To the Editor June 1, 2020

What the Heck is a Blockchain?

A blockchain is a list of digital records, called blocks, that are linked using digital computer cryptography . Each of these block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).
https://en.wikipedia.org/wiki/Blockchain

It can and has been used since 2009 shortly after the Great Recession, for cryptocurrencies, like Bitcoin, but it also has potential to be used for many other things. It could be used for encrypted messaging, decentralized marketing, proof of ownership, for all kinds of contracts and legal documents like real estate transactions, for decentralized social networking sites, and importantly for a decentralized Internet which will increase the resiliency of the World Wide Web, preventing its shutdown by governments in any country.

Some say that blockchain is the second coming of the Internet as a decentralized and anonymous web of computer networks. Others call it a scam. The blockchain redefines accounting for the first time in 500 years with an immutable decentralized and distributed triple entry ledger. In its early stages it has enabled the making of billionaires, and also put people in jail. What makes blockchain so fascinating yet controversial? What does it mean to have blockchain in our lives, what will it bring next? https://www.amazon.com/gp/video/detail/B07C7S751X/ref=atv_wl_hom_c_unkc_1_3

The Central Banks are currently counterfeiting money, called Fiat currency. Fiat money is a currency without intrinsic value that has been established as money, often by government regulation. Fiat money does not have use value, and has value only because a government maintains its value, or because parties engaging in exchange agree on its value. It is also slow and can be hacked at a single point