65 6c  6c 6f 72 20 6f 6e 20 62  | Chancellor on b|
000000b0  72 69 6e 6b 20 6f 66 20  73 65 63 6f 6e 64 20 62  |rink of second b|
000000c0  61 69 6c 6f 75 74 20 66  6f 72 20 62 61 6e 6b 73  |ailout for banks|
000000d0  ff ff ff ff 01 00 f2 05  2a 01 00 00 00 43 41 04  |........*....CA.|
000000e0  67 8a fd b0 fe 55 48 27  19 67 f1 a6 71 30 b7 10  |g....UH'.g..q0..|
000000f0  5c d6 a8 28 e0 39 09 a6  79 62 e0 ea 1f 61 de     |\..(.9..yb...a.|
000000ff
```

Bitcoins Genesis Block with the famous lines in the right down corner

Bitcoin Forks



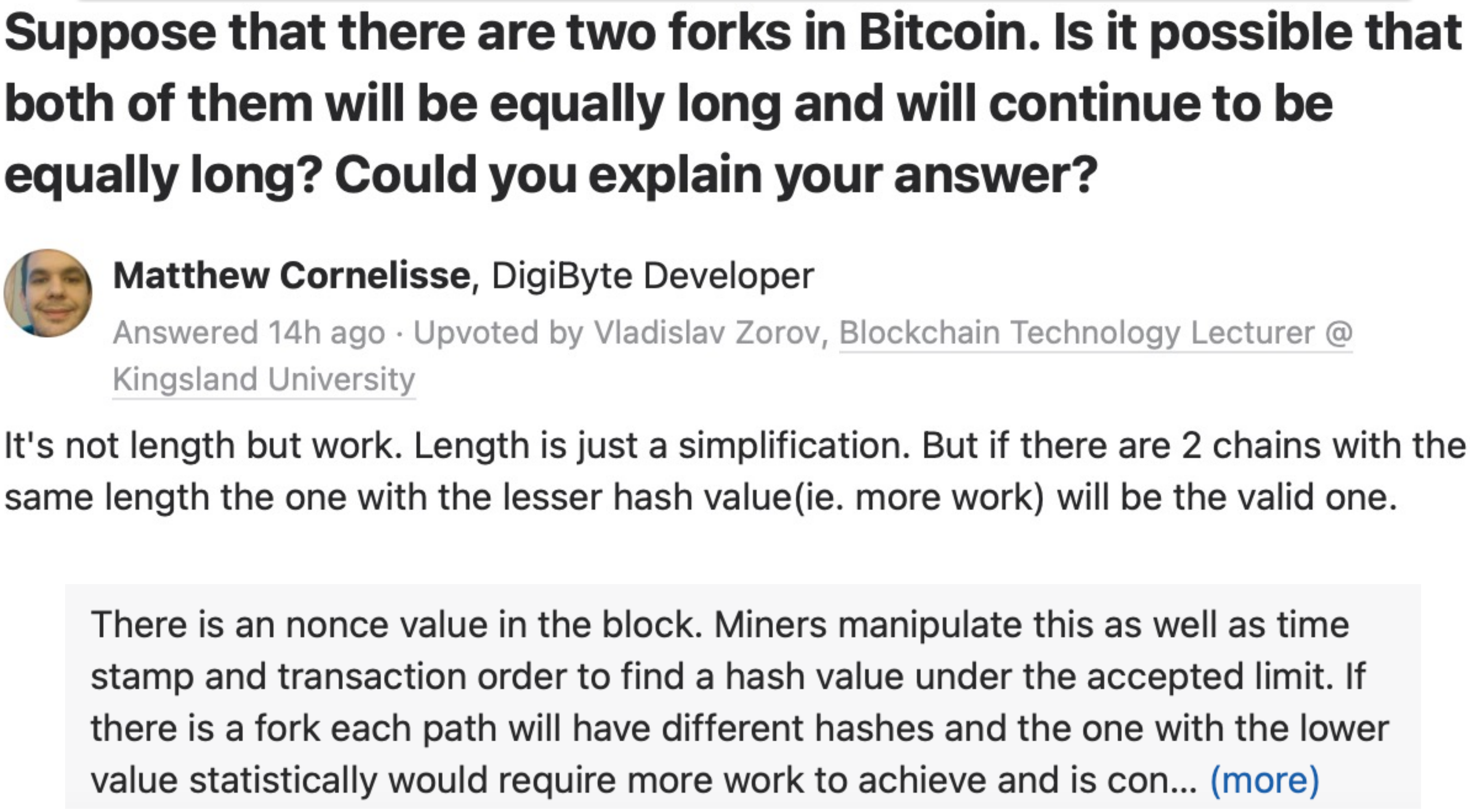
List of bitcoin forks

From Wikipedia, the free encyclopedia

Main article: Fork (blockchain)

Bitcoin forks are defined variantly as changes in the protocol of the bitcoin network or as the situations that occur "when two or more blocks have the same block height".[1] A fork influences the validity of the rules. Forks are typically conducted in order to add new features to a blockchain, to reverse the effects of hacking or catastrophic bugs. Forks require consensus to be resolved or else a permanent split emerges.

Bitcoin Forks



Suppose that there are two forks in Bitcoin. Is it possible that both of them will be equally long and will continue to be equally long? Could you explain your answer?

Matthew Cornelisse, DigiByte Developer

Answered 14h ago · Upvoted by Vladislav Zorov, Blockchain Technology Lecturer @ Kingsland University

It's not length but work. Length is just a simplification. But if there are 2 chains with the same length the one with the lesser hash value(ie. more work) will be the valid one.

> There is an nonce value in the block. Miners manipulate this as well as time stamp and transaction order to find a hash value under the accepted limit. If there is a fork each path will have different hashes and the one with the lower value statistically would require more work to achieve and is con... (more)

Bitcoin Mining

Medium-Pathania

Bitcoin Mining With 12 Lines of Code in Python

Mint money using the power of coding

Shubham Pathania Follow
Feb 5 · 5 min read ★

Bitcoin Mining

Medium

What’s the Benefit of Mining a Bitcoin?

Bitcoin miners receive bitcoin for mining a block. In 2009, for mining one block, you’d receive 50 BTC. In 2012, it was reduced to 25 BTC.

Every four years, the reward is halved for mining a block. In 2020, the reward was reduced to 6.25 BTC. But bitcoin appreciated a lot in the last few years. Even 6.25 BTC per block means 190,000 dollars. That’s quite a lot of money for doing such work.

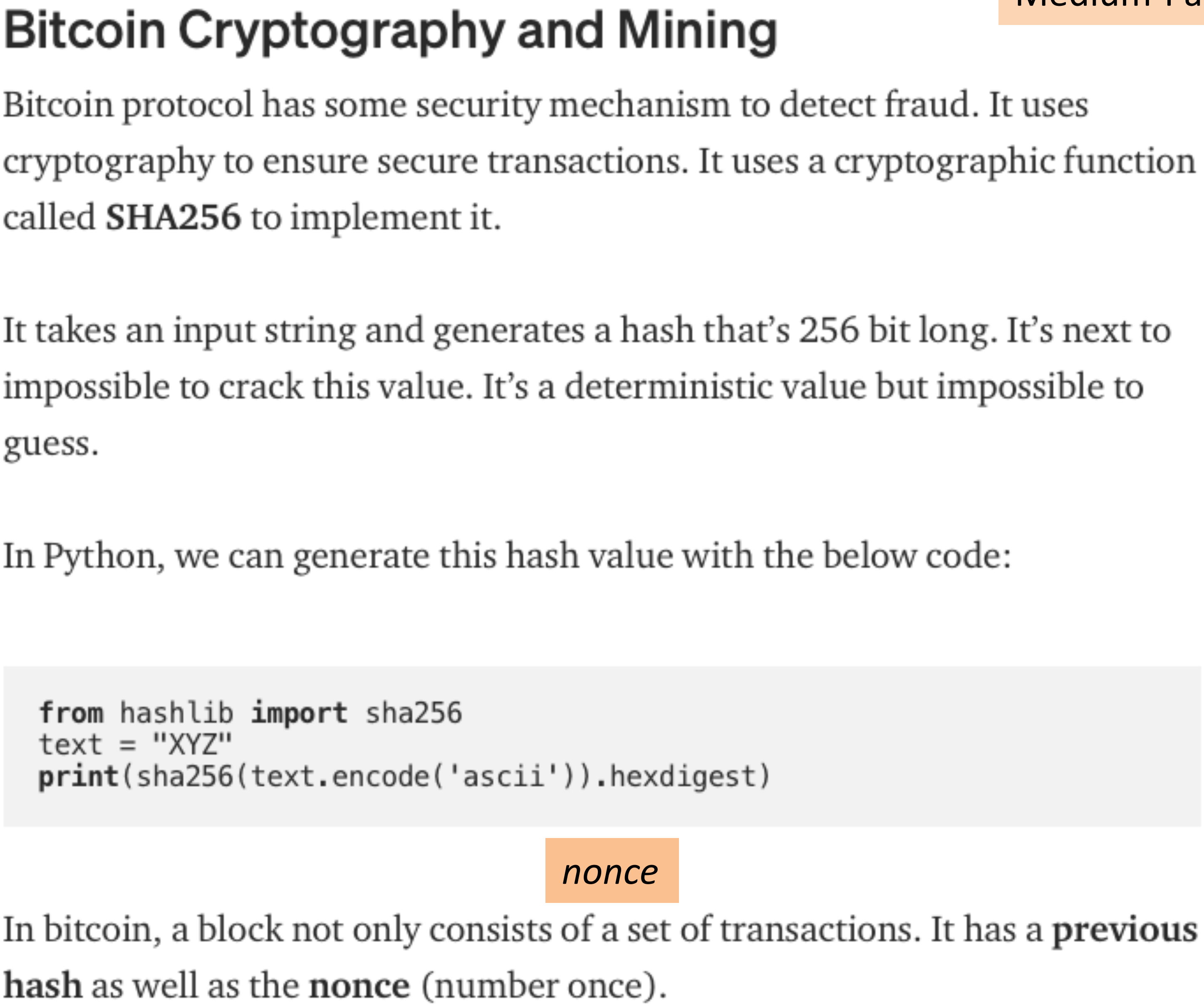
6.25 BTC =~ $250,000

Many people around the world are doing bitcoin mining. It’s not very difficult, but it is a time-consuming task. It takes a lot of computation power to get the right value. If 10 people are doing the guessing work, then whoever gets the result first wins the reward.

Therefore, it takes both time and luck to win the reward in bitcoin mining.

Bitcoin Mining

Medium-Pathania



Bitcoin Cryptography and Mining

Bitcoin protocol has some security mechanism to detect fraud. It uses cryptography to ensure secure transactions. It uses a cryptographic function called **SHA256** to implement it.

It takes an input string and generates a hash that's 256 bit long. It's next to impossible to crack this value. It's a deterministic value but impossible to guess.

In Python, we can generate this hash value with the below code:

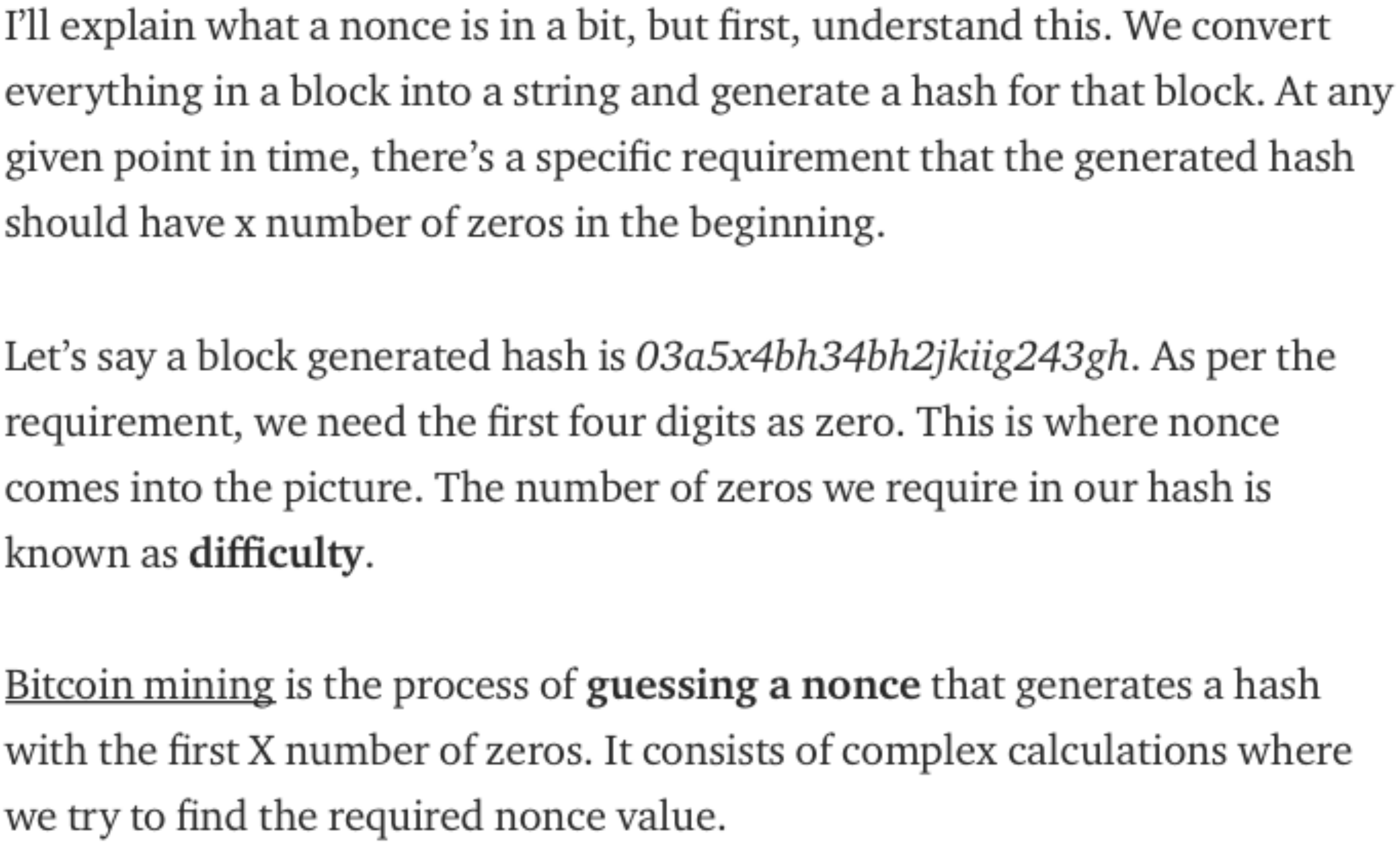
```
from hashlib import sha256
text = "XYZ"
print(sha256(text.encode('ascii')).hexdigest)
```

nonce

In bitcoin, a block not only consists of a set of transactions. It has a **previous hash** as well as the **nonce** (number once).

Bitcoin Mining

Medium-Pathania



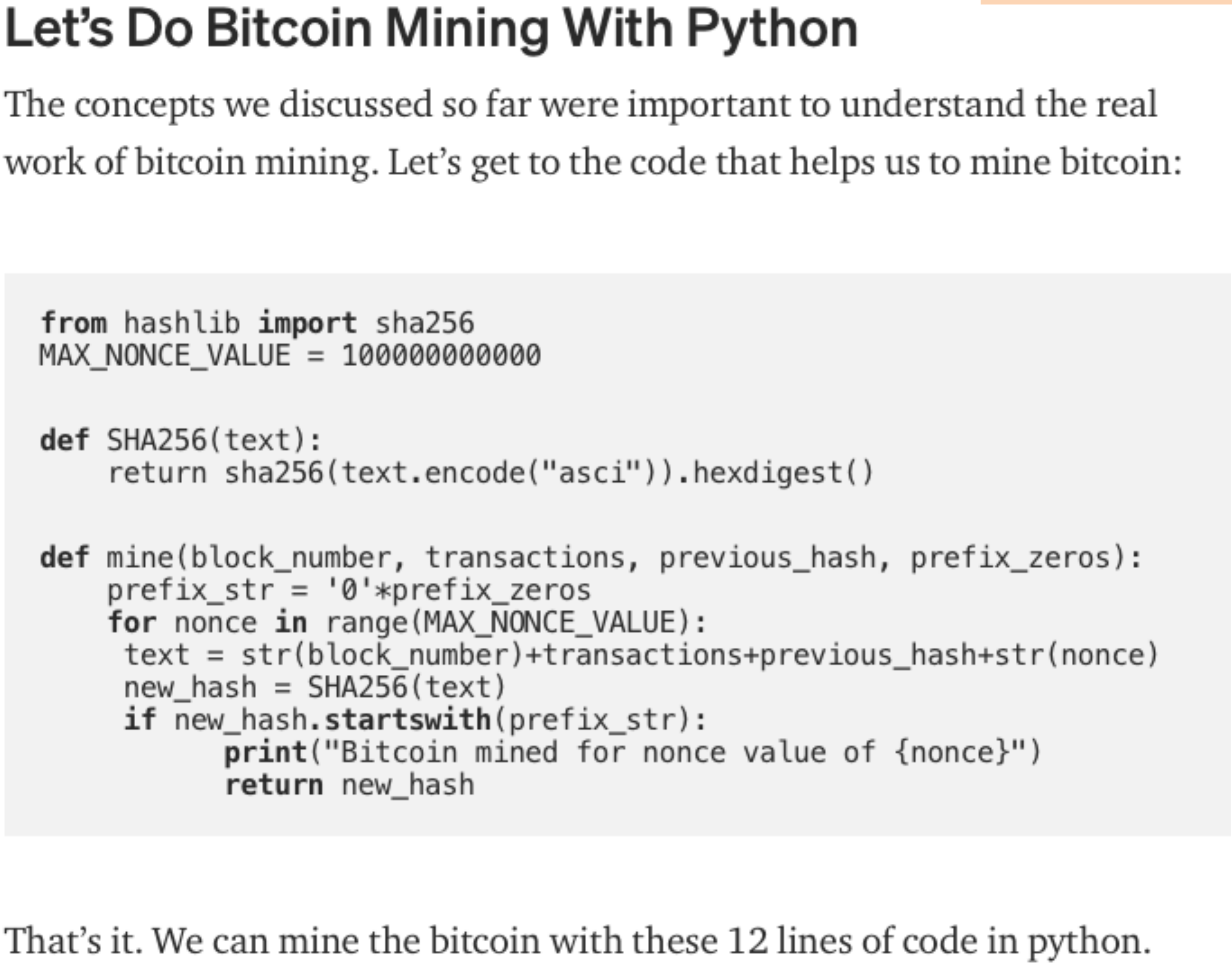
I'll explain what a nonce is in a bit, but first, understand this. We convert everything in a block into a string and generate a hash for that block. At any given point in time, there's a specific requirement that the generated hash should have x number of zeros in the beginning.

Let's say a block generated hash is *03a5x4bh34bh2jkiig243gh*. As per the requirement, we need the first four digits as zero. This is where nonce comes into the picture. The number of zeros we require in our hash is known as **difficulty**.

Bitcoin mining is the process of **guessing a nonce** that generates a hash with the first X number of zeros. It consists of complex calculations where we try to find the required nonce value.

Bitcoin Mining

Medium-Pathania



Let’s Do Bitcoin Mining With Python

The concepts we discussed so far were important to understand the real work of bitcoin mining. Let’s get to the code that helps us to mine bitcoin:

```
from hashlib import sha256
MAX_NONCE_VALUE = 100000000000

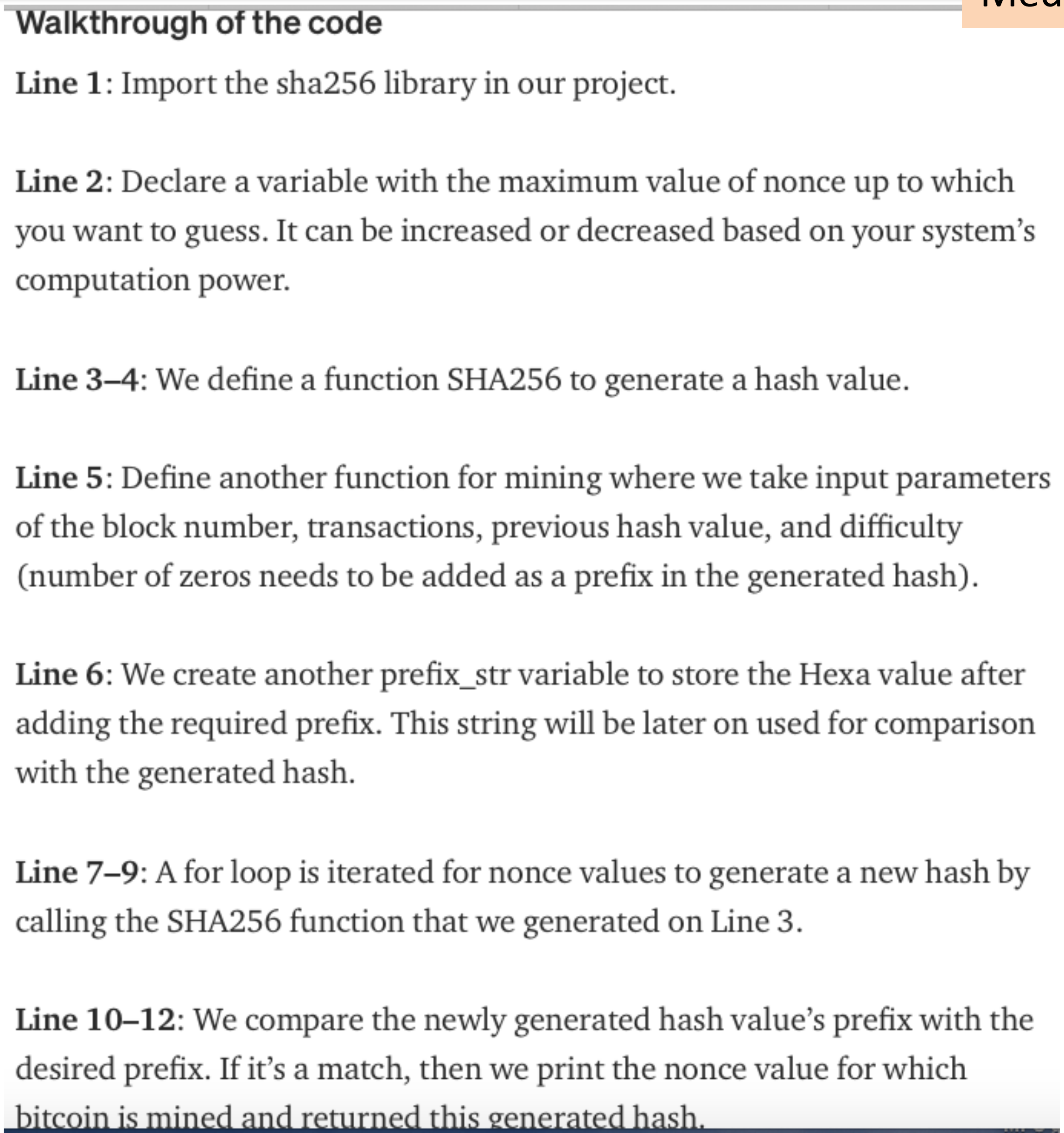

def SHA256(text):
    return sha256(text.encode("asci")).hexdigest()


def mine(block_number, transactions, previous_hash, prefix_zeros):
    prefix_str = '0'*prefix_zeros
    for nonce in range(MAX_NONCE_VALUE):
     text = str(block_number)+transactions+previous_hash+str(nonce)
     new_hash = SHA256(text)
     if new_hash.startswith(prefix_str):
           print("Bitcoin mined for nonce value of {nonce}")
           return new_hash
```

That’s it. We can mine the bitcoin with these 12 lines of code in python.

Bitcoin Mining

Medium-Pathania



Walkthrough of the code

Line 1: Import the sha256 library in our project.

Line 2: Declare a variable with the maximum value of nonce up to which you want to guess. It can be increased or decreased based on your system's computation power.

Line 3–4: We define a function SHA256 to generate a hash value.

Line 5: Define another function for mining where we take input parameters of the block number, transactions, previous hash value, and difficulty (number of zeros needs to be added as a prefix in the generated hash).

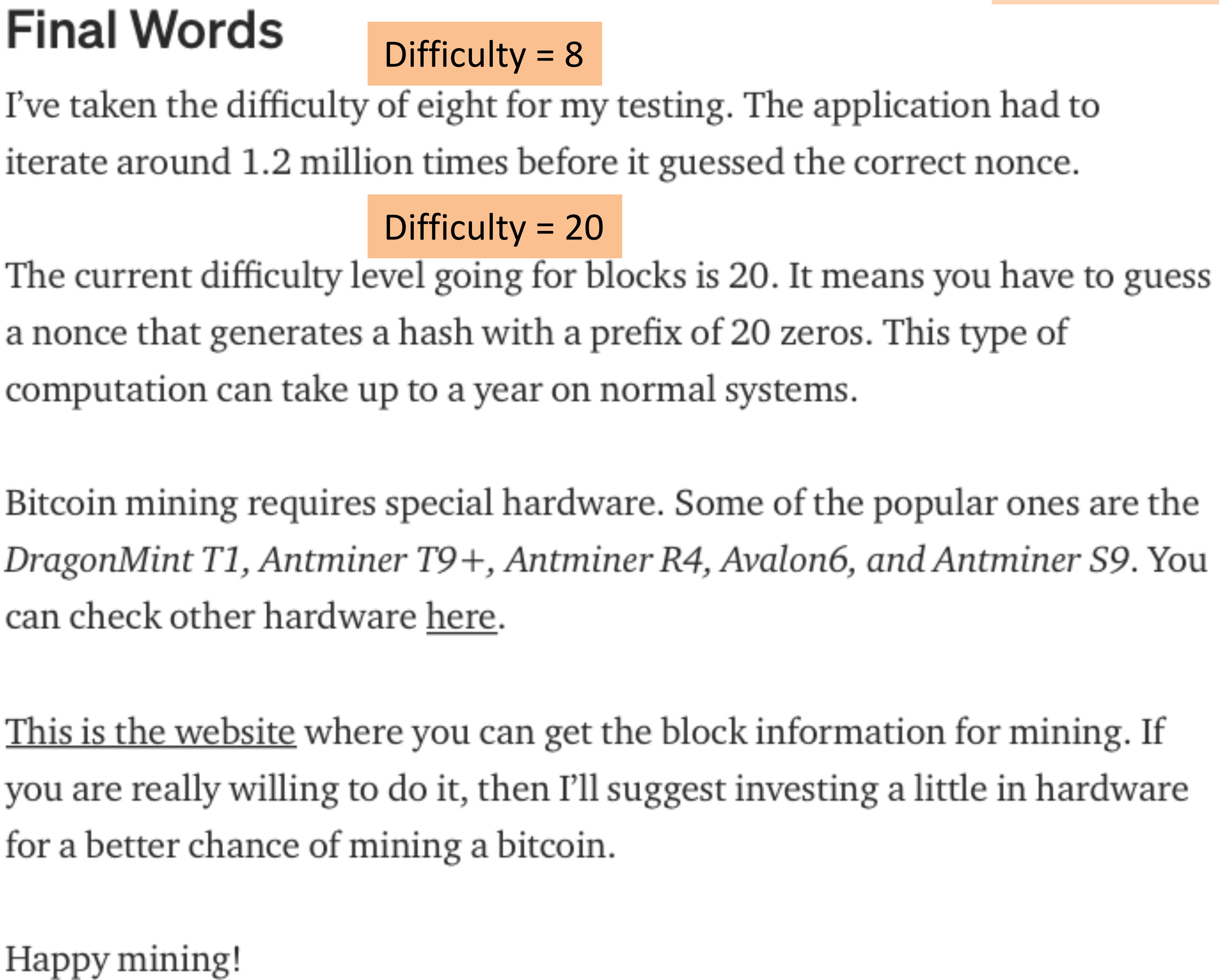
Line 6: We create another prefix_str variable to store the Hexa value after adding the required prefix. This string will be later on used for comparison with the generated hash.

Line 7–9: A for loop is iterated for nonce values to generate a new hash by calling the SHA256 function that we generated on Line 3.

Line 10–12: We compare the newly generated hash value's prefix with the desired prefix. If it's a match, then we print the nonce value for which bitcoin is mined and returned this generated hash.

Bitcoin Mining

Medium-Pathania



Final Words

Difficulty = 8

I've taken the difficulty of eight for my testing. The application had to iterate around 1.2 million times before it guessed the correct nonce.

Difficulty = 20

The current difficulty level going for blocks is 20. It means you have to guess a nonce that generates a hash with a prefix of 20 zeros. This type of computation can take up to a year on normal systems.

Bitcoin mining requires special hardware. Some of the popular ones are the *DragonMint T1, Antminer T9+, Antminer R4, Avalon6, and Antminer S9*. You can check other hardware here.

This is the website where you can get the block information for mining. If you are really willing to do it, then I'll suggest investing a little in hardware for a better chance of mining a bitcoin.

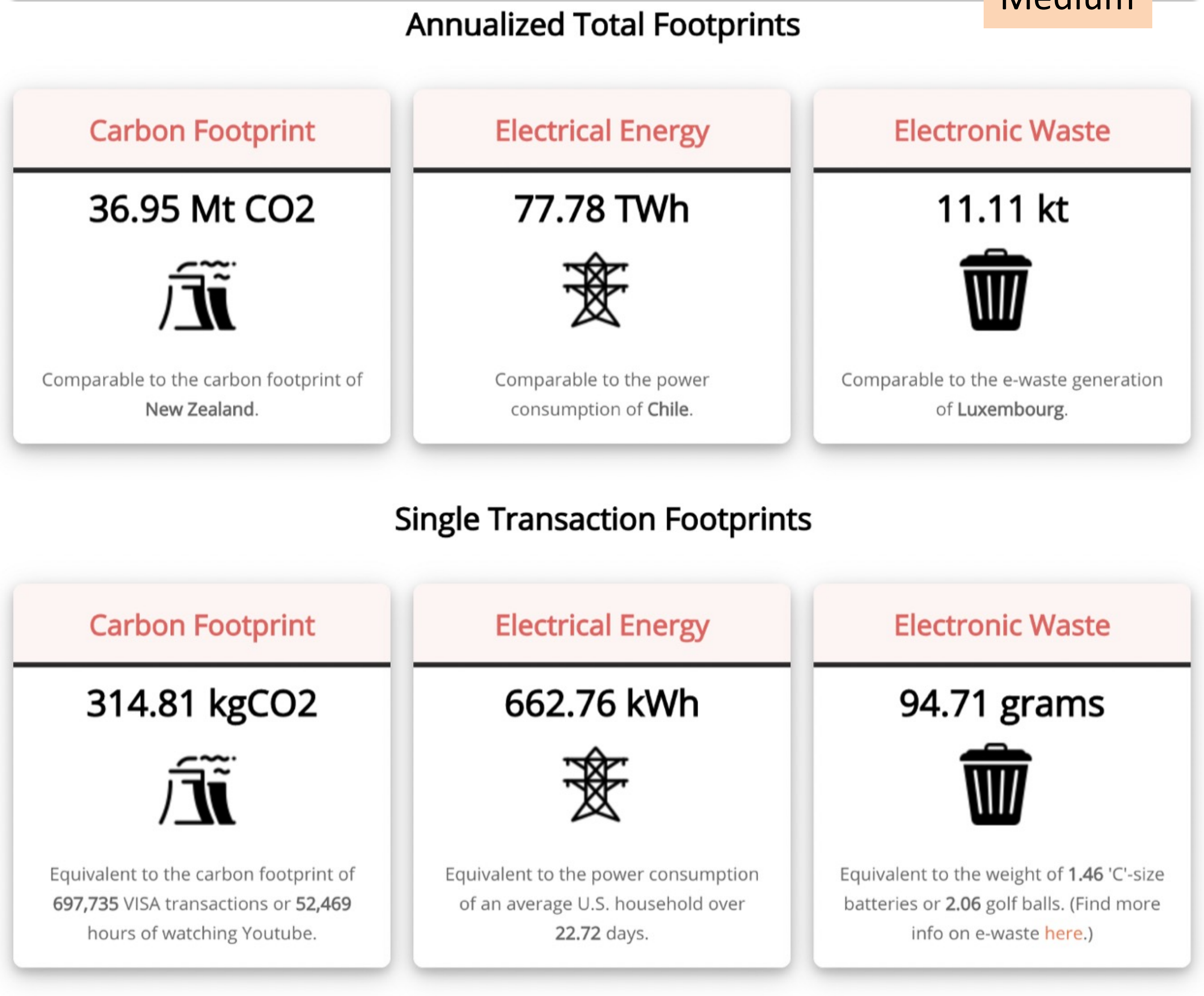
Happy mining!

CSUN
CALIFORNIA STATE UNIVERSITY NORTHRIDGE

Bitcoin Mining Costs

DR JEFF SOFTWARE
©Jeff Drobman
2017-23

Medium



Annualized Total Footprints

Carbon Footprint

36.95 Mt CO2

Comparable to the carbon footprint of **New Zealand**.

Electrical Energy

77.78 TWh

Comparable to the power consumption of **Chile**.

Electronic Waste

11.11 kt

Comparable to the e-waste generation of **Luxembourg**.

Single Transaction Footprints

Carbon Footprint

314.81 kgCO2

Equivalent to the carbon footprint of **697,735** VISA transactions or **52,469** hours of watching Youtube.

Electrical Energy

662.76 kWh

Equivalent to the power consumption of an average U.S. household over **22.72** days.

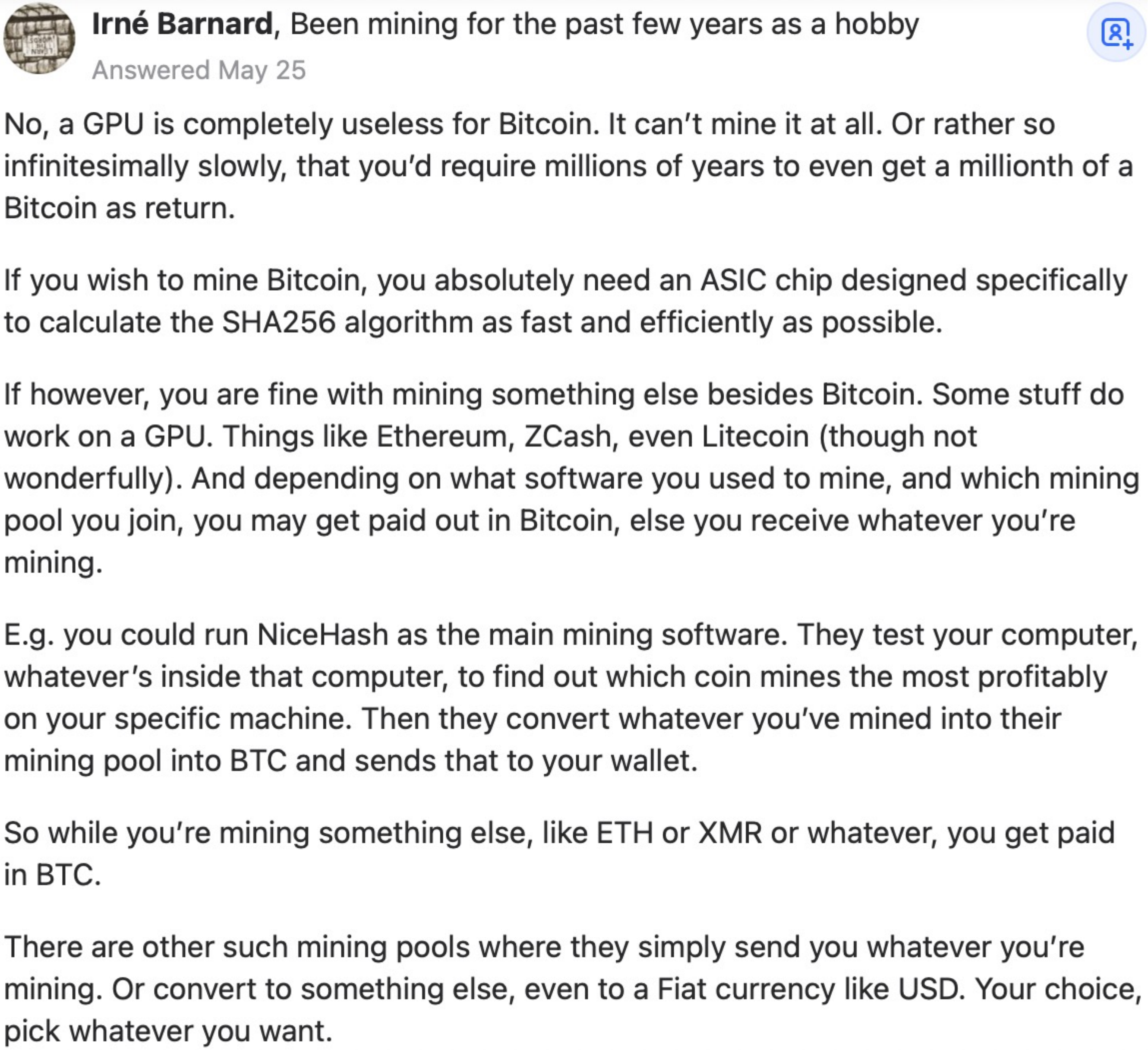
Electronic Waste

94.71 grams

Equivalent to the weight of **1.46** 'C'-size batteries or **2.06** golf balls. (Find more info on e-waste here.)

Bitcoin Mining Posts

Quora



Irné Barnard, Been mining for the past few years as a hobby

Answered May 25

No, a GPU is completely useless for Bitcoin. It can’t mine it at all. Or rather so infinitesimally slowly, that you’d require millions of years to even get a millionth of a Bitcoin as return.

If you wish to mine Bitcoin, you absolutely need an ASIC chip designed specifically to calculate the SHA256 algorithm as fast and efficiently as possible.

If however, you are fine with mining something else besides Bitcoin. Some stuff do work on a GPU. Things like Ethereum, ZCash, even Litecoin (though not wonderfully). And depending on what software you used to mine, and which mining pool you join, you may get paid out in Bitcoin, else you receive whatever you’re mining.

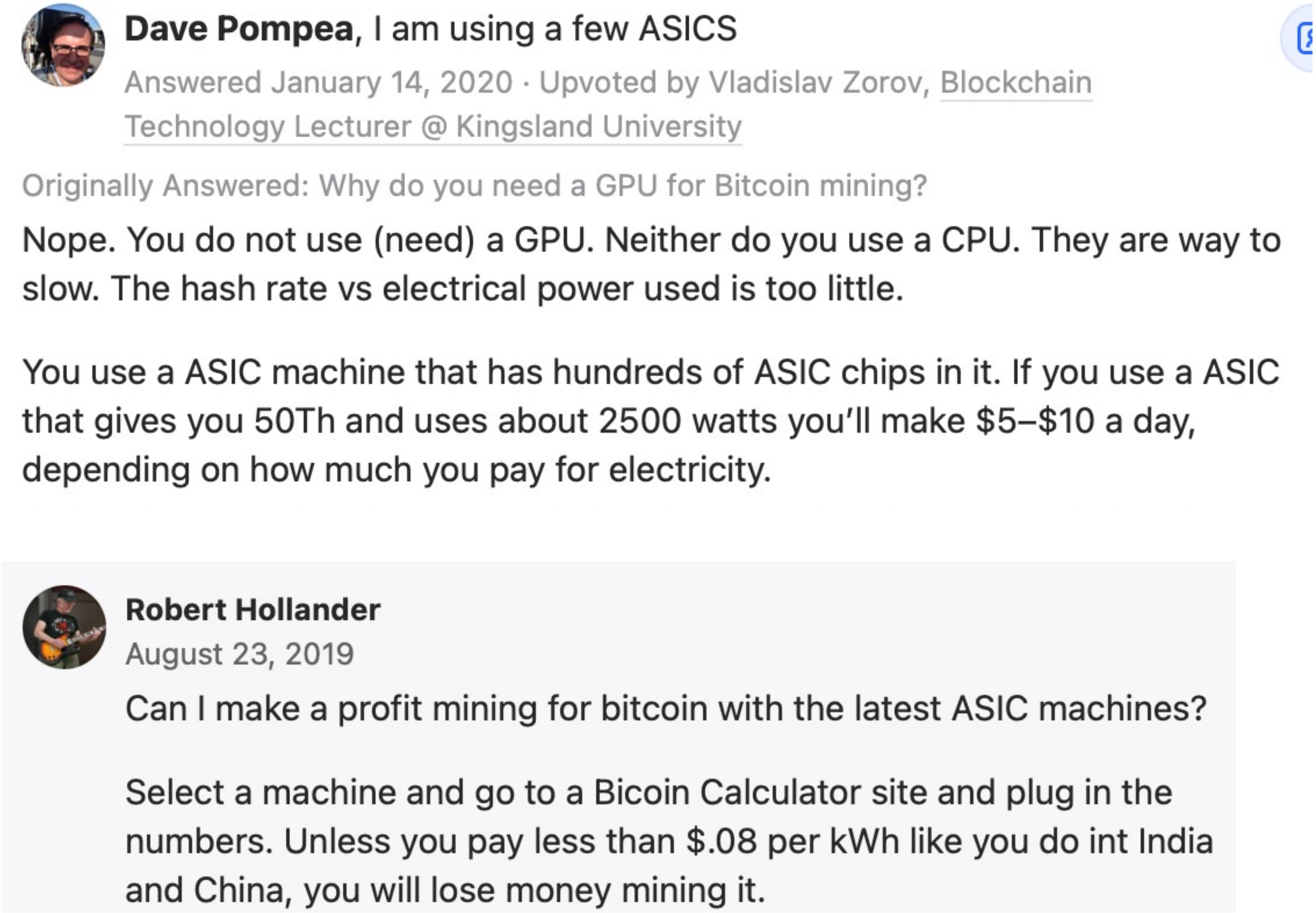
E.g. you could run NiceHash as the main mining software. They test your computer, whatever’s inside that computer, to find out which coin mines the most profitably on your specific machine. Then they convert whatever you’ve mined into their mining pool into BTC and sends that to your wallet.

So while you’re mining something else, like ETH or XMR or whatever, you get paid in BTC.

There are other such mining pools where they simply send you whatever you’re mining. Or convert to something else, even to a Fiat currency like USD. Your choice, pick whatever you want.

Bitcoin Mining Posts

Quora



Dave Pompea, I am using a few ASICS

Answered January 14, 2020 · Upvoted by Vladislav Zorov, Blockchain Technology Lecturer @ Kingsland University

Originally Answered: Why do you need a GPU for Bitcoin mining?

Nope. You do not use (need) a GPU. Neither do you use a CPU. They are way to slow. The hash rate vs electrical power used is too little.

You use a ASIC machine that has hundreds of ASIC chips in it. If you use a ASIC that gives you 50Th and uses about 2500 watts you'll make $5–$10 a day, depending on how much you pay for electricity.

Robert Hollander

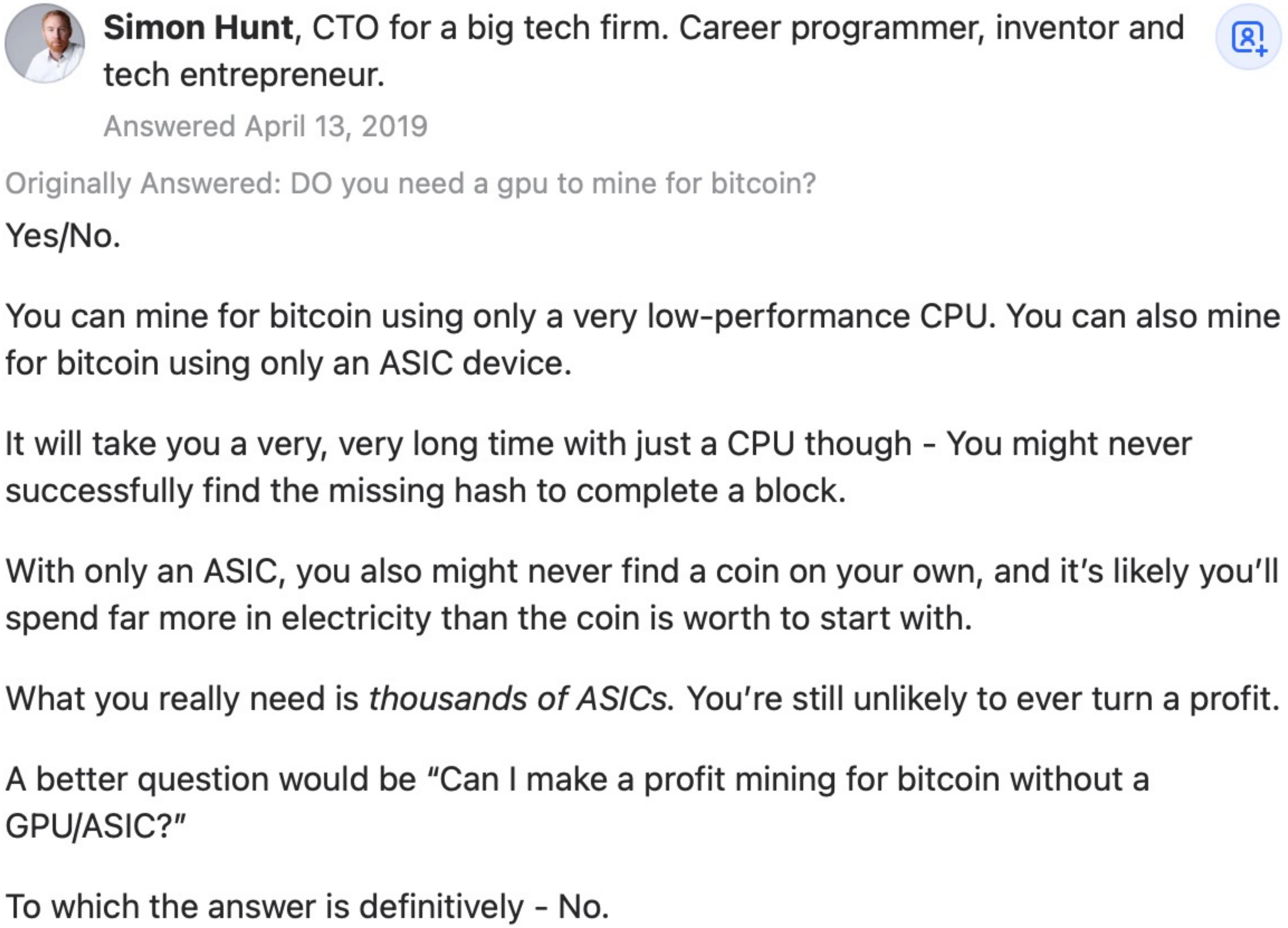
August 23, 2019

Can I make a profit mining for bitcoin with the latest ASIC machines?

Select a machine and go to a Bicoin Calculator site and plug in the numbers. Unless you pay less than $.08 per kWh like you do int India and China, you will lose money mining it.

Bitcoin Mining Posts

Quora



Simon Hunt, CTO for a big tech firm. Career programmer, inventor and tech entrepreneur.

Answered April 13, 2019

Originally Answered: DO you need a gpu to mine for bitcoin?

Yes/No.

You can mine for bitcoin using only a very low-performance CPU. You can also mine for bitcoin using only an ASIC device.

It will take you a very, very long time with just a CPU though - You might never successfully find the missing hash to complete a block.

With only an ASIC, you also might never find a coin on your own, and it's likely you'll spend far more in electricity than the coin is worth to start with.

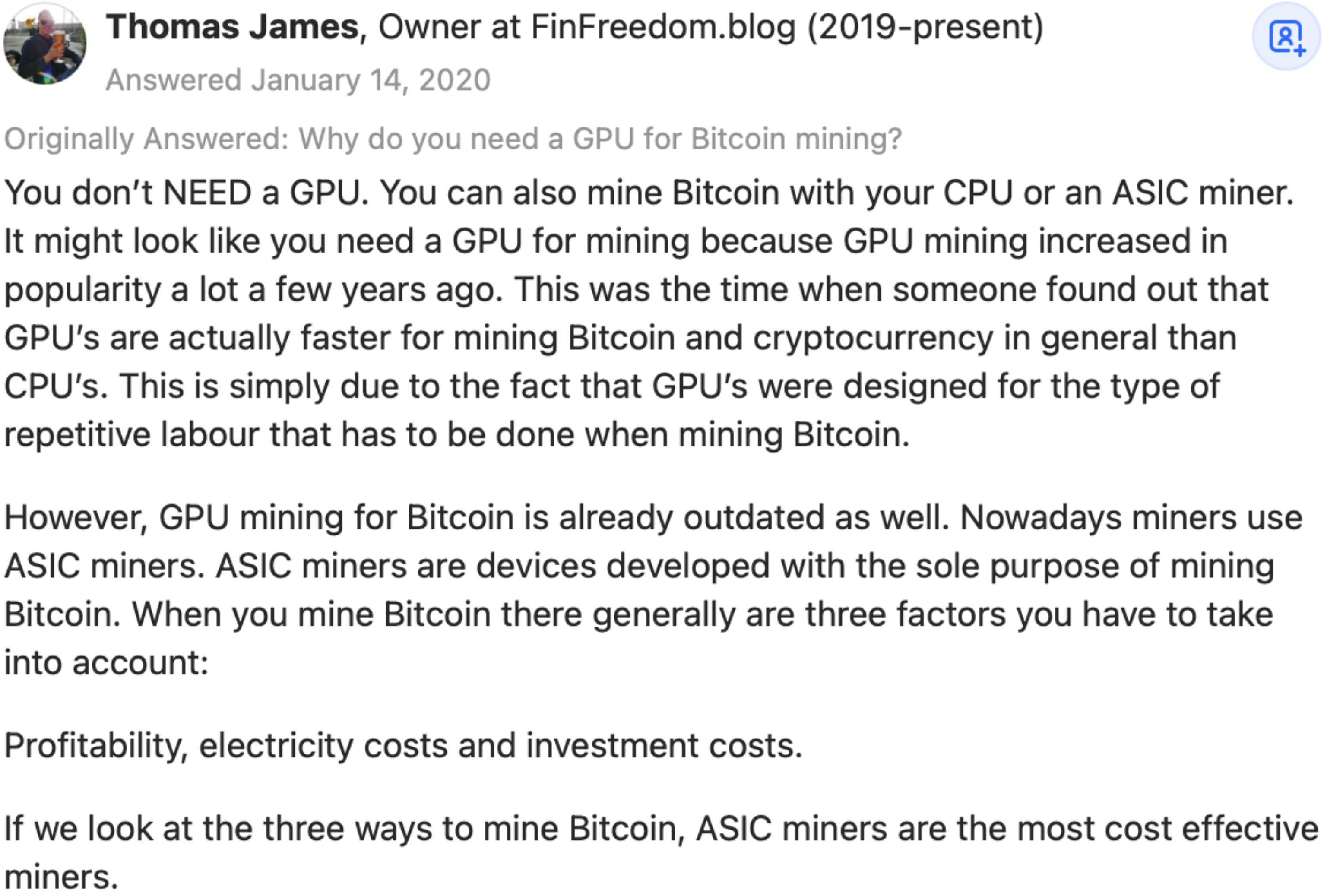
What you really need is *thousands of ASICs*. You're still unlikely to ever turn a profit.

A better question would be "Can I make a profit mining for bitcoin without a GPU/ASIC?"

To which the answer is definitively - No.

Bitcoin Mining Posts

Quora



Thomas James, Owner at FinFreedom.blog (2019-present)

Answered January 14, 2020

Originally Answered: Why do you need a GPU for Bitcoin mining?

You don't NEED a GPU. You can also mine Bitcoin with your CPU or an ASIC miner. It might look like you need a GPU for mining because GPU mining increased in popularity a lot a few years ago. This was the time when someone found out that GPU's are actually faster for mining Bitcoin and cryptocurrency in general than CPU's. This is simply due to the fact that GPU's were designed for the type of repetitive labour that has to be done when mining Bitcoin.

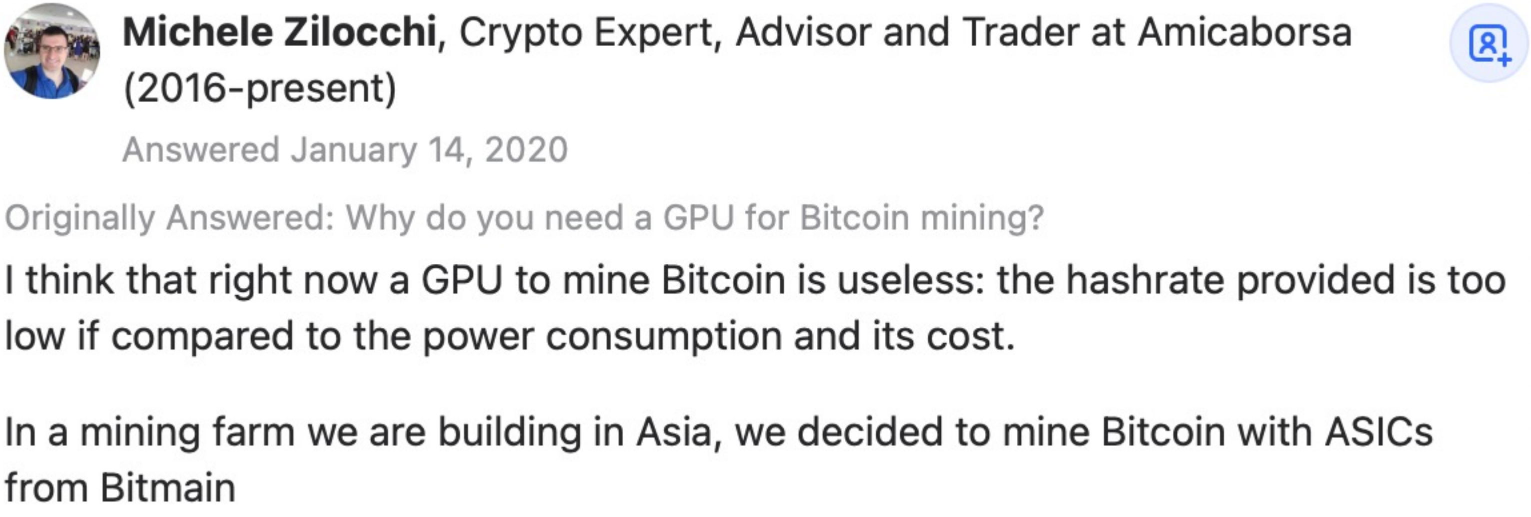
However, GPU mining for Bitcoin is already outdated as well. Nowadays miners use ASIC miners. ASIC miners are devices developed with the sole purpose of mining Bitcoin. When you mine Bitcoin there generally are three factors you have to take into account:

Profitability, electricity costs and investment costs.

If we look at the three ways to mine Bitcoin, ASIC miners are the most cost effective miners.

Bitcoin Mining Posts

Quora



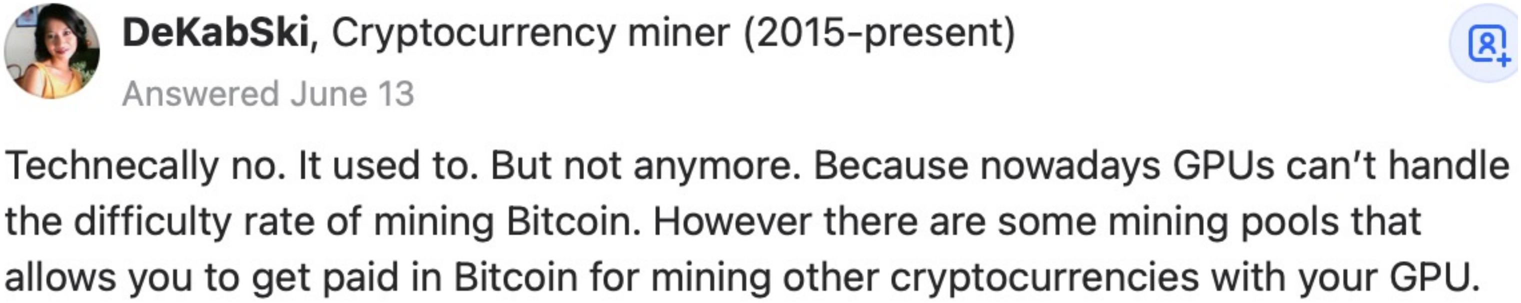
Michele Zilocchi, Crypto Expert, Advisor and Trader at Amicaborsa (2016-present)

Answered January 14, 2020

Originally Answered: Why do you need a GPU for Bitcoin mining?

I think that right now a GPU to mine Bitcoin is useless: the hashrate provided is too low if compared to the power consumption and its cost.

In a mining farm we are building in Asia, we decided to mine Bitcoin with ASICs from Bitmain



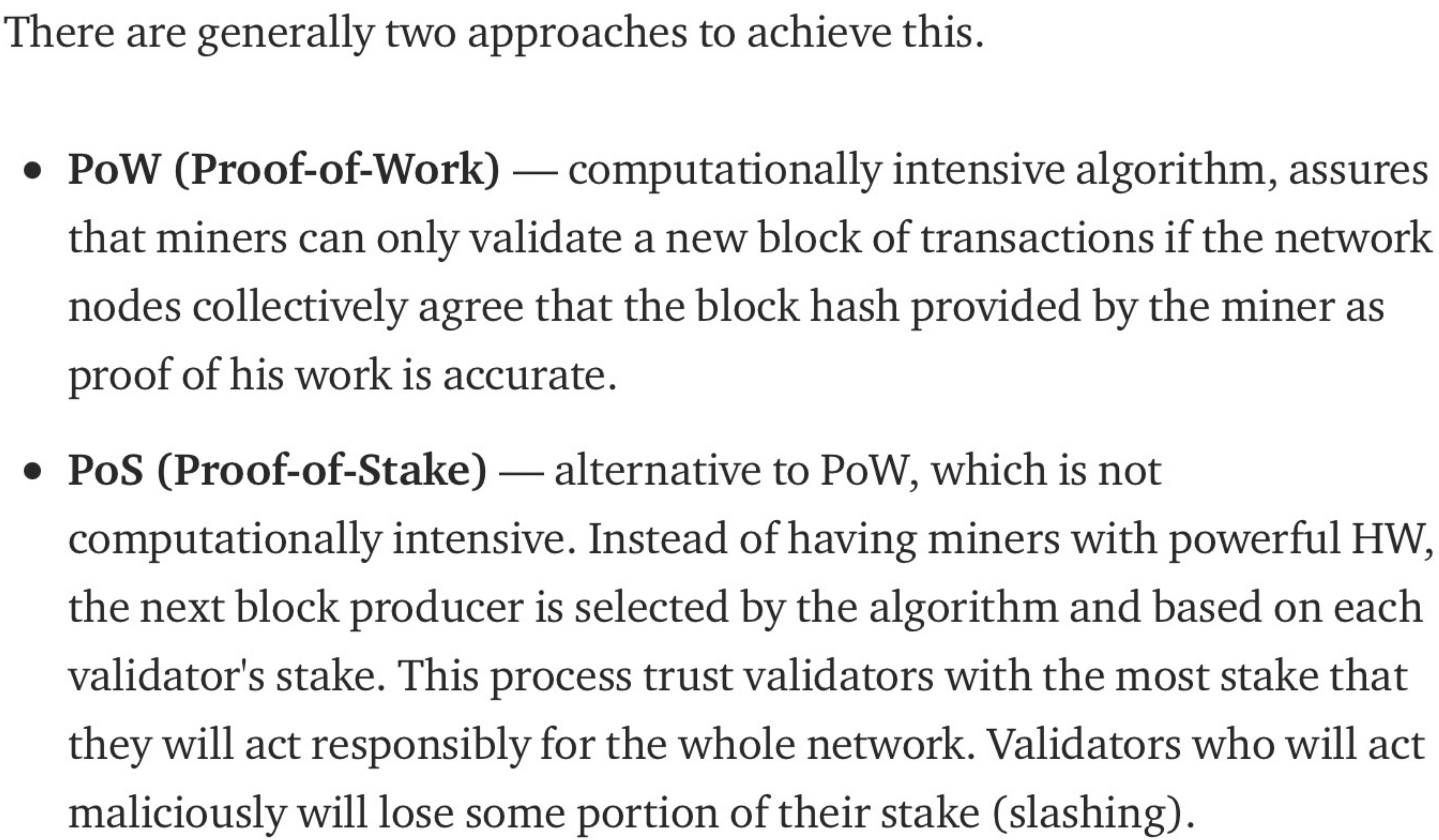
DeKabSki, Cryptocurrency miner (2015-present)

Answered June 13

Technecally no. It used to. But not anymore. Because nowadays GPUs can’t handle the difficulty rate of mining Bitcoin. However there are some mining pools that allows you to get paid in Bitcoin for mining other cryptocurrencies with your GPU.

PoW vs PoS

Medium



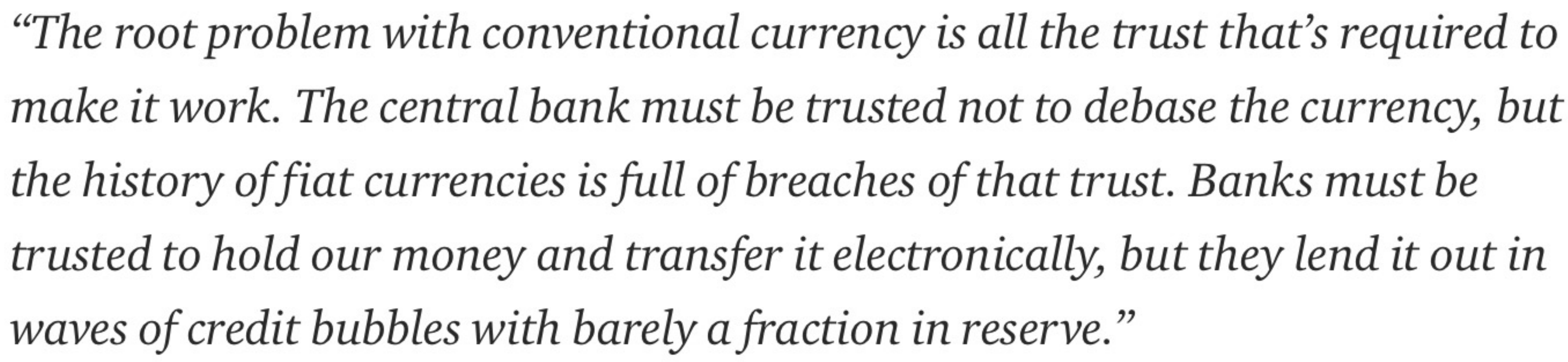
There are generally two approaches to achieve this.

- **PoW (Proof-of-Work)** — computationally intensive algorithm, assures that miners can only validate a new block of transactions if the network nodes collectively agree that the block hash provided by the miner as proof of his work is accurate.
- **PoS (Proof-of-Stake)** — alternative to PoW, which is not computationally intensive. Instead of having miners with powerful HW, the next block producer is selected by the algorithm and based on each validator's stake. This process trust validators with the most stake that they will act responsibly for the whole network. Validators who will act maliciously will lose some portion of their stake (slashing).

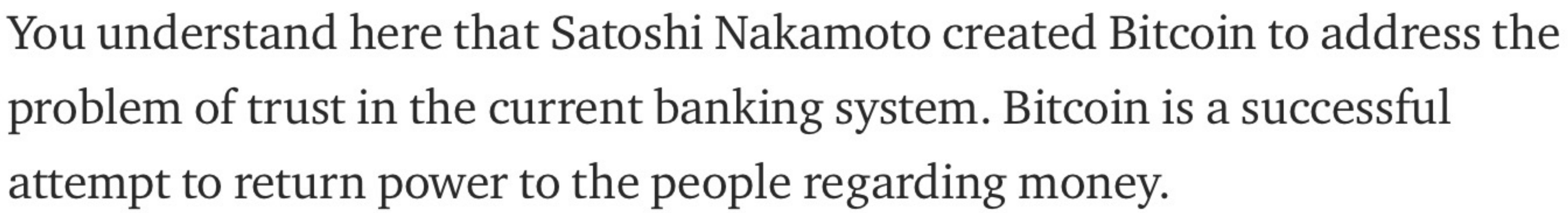
Bitcoin Cap

Cap = 21M

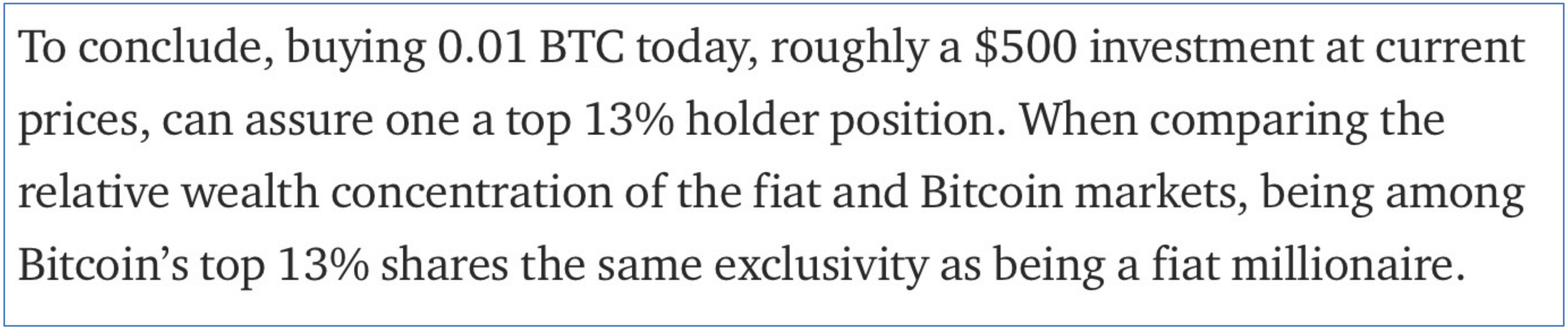
Medium



"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."



You understand here that Satoshi Nakamoto created Bitcoin to address the problem of trust in the current banking system. Bitcoin is a successful attempt to return power to the people regarding money.

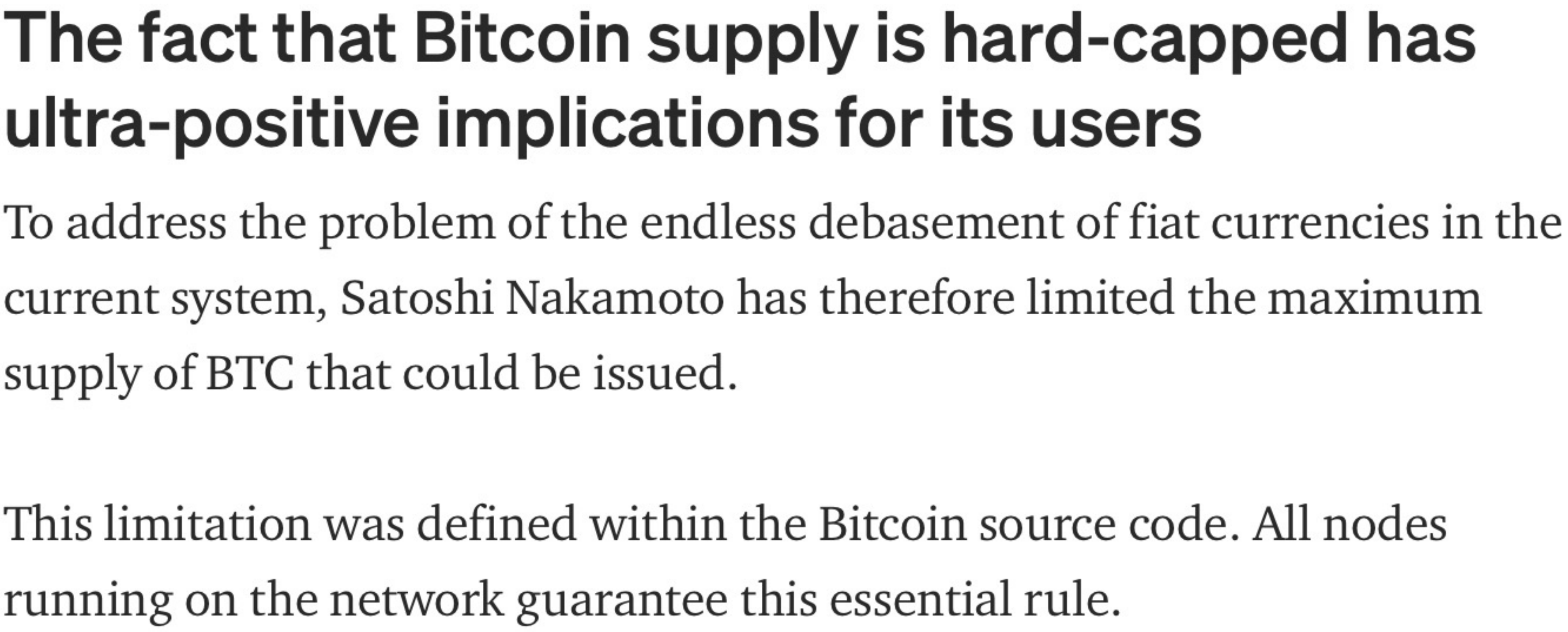


To conclude, buying 0.01 BTC today, roughly a $500 investment at current prices, can assure one a top 13% holder position. When comparing the relative wealth concentration of the fiat and Bitcoin markets, being among Bitcoin's top 13% shares the same exclusivity as being a fiat millionaire.

Bitcoin Cap

Cap = 21M

Medium



The fact that Bitcoin supply is hard-capped has ultra-positive implications for its users

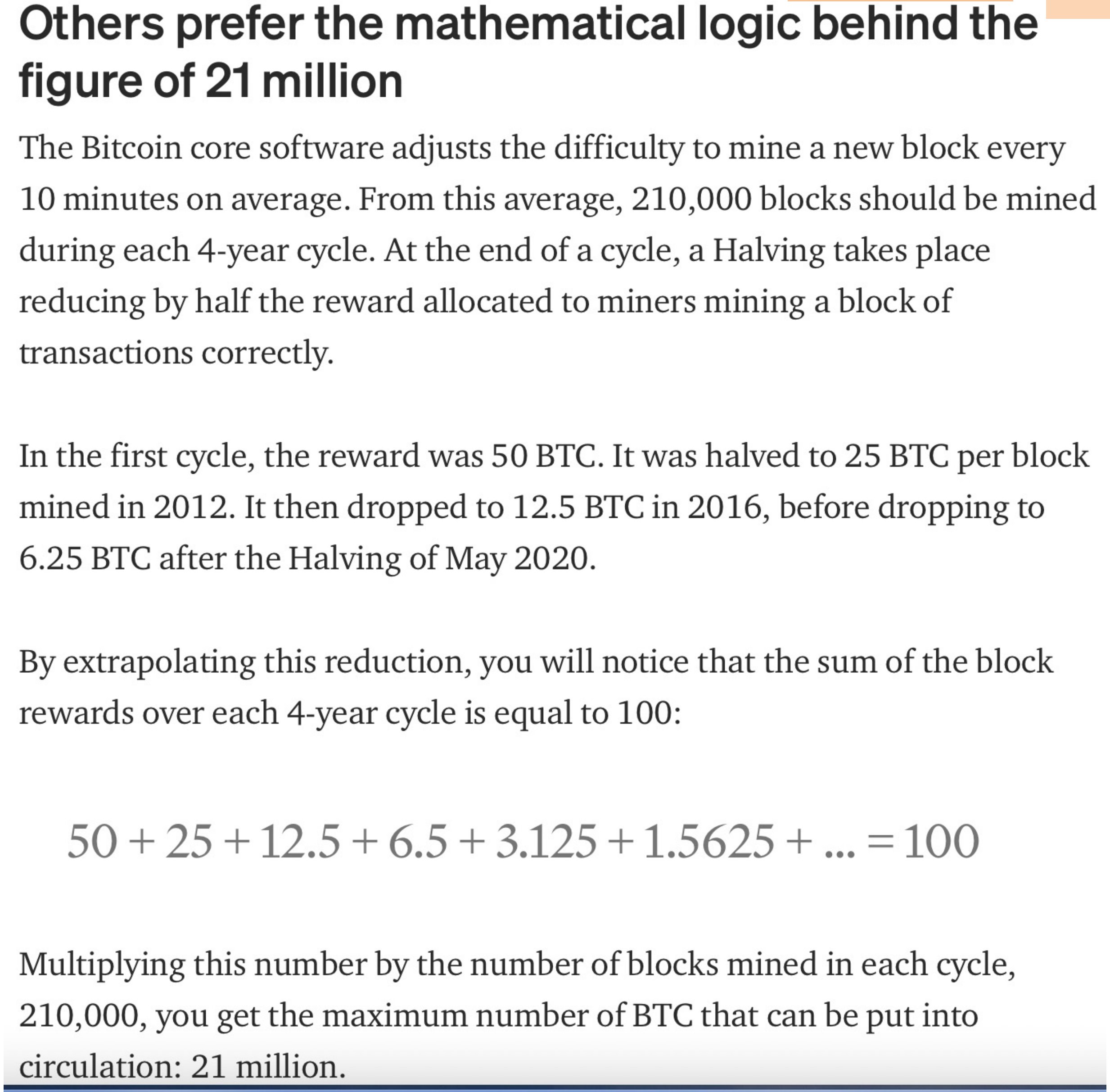
To address the problem of the endless debasement of fiat currencies in the current system, Satoshi Nakamoto has therefore limited the maximum supply of BTC that could be issued.

This limitation was defined within the Bitcoin source code. All nodes running on the network guarantee this essential rule.

Bitcoin Cap

Cap = 21M

Medium



Others prefer the mathematical logic behind the figure of 21 million

The Bitcoin core software adjusts the difficulty to mine a new block every 10 minutes on average. From this average, 210,000 blocks should be mined during each 4-year cycle. At the end of a cycle, a Halving takes place reducing by half the reward allocated to miners mining a block of transactions correctly.

In the first cycle, the reward was 50 BTC. It was halved to 25 BTC per block mined in 2012. It then dropped to 12.5 BTC in 2016, before dropping to 6.25 BTC after the Halving of May 2020.

By extrapolating this reduction, you will notice that the sum of the block rewards over each 4-year cycle is equal to 100:

$$50 + 25 + 12.5 + 6.5 + 3.125 + 1.5625 + \ldots = 100$$

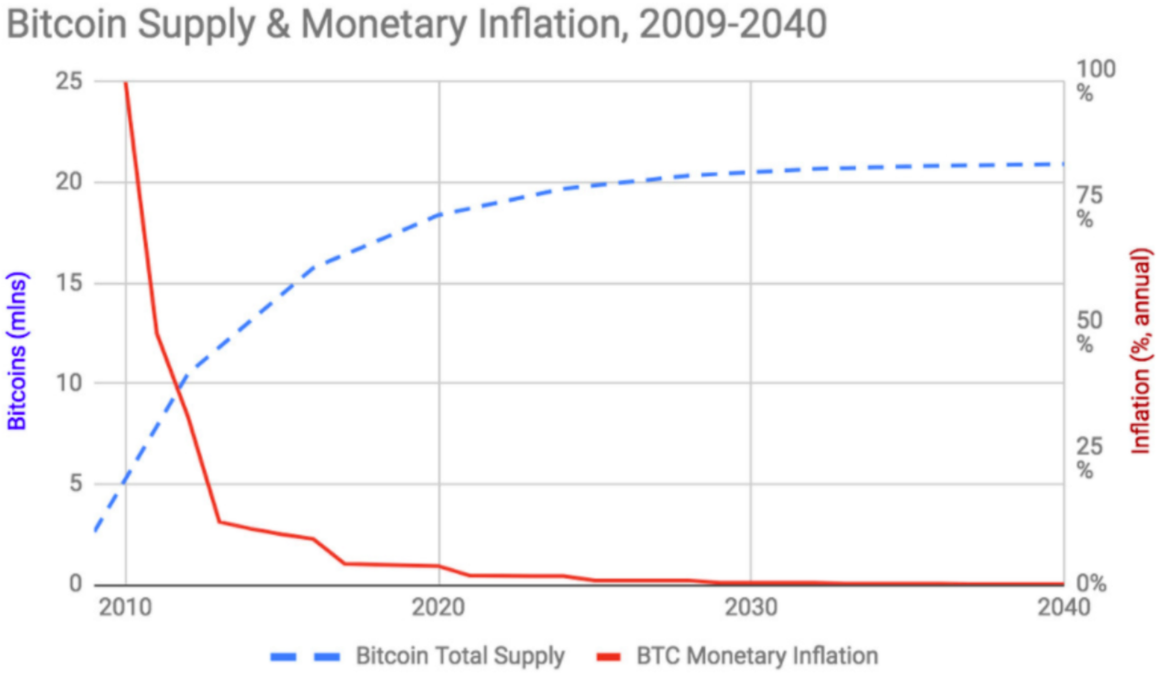
Multiplying this number by the number of blocks mined in each cycle, 210,000, you get the maximum number of BTC that can be put into circulation: 21 million.

Bitcoin Cap

Cap = 21M

Medium

Bitcoin's finite supply will reach 98% in 10 years



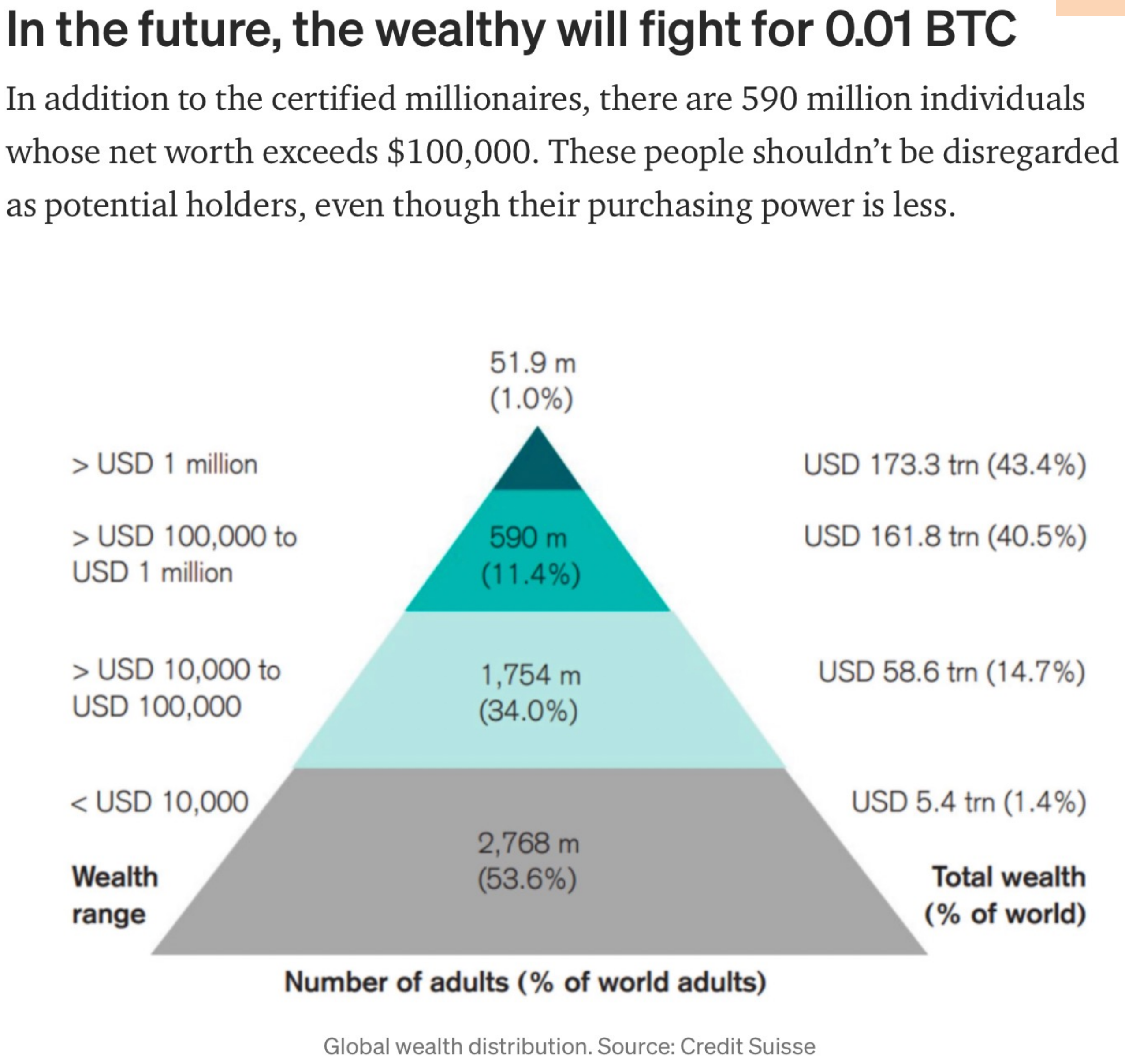
Bitcoin Supply and equivalent inflation. Source: Medium.com/@CryptoProfG

As of March 1, Bitcoin's total supply consists of 18.64 million BTC, leaving 2.37 million coins to be mined. In 10 years, the supply will reach 20.6 million, or 98% of the 21 million coins from the total supply.

Bitcoin Cap

Cap = 21M

Medium

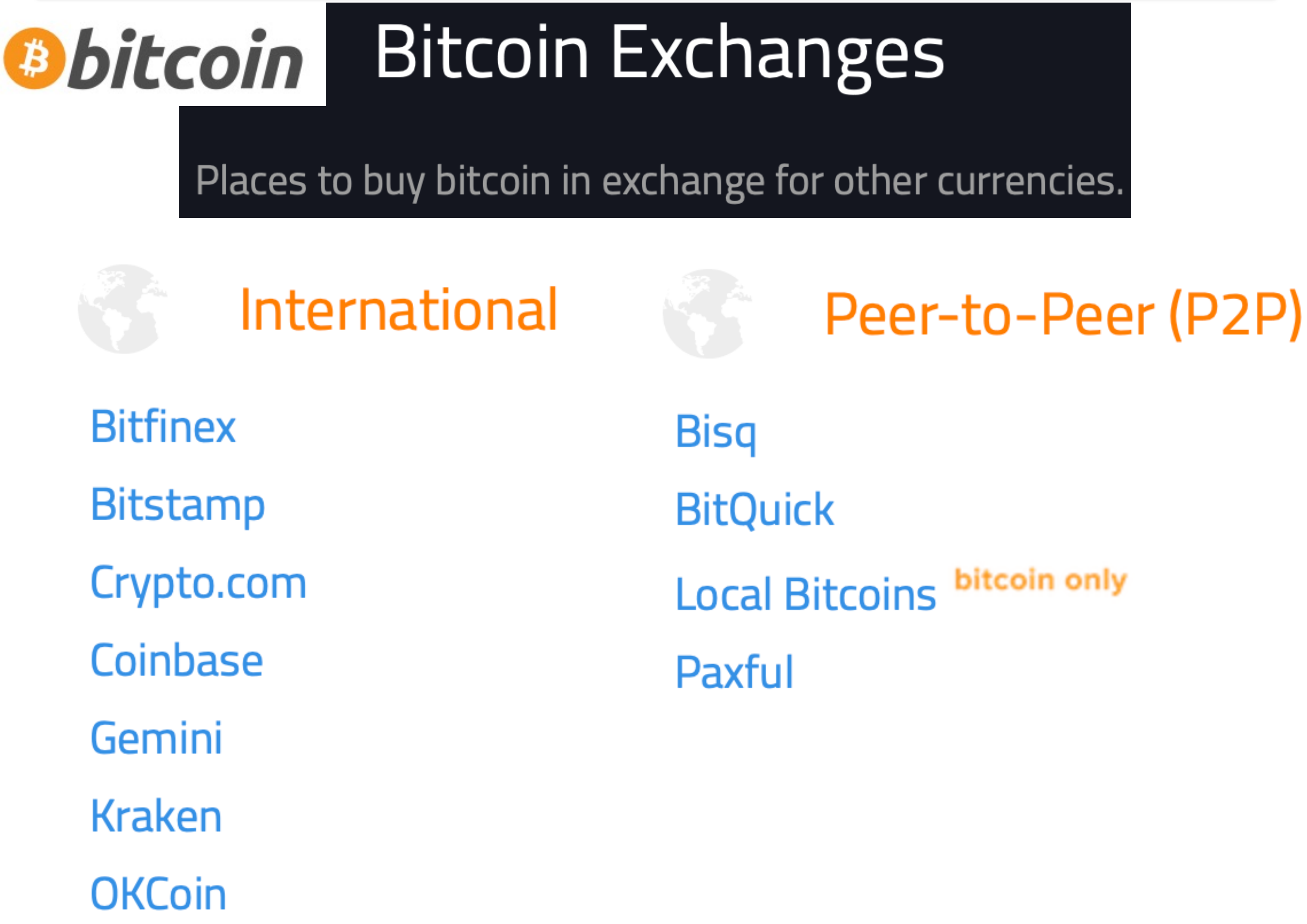


In the future, the wealthy will fight for 0.01 BTC

In addition to the certified millionaires, there are 590 million individuals whose net worth exceeds $100,000. These people shouldn't be disregarded as potential holders, even though their purchasing power is less.

Global wealth distribution. Source: Credit Suisse

Bitcoin Exchanges



bitcoin

Bitcoin Exchanges

Places to buy bitcoin in exchange for other currencies.

International

- Bitfinex
- Bitstamp
- Crypto.com
- Coinbase
- Gemini
- Kraken
- OKCoin

Peer-to-Peer (P2P)

- Bisq
- BitQuick
- Local Bitcoins bitcoin only
- Paxful

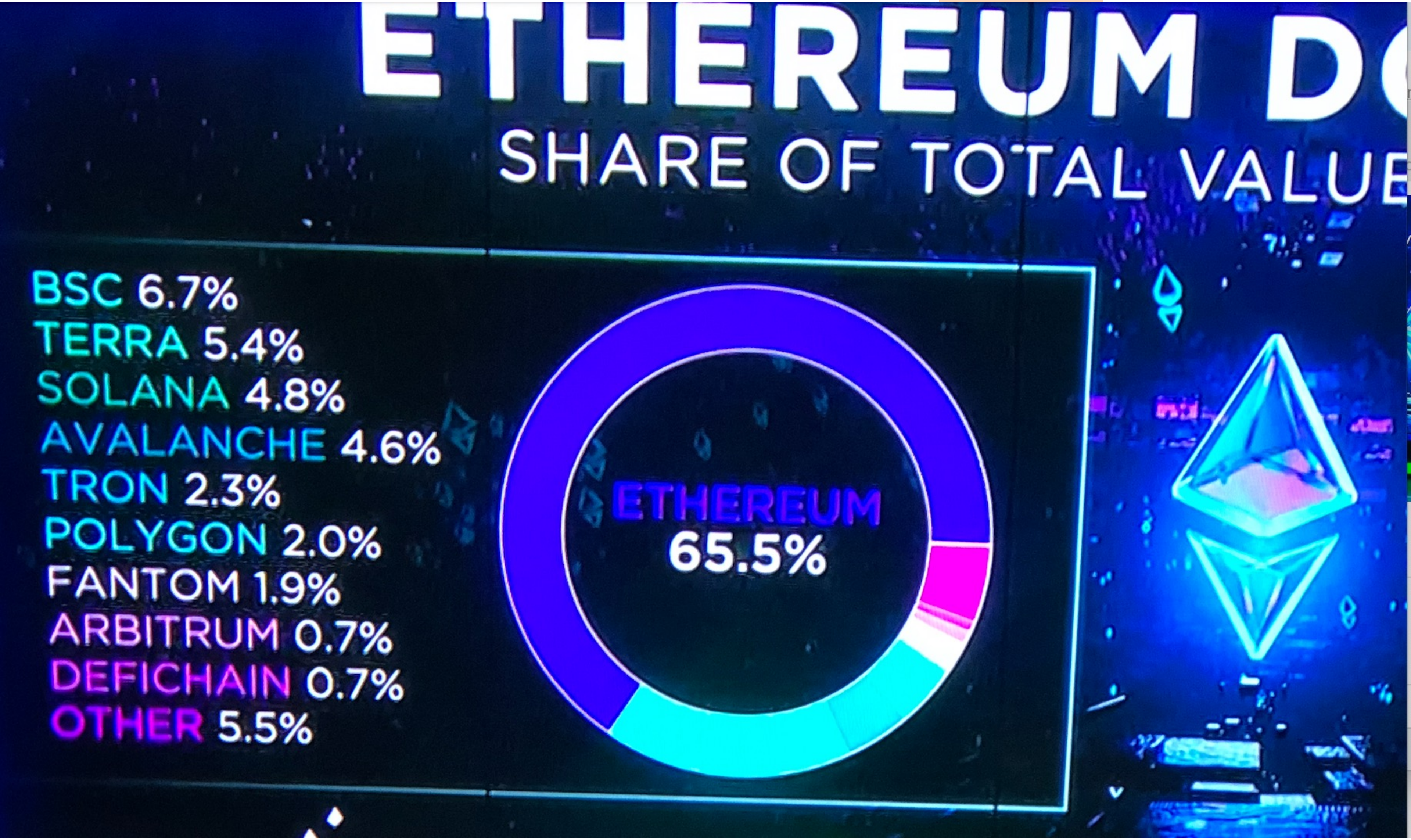
Cryptography

Crypto Currencies

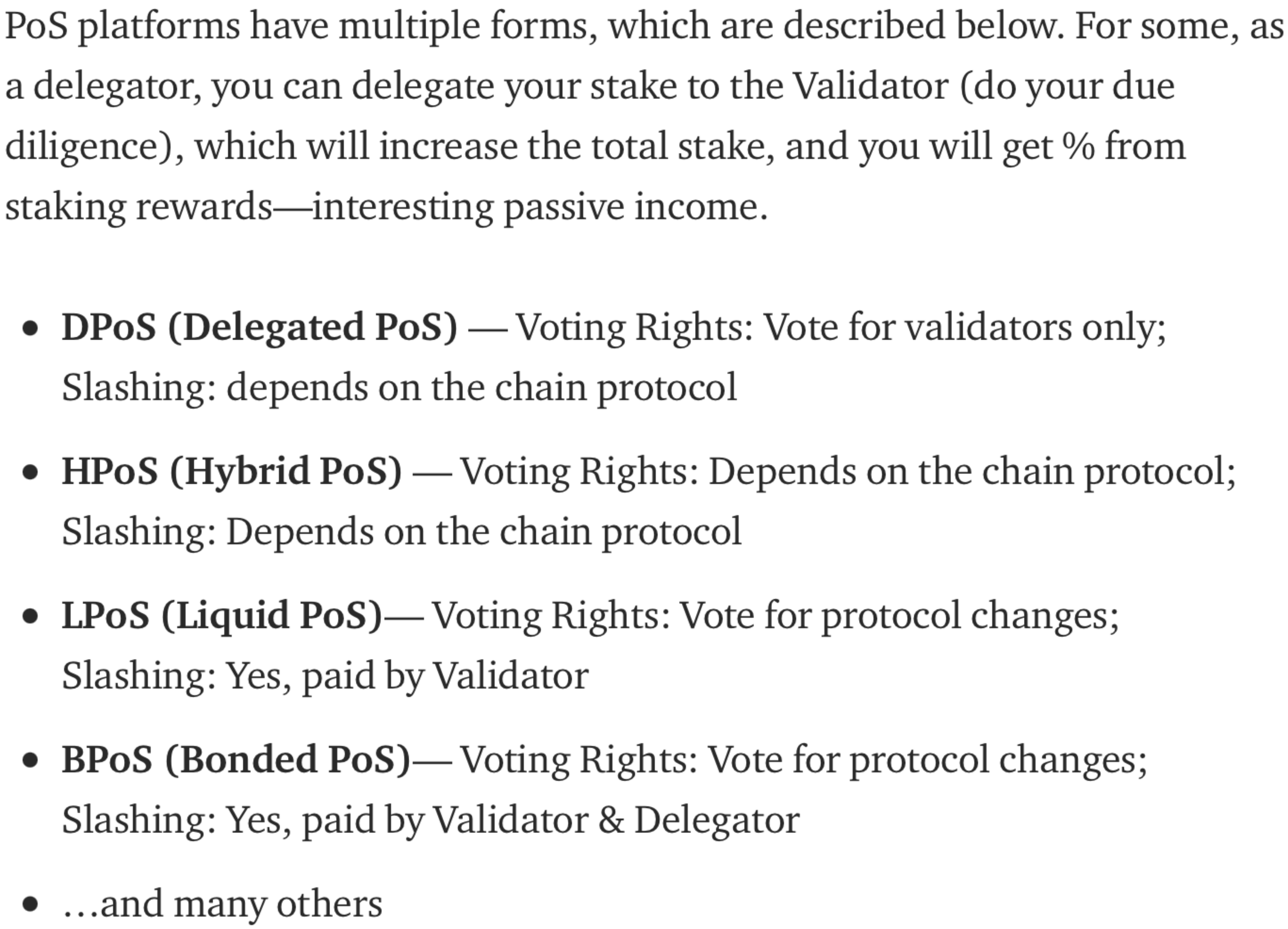
- ❖Ethereum

Top Ethereum Comp

Dec 2021



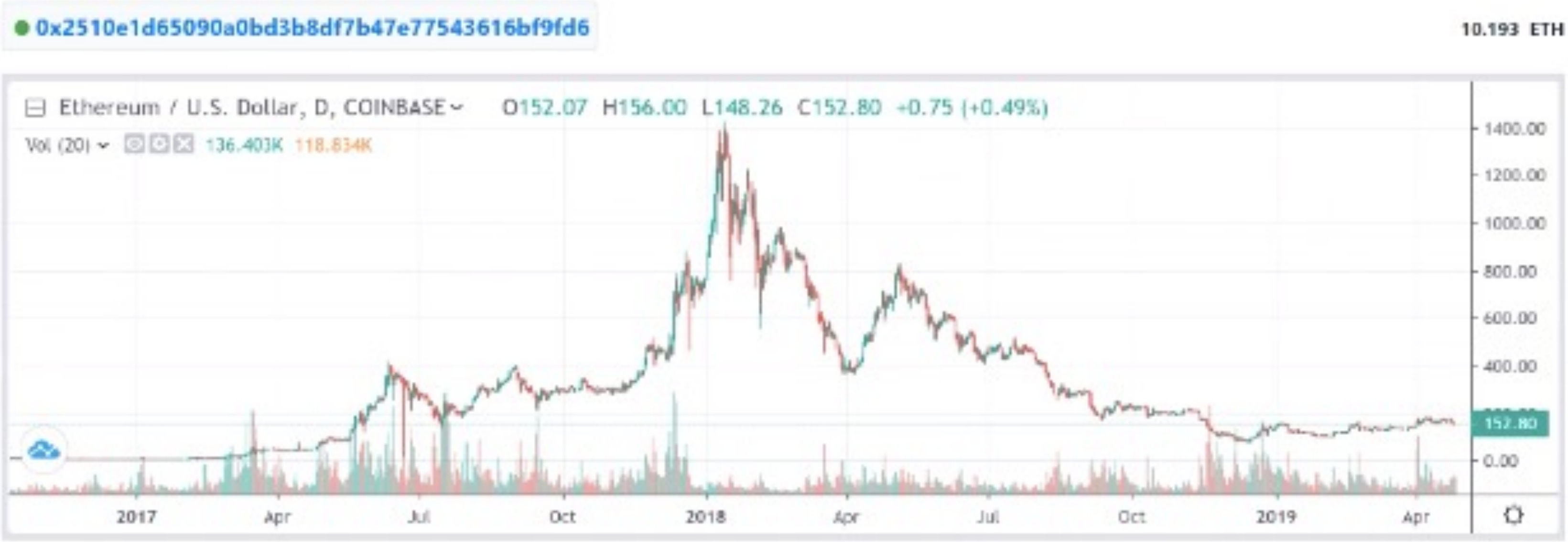
Ethereum PoS



PoS platforms have multiple forms, which are described below. For some, as a delegator, you can delegate your stake to the Validator (do your due diligence), which will increase the total stake, and you will get % from staking rewards—interesting passive income.

- **DPoS (Delegated PoS)** — Voting Rights: Vote for validators only; Slashing: depends on the chain protocol
- **HPoS (Hybrid PoS)** — Voting Rights: Depends on the chain protocol; Slashing: Depends on the chain protocol
- **LPoS (Liquid PoS)**— Voting Rights: Vote for protocol changes; Slashing: Yes, paid by Validator
- **BPoS (Bonded PoS)**— Voting Rights: Vote for protocol changes; Slashing: Yes, paid by Validator & Delegator
- …and many others

Ethereum 1-Yr Chart



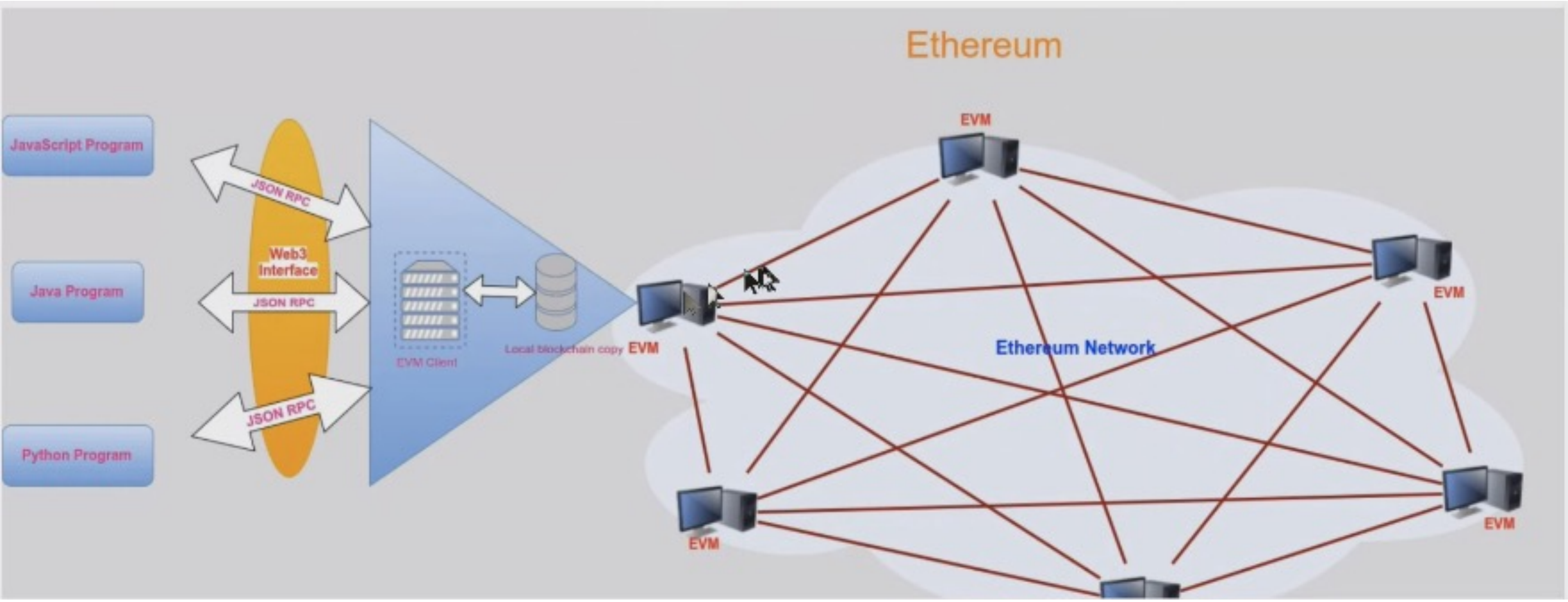
● 0x2510e1d65090a0bd3b8df7b47e77543616bf9fd6

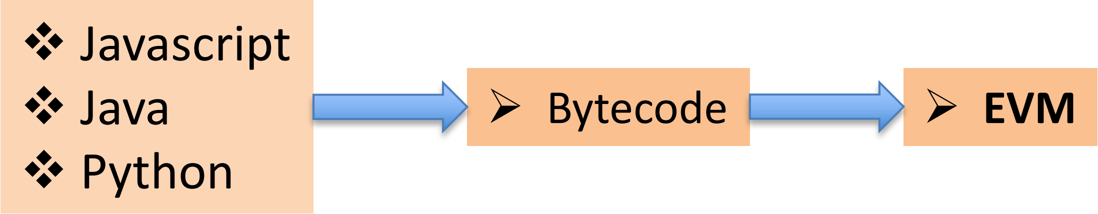
10.193 ETH

Ethereum / U.S. Dollar, D, COINBASE O152.07 H156.00 L148.26 C152.80 +0.75 (+0.49%)

Vol (20) 136.403K 118.834K

Ethereum Network





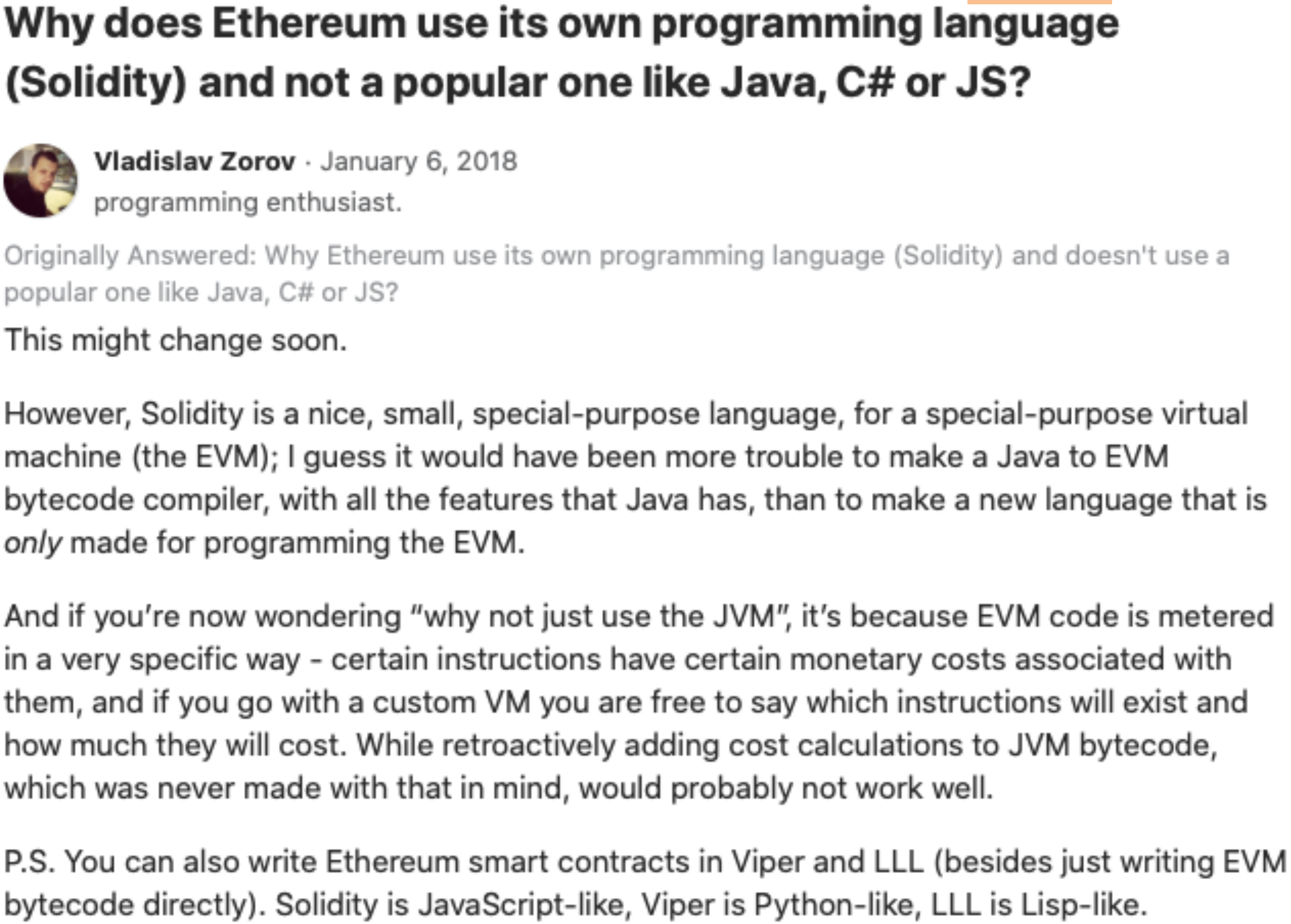
- ❖ Javascript
- ❖ Java
- ❖ Python

➢ Bytecode

➢ **EVM**

Ethereum Network

Solidity



Why does Ethereum use its own programming language (Solidity) and not a popular one like Java, C# or JS?

Vladislav Zorov · January 6, 2018
programming enthusiast.

Originally Answered: Why Ethereum use its own programming language (Solidity) and doesn't use a popular one like Java, C# or JS?

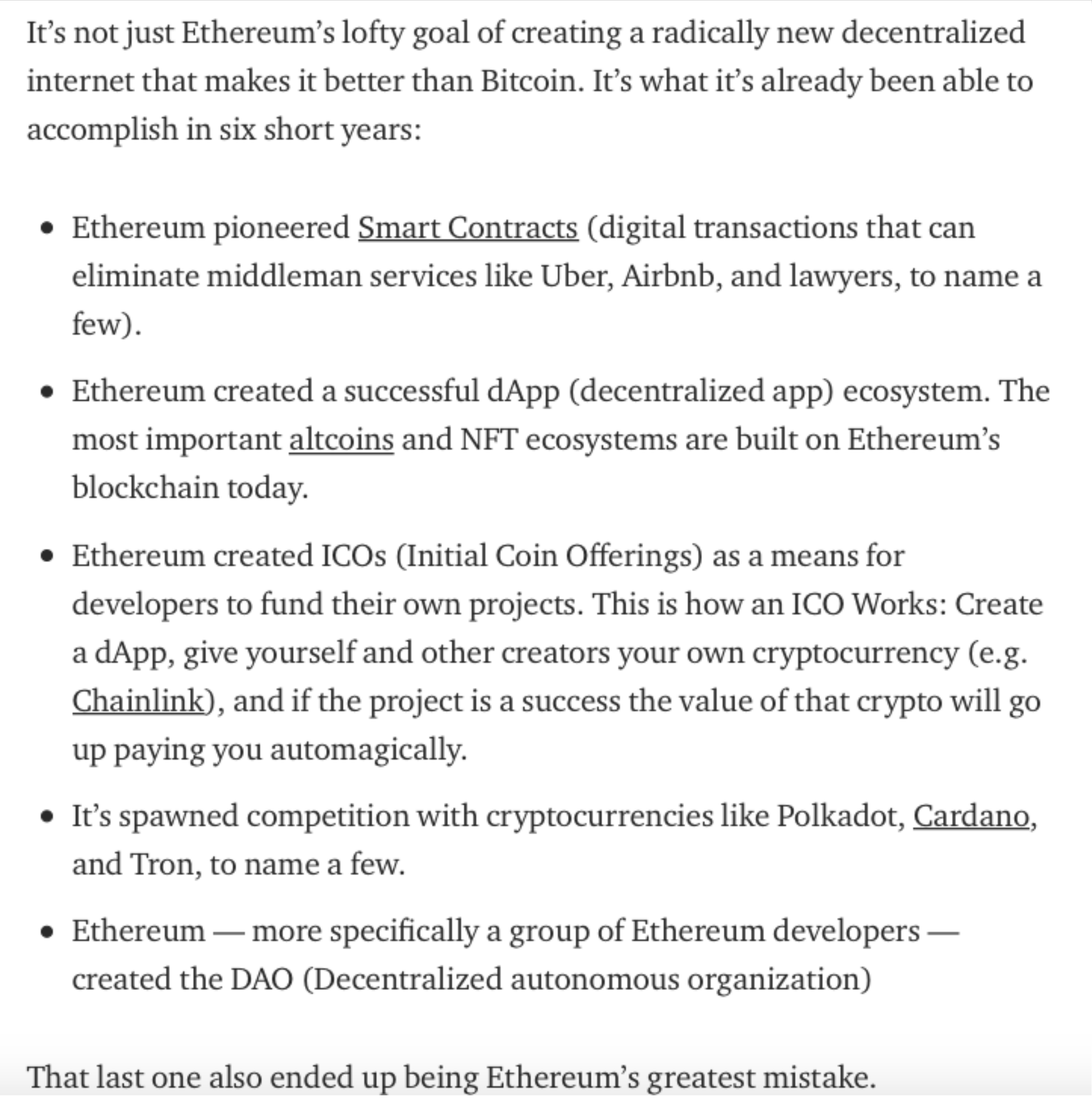
This might change soon.

However, Solidity is a nice, small, special-purpose language, for a special-purpose virtual machine (the EVM); I guess it would have been more trouble to make a Java to EVM bytecode compiler, with all the features that Java has, than to make a new language that is *only* made for programming the EVM.

And if you're now wondering "why not just use the JVM", it's because EVM code is metered in a very specific way - certain instructions have certain monetary costs associated with them, and if you go with a custom VM you are free to say which instructions will exist and how much they will cost. While retroactively adding cost calculations to JVM bytecode, which was never made with that in mind, would probably not work well.

P.S. You can also write Ethereum smart contracts in Viper and LLL (besides just writing EVM bytecode directly). Solidity is JavaScript-like, Viper is Python-like, LLL is Lisp-like.

Ethereum

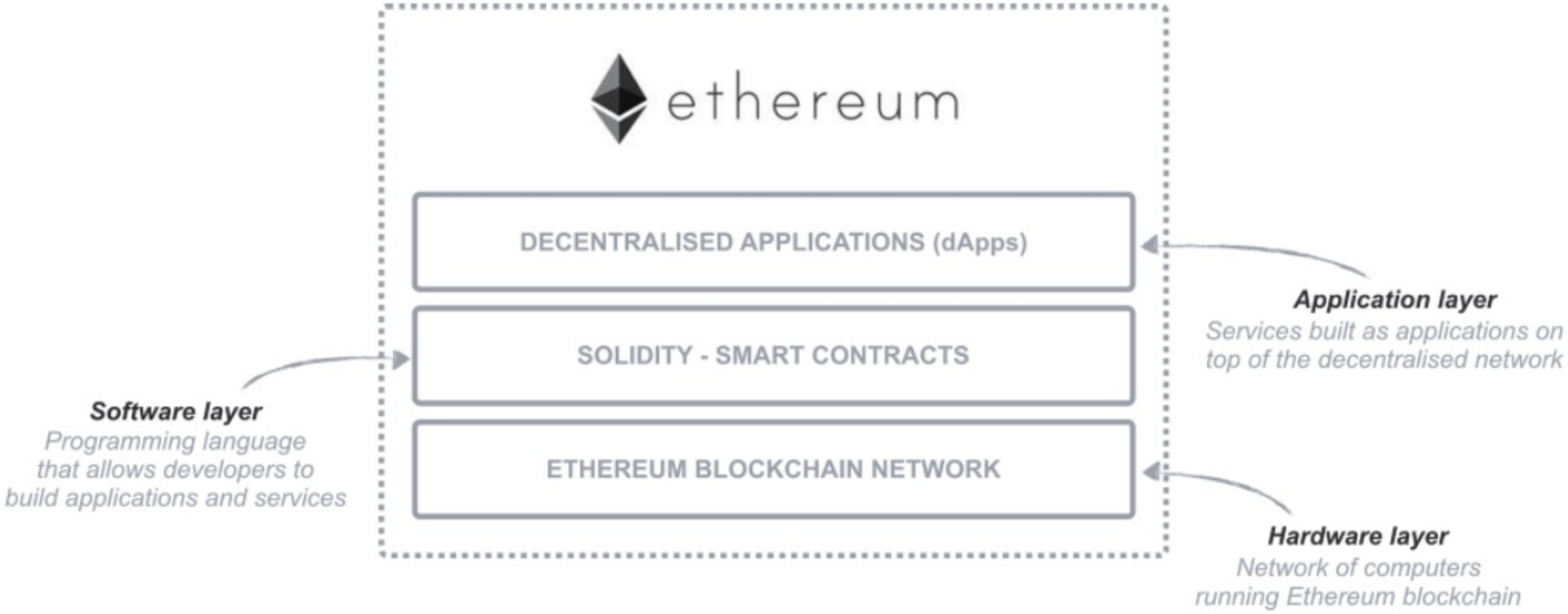


It's not just Ethereum's lofty goal of creating a radically new decentralized internet that makes it better than Bitcoin. It's what it's already been able to accomplish in six short years:

- Ethereum pioneered Smart Contracts (digital transactions that can eliminate middleman services like Uber, Airbnb, and lawyers, to name a few).
- Ethereum created a successful dApp (decentralized app) ecosystem. The most important altcoins and NFT ecosystems are built on Ethereum's blockchain today.
- Ethereum created ICOs (Initial Coin Offerings) as a means for developers to fund their own projects. This is how an ICO Works: Create a dApp, give yourself and other creators your own cryptocurrency (e.g. Chainlink), and if the project is a success the value of that crypto will go up paying you automagically.
- It's spawned competition with cryptocurrencies like Polkadot, Cardano, and Tron, to name a few.
- Ethereum — more specifically a group of Ethereum developers — created the DAO (Decentralized autonomous organization)

That last one also ended up being Ethereum's greatest mistake.

Ethereum Layers



ethereum

DECENTRALISED APPLICATIONS (dApps)

SOLIDITY - SMART CONTRACTS

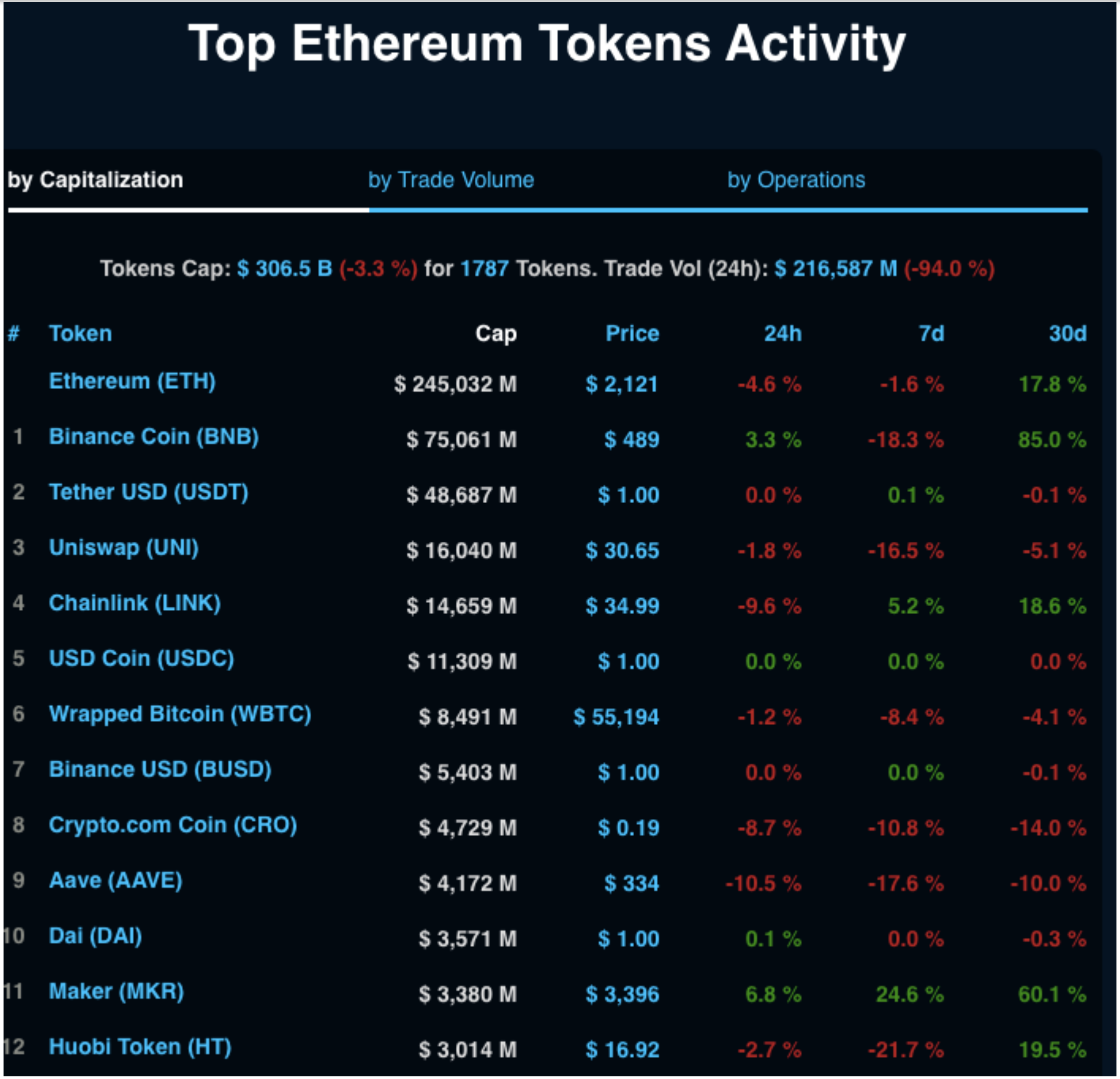
ETHEREUM BLOCKCHAIN NETWORK

Application layer
Services built as applications on top of the decentralised network

Software layer
Programming language that allows developers to build applications and services

Hardware layer
Network of computers running Ethereum blockchain

Ethereum Tokens



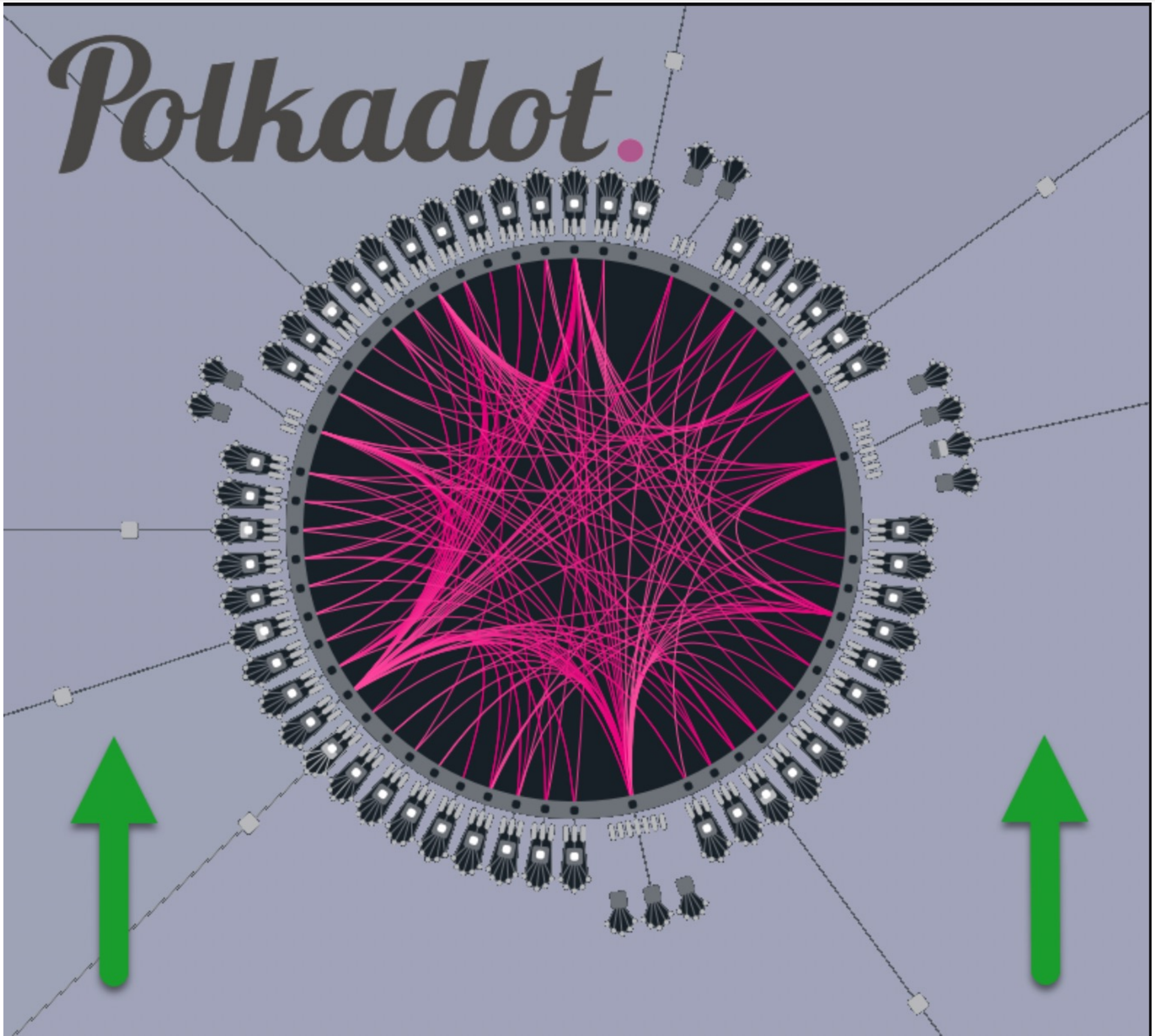
Top Ethereum Tokens Activity

by Capitalization | by Trade Volume | by Operations

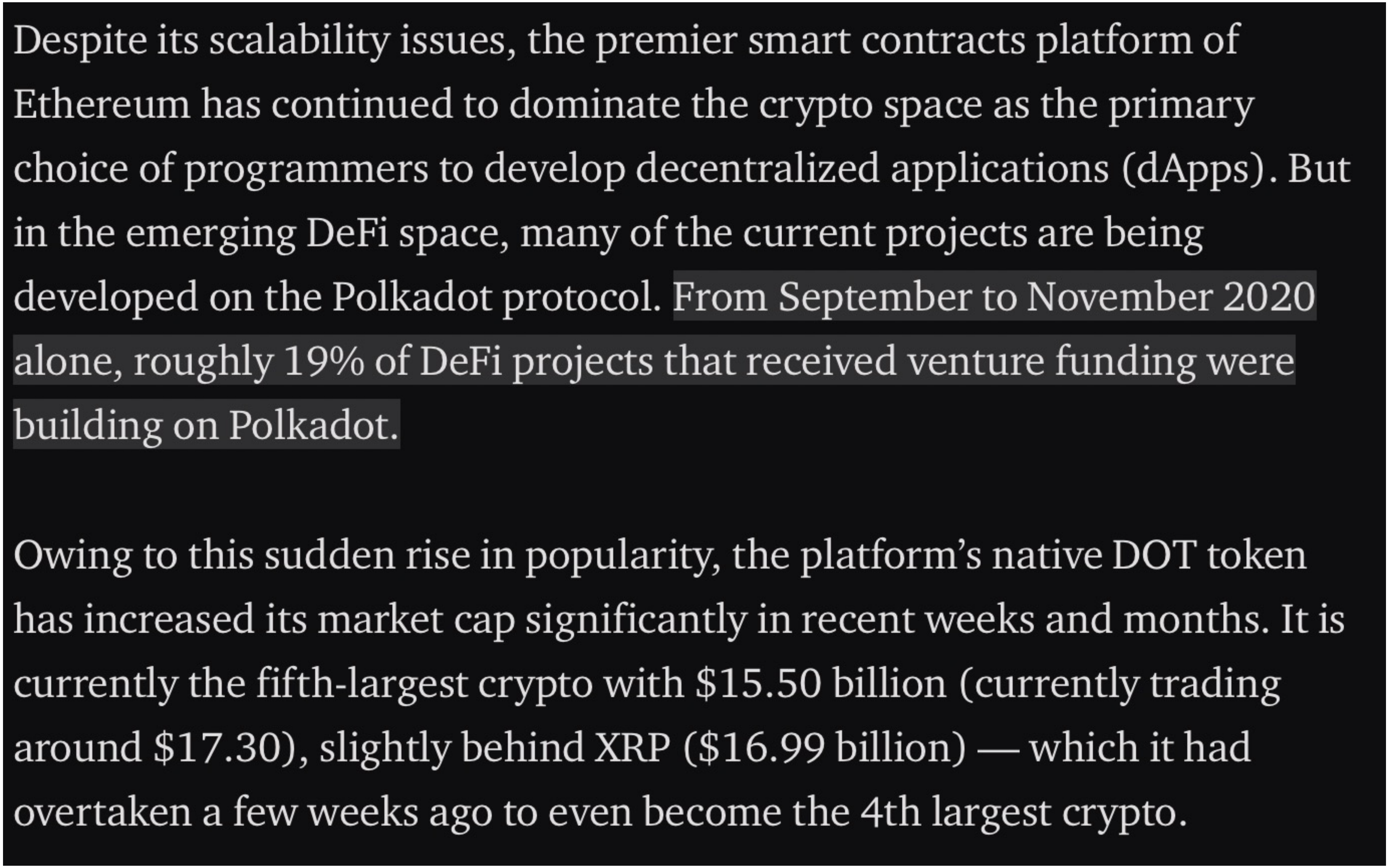
Tokens Cap: $ 306.5 B (-3.3 %) for 1787 Tokens. Trade Vol (24h): $ 216,587 M (-94.0 %)

#	Token	Cap	Price	24h	7d	30d
	Ethereum (ETH)	$ 245,032 M	$ 2,121	-4.6 %	-1.6 %	17.8 %
1	Binance Coin (BNB)	$ 75,061 M	$ 489	3.3 %	-18.3 %	85.0 %
2	Tether USD (USDT)	$ 48,687 M	$ 1.00	0.0 %	0.1 %	-0.1 %
3	Uniswap (UNI)	$ 16,040 M	$ 30.65	-1.8 %	-16.5 %	-5.1 %
4	Chainlink (LINK)	$ 14,659 M	$ 34.99	-9.6 %	5.2 %	18.6 %
5	USD Coin (USDC)	$ 11,309 M	$ 1.00	0.0 %	0.0 %	0.0 %
6	Wrapped Bitcoin (WBTC)	$ 8,491 M	$ 55,194	-1.2 %	-8.4 %	-4.1 %
7	Binance USD (BUSD)	$ 5,403 M	$ 1.00	0.0 %	0.0 %	-0.1 %
8	Crypto.com Coin (CRO)	$ 4,729 M	$ 0.19	-8.7 %	-10.8 %	-14.0 %
9	Aave (AAVE)	$ 4,172 M	$ 334	-10.5 %	-17.6 %	-10.0 %
10	Dai (DAI)	$ 3,571 M	$ 1.00	0.1 %	0.0 %	-0.3 %
11	Maker (MKR)	$ 3,380 M	$ 3,396	6.8 %	24.6 %	60.1 %
12	Huobi Token (HT)	$ 3,014 M	$ 16.92	-2.7 %	-21.7 %	19.5 %

Other Cryptos



Polkadot



Despite its scalability issues, the premier smart contracts platform of Ethereum has continued to dominate the crypto space as the primary choice of programmers to develop decentralized applications (dApps). But in the emerging DeFi space, many of the current projects are being developed on the Polkadot protocol. From September to November 2020 alone, roughly 19% of DeFi projects that received venture funding were building on Polkadot.

Owing to this sudden rise in popularity, the platform's native DOT token has increased its market cap significantly in recent weeks and months. It is currently the fifth-largest crypto with $15.50 billion (currently trading around $17.30), slightly behind XRP ($16.99 billion) — which it had overtaken a few weeks ago to even become the 4th largest crypto.

Polkadot

I remember introducing the Polkadot blockchain in one of my writeups, back in mid-2019. Just to briefly summarize, it is an open-source "para chain (parallelized chains)" framework whose aim is to address scalability, interoperability, developability and governance issues — visualize a multi-chain decentralized economic hub, where all networks can communicate in a secure, scalable & decentralized fashion.

What makes it even more interesting is that the project is the brainchild of Ethereum co-founder Dr. Gavin Wood. While Ethereum recently took the first steps towards the long and arduous journey towards a Proof of Stake network dubbed as Ethereum 2.0, Polkadot is already a proof-of-stake blockchain network — going live back in May 2020.

No doubt then, that it has emerged as the most popular alternative to Ethereum for decentralized finance (DeFi) investment purposes. According to Block Research, Polkadot's ecosystem already consists of a total of 127 projects across sixteen different verticals that are currently building on the network.

Polkadot

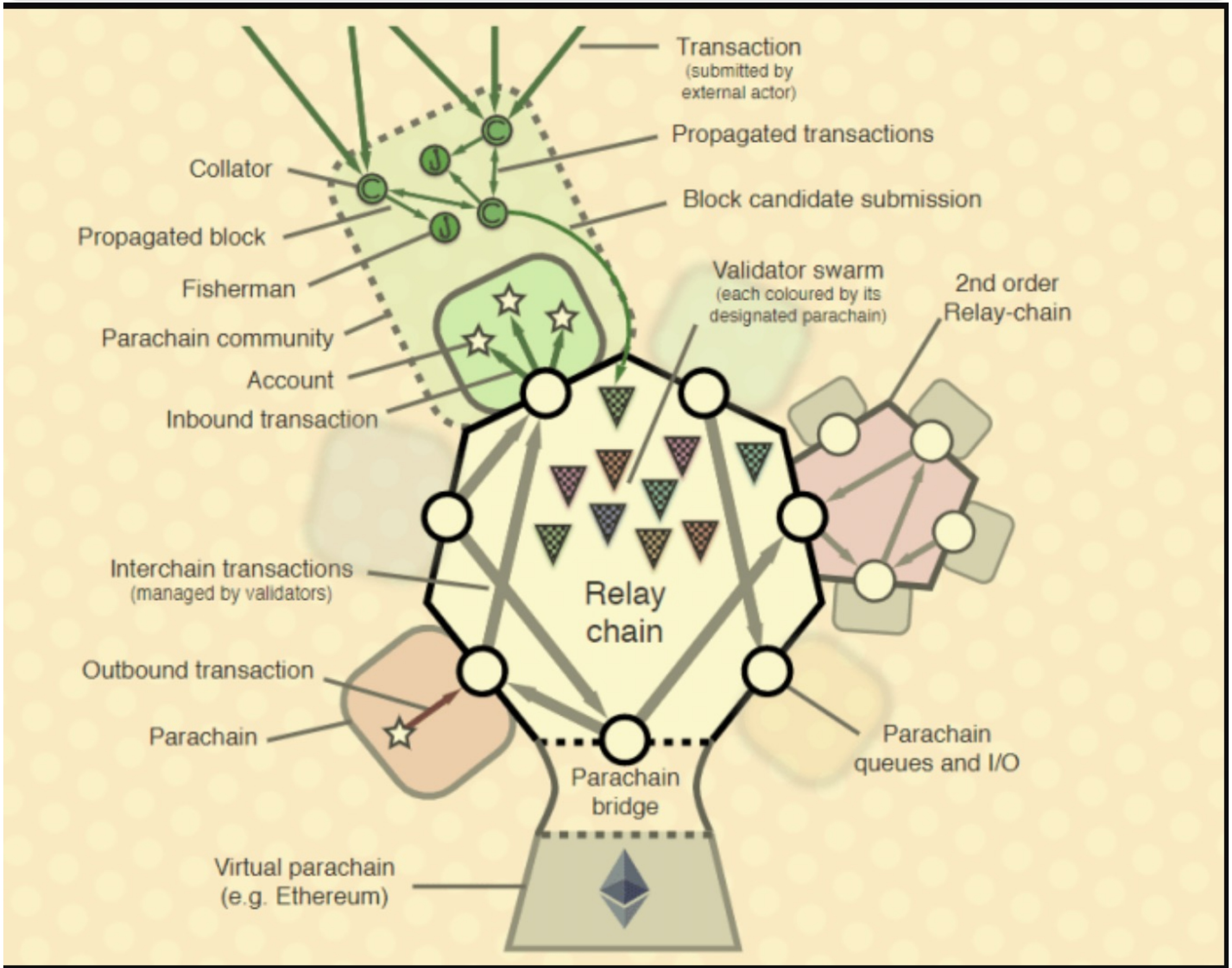
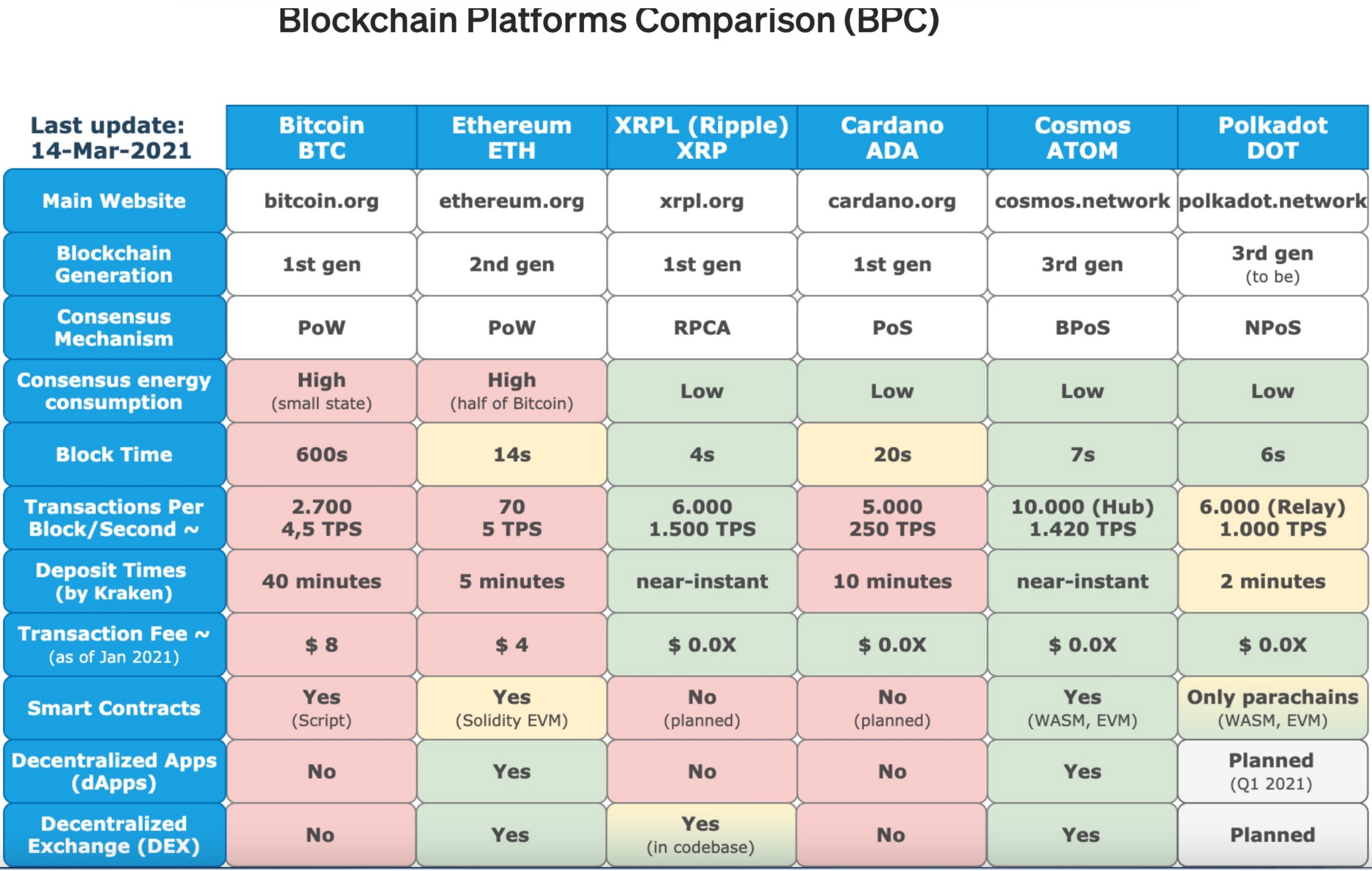


Image Credit: Polkadot White Paper

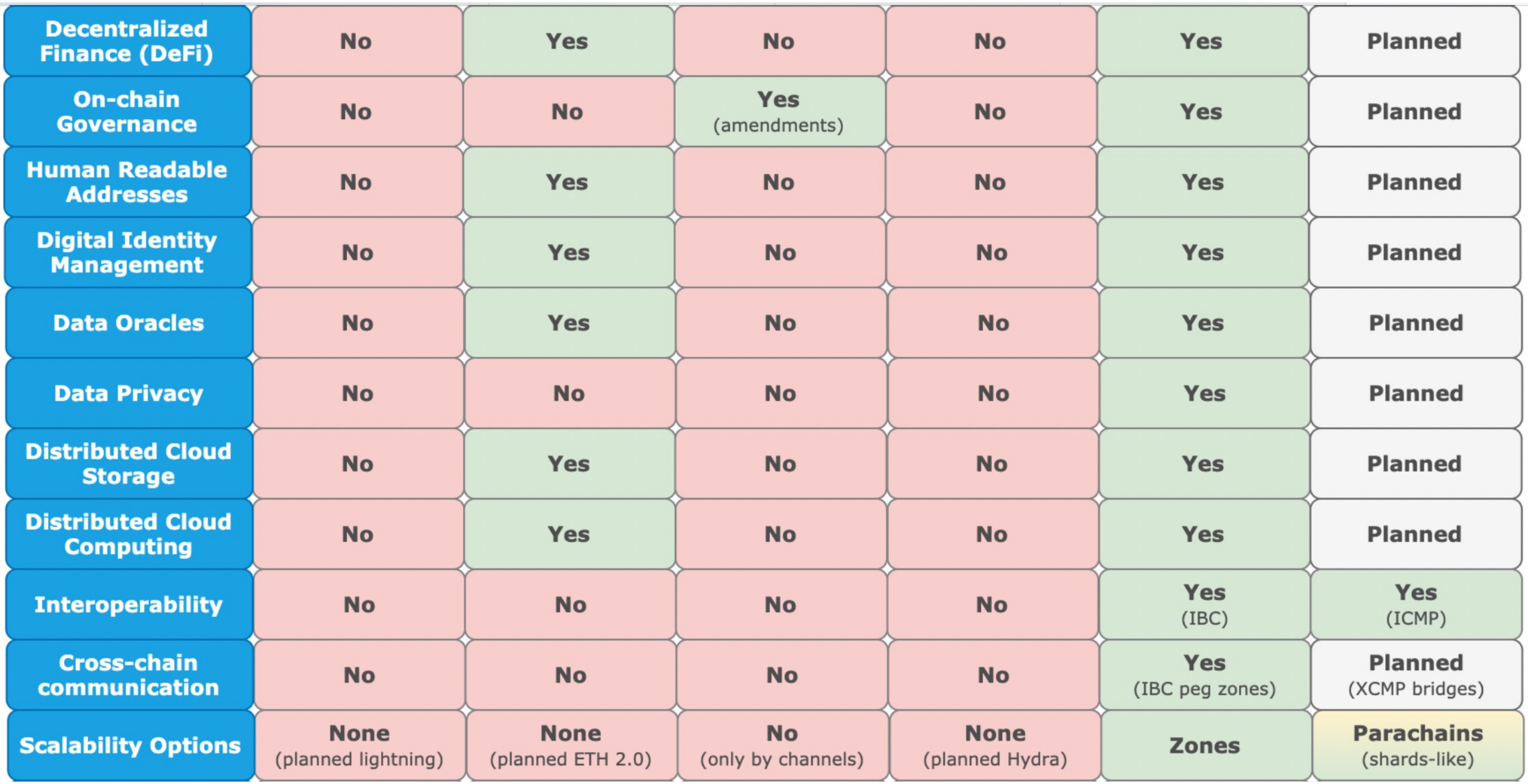
Compare Cryptos



Blockchain Platforms Comparison (BPC)

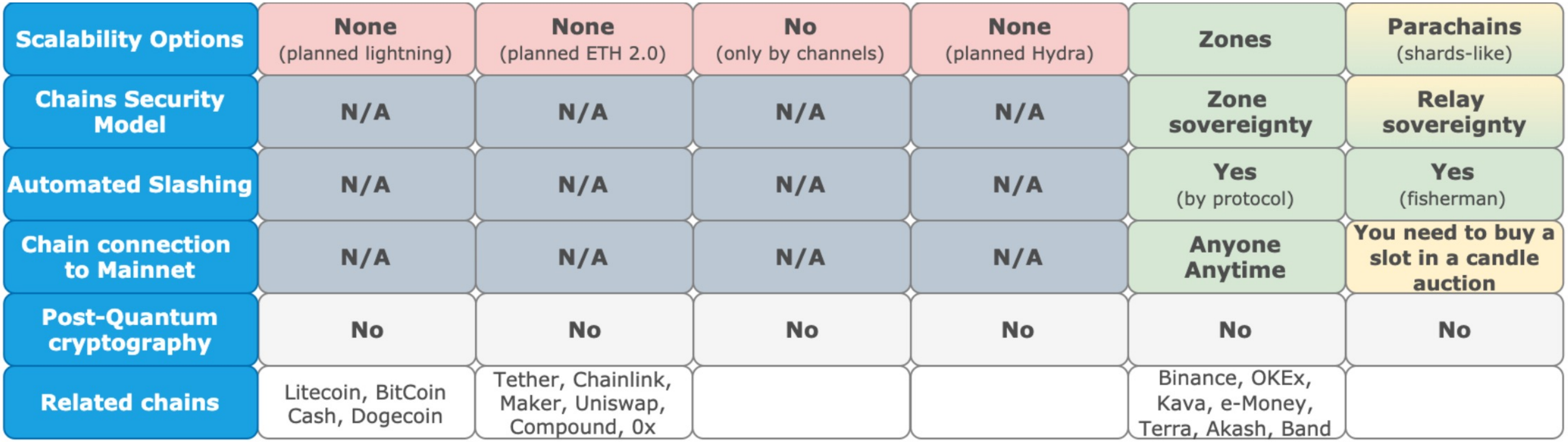
Last update: 14-Mar-2021	Bitcoin BTC	Ethereum ETH	XRPL (Ripple) XRP	Cardano ADA	Cosmos ATOM	Polkadot DOT
Main Website	bitcoin.org	ethereum.org	xrpl.org	cardano.org	cosmos.network	polkadot.network
Blockchain Generation	1st gen	2nd gen	1st gen	1st gen	3rd gen	3rd gen (to be)
Consensus Mechanism	PoW	PoW	RPCA	PoS	BPoS	NPoS
Consensus energy consumption	High (small state)	High (half of Bitcoin)	Low	Low	Low	Low
Block Time	600s	14s	4s	20s	7s	6s
Transactions Per Block/Second ~	2.700 4,5 TPS	70 5 TPS	6.000 1.500 TPS	5.000 250 TPS	10.000 (Hub) 1.420 TPS	6.000 (Relay) 1.000 TPS
Deposit Times (by Kraken)	40 minutes	5 minutes	near-instant	10 minutes	near-instant	2 minutes
Transaction Fee ~ (as of Jan 2021)	$ 8	$ 4	$ 0.0X	$ 0.0X	$ 0.0X	$ 0.0X
Smart Contracts	Yes (Script)	Yes (Solidity EVM)	No (planned)	No (planned)	Yes (WASM, EVM)	Only parachains (WASM, EVM)
Decentralized Apps (dApps)	No	Yes	No	No	Yes	Planned (Q1 2021)
Decentralized Exchange (DEX)	No	Yes	Yes (in codebase)	No	Yes	Planned

Compare Cryptos



Decentralized Finance (DeFi)	No	Yes	No	No	Yes	Planned
On-chain Governance	No	No	Yes (amendments)	No	Yes	Planned
Human Readable Addresses	No	Yes	No	No	Yes	Planned
Digital Identity Management	No	Yes	No	No	Yes	Planned
Data Oracles	No	Yes	No	No	Yes	Planned
Data Privacy	No	No	No	No	Yes	Planned
Distributed Cloud Storage	No	Yes	No	No	Yes	Planned
Distributed Cloud Computing	No	Yes	No	No	Yes	Planned
Interoperability	No	No	No	No	Yes (IBC)	Yes (ICMP)
Cross-chain communication	No	No	No	No	Yes (IBC peg zones)	Planned (XCMP bridges)
Scalability Options	None (planned lightning)	None (planned ETH 2.0)	No (only by channels)	None (planned Hydra)	Zones	Parachains (shards-like)

Compare Cryptos



Scalability Options	**None** (planned lightning)	**None** (planned ETH 2.0)	**No** (only by channels)	**None** (planned Hydra)	**Zones**	**Parachains** (shards-like)
Chains Security Model	**N/A**	**N/A**	**N/A**	**N/A**	**Zone sovereignty**	**Relay sovereignty**
Automated Slashing	**N/A**	**N/A**	**N/A**	**N/A**	**Yes** (by protocol)	**Yes** (fisherman)
Chain connection to Mainnet	**N/A**	**N/A**	**N/A**	**N/A**	**Anyone Anytime**	**You need to buy a slot in a candle auction**
Post-Quantum cryptography	**No**	**No**	**No**	**No**	**No**	**No**
Related chains	Litecoin, BitCoin Cash, Dogecoin	Tether, Chainlink, Maker, Uniswap, Compound, 0x			Binance, OKEx, Kava, e-Money, Terra, Akash, Band	

Poly Hack

8-23-21

LIVE
POWER LUNCH
HACKER RETURNS REMAINING FUNDS TO POLY NETWORK
5.93 ▲ 0.84 Teledyne Tech. (TDY) 457.79 ▲ 7.33 Avangrid Inc (
.A) 211 Issues Declined (.AD.A) 67 Issues Unchanged (.AD.A) 1

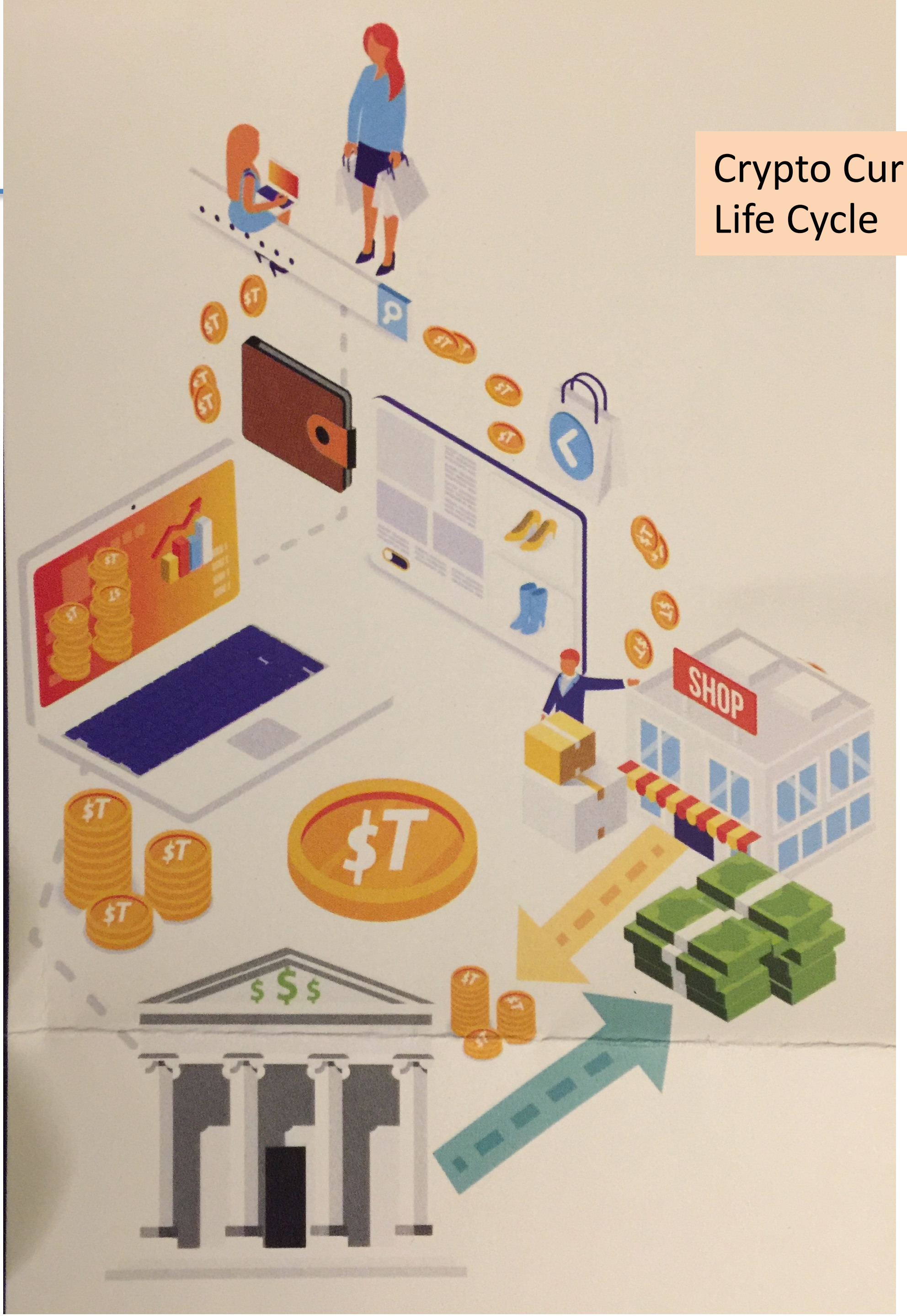
White Hat?

Cryptography

Digital Wallets

Crypto Currency Life Cycle

- ❖ Tokens
- ❖ Coins
- ❖ Wallets
- ❖ Ledgers
- ❖ Blockchains



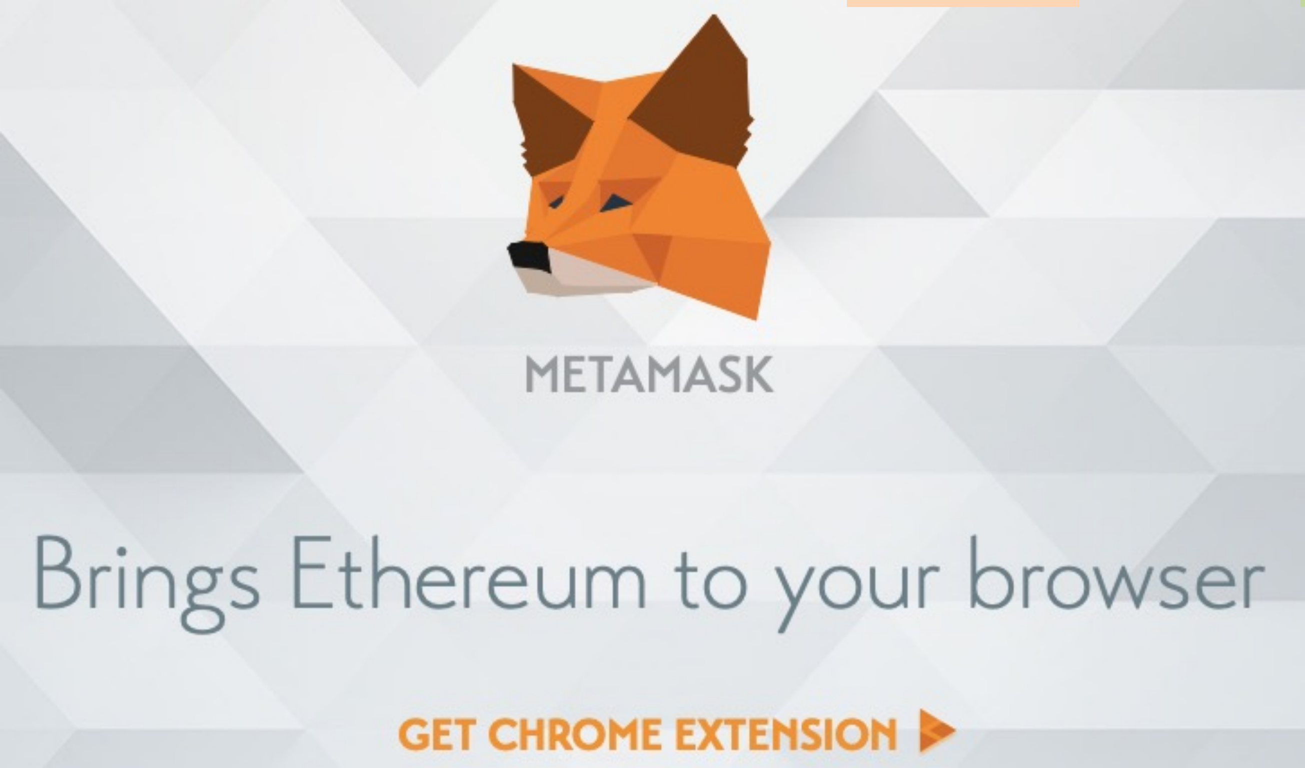
CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

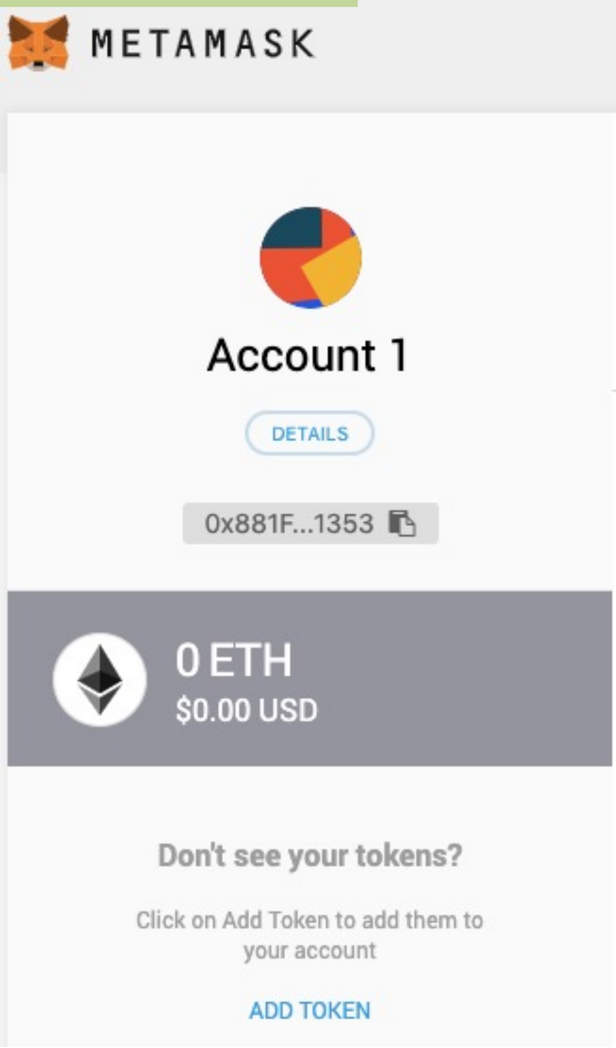
Digital Wallet

DR JEFF SOFTWARE
©Jeff Drobman
2017-23

Ethereum

Crypto-Currency





0x881F...1353

0 ETH

$0.00 USD

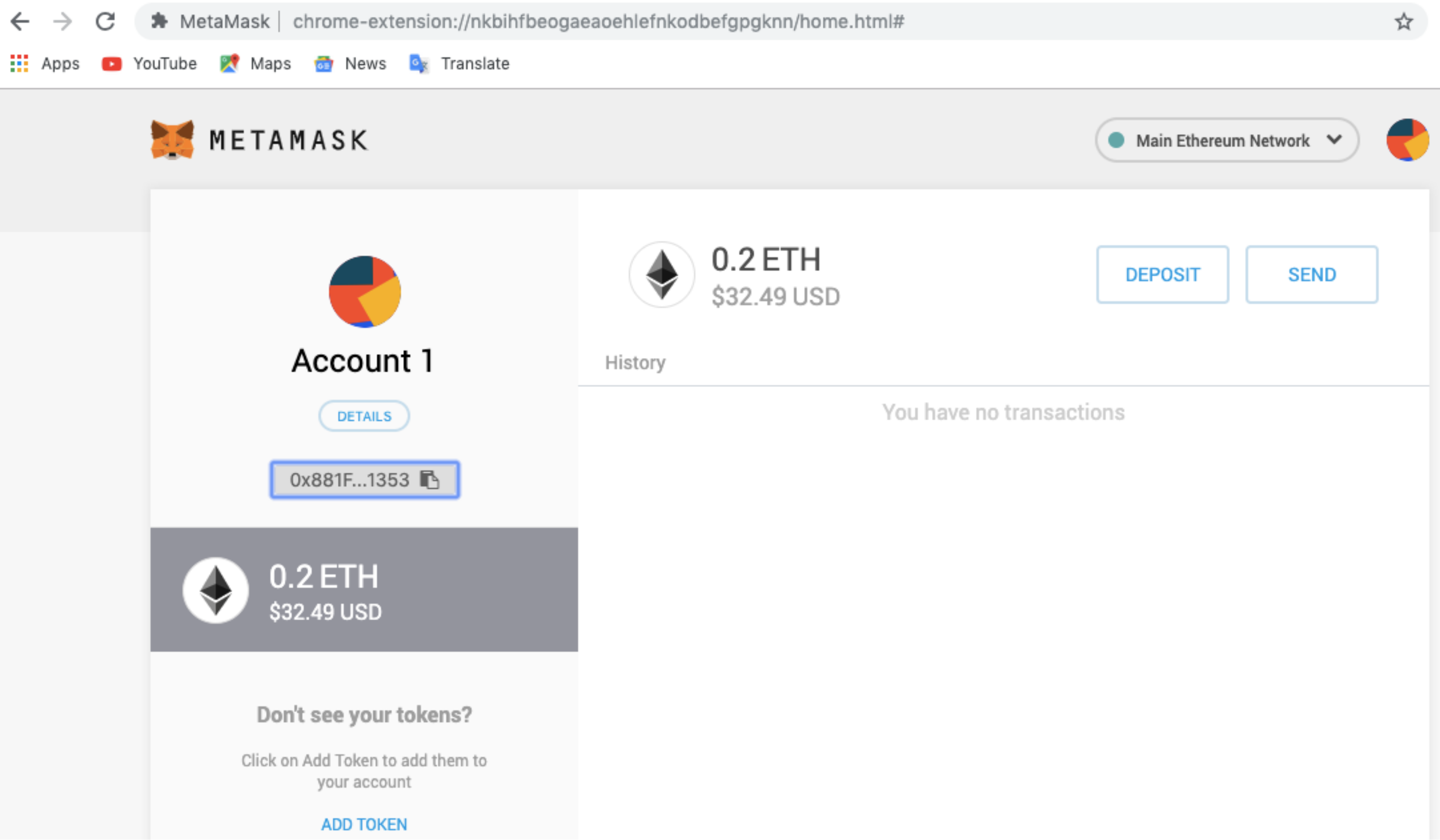
Don't see your tokens?

Click on Add Token to add them to your account

Digital Wallet

Ethereum

Crypto-Currency



Account 1

0x881F...1353

0.2 ETH
$32.49 USD

History

You have no transactions

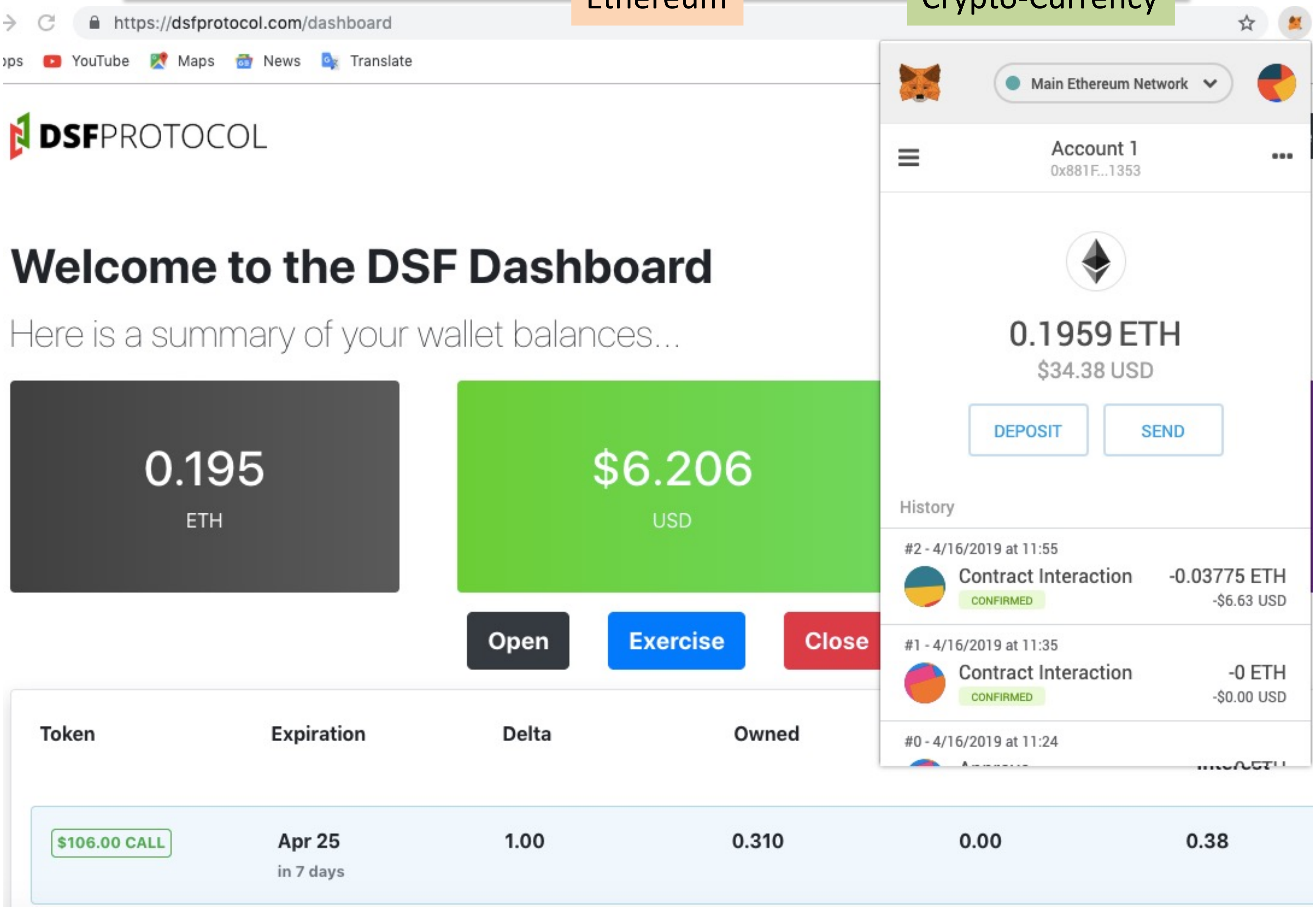
Don't see your tokens?

Click on Add Token to add them to your account

Digital Wallet

Ethereum

Crypto-Currency



https://dsfprotocol.com/dashboard

DSFPROTOCOL

Welcome to the DSF Dashboard

Here is a summary of your wallet balances...

0.195
ETH

$6.206
USD

Token	Expiration	Delta	Owned		
$106.00 CALL	Apr 25 in 7 days	1.00	0.310	0.00	0.38

Main Ethereum Network

Account 1
0x881F...1353

0.1959 ETH
$34.38 USD

History

#2 - 4/16/2019 at 11:55
Contract Interaction -0.03775 ETH
CONFIRMED -$6.63 USD

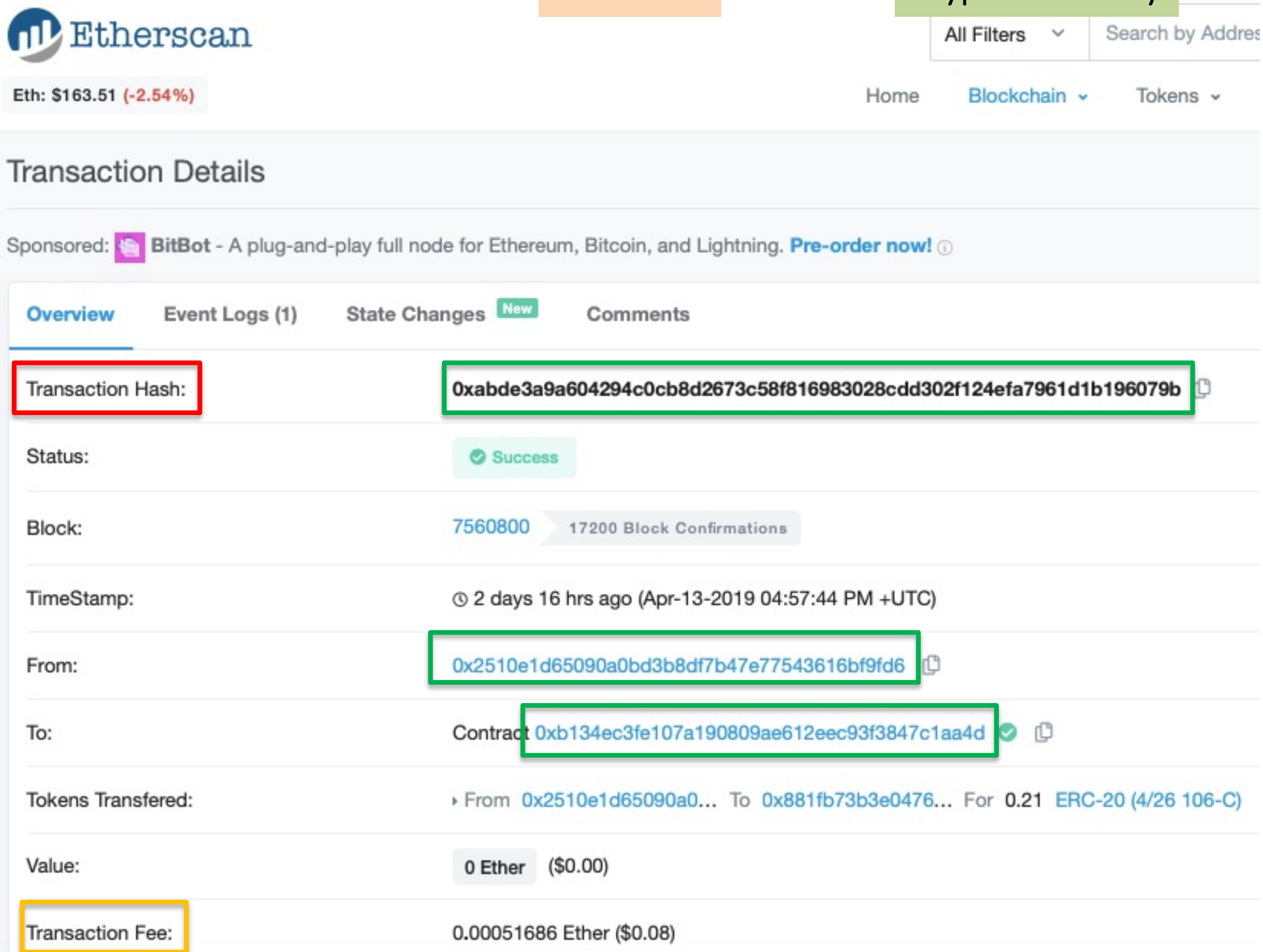
#1 - 4/16/2019 at 11:35
Contract Interaction -0 ETH
CONFIRMED -$0.00 USD

#0 - 4/16/2019 at 11:24

Digital Wallet

Ethereum

Crypto-Currency



Eth: $163.51 (-2.54%)

Transaction Details

Sponsored: BitBot - A plug-and-play full node for Ethereum, Bitcoin, and Lightning. Pre-order now!

Transaction Hash:	0xabde3a9a604294c0cb8d2673c58f816983028cdd302f124efa7961d1b196079b
Status:	Success
Block:	7560800 17200 Block Confirmations
TimeStamp:	2 days 16 hrs ago (Apr-13-2019 04:57:44 PM +UTC)
From:	0x2510e1d65090a0bd3b8df7b47e77543616bf9fd6
To:	Contract 0xb134ec3fe107a190809ae612eec93f3847c1aa4d ✓
Tokens Transfered:	From 0x2510e1d65090a0... To 0x881fb73b3e0476... For 0.21 ERC-20 (4/26 106-C)
Value:	0 Ether ($0.00)
Transaction Fee:	0.00051686 Ether ($0.08)

CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

Digital Wallet

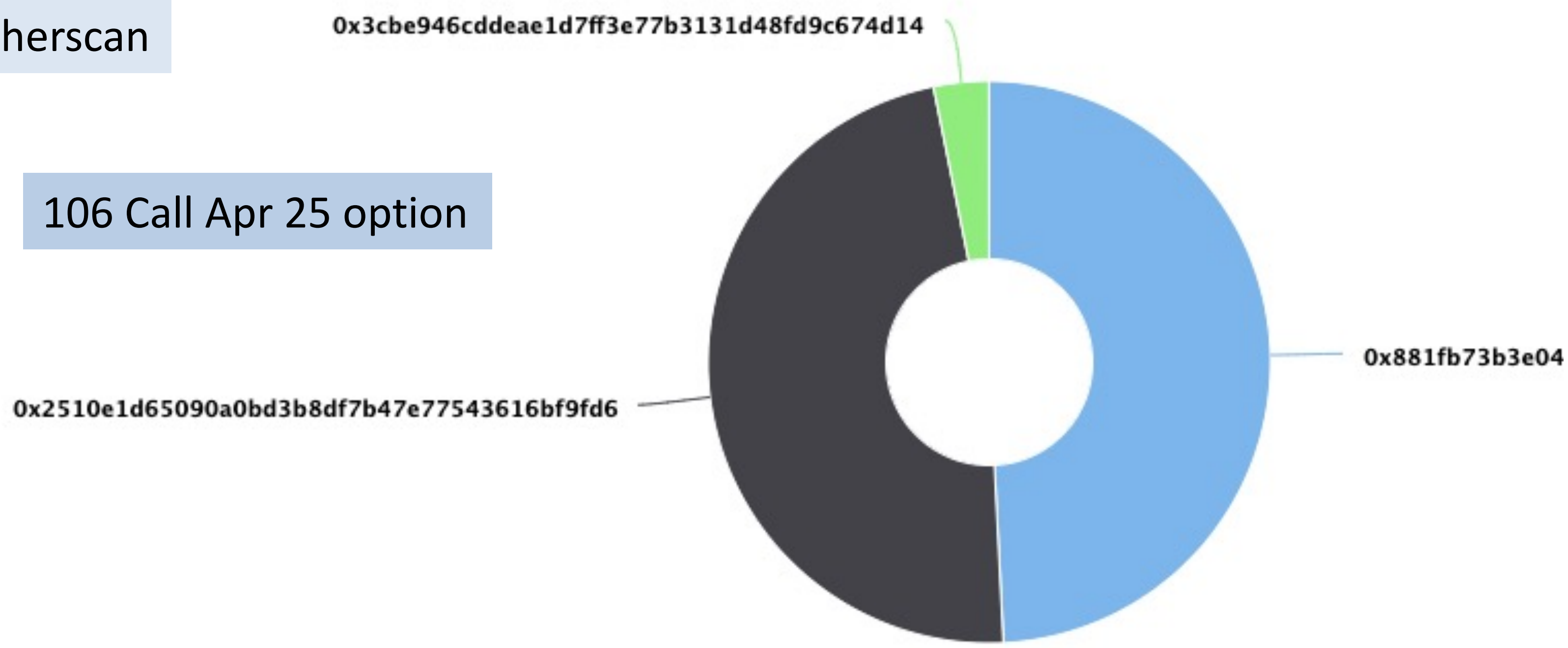
DR JEFF SOFTWARE
©Jeff Drobman
2017-23

Ethereum

Crypto-Currency

Etherscan

106 Call Apr 25 option



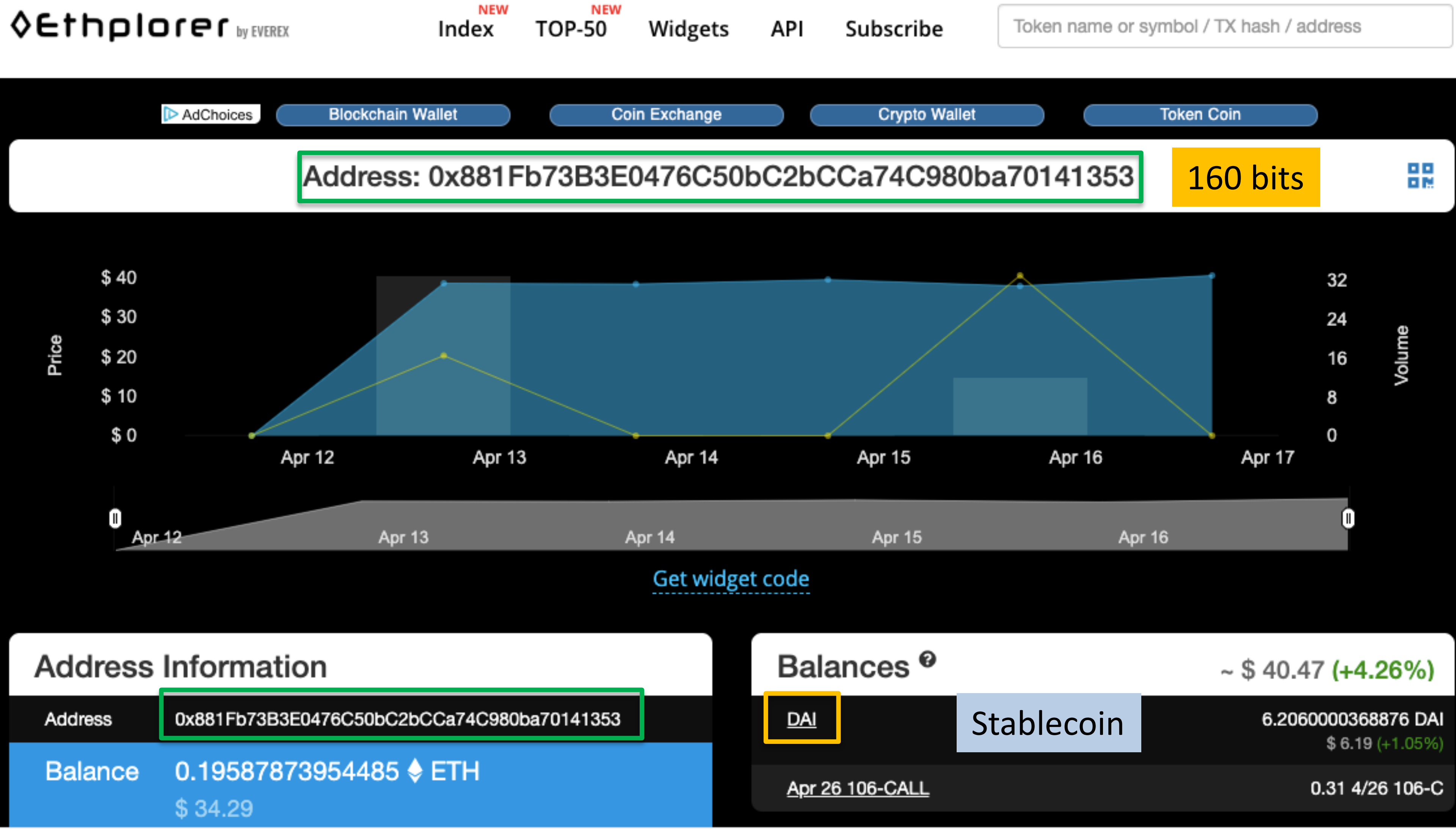
(A total of 0.63 tokens held by the top 100 accounts from the total supply of 0.38 token)

Rank	Address	Quantity (Token)
1	0x881fb73b3e0476c50bc2bcca74c980ba70141353	0.31
2	0x2510e1d65090a0bd3b8df7b47e77543616bf9fd6	0.3
3	0x3cbe946cddeae1d7ff3e77b3131d48fd9c674d14	0.02

Digital Wallet

Ethereum

Crypto-Currency



Address: 0x881Fb73B3E0476C50bC2bCCa74C980ba70141353

160 bits

Address Information

Address	0x881Fb73B3E0476C50bC2bCCa74C980ba70141353
Balance	0.19587873954485 ETH $ 34.29

Balances

~ $ 40.47 (+4.26%)

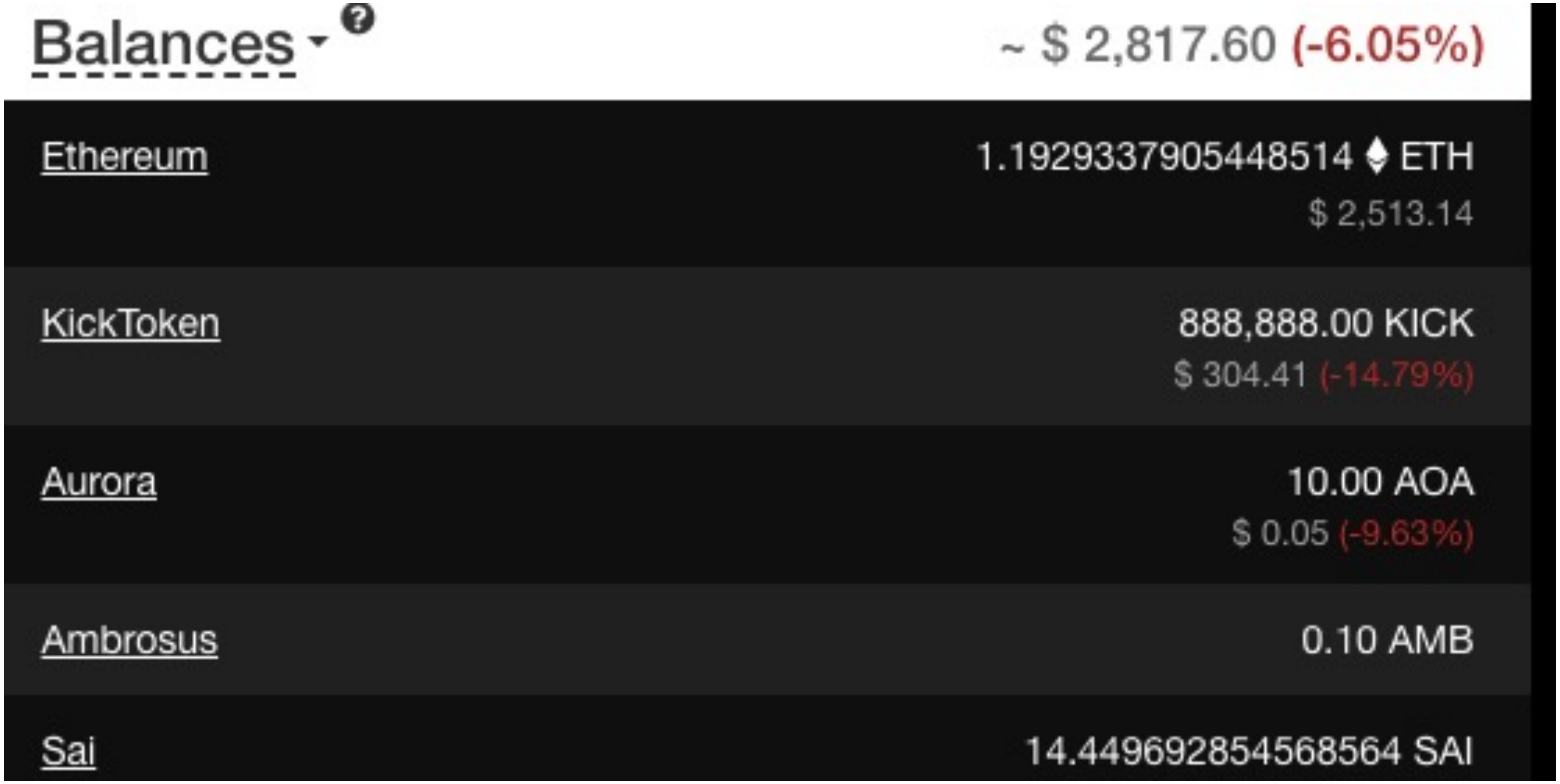
DAI	6.2060000368876 DAI $ 6.19 (+1.05%)
Apr 26 106-CALL	0.31 4/26 106-C

Stablecoin

Digital Wallet

Ethereum

Crypto-Currency



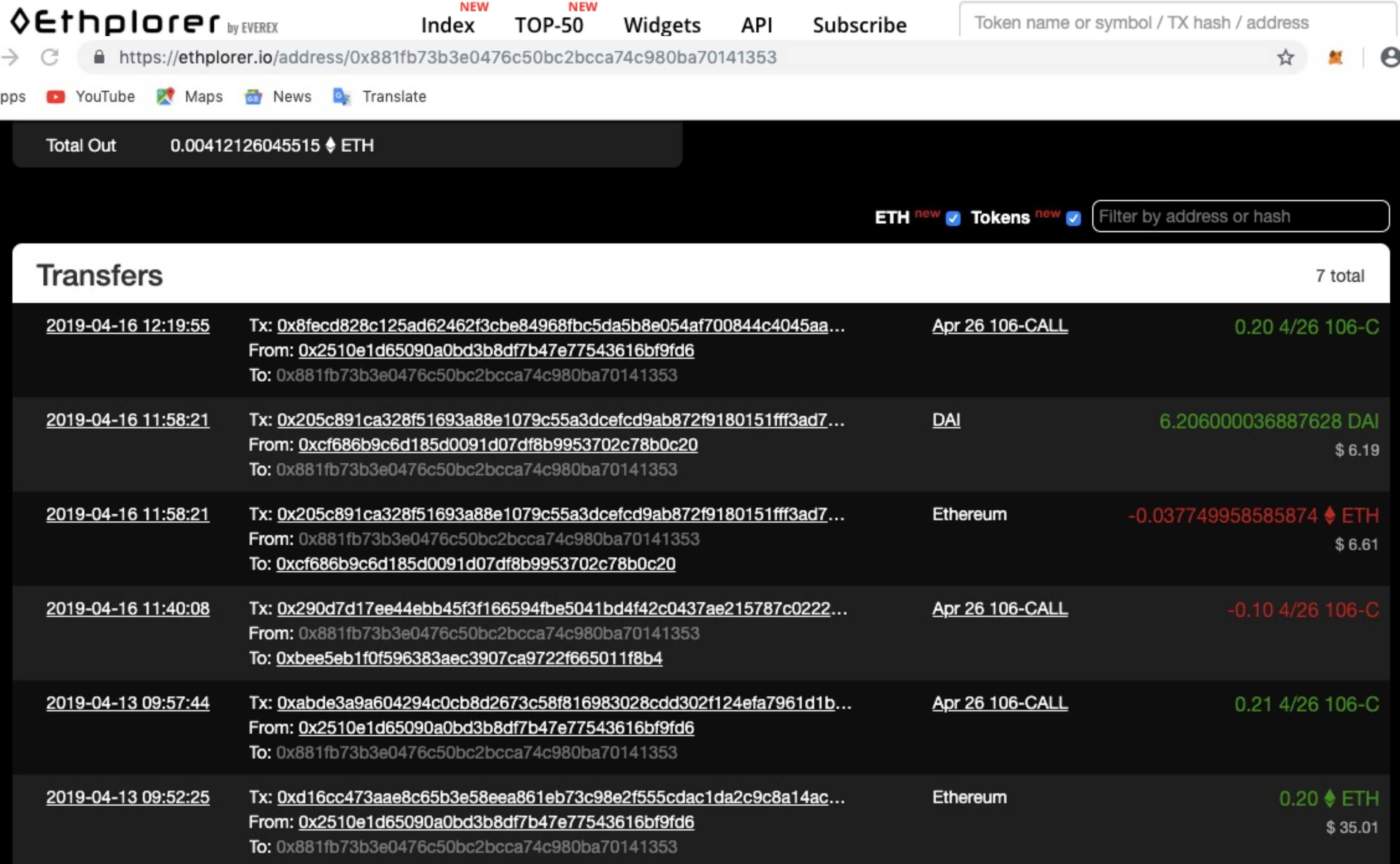
Balances ~ $ 2,817.60 (-6.05%)

Ethereum	1.1929337905448514 ETH $ 2,513.14
KickToken	888,888.00 KICK $ 304.41 (-14.79%)
Aurora	10.00 AOA $ 0.05 (-9.63%)
Ambrosus	0.10 AMB
Sai	14.449692854568564 SAI

Digital Wallet

Ethereum

Crypto-Currency



https://ethplorer.io/address/0x881fb73b3e0476c50bc2bcca74c980ba70141353

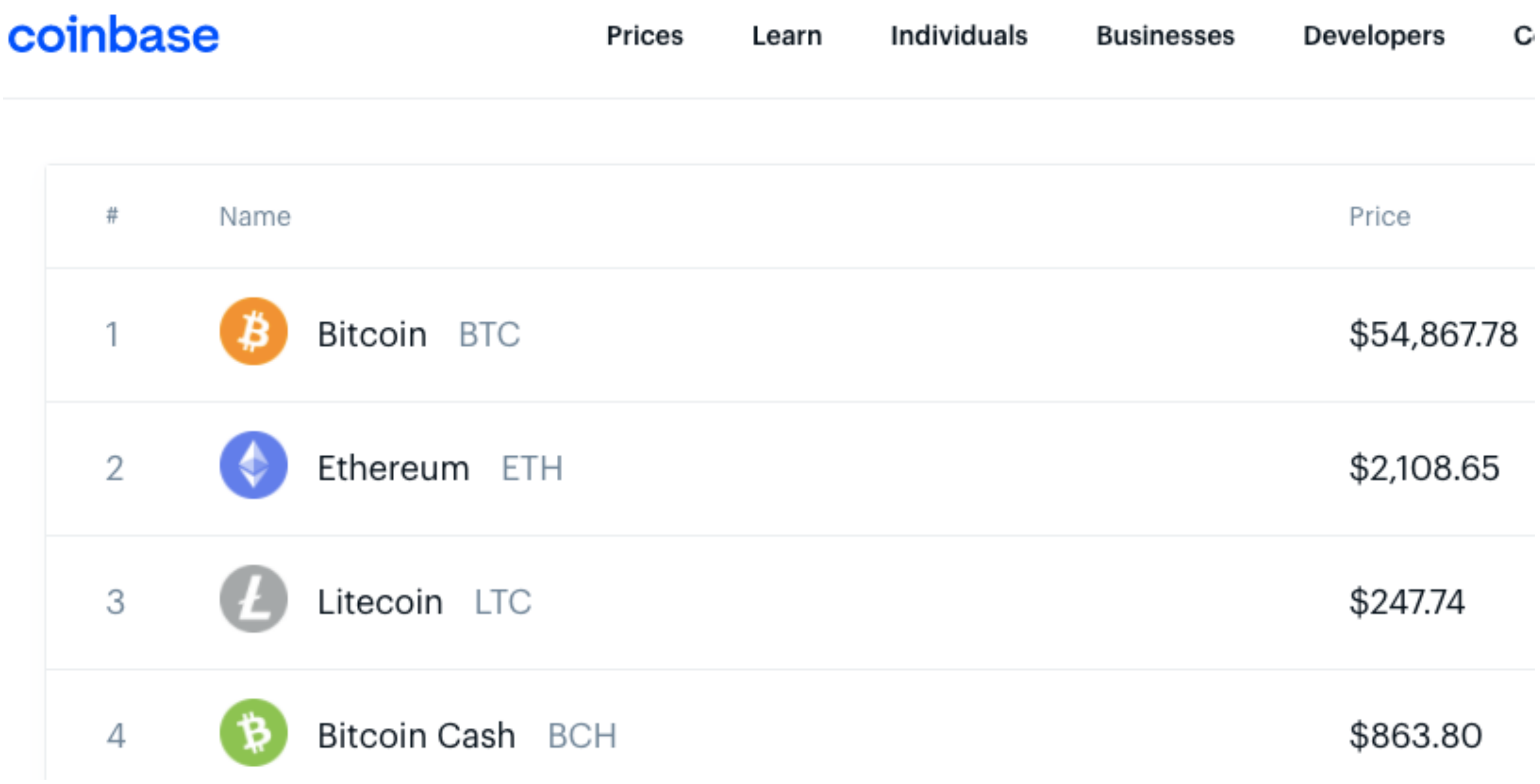
Total Out 0.00412126045515 ETH

Transfers

7 total

2019-04-16 12:19:55	Tx: 0x8fecd828c125ad62462f3cbe84968fbc5da5b8e054af700844c4045aa… From: 0x2510e1d65090a0bd3b8df7b47e77543616bf9fd6 To: 0x881fb73b3e0476c50bc2bcca74c980ba70141353	Apr 26 106-CALL	0.20 4/26 106-C
2019-04-16 11:58:21	Tx: 0x205c891ca328f51693a88e1079c55a3dcefcd9ab872f9180151fff3ad7… From: 0xcf686b9c6d185d0091d07df8b9953702c78b0c20 To: 0x881fb73b3e0476c50bc2bcca74c980ba70141353	DAI	6.206000036887628 DAI $ 6.19
2019-04-16 11:58:21	Tx: 0x205c891ca328f51693a88e1079c55a3dcefcd9ab872f9180151fff3ad7… From: 0x881fb73b3e0476c50bc2bcca74c980ba70141353 To: 0xcf686b9c6d185d0091d07df8b9953702c78b0c20	Ethereum	-0.037749958585874 ETH $ 6.61
2019-04-16 11:40:08	Tx: 0x290d7d17ee44ebb45f3f166594fbe5041bd4f42c0437ae215787c0222… From: 0x881fb73b3e0476c50bc2bcca74c980ba70141353 To: 0xbee5eb1f0f596383aec3907ca9722f665011f8b4	Apr 26 106-CALL	-0.10 4/26 106-C
2019-04-13 09:57:44	Tx: 0xabde3a9a604294c0cb8d2673c58f816983028cdd302f124efa7961d1b… From: 0x2510e1d65090a0bd3b8df7b47e77543616bf9fd6 To: 0x881fb73b3e0476c50bc2bcca74c980ba70141353	Apr 26 106-CALL	0.21 4/26 106-C
2019-04-13 09:52:25	Tx: 0xd16cc473aae8c65b3e58eea861eb73c98e2f555cdac1da2c9c8a14ac… From: 0x2510e1d65090a0bd3b8df7b47e77543616bf9fd6 To: 0x881fb73b3e0476c50bc2bcca74c980ba70141353	Ethereum	0.20 ETH $ 35.01

Coinbase



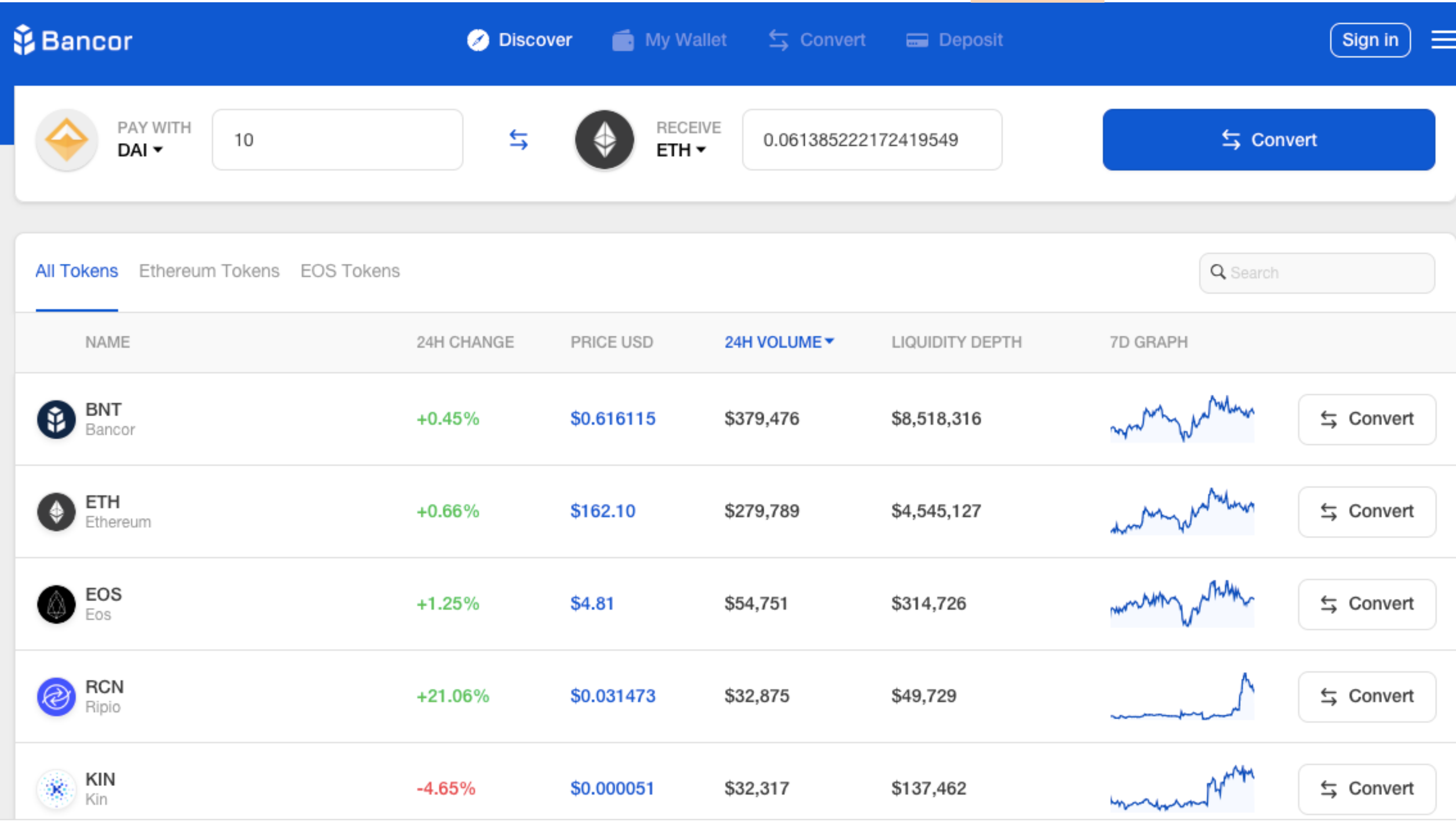
#	Name	Price
1	Bitcoin BTC	$54,867.78
2	Ethereum ETH	$2,108.65
3	Litecoin LTC	$247.74
4	Bitcoin Cash BCH	$863.80

CSUN
CALIFORNIA STATE UNIVERSITY NORTHRIDGE

Crypto Currency Exchange

DR JEFF SOFTWARE
© Jeff Drobman
2017-23

Bancor



PAY WITH DAI: 10

RECEIVE ETH: 0.0613852221724195 49

Convert

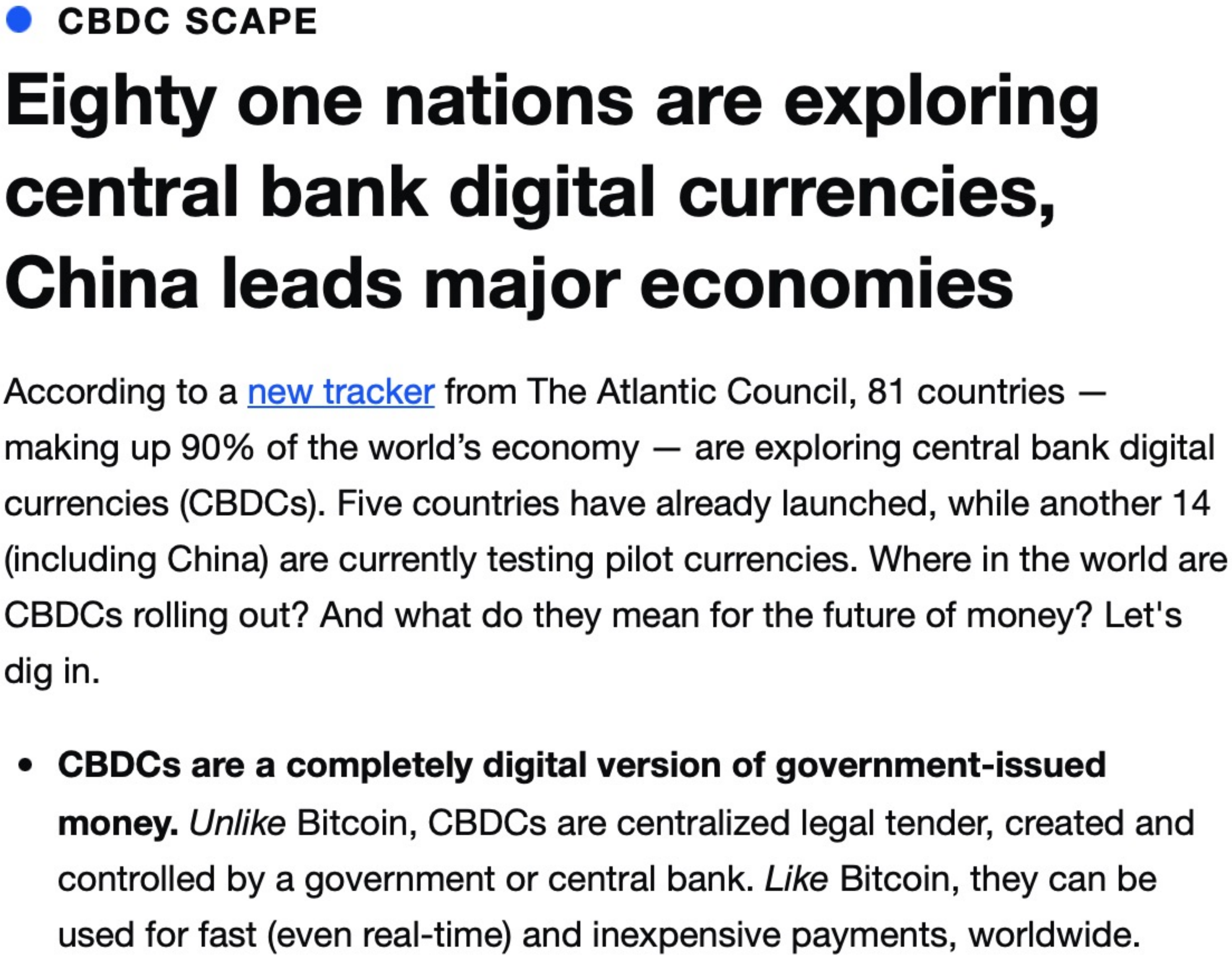
All Tokens | Ethereum Tokens | EOS Tokens | Search

NAME	24H CHANGE	PRICE USD	24H VOLUME	LIQUIDITY DEPTH	7D GRAPH	
BNT Bancor	+0.45%	$0.616115	$379,476	$8,518,316		Convert
ETH Ethereum	+0.66%	$162.10	$279,789	$4,545,127		Convert
EOS Eos	+1.25%	$4.81	$54,751	$314,726		Convert
RCN Ripio	+21.06%	$0.031473	$32,875	$49,729		Convert
KIN Kin	-4.65%	$0.000051	$32,317	$137,462		Convert

Crypto Currency

CBDC

CBDC



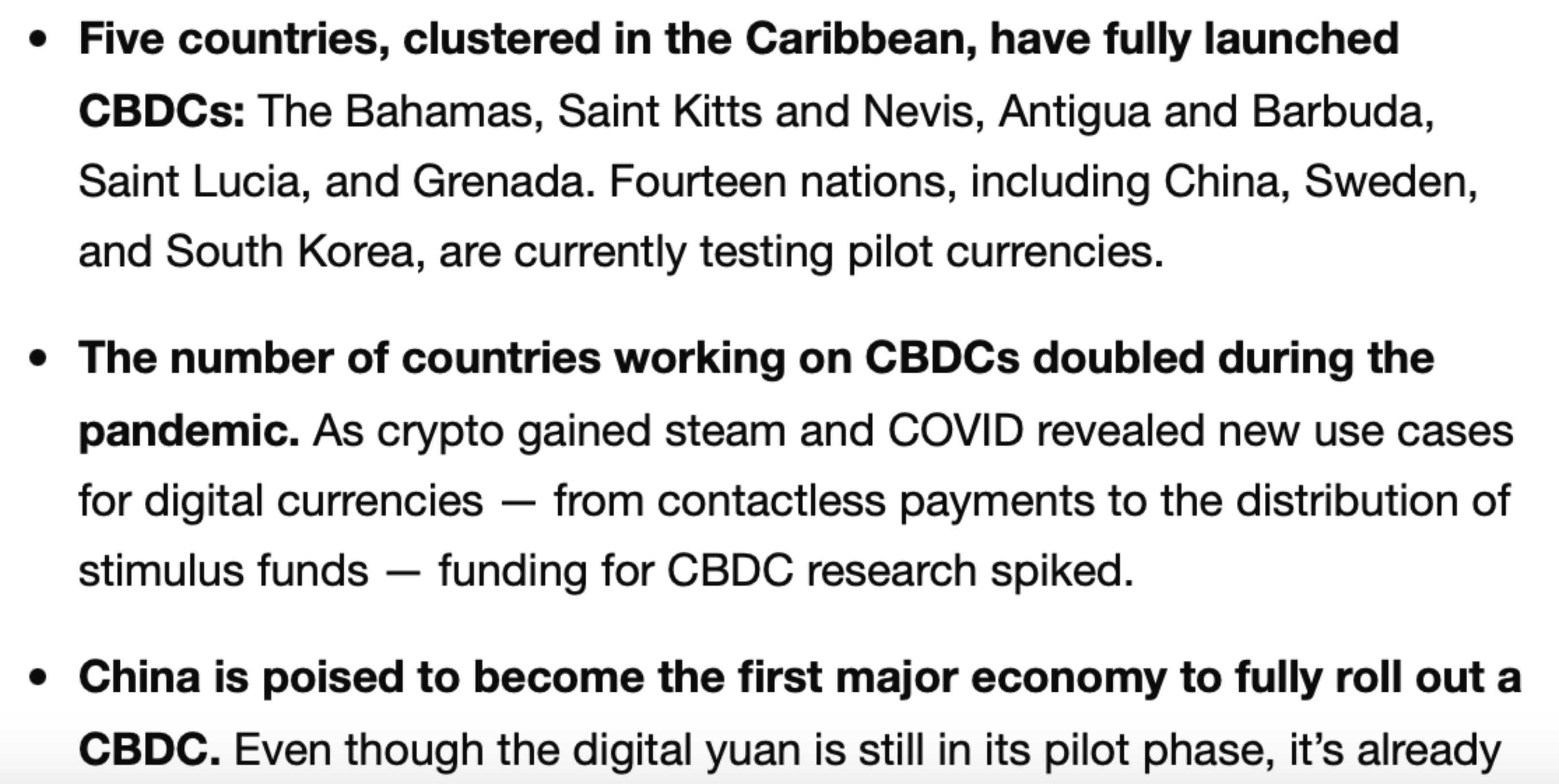
● CBDC SCAPE

Eighty one nations are exploring central bank digital currencies, China leads major economies

According to a new tracker from The Atlantic Council, 81 countries — making up 90% of the world's economy — are exploring central bank digital currencies (CBDCs). Five countries have already launched, while another 14 (including China) are currently testing pilot currencies. Where in the world are CBDCs rolling out? And what do they mean for the future of money? Let's dig in.

- **CBDCs are a completely digital version of government-issued money.** *Unlike* Bitcoin, CBDCs are centralized legal tender, created and controlled by a government or central bank. *Like* Bitcoin, they can be used for fast (even real-time) and inexpensive payments, worldwide.

CBDC



- **Five countries, clustered in the Caribbean, have fully launched CBDCs:** The Bahamas, Saint Kitts and Nevis, Antigua and Barbuda, Saint Lucia, and Grenada. Fourteen nations, including China, Sweden, and South Korea, are currently testing pilot currencies.

- **The number of countries working on CBDCs doubled during the pandemic.** As crypto gained steam and COVID revealed new use cases for digital currencies — from contactless payments to the distribution of stimulus funds — funding for CBDC research spiked.

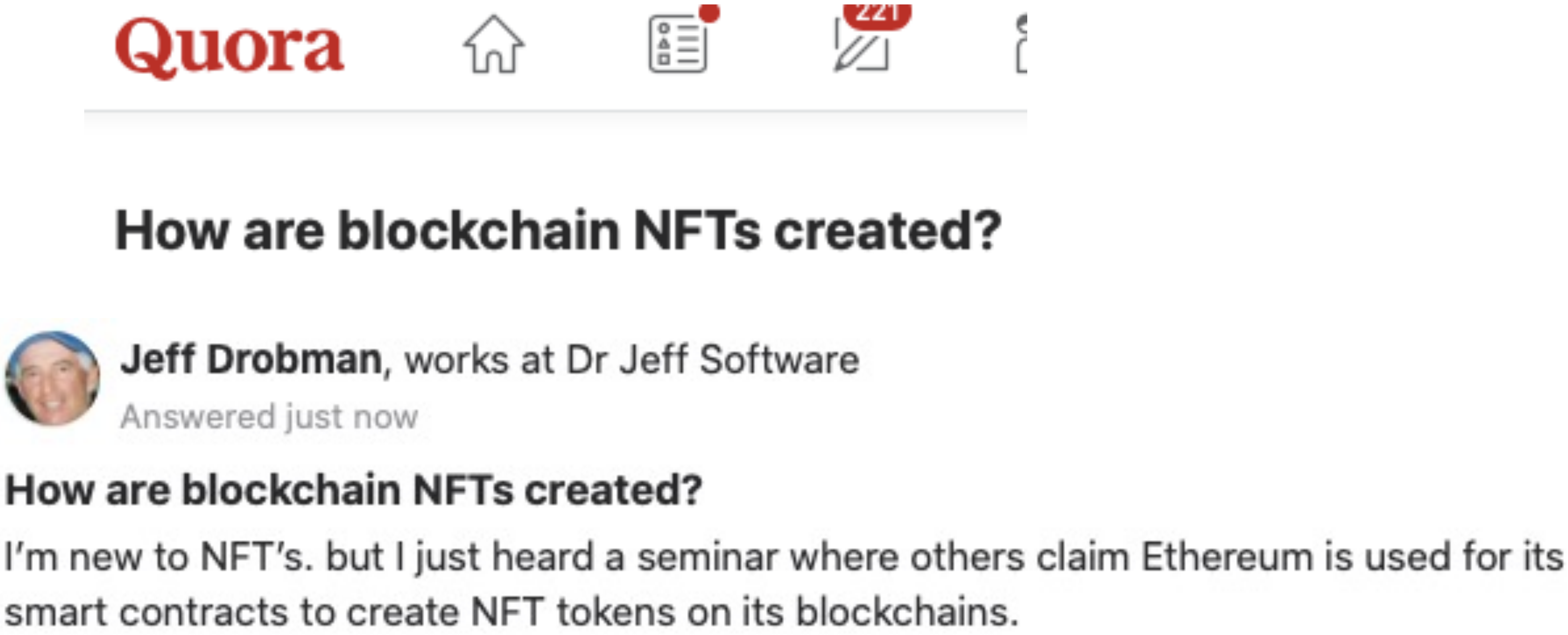
- **China is poised to become the first major economy to fully roll out a CBDC.** Even though the digital yuan is still in its pilot phase, it’s already

Section

NFT

Non-Fungible Tokens

NFT



How are blockchain NFTs created?

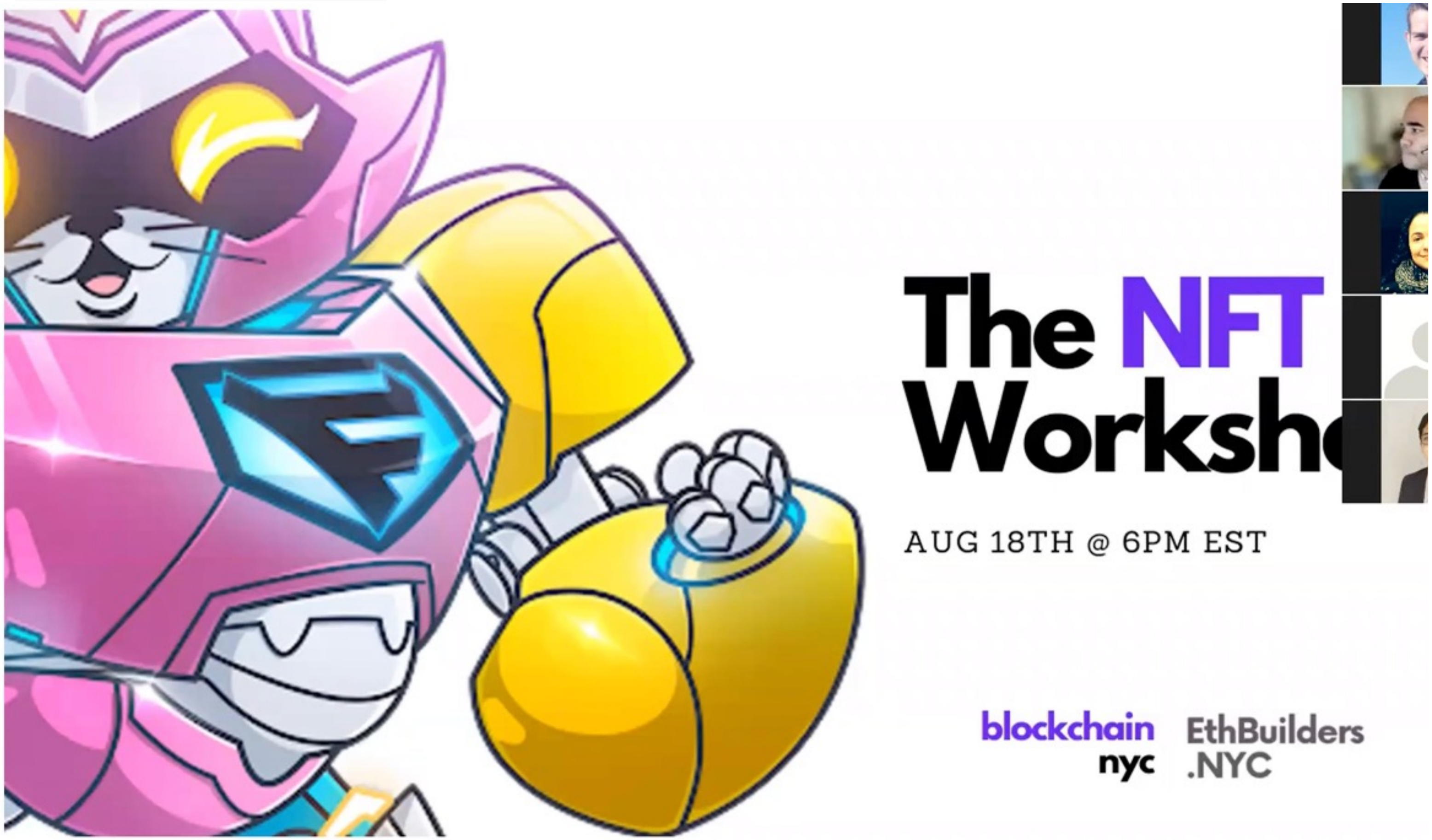
Jeff Drobman, works at Dr Jeff Software

Answered just now

How are blockchain NFTs created?

I'm new to NFT's. but I just heard a seminar where others claim Ethereum is used for its smart contracts to create NFT tokens on its blockchains.

NFT



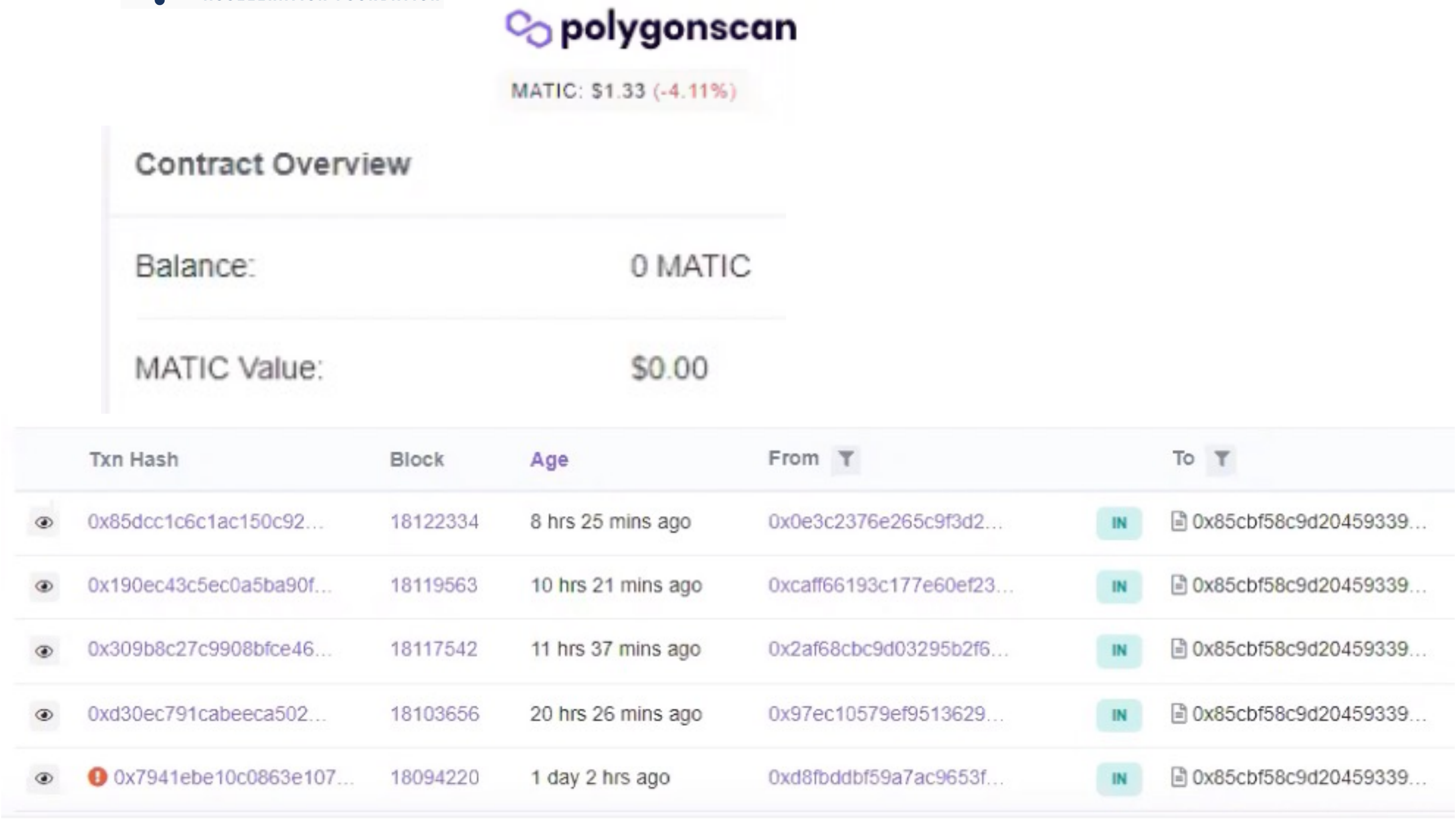
The NFT Worksh

AUG 18TH @ 6PM EST

blockchain nyc

EthBuilders .NYC

NFT



polygonscan

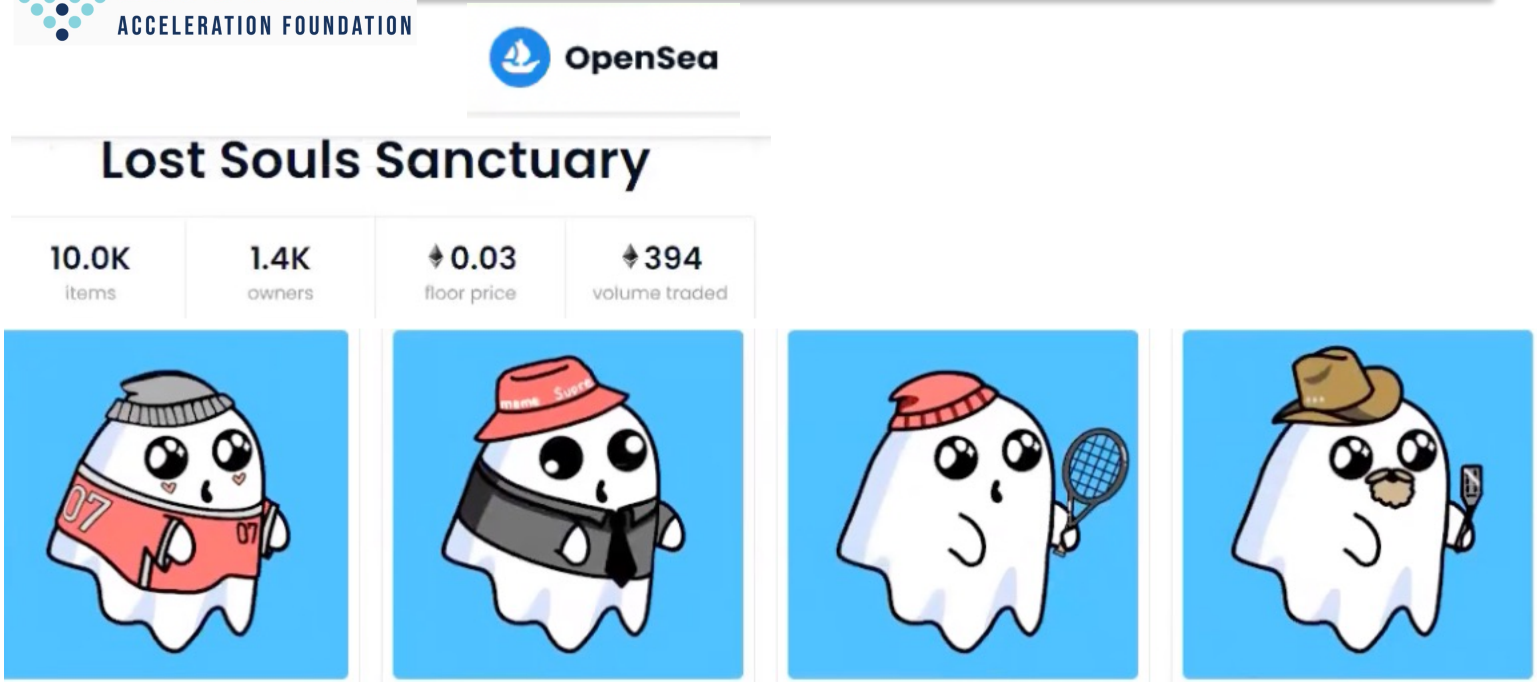
MATIC: $1.33 (-4.11%)

Contract Overview

Balance:	0 MATIC
MATIC Value:	$0.00

Txn Hash	Block	Age	From		To
0x85dcc1c6c1ac150c92...	18122334	8 hrs 25 mins ago	0x0e3c2376e265c9f3d2...	IN	0x85cbf58c9d20459339...
0x190ec43c5ec0a5ba90f...	18119563	10 hrs 21 mins ago	0xcaff66193c177e60ef23...	IN	0x85cbf58c9d20459339...
0x309b8c27c9908bfce46...	18117542	11 hrs 37 mins ago	0x2af68cbc9d03295b2f6...	IN	0x85cbf58c9d20459339...
0xd30ec791cabeeca502...	18103656	20 hrs 26 mins ago	0x97ec10579ef9513629...	IN	0x85cbf58c9d20459339...
! 0x7941ebe10c0863e107...	18094220	1 day 2 hrs ago	0xd8fbddbf59a7ac9653f...	IN	0x85cbf58c9d20459339...

NFT Art

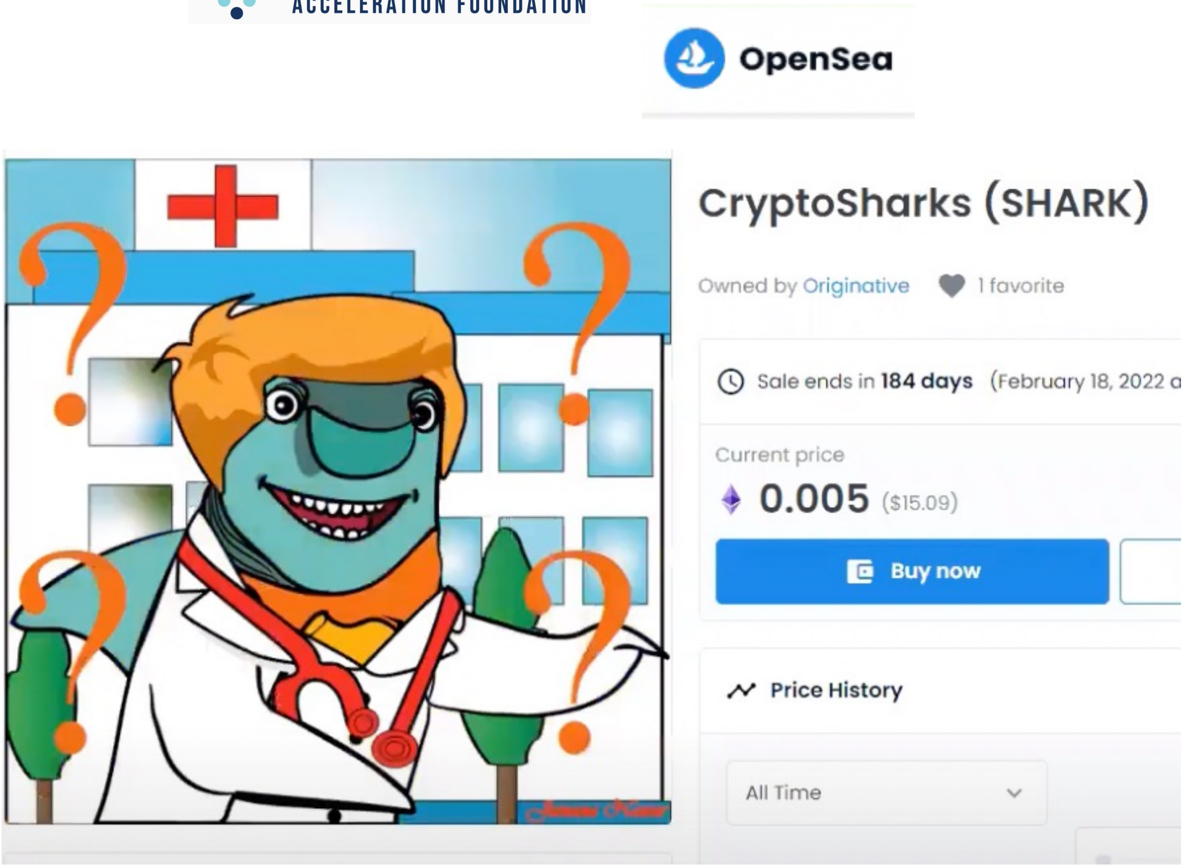


OpenSea

Lost Souls Sanctuary

10.0K	1.4K	♦0.03	♦394
items	owners	floor price	volume traded

NFT Art



OpenSea

CryptoSharks (SHARK)

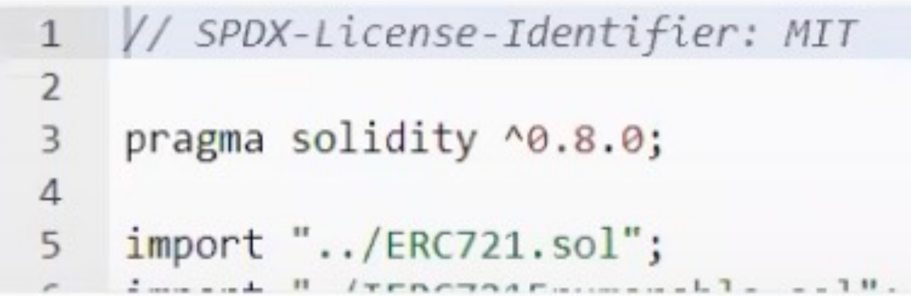
Owned by Originative   1 favorite

Sale ends in **184 days** (February 18, 2022 a

Current price
0.005 ($15.09)

1st
SPACE ROCK
© 2021 Mr Vector Man
MADE ON THE BLOCKCHAIN
007-FS

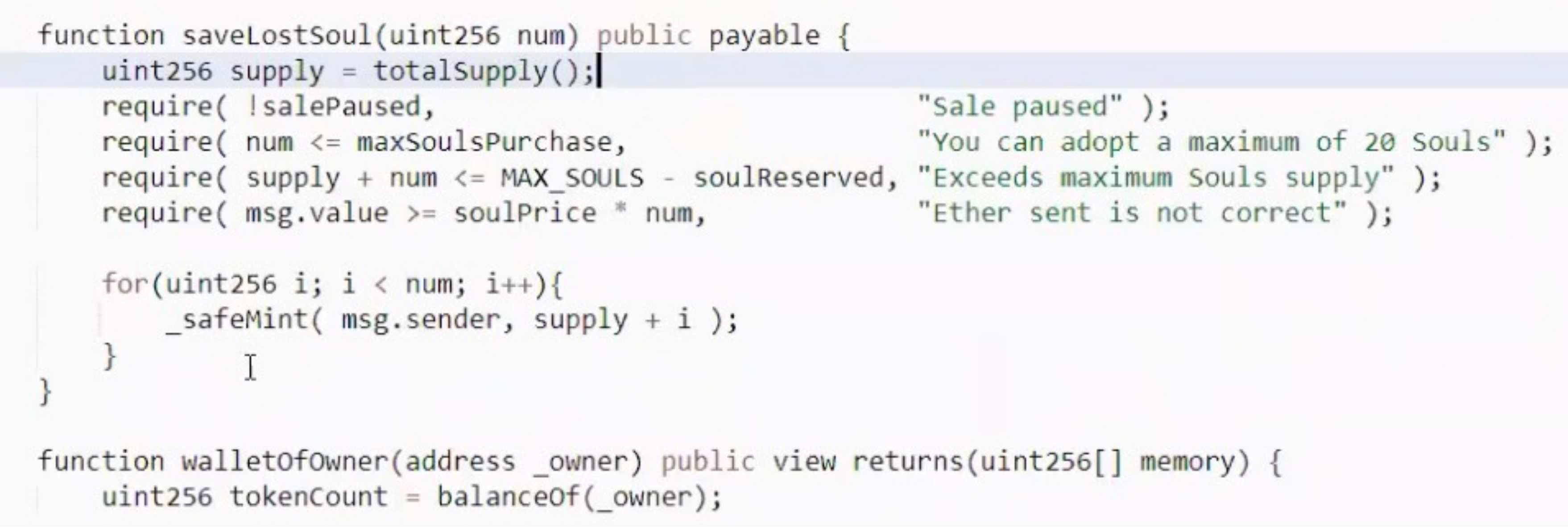
NFT Code



```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

import "../ERC721.sol";
```

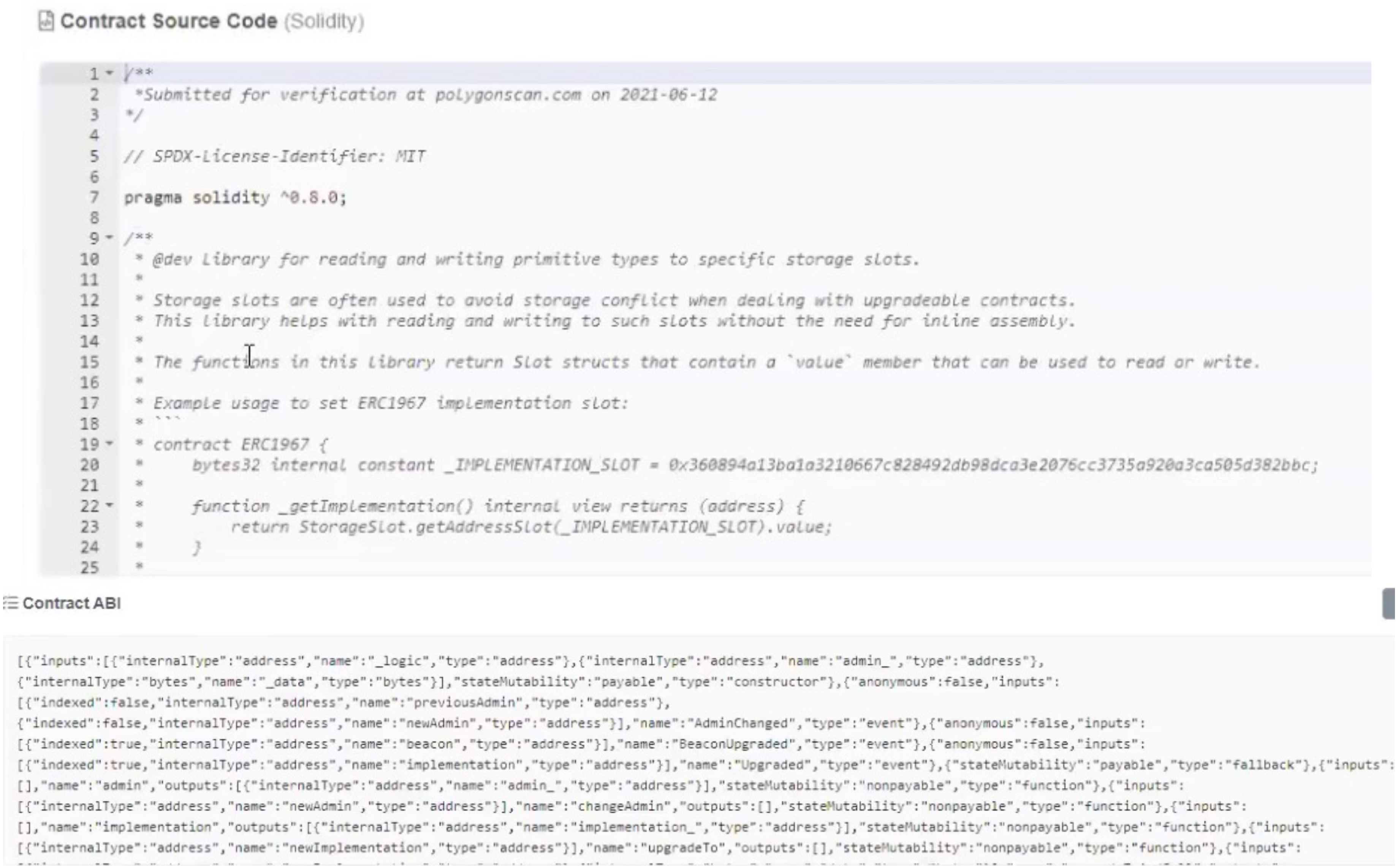


```
function saveLostSoul(uint256 num) public payable {
    uint256 supply = totalSupply();
    require( !salePaused,                              "Sale paused" );
    require( num <= maxSoulsPurchase,                  "You can adopt a maximum of 20 Souls" );
    require( supply + num <= MAX_SOULS - soulReserved, "Exceeds maximum Souls supply" );
    require( msg.value >= soulPrice * num,             "Ether sent is not correct" );

    for(uint256 i; i < num; i++){
        _safeMint( msg.sender, supply + i );
    }
}

function walletOfOwner(address _owner) public view returns(uint256[] memory) {
    uint256 tokenCount = balanceOf(_owner);
```

NFT Code



Contract Source Code (Solidity)

```
/**
 *Submitted for verification at polygonscan.com on 2021-06-12
*/

// SPDX-License-Identifier: MIT

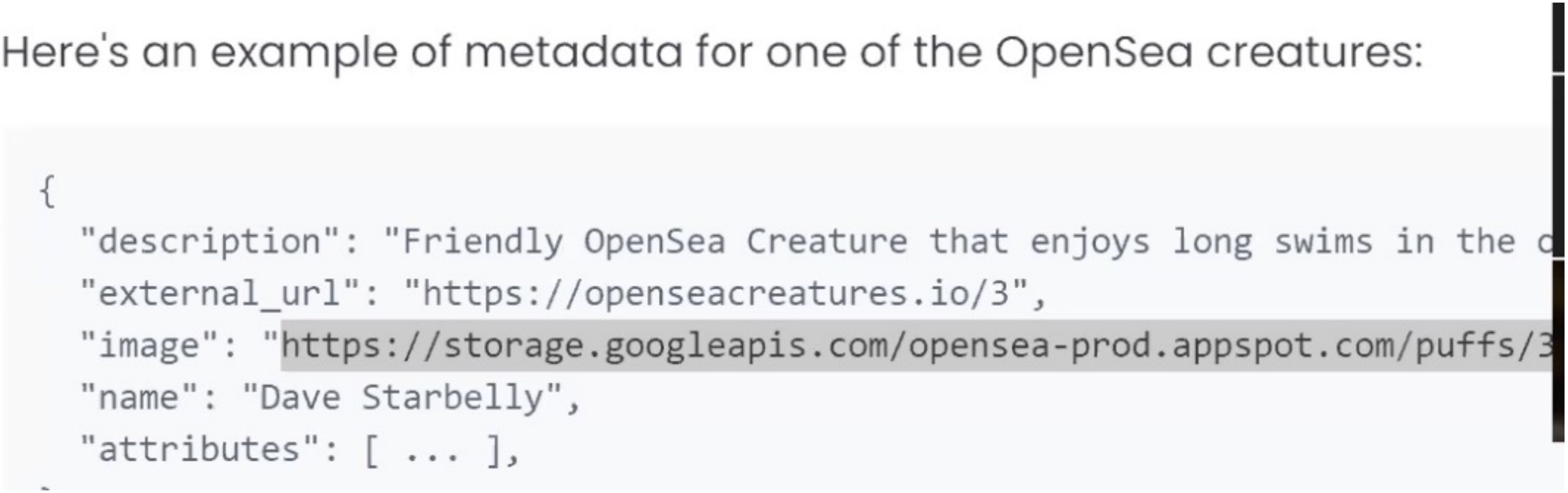
pragma solidity ^0.8.0;

/**
 * @dev Library for reading and writing primitive types to specific storage slots.
 *
 * Storage slots are often used to avoid storage conflict when dealing with upgradeable contracts.
 * This library helps with reading and writing to such slots without the need for inline assembly.
 *
 * The functions in this library return Slot structs that contain a `value` member that can be used to read or write.
 *
 * Example usage to set ERC1967 implementation slot:
 * ```
 * contract ERC1967 {
 *     bytes32 internal constant _IMPLEMENTATION_SLOT = 0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc;
 *
 *     function _getImplementation() internal view returns (address) {
 *         return StorageSlot.getAddressSlot(_IMPLEMENTATION_SLOT).value;
 *     }
 *
```

Contract ABI

[{"inputs":[{"internalType":"address","name":"_logic","type":"address"},{"internalType":"address","name":"admin_","type":"address"},
{"internalType":"bytes","name":"_data","type":"bytes"}],"stateMutability":"payable","type":"constructor"},{"anonymous":false,"inputs":
[{"indexed":false,"internalType":"address","name":"previousAdmin","type":"address"},
{"indexed":false,"internalType":"address","name":"newAdmin","type":"address"}],"name":"AdminChanged","type":"event"},{"anonymous":false,"inputs":
[{"indexed":true,"internalType":"address","name":"beacon","type":"address"}],"name":"BeaconUpgraded","type":"event"},{"anonymous":false,"inputs":
[{"indexed":true,"internalType":"address","name":"implementation","type":"address"}],"name":"Upgraded","type":"event"},{"stateMutability":"payable","type":"fallback"},{"inputs":
[],"name":"admin","outputs":[{"internalType":"address","name":"admin_","type":"address"}],"stateMutability":"nonpayable","type":"function"},{"inputs":
[{"internalType":"address","name":"newAdmin","type":"address"}],"name":"changeAdmin","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs":
[],"name":"implementation","outputs":[{"internalType":"address","name":"implementation_","type":"address"}],"stateMutability":"nonpayable","type":"function"},{"inputs":
[{"internalType":"address","name":"newImplementation","type":"address"}],"name":"upgradeTo","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs":

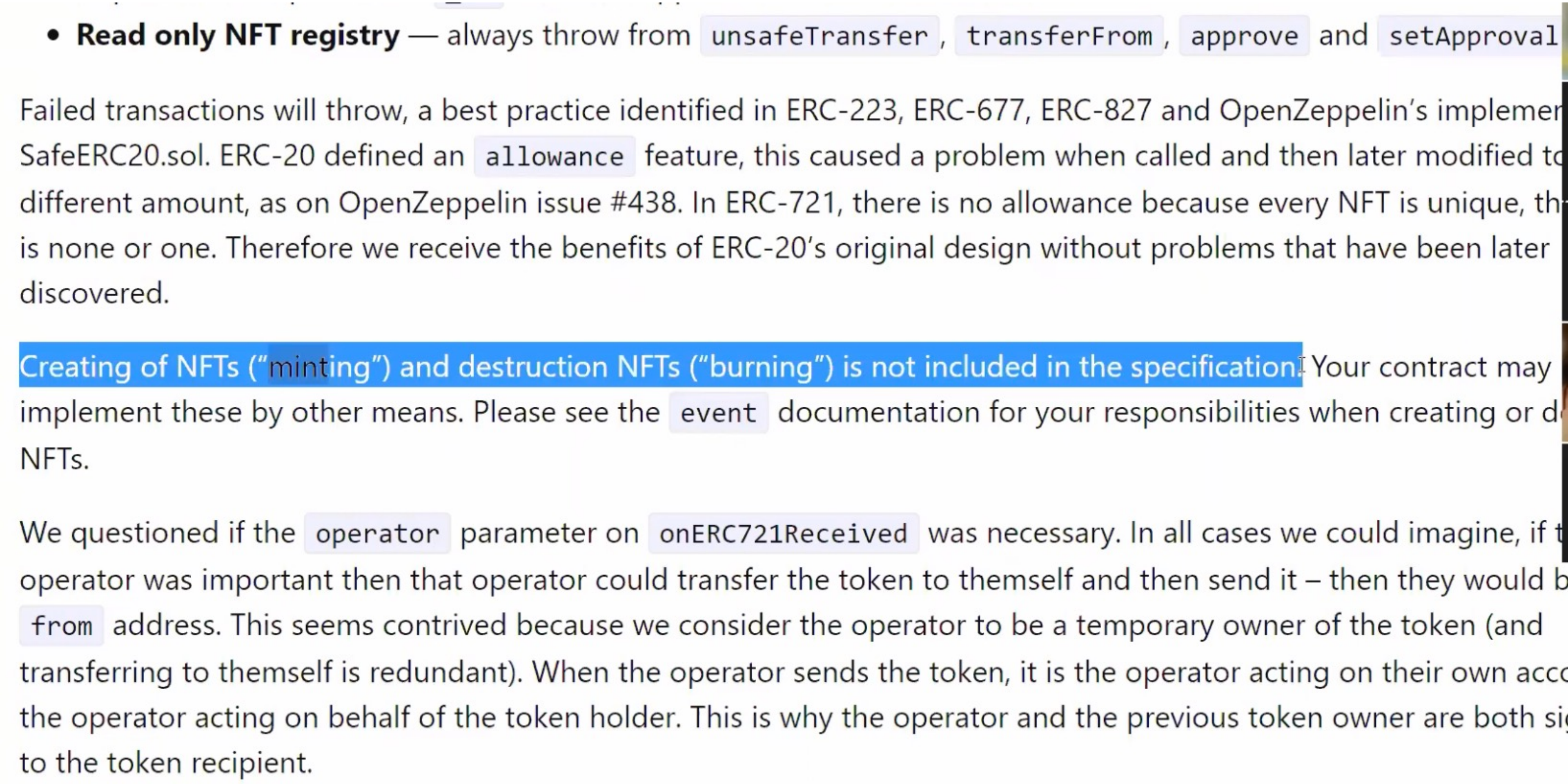
NFT Metadata



Here's an example of metadata for one of the OpenSea creatures:

```
{
   "description": "Friendly OpenSea Creature that enjoys long swims in the o
   "external_url": "https://openseacreatures.io/3",
   "image": "https://storage.googleapis.com/opensea-prod.appspot.com/puffs/3
   "name": "Dave Starbelly",
   "attributes": [ ... ],
```

NFT



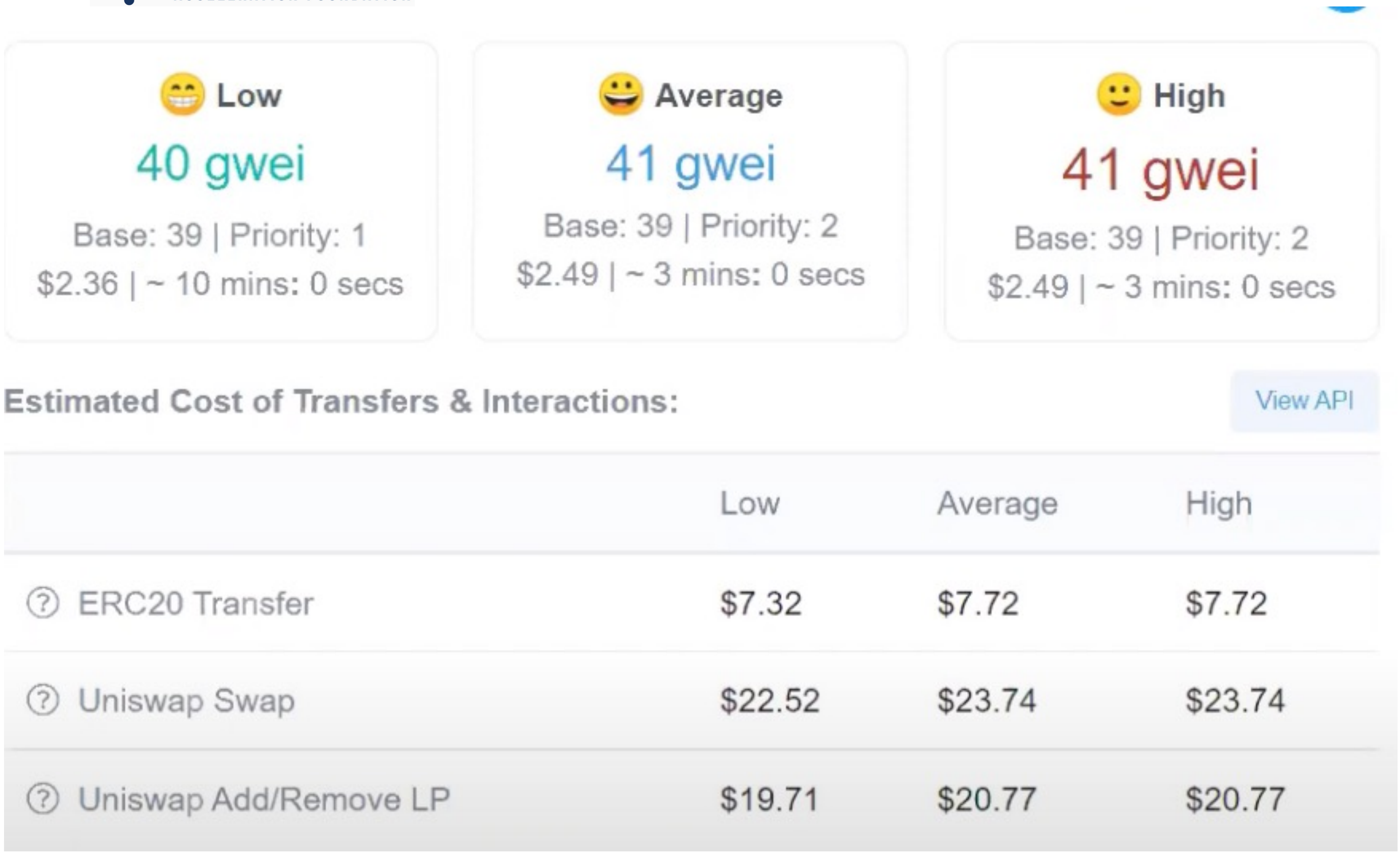
- **Read only NFT registry** — always throw from `unsafeTransfer`, `transferFrom`, `approve` and `setApproval`

Failed transactions will throw, a best practice identified in ERC-223, ERC-677, ERC-827 and OpenZeppelin's implemen SafeERC20.sol. ERC-20 defined an `allowance` feature, this caused a problem when called and then later modified to different amount, as on OpenZeppelin issue #438. In ERC-721, there is no allowance because every NFT is unique, th is none or one. Therefore we receive the benefits of ERC-20's original design without problems that have been later discovered.

Creating of NFTs ("minting") and destruction NFTs ("burning") is not included in the specification. Your contract may implement these by other means. Please see the `event` documentation for your responsibilities when creating or d NFTs.

We questioned if the `operator` parameter on `onERC721Received` was necessary. In all cases we could imagine, if t operator was important then that operator could transfer the token to themself and then send it – then they would b `from` address. This seems contrived because we consider the operator to be a temporary owner of the token (and transferring to themself is redundant). When the operator sends the token, it is the operator acting on their own acco the operator acting on behalf of the token holder. This is why the operator and the previous token owner are both si to the token recipient.

NFT

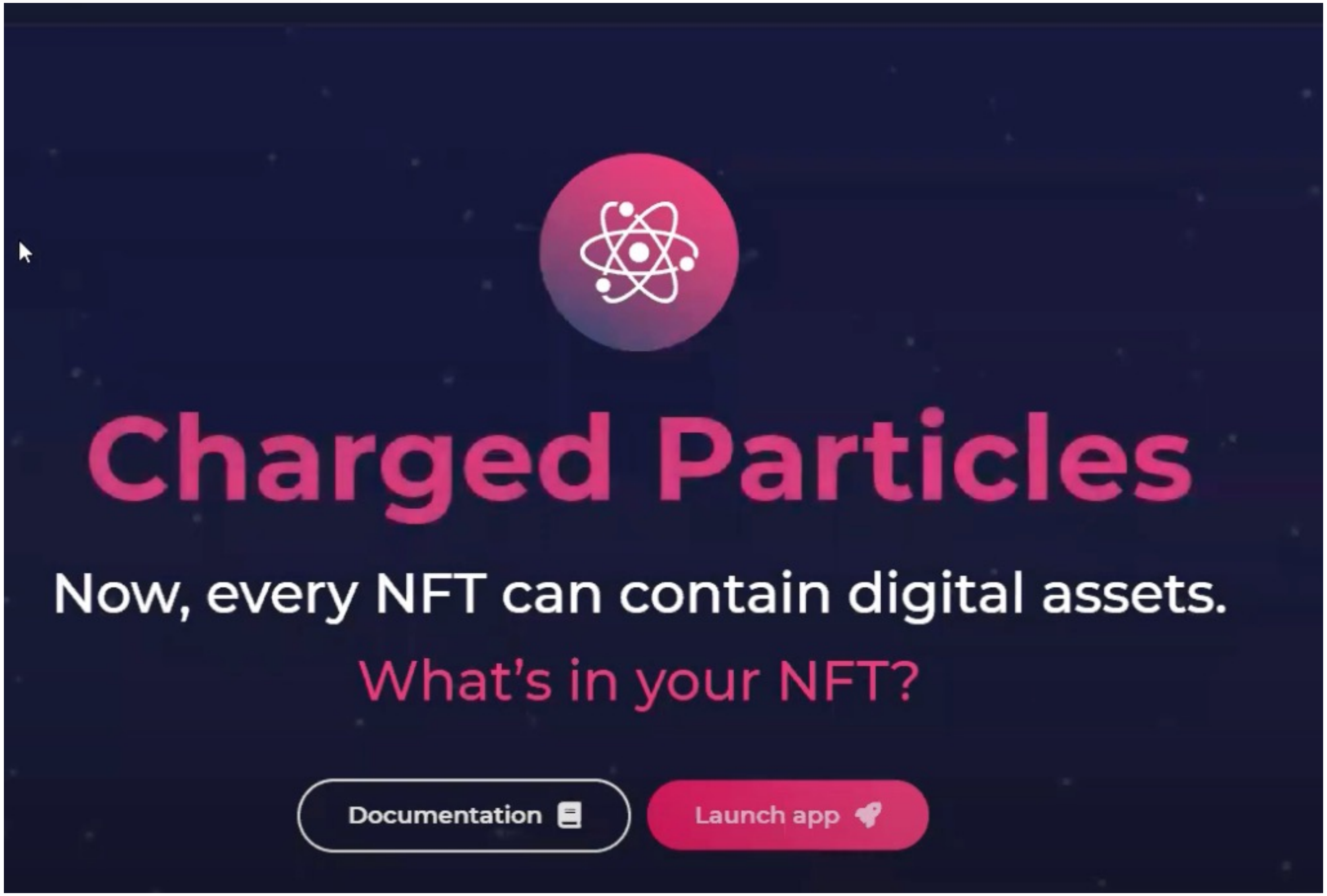


Low	Average	High
40 gwei	41 gwei	41 gwei
Base: 39 | Priority: 1	Base: 39 | Priority: 2	Base: 39 | Priority: 2
$2.36 | ~ 10 mins: 0 secs	$2.49 | ~ 3 mins: 0 secs	$2.49 | ~ 3 mins: 0 secs

Estimated Cost of Transfers & Interactions:

	Low	Average	High
ERC20 Transfer	$7.32	$7.72	$7.72
Uniswap Swap	$22.52	$23.74	$23.74
Uniswap Add/Remove LP	$19.71	$20.77	$20.77

NFT

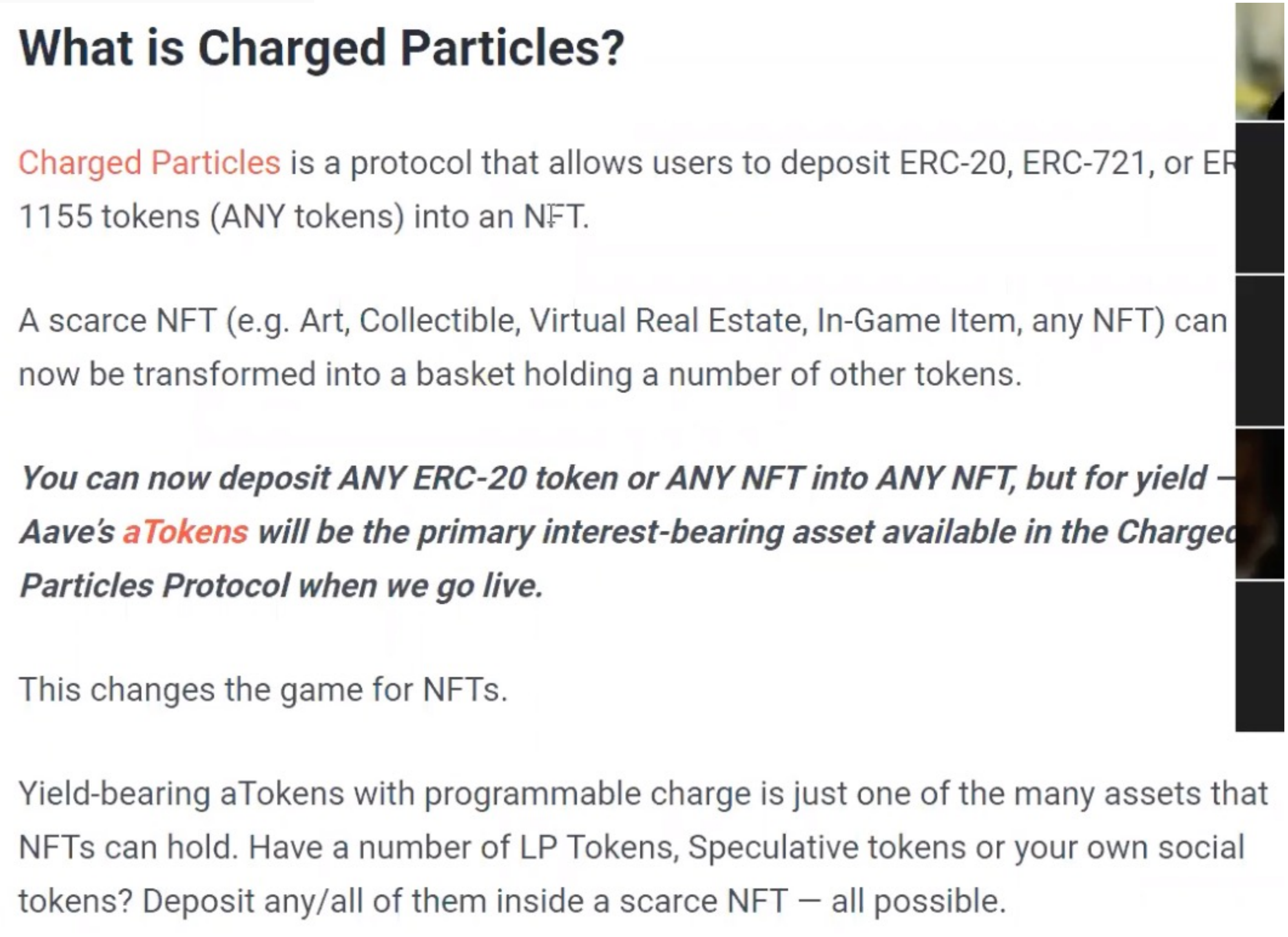


Charged Particles

Now, every NFT can contain digital assets.

What's in your NFT?

NFT



What is Charged Particles?

Charged Particles is a protocol that allows users to deposit ERC-20, ERC-721, or ER
1155 tokens (ANY tokens) into an NFT.

A scarce NFT (e.g. Art, Collectible, Virtual Real Estate, In-Game Item, any NFT) can now be transformed into a basket holding a number of other tokens.

You can now deposit ANY ERC-20 token or ANY NFT into ANY NFT, but for yield — Aave's aTokens will be the primary interest-bearing asset available in the Chargec Particles Protocol when we go live.

This changes the game for NFTs.

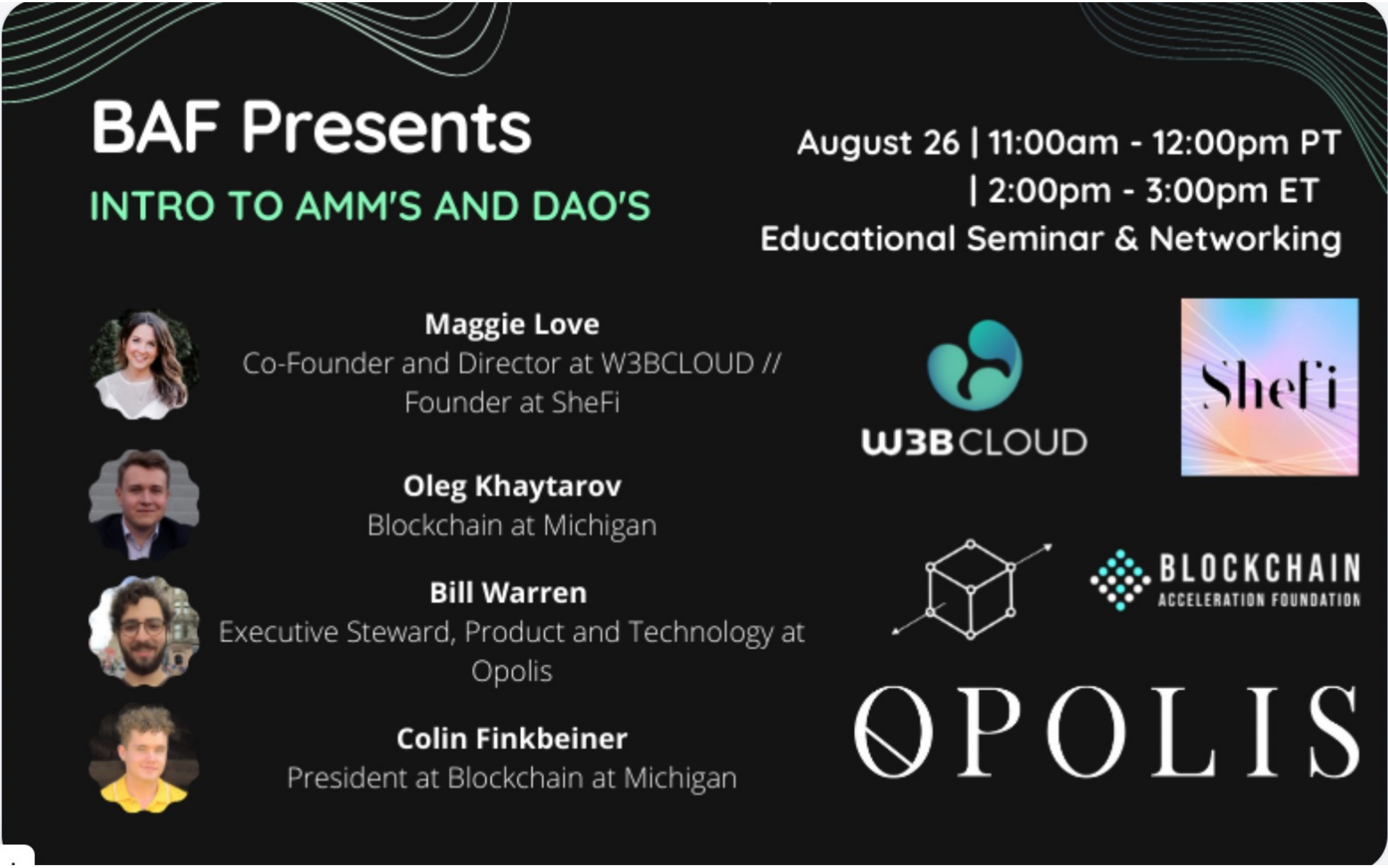
Yield-bearing aTokens with programmable charge is just one of the many assets that NFTs can hold. Have a number of LP Tokens, Speculative tokens or your own social tokens? Deposit any/all of them inside a scarce NFT — all possible.

Section

Misc

❖CSUN Club (BAF)
❖Polygon
❖ZKP

BAF



BAF Presents

INTRO TO AMM'S AND DAO'S

August 26 | 11:00am - 12:00pm PT
| 2:00pm - 3:00pm ET
Educational Seminar & Networking

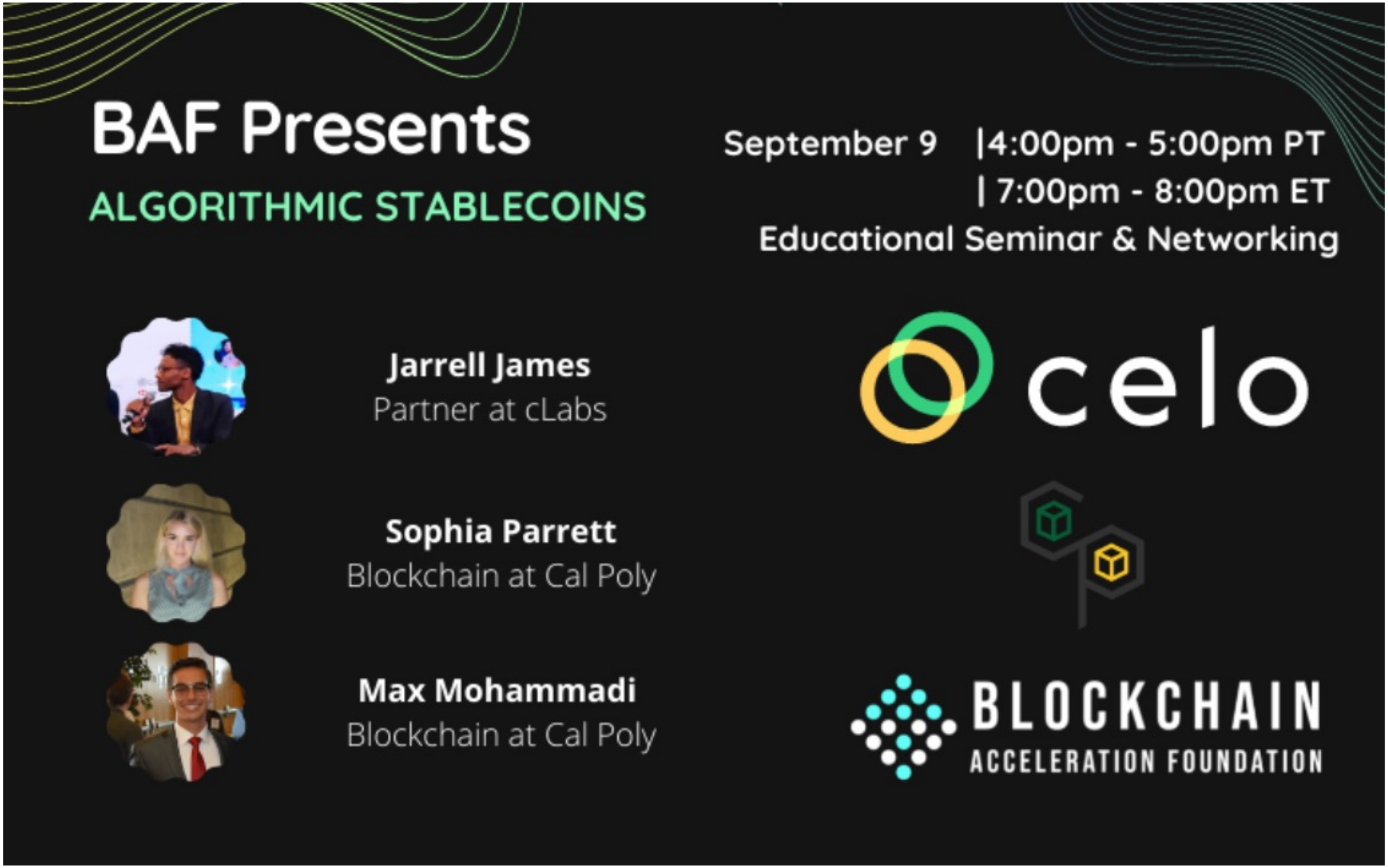
Maggie Love
Co-Founder and Director at W3BCLOUD //
Founder at SheFi

Oleg Khaytarov
Blockchain at Michigan

Bill Warren
Executive Steward, Product and Technology at
Opolis

Colin Finkbeiner
President at Blockchain at Michigan

BAF



BAF Presents

ALGORITHMIC STABLECOINS

September 9 | 4:00pm - 5:00pm PT
| 7:00pm - 8:00pm ET
Educational Seminar & Networking

Jarrell James
Partner at cLabs

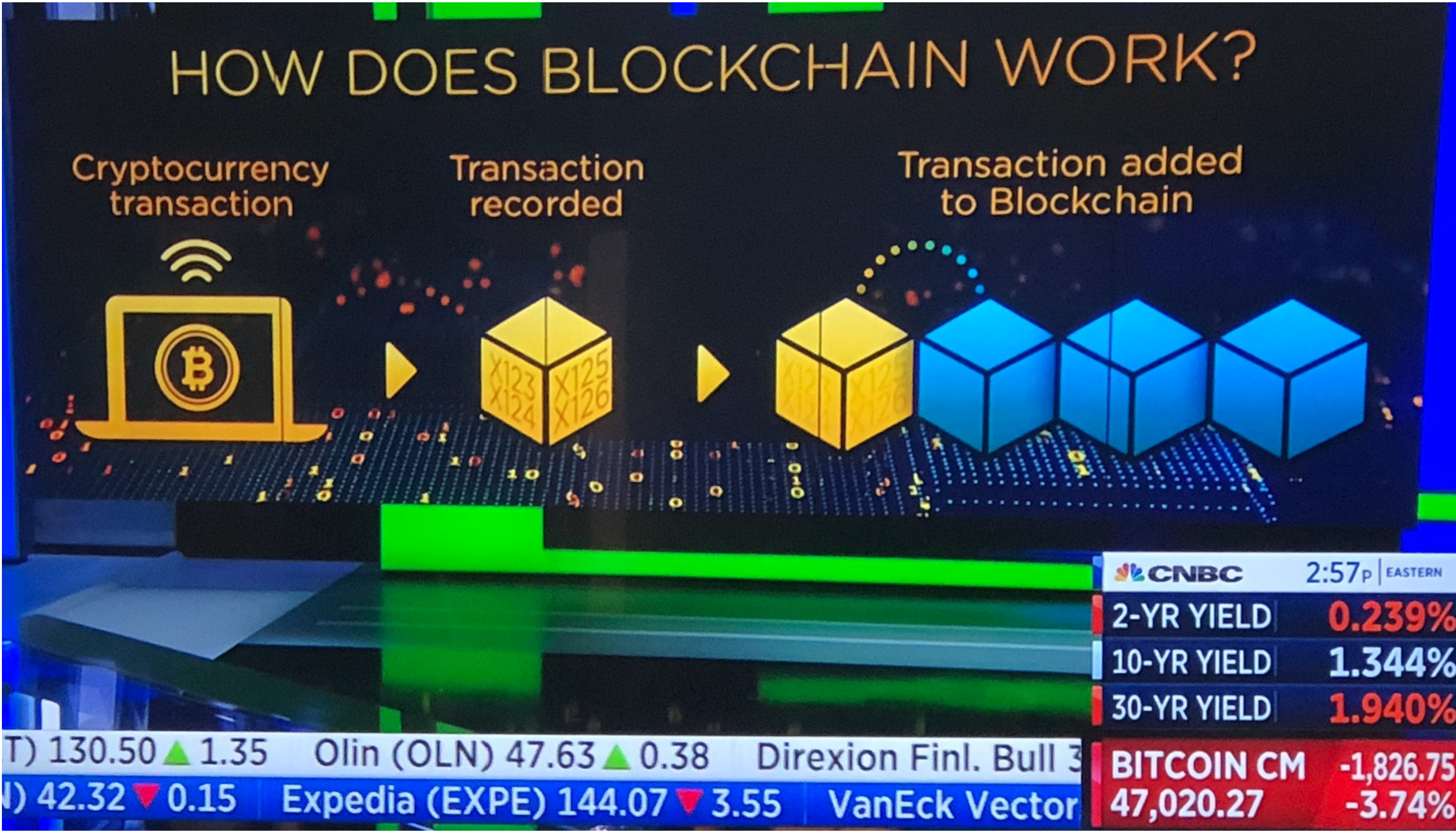
Sophia Parrett
Blockchain at Cal Poly

Max Mohammadi
Blockchain at Cal Poly

celo
BLOCKCHAIN ACCELERATION FOUNDATION

Blockchains

Public vs Private


HOW DOES BLOCKCHAIN WORK?
Cryptocurrency transaction
Transaction recorded
Transaction added to Blockchain
X123 X124 X125 X126
CNBC 2:57P EASTERN
2-YR YIELD 0.239%
10-YR YIELD 1.344%
30-YR YIELD 1.940%
BITCOIN CM 47,020.27 -1,826.75 -3.74%
T) 130.50 ▲ 1.35 Olin (OLN) 47.63 ▲ 0.38 Direxion Finl. Bull 3
I) 42.32 ▼ 0.15 Expedia (EXPE) 144.07 ▼ 3.55 VanEck Vector

CIS Blockchain Summit

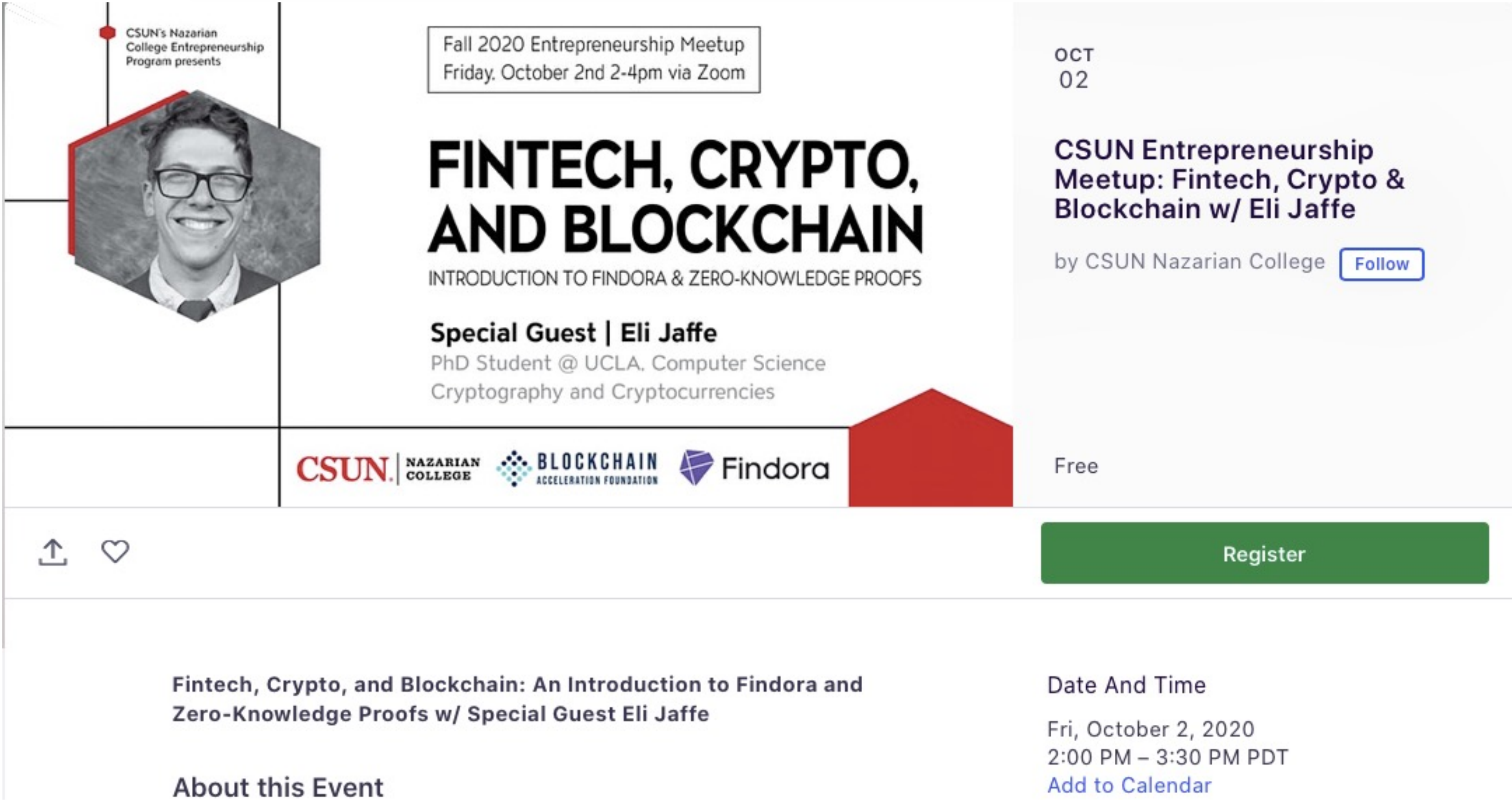
CIS

CSUN Blockchain Club (Biz School)

CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

CSUN Blockchain Club

DSJ Dr Jeff
DR JEFF
SOFTWARE



CSUN's Nazarian College Entrepreneurship Program presents

Fall 2020 Entrepreneurship Meetup
Friday. October 2nd 2-4pm via Zoom

FINTECH, CRYPTO, AND BLOCKCHAIN

INTRODUCTION TO FINDORA & ZERO-KNOWLEDGE PROOFS

Special Guest | Eli Jaffe
PhD Student @ UCLA. Computer Science
Cryptography and Cryptocurrencies

OCT
02

CSUN Entrepreneurship Meetup: Fintech, Crypto & Blockchain w/ Eli Jaffe

by CSUN Nazarian College

Free

Fintech, Crypto, and Blockchain: An Introduction to Findora and Zero-Knowledge Proofs w/ Special Guest Eli Jaffe

About this Event

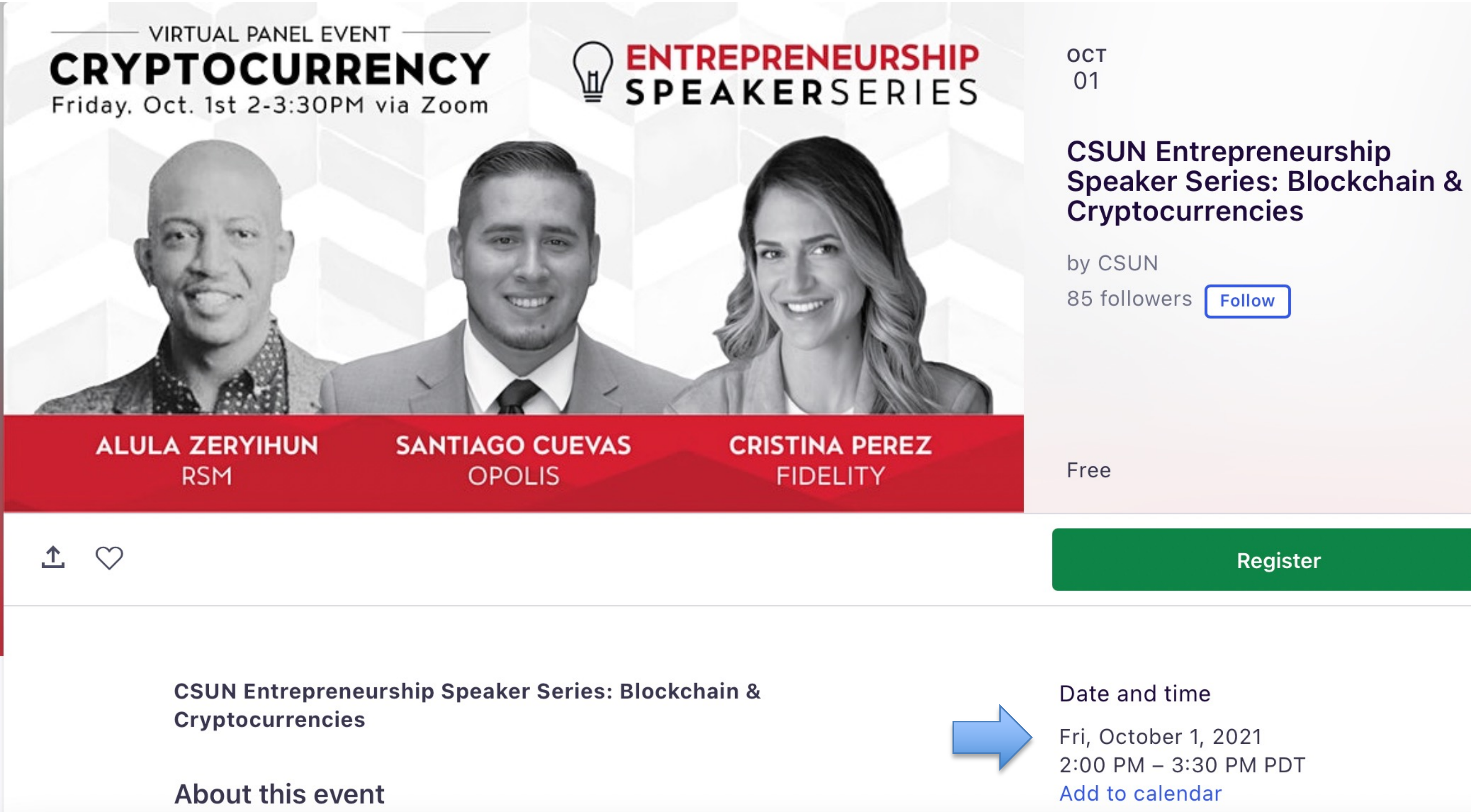
Date And Time

Fri, October 2, 2020
2:00 PM – 3:30 PM PDT

CSUN
CALIFORNIA
STATE UNIVERSITY
NORTHRIDGE

CSUN Blockchain Club

DR JEFF
SOFTWARE
©Jeff Drobman
2017-23



VIRTUAL PANEL EVENT

CRYPTOCURRENCY

Friday. Oct. 1st 2-3:30PM via Zoom

ENTREPRENEURSHIP
SPEAKERSERIES

ALULA ZERYIHUN
RSM

SANTIAGO CUEVAS
OPOLIS

CRISTINA PEREZ
FIDELITY

OCT
01

CSUN Entrepreneurship Speaker Series: Blockchain & Cryptocurrencies

by CSUN

85 followers Follow

Free

Register

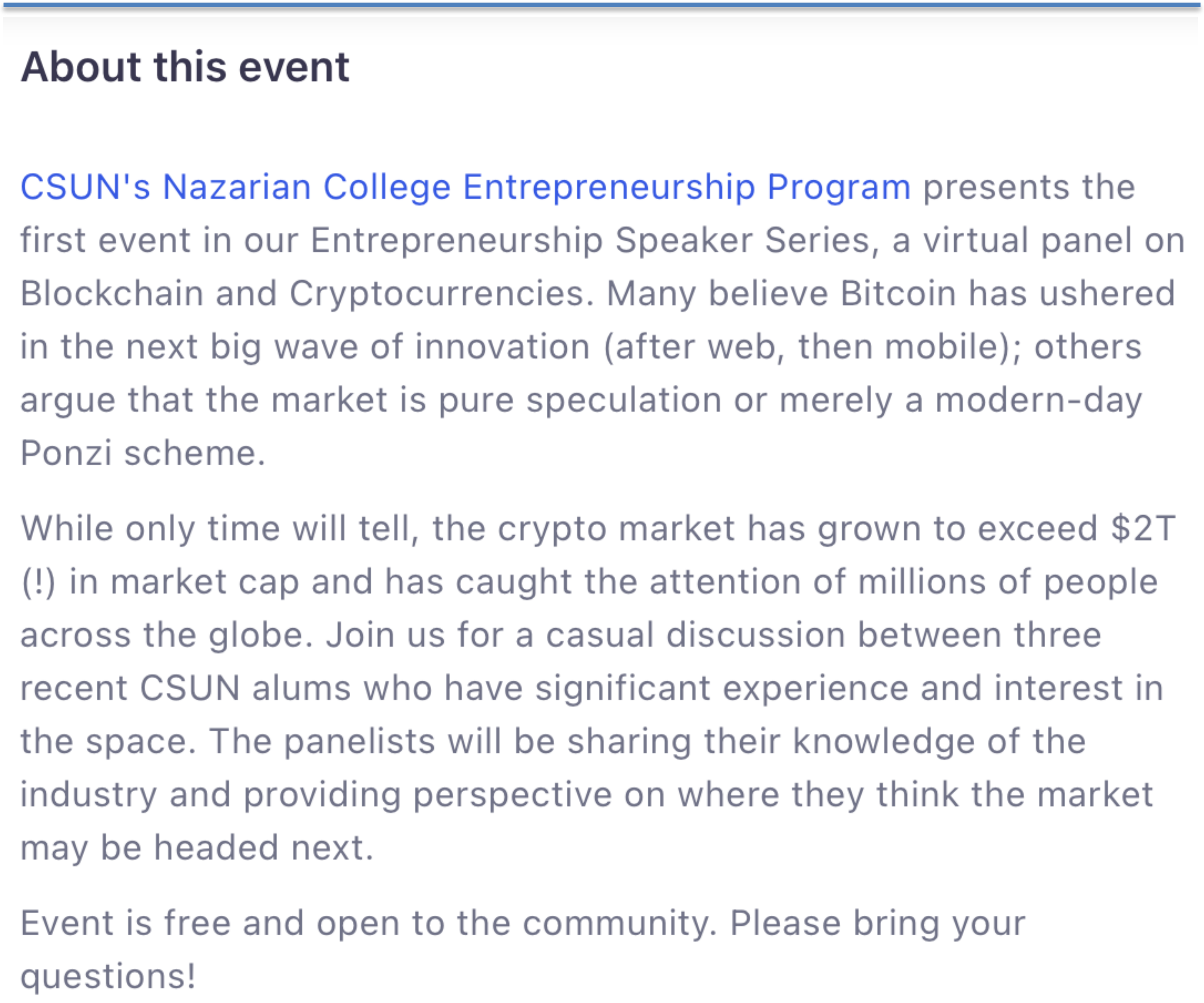
CSUN Entrepreneurship Speaker Series: Blockchain & Cryptocurrencies

About this event

Date and time

Fri, October 1, 2021
2:00 PM – 3:30 PM PDT
Add to calendar

CSUN Blockchain Club



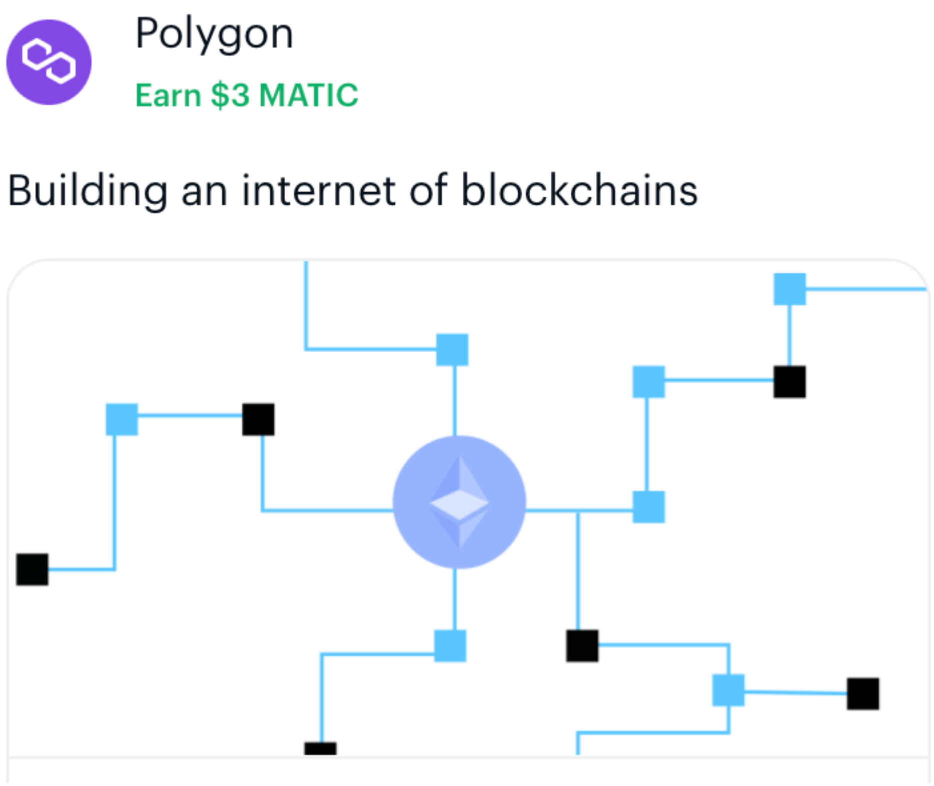
About this event

CSUN's Nazarian College Entrepreneurship Program presents the first event in our Entrepreneurship Speaker Series, a virtual panel on Blockchain and Cryptocurrencies. Many believe Bitcoin has ushered in the next big wave of innovation (after web, then mobile); others argue that the market is pure speculation or merely a modern-day Ponzi scheme.

While only time will tell, the crypto market has grown to exceed $2T (!) in market cap and has caught the attention of millions of people across the globe. Join us for a casual discussion between three recent CSUN alums who have significant experience and interest in the space. The panelists will be sharing their knowledge of the industry and providing perspective on where they think the market may be headed next.

Event is free and open to the community. Please bring your questions!

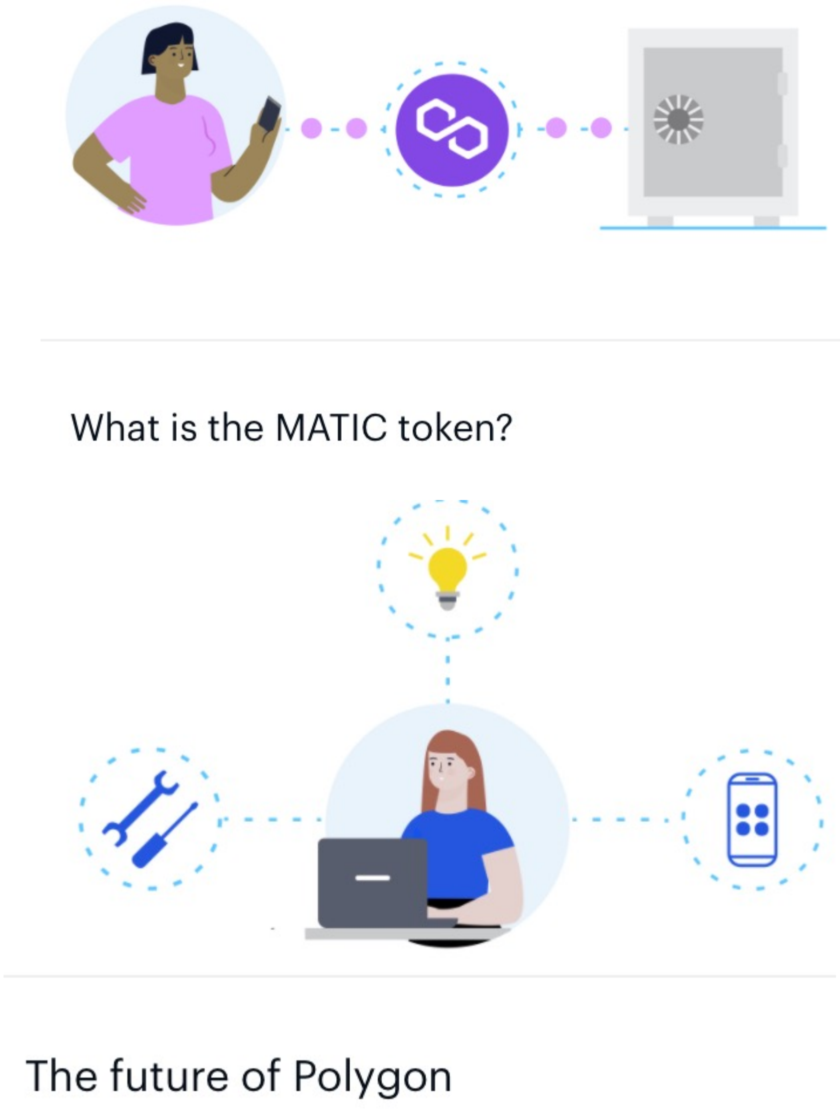
Polygon



Polygon

Earn $3 MATIC

Building an internet of blockchains



What is the MATIC token?

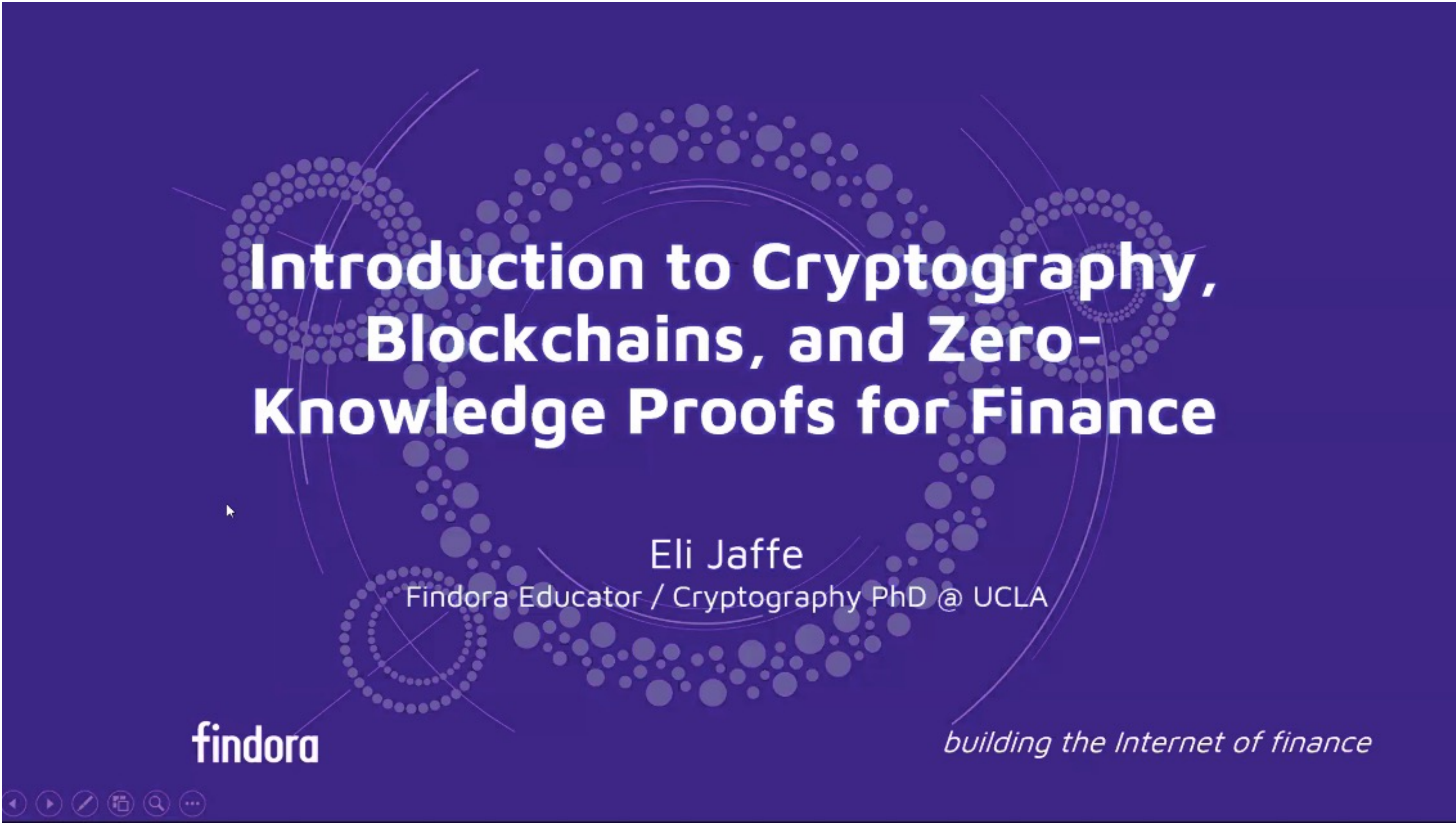
The future of Polygon

Section

ZKP
Zero Knowledge Proofs

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



Introduction to Cryptography, Blockchains, and Zero-Knowledge Proofs for Finance

Eli Jaffe

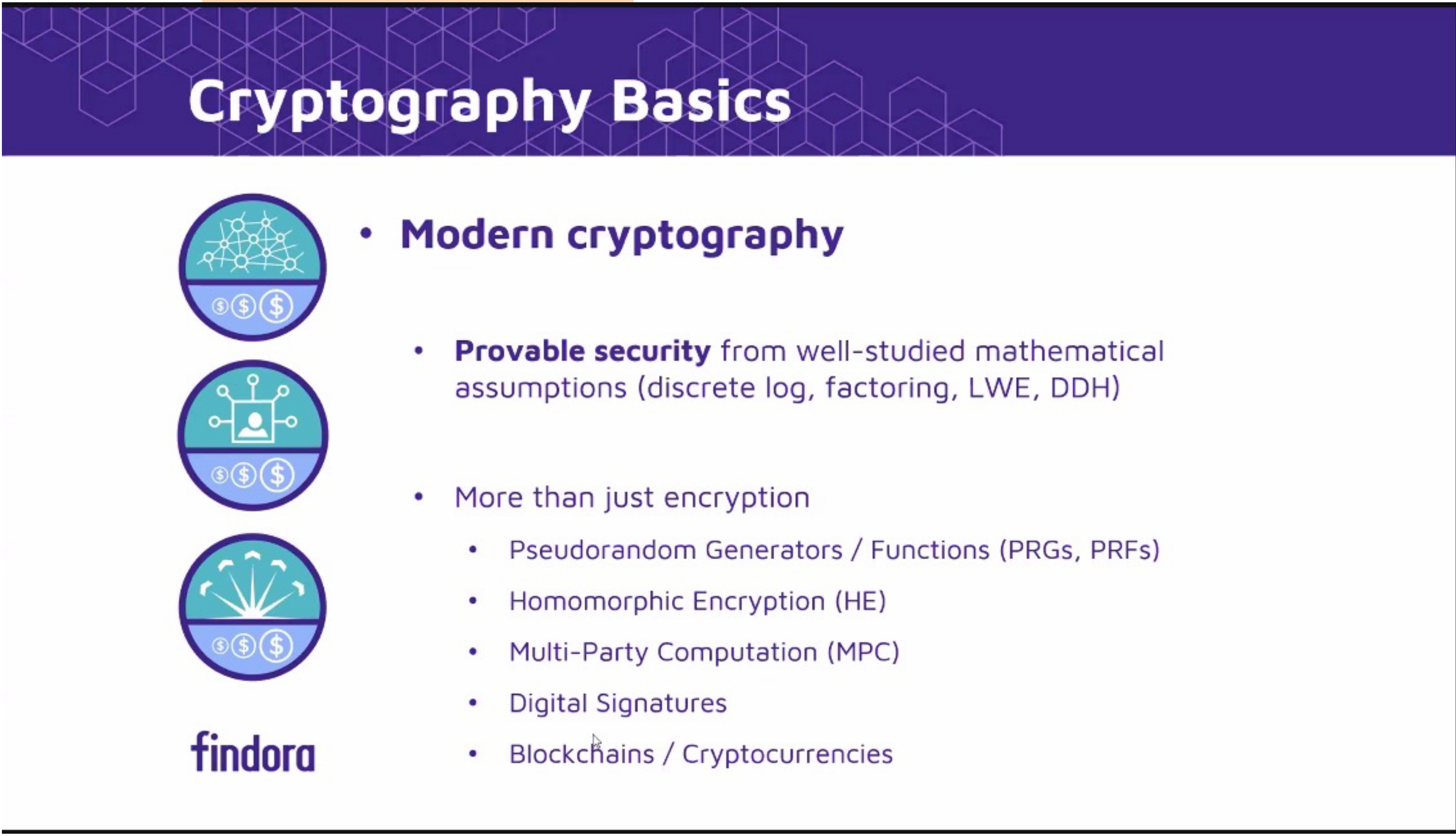
Findora Educator / Cryptography PhD @ UCLA

findora

building the Internet of finance

Blockchains/ZKP

Eli Jaffe, UCLA PhD student

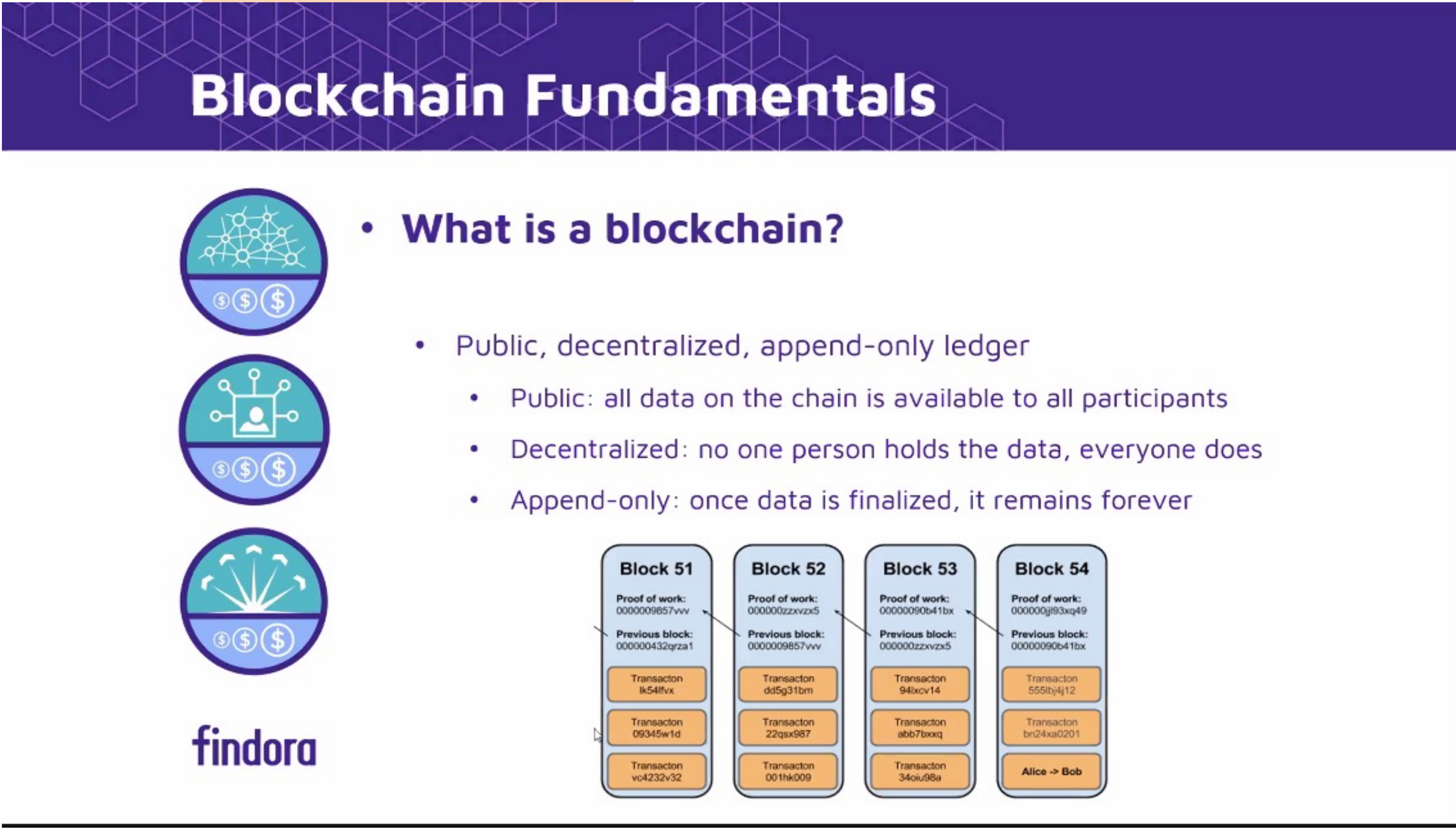


Cryptography Basics

- **Modern cryptography**
  - **Provable security** from well-studied mathematical assumptions (discrete log, factoring, LWE, DDH)
  - More than just encryption
    - Pseudorandom Generators / Functions (PRGs, PRFs)
    - Homomorphic Encryption (HE)
    - Multi-Party Computation (MPC)
    - Digital Signatures
    - Blockchains / Cryptocurrencies

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



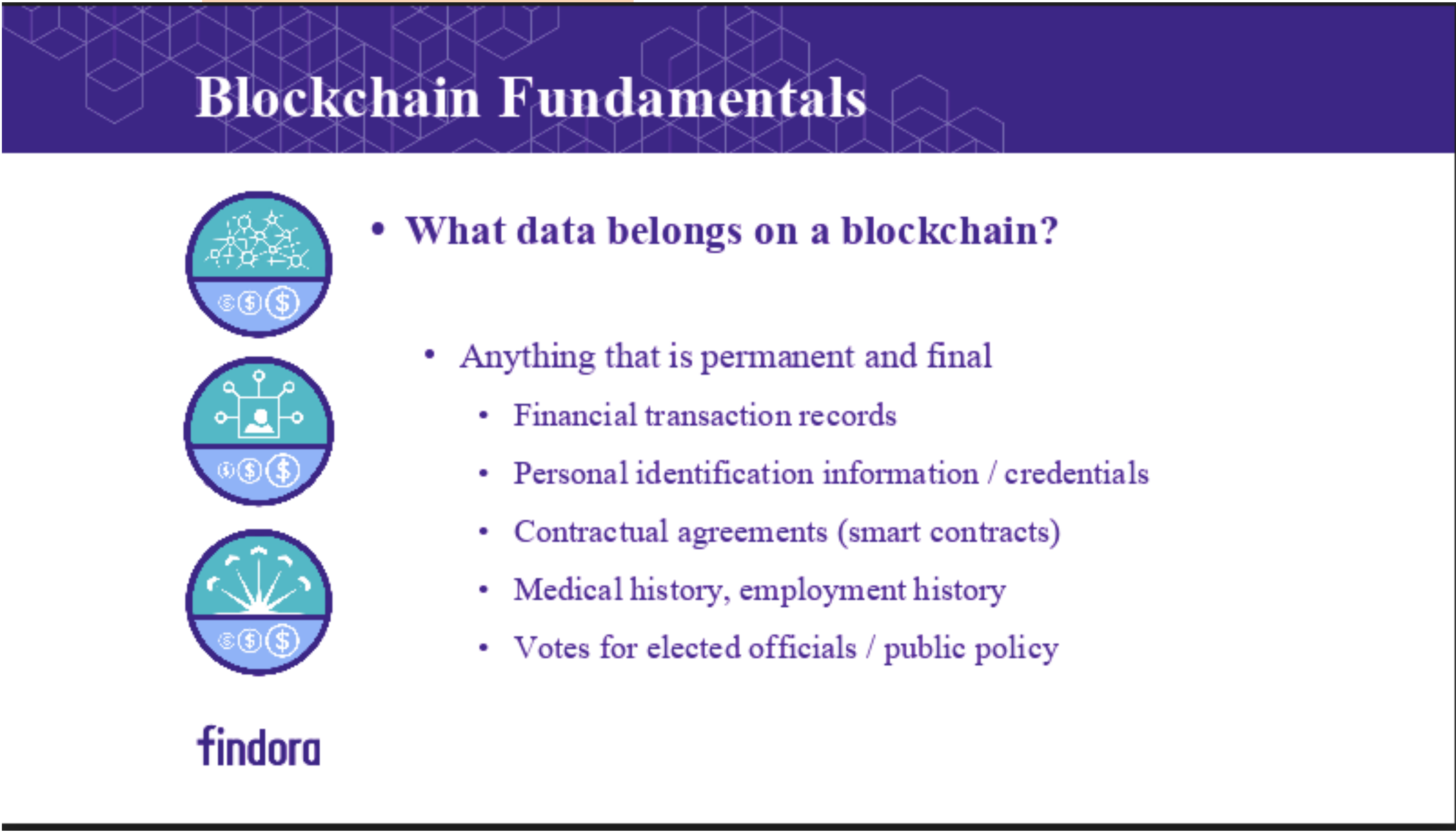
Blockchain Fundamentals

- **What is a blockchain?**
  - Public, decentralized, append-only ledger
    - Public: all data on the chain is available to all participants
    - Decentralized: no one person holds the data, everyone does
    - Append-only: once data is finalized, it remains forever

Block 51	Block 52	Block 53	Block 54
Proof of work: 0000009857vvv	**Proof of work:** 000000zzxvzx5	**Proof of work:** 00000090b41bx	**Proof of work:** 000000jjl93xq49
Previous block: 000000432qrza1	**Previous block:** 0000009857vvv	**Previous block:** 000000zzxvzx5	**Previous block:** 00000090b41bx
Transacton lk54lfvx	Transacton dd5g31bm	Transacton 94lxcv14	Transacton 555lbj4j12
Transacton 09345w1d	Transacton 22qsx987	Transacton abb7bxxq	Transacton bn24xa0201
Transacton vc4232v32	Transacton 001hk009	Transacton 34oiu98a	**Alice -> Bob**

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



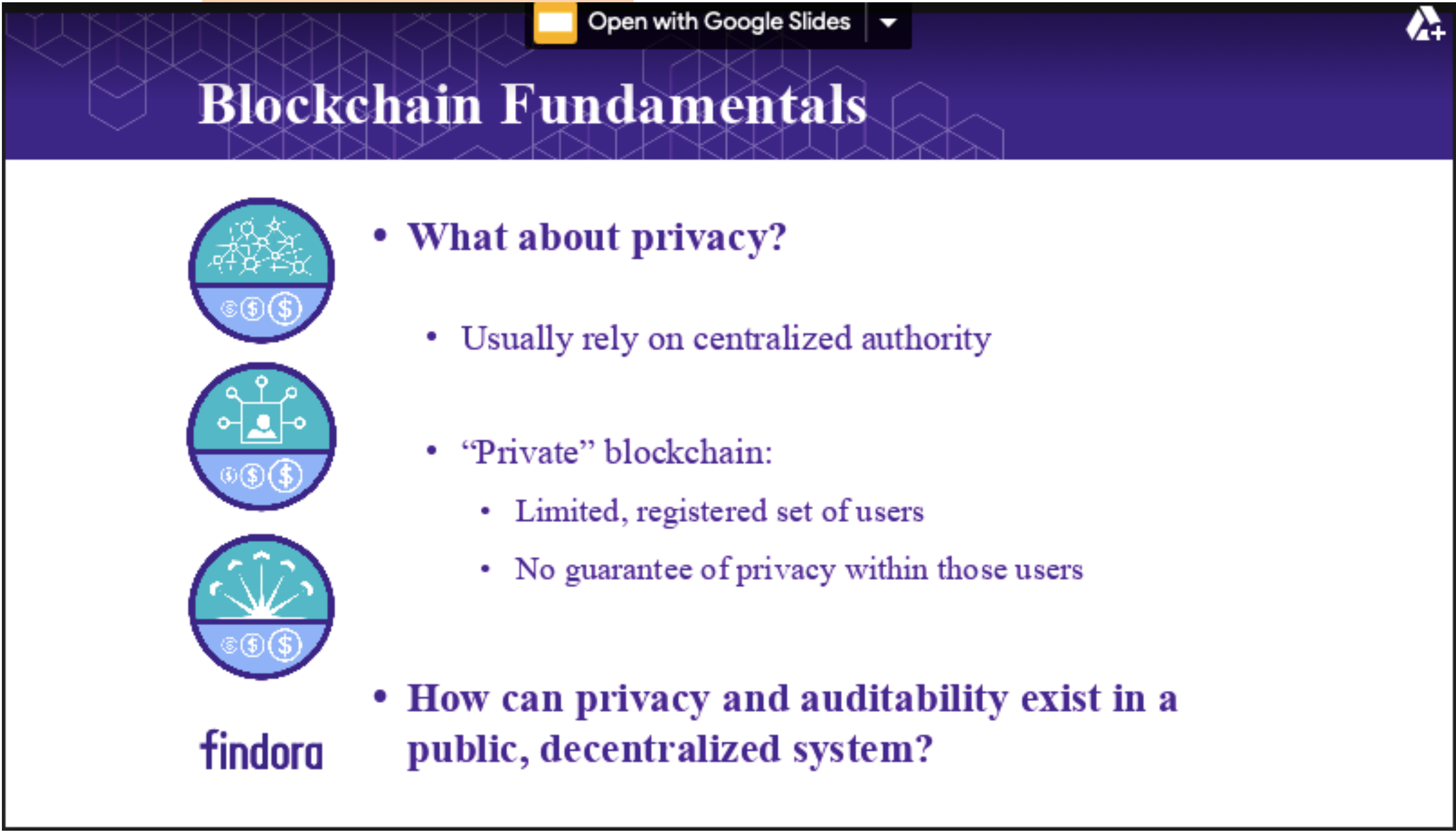
Blockchain Fundamentals

- **What data belongs on a blockchain?**
  - Anything that is permanent and final
    - Financial transaction records
    - Personal identification information / credentials
    - Contractual agreements (smart contracts)
    - Medical history, employment history
    - Votes for elected officials / public policy

findora

Blockchains/ZKP

Eli Jaffe, UCLA PhD student

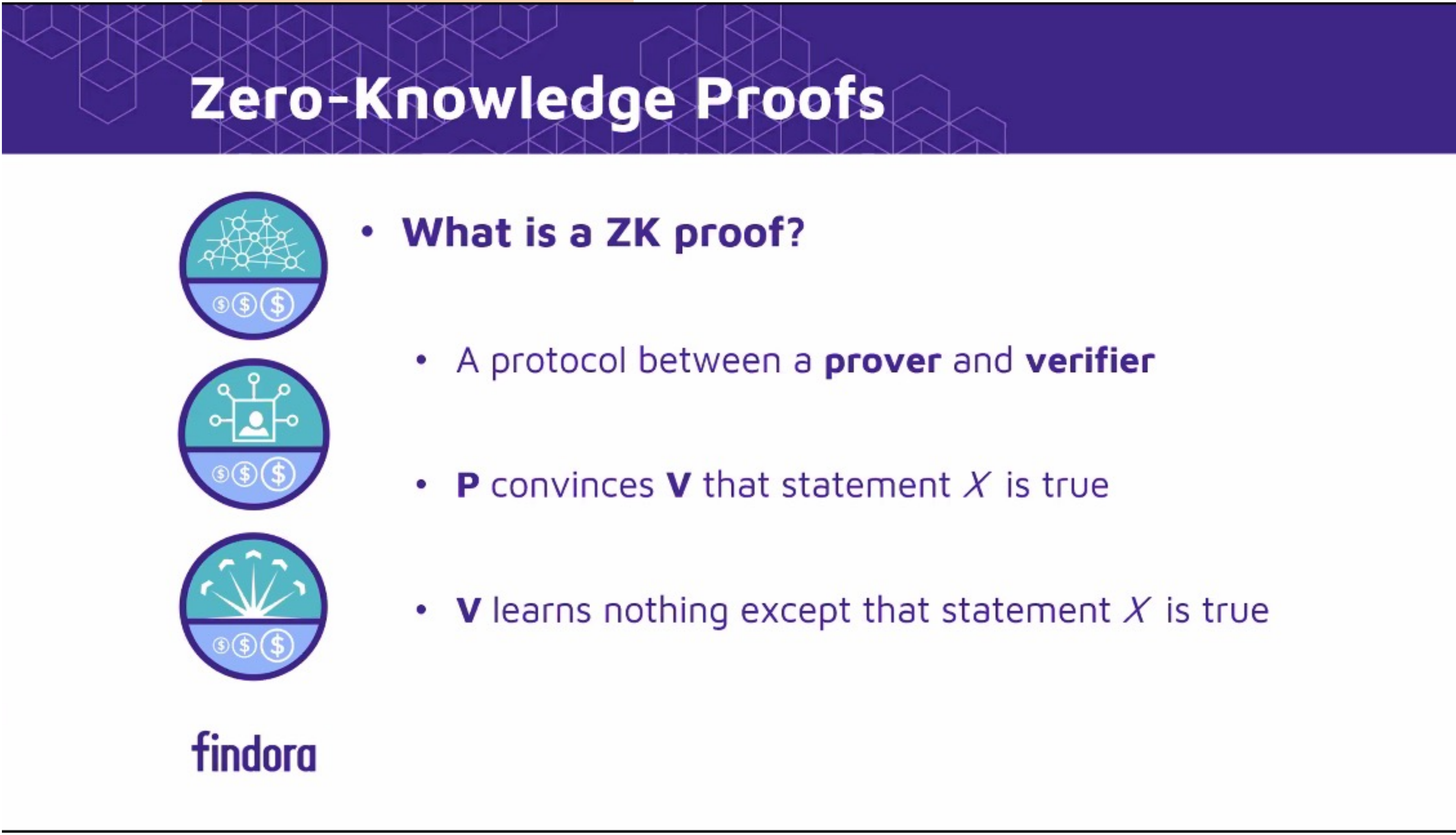


Blockchain Fundamentals

- **What about privacy?**
  - Usually rely on centralized authority
  - “Private” blockchain:
    - Limited, registered set of users
    - No guarantee of privacy within those users
- **How can privacy and auditability exist in a public, decentralized system?**

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



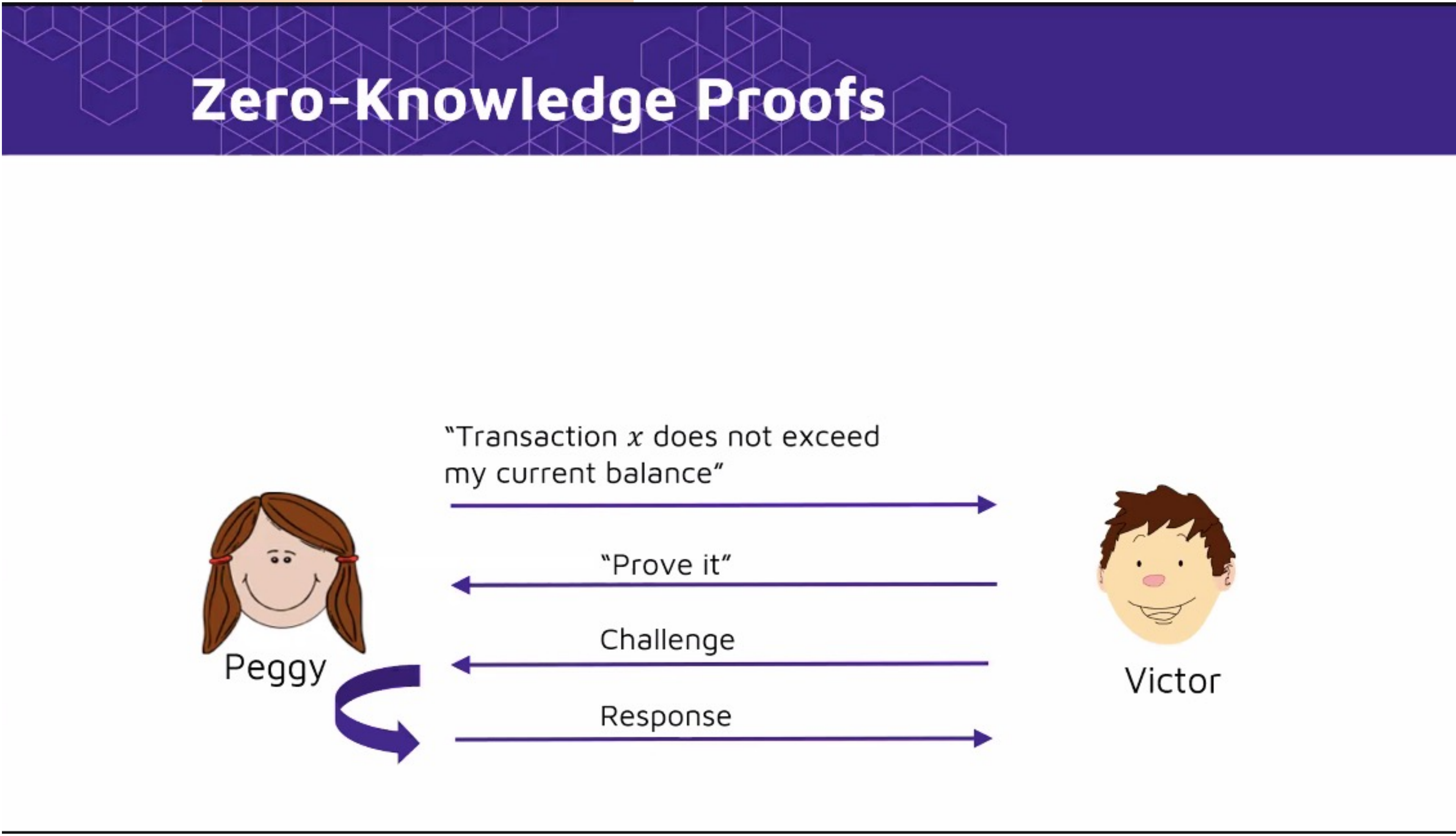
Zero-Knowledge Proofs

- **What is a ZK proof?**
  - A protocol between a **prover** and **verifier**
  - **P** convinces **V** that statement X is true
  - **V** learns nothing except that statement X is true

findora

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



Zero-Knowledge Proofs

"Transaction x does not exceed my current balance"

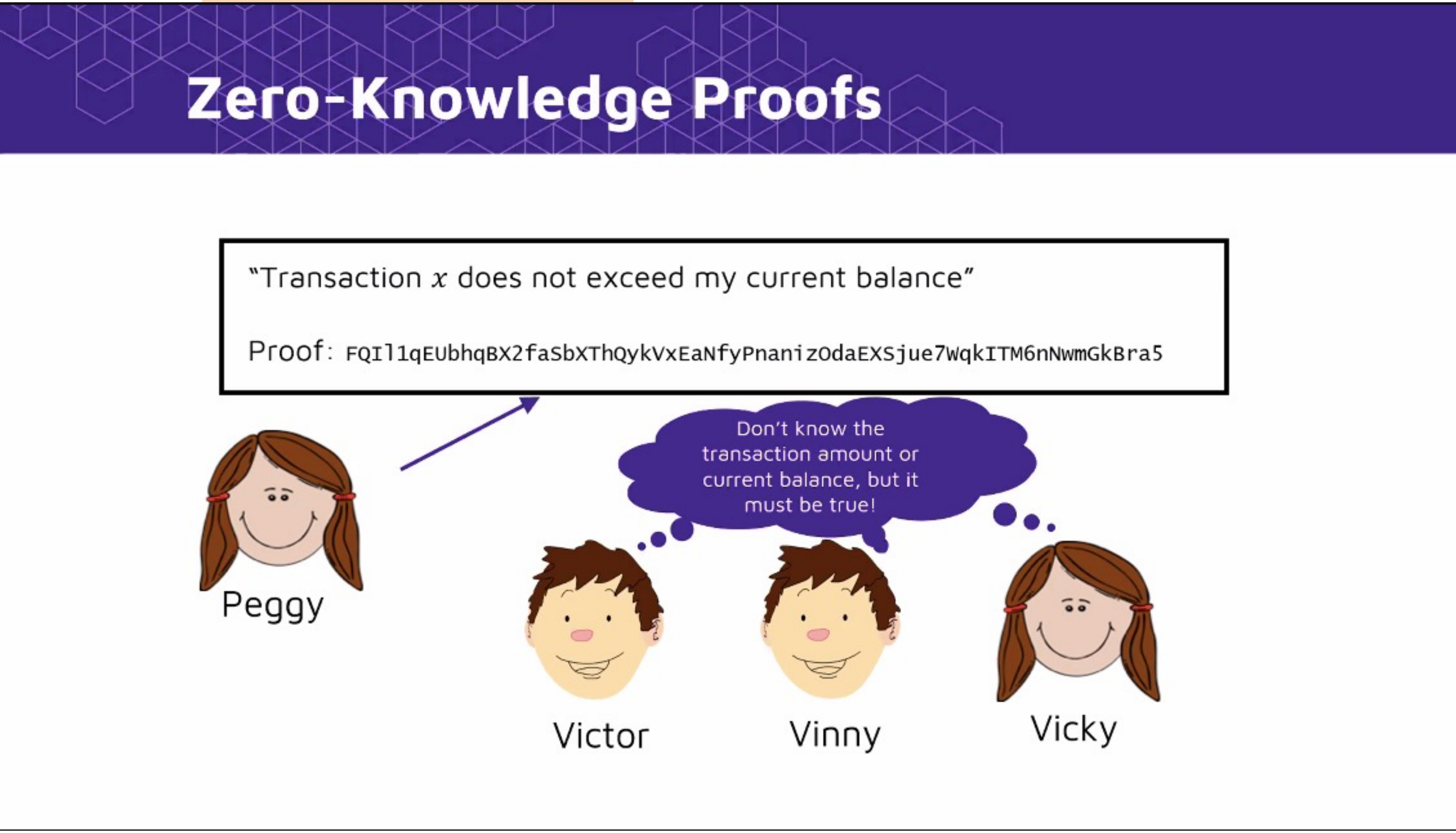
"Prove it"

Challenge

Response

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



Zero-Knowledge Proofs

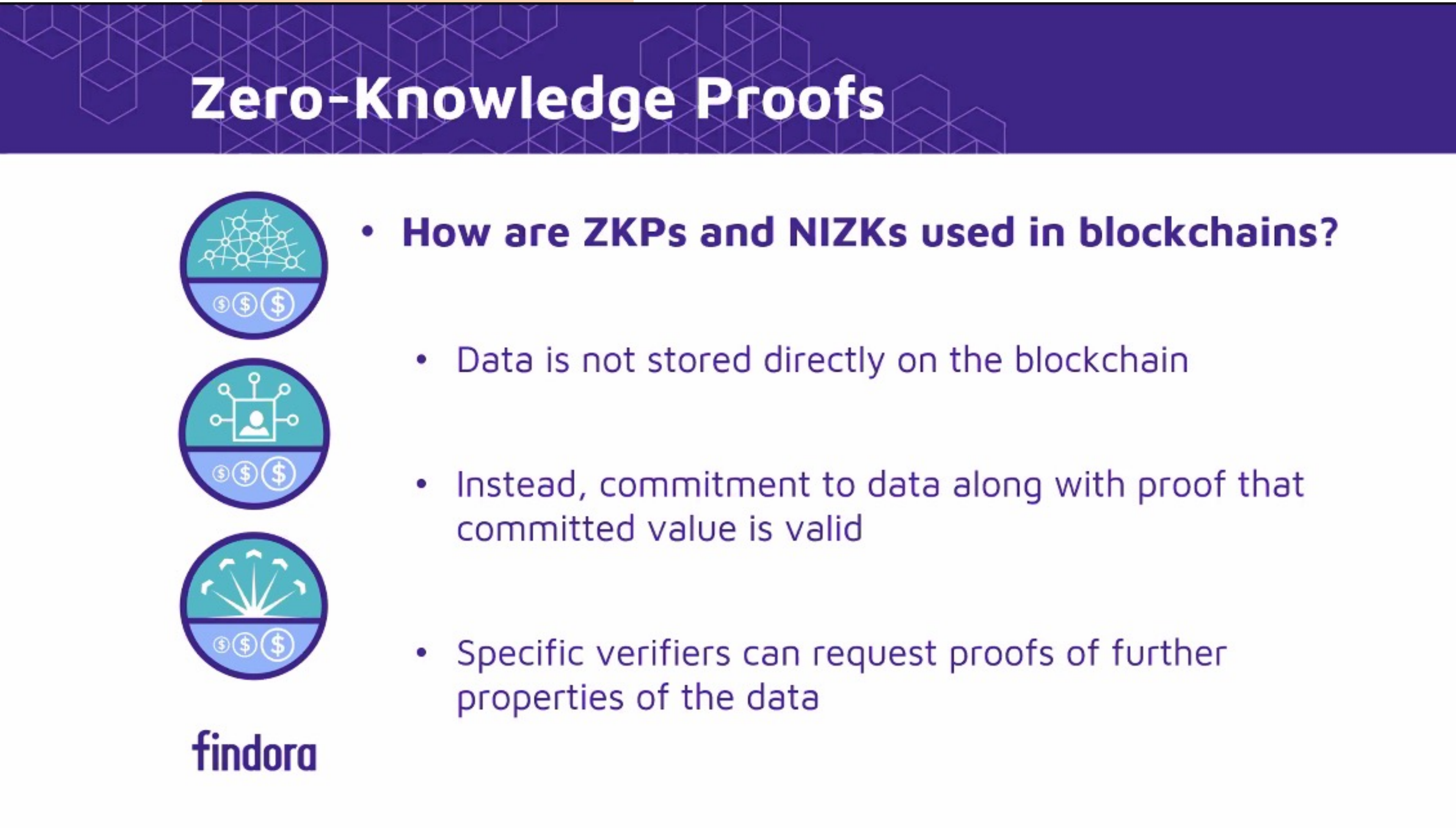
"Transaction x does not exceed my current balance"

Proof: FQIl1qEUbhqBX2faSbXThQykVxEaNfyPnanizOdaEXSjue7WqkITM6nNwmGkBra5

Don't know the transaction amount or current balance, but it must be true!

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



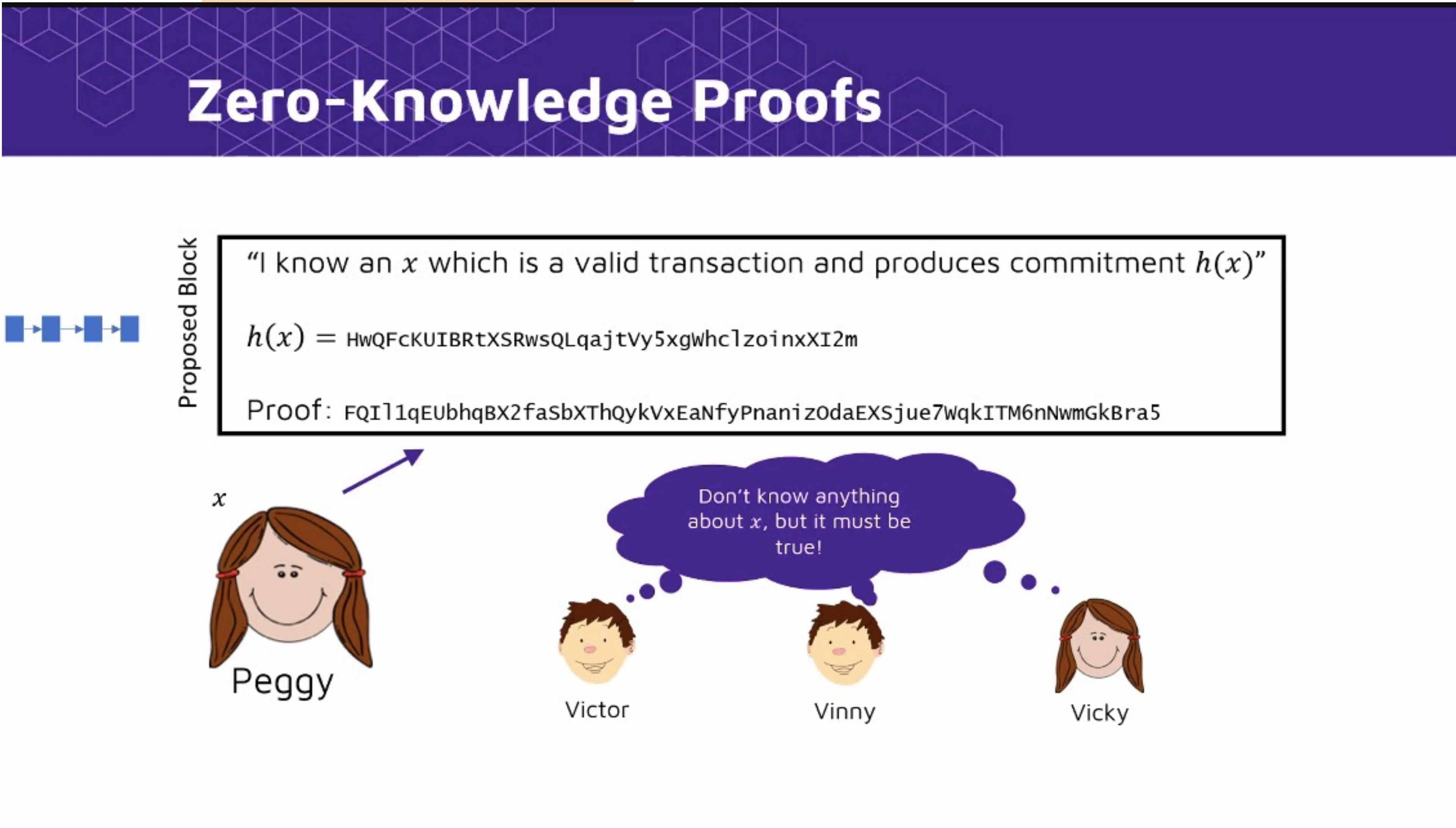
Zero-Knowledge Proofs

- **How are ZKPs and NIZKs used in blockchains?**
  - Data is not stored directly on the blockchain
  - Instead, commitment to data along with proof that committed value is valid
  - Specific verifiers can request proofs of further properties of the data

findora

Blockchains/ZKP

Eli Jaffe, UCLA PhD student



Zero-Knowledge Proofs

Proposed Block

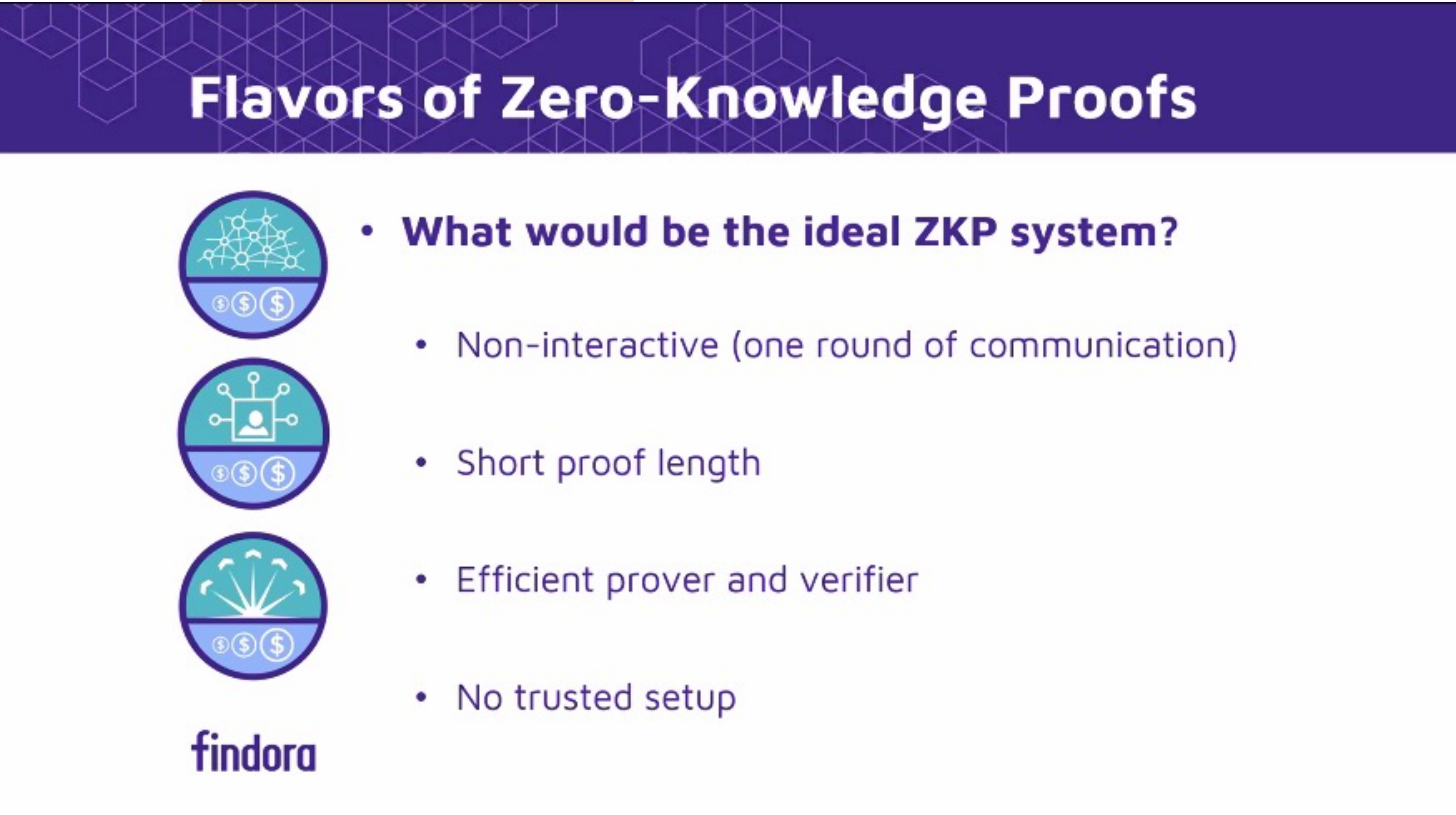
"I know an x which is a valid transaction and produces commitment $h(x)$"

$h(x) =$ HwQFcKUIBRtXSRwsQLqajtVy5xgWhclzoinxXI2m

Proof: FQIl1qEUbhqBX2faSbXThQykVxEaNfyPnanizOdaEXSjue7WqkITM6nNwmGkBra5

Blockchains/ZKP

Eli Jaffe, UCLA PhD student

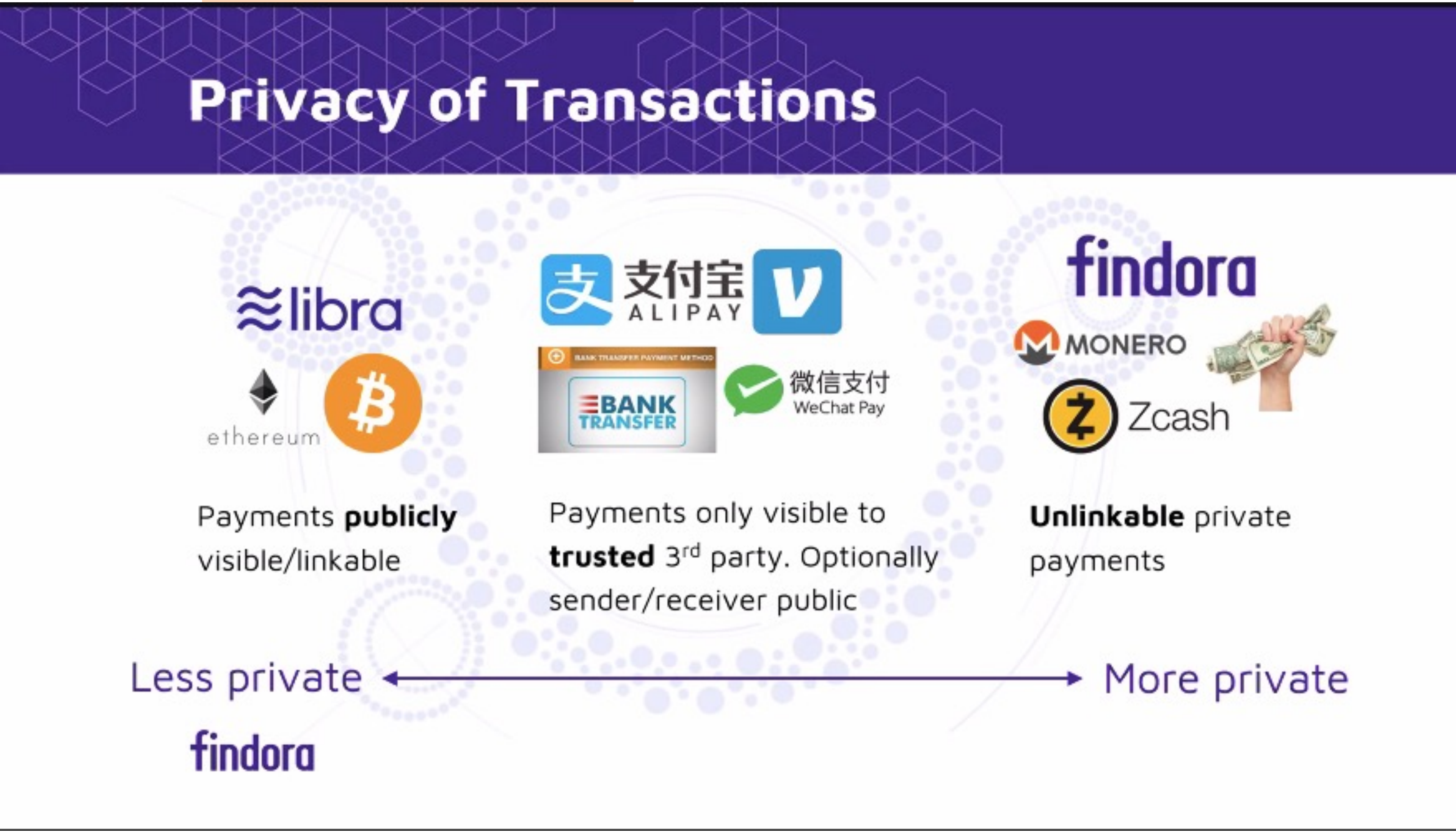


Flavors of Zero-Knowledge Proofs

- **What would be the ideal ZKP system?**
  - Non-interactive (one round of communication)
  - Short proof length
  - Efficient prover and verifier
  - No trusted setup

Blockchains

Eli Jaffe, UCLA PhD student



Privacy of Transactions

Payments **publicly** visible/linkable

Payments only visible to **trusted** 3rd party. Optionally sender/receiver public

Unlinkable private payments

Less private ⟷ More private

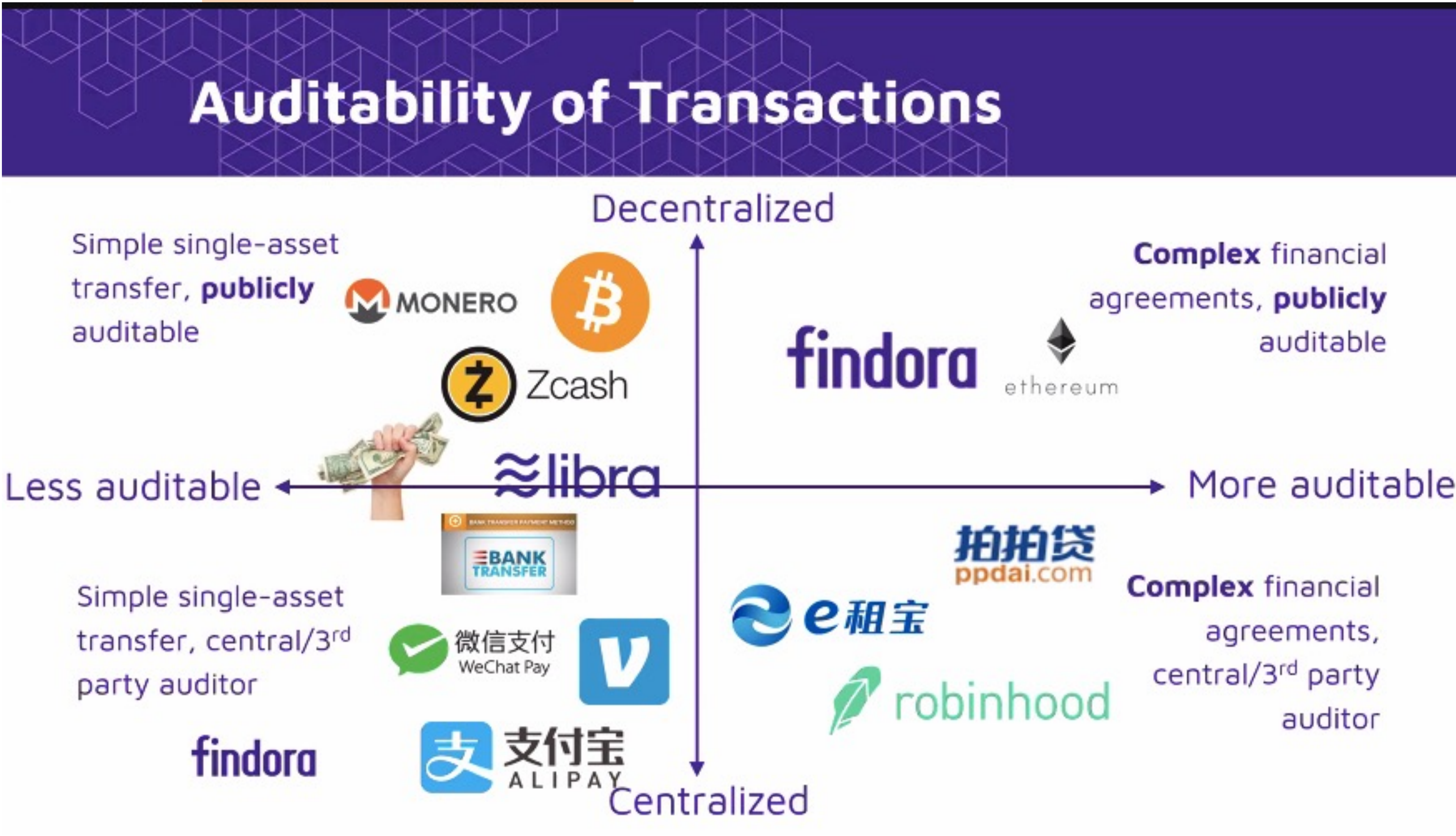
findora

CSUN
CALIFORNIA STATE UNIVERSITY NORTHRIDGE

Blockchains

DR JEFF SOFTWARE
©Jeff Drobman
2017-23

Eli Jaffe, UCLA PhD student



Auditability of Transactions

Decentralized

Centralized

Less auditable

More auditable

Simple single-asset transfer, **publicly** auditable

Complex financial agreements, **publicly** auditable

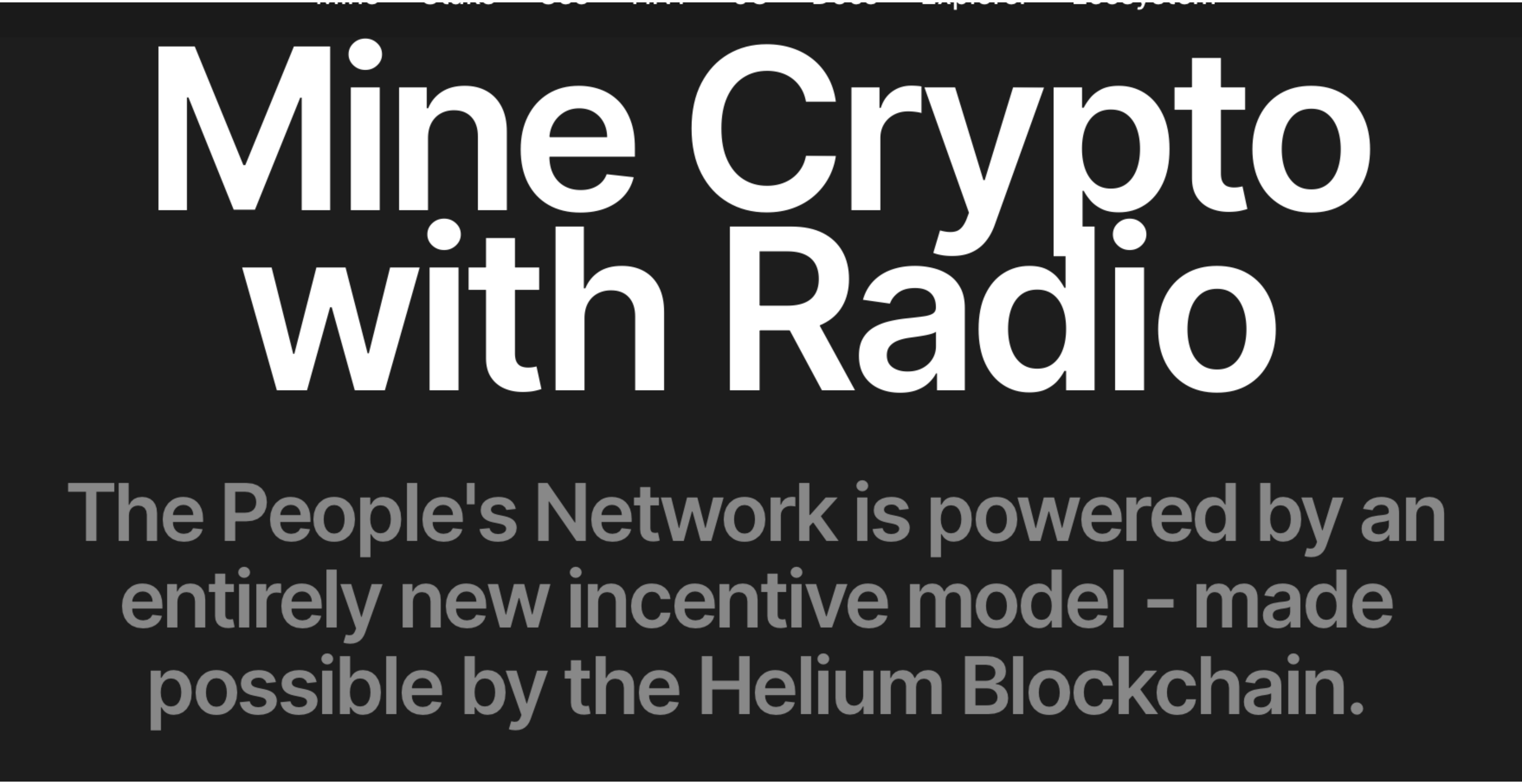
Simple single-asset transfer, central/3rd party auditor

Complex financial agreements, central/3rd party auditor

Section

Helium-HNT
Radio Hotspot Mining

Helium



Mine Crypto with Radio

The People's Network is powered by an entirely new incentive model - made possible by the Helium Blockchain.

Helium

The New Wireless Economy.

The People's Network creates an entirely new wireless economy that flips the traditional telecom model of building wireless infrastructure on its head.

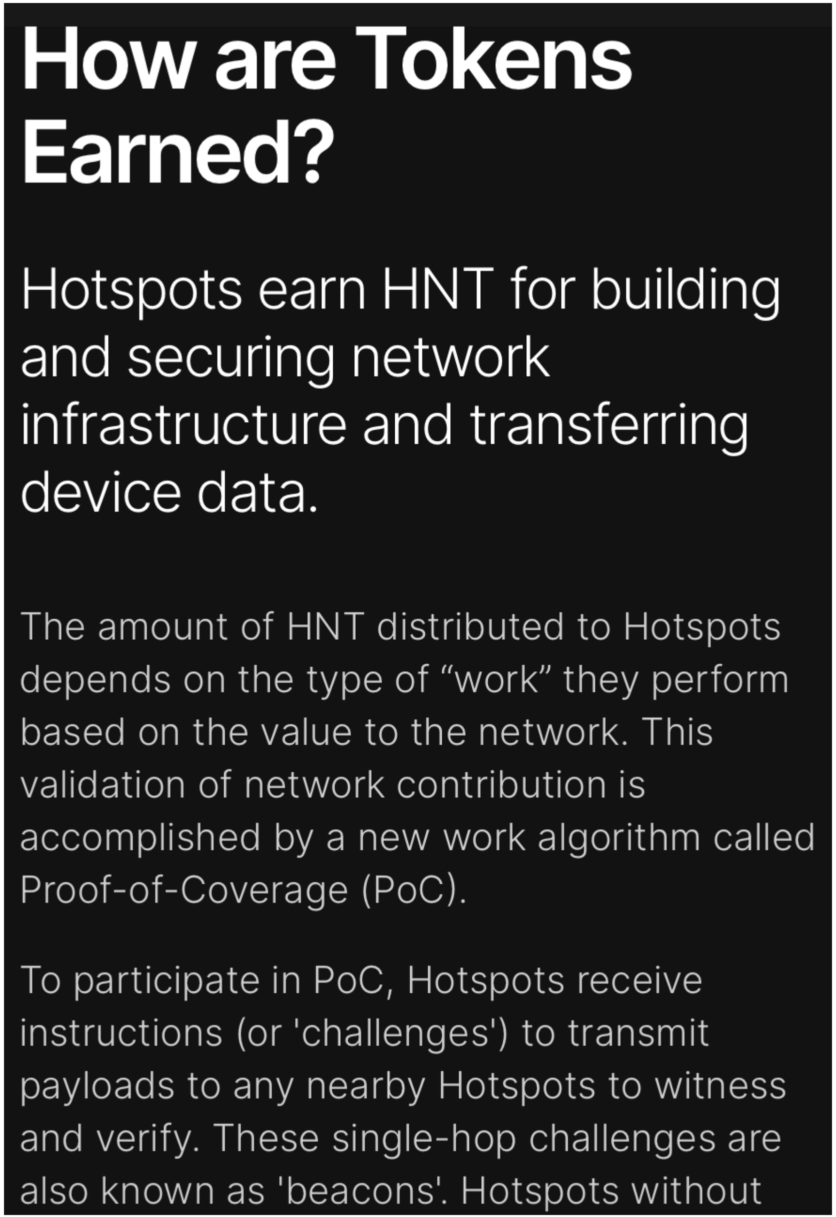
Using a Burn-and-Mint Equilibrium token model, The People's Network utilizes two units of exchange: HNT and Data Credits.

Helium

Over 20,000 Helium Hotspots have been sold to 2,000+ cities. It was the first HNT Miner to deliver a friendly aesthetic and simple user interface.

Launched in 2019, and originally exclusively sold to US customers, the Helium Hotspot is the original HNT Mining device. The goal of the Hotspot was to show that mining equipment can be simple to operate and provide innovative utility, in building The People's Network.

HNT

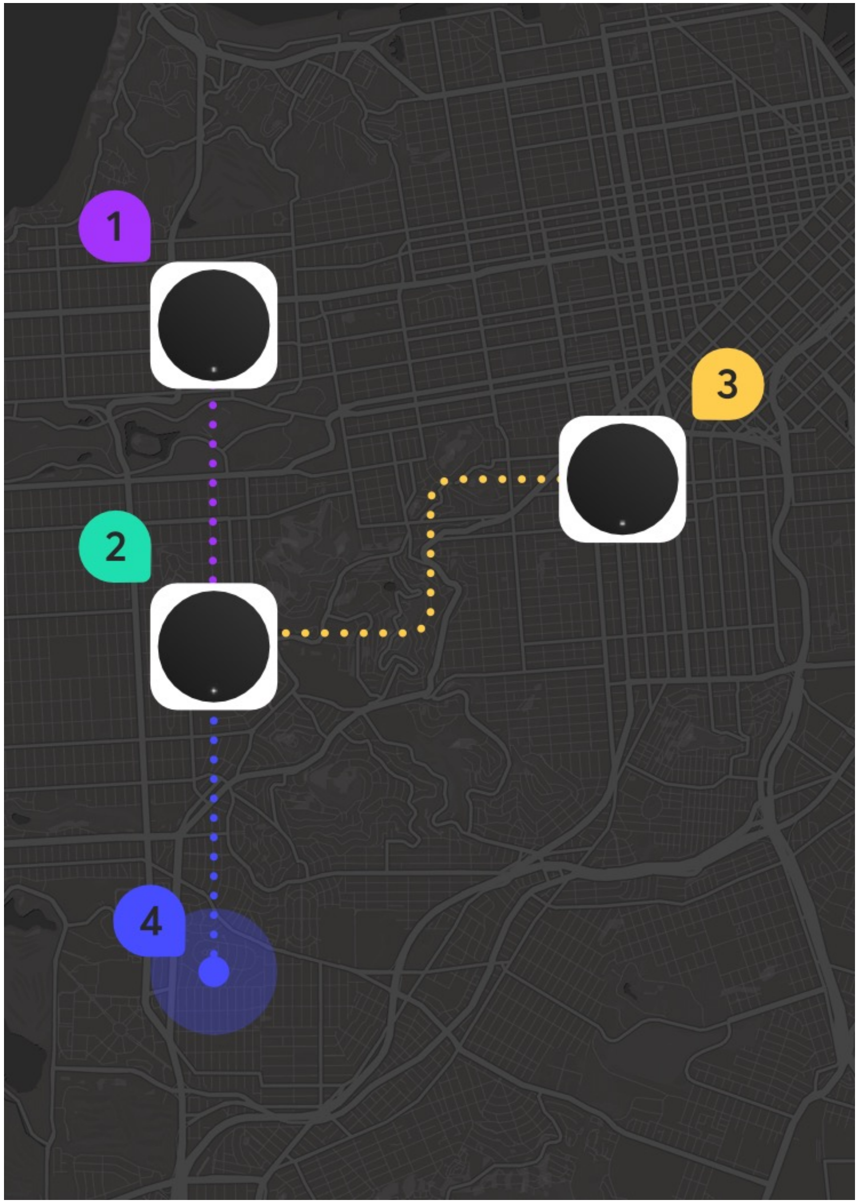


How are Tokens Earned?

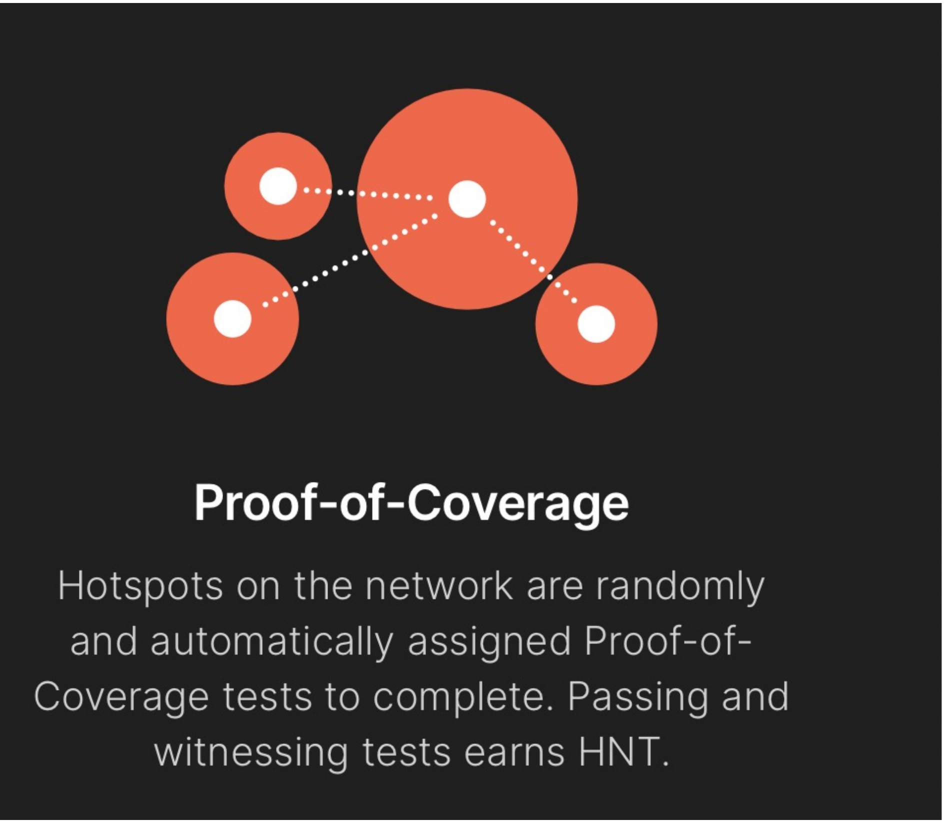
Hotspots earn HNT for building and securing network infrastructure and transferring device data.

The amount of HNT distributed to Hotspots depends on the type of "work" they perform based on the value to the network. This validation of network contribution is accomplished by a new work algorithm called Proof-of-Coverage (PoC).

To participate in PoC, Hotspots receive instructions (or 'challenges') to transmit payloads to any nearby Hotspots to witness and verify. These single-hop challenges are also known as 'beacons'. Hotspots without

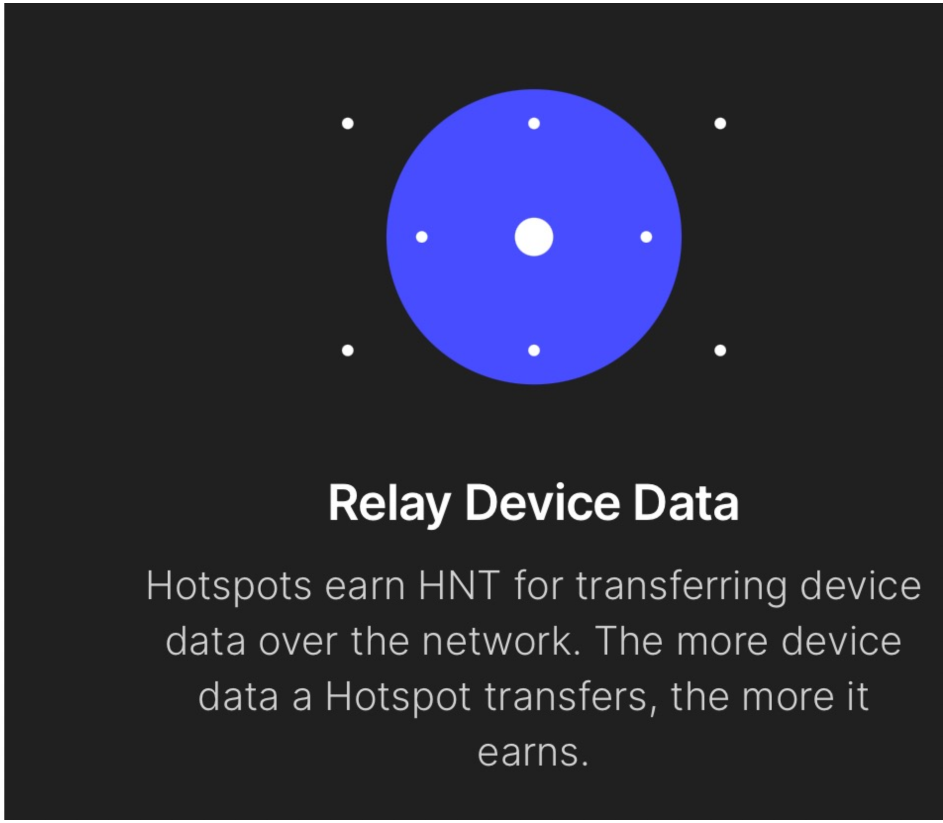


HNT



Proof-of-Coverage

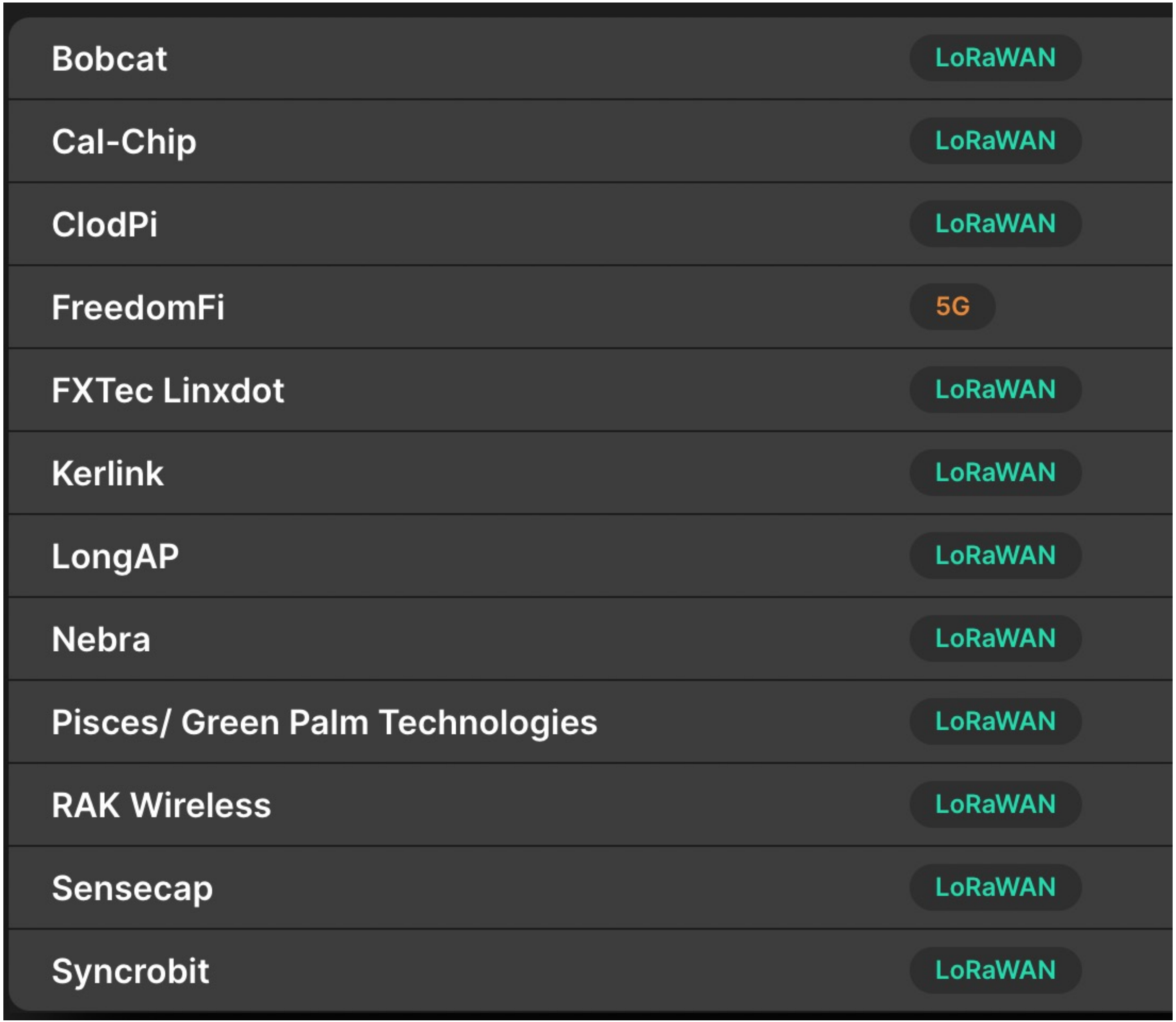
Hotspots on the network are randomly and automatically assigned Proof-of-Coverage tests to complete. Passing and witnessing tests earns HNT.



Relay Device Data

Hotspots earn HNT for transferring device data over the network. The more device data a Hotspot transfers, the more it earns.

Helium Mining Gear



Bobcat	LoRaWAN
Cal-Chip	LoRaWAN
ClodPi	LoRaWAN
FreedomFi	5G
FXTec Linxdot	LoRaWAN
Kerlink	LoRaWAN
LongAP	LoRaWAN
Nebra	LoRaWAN
Pisces/ Green Palm Technologies	LoRaWAN
RAK Wireless	LoRaWAN
Sensecap	LoRaWAN
Syncrobit	LoRaWAN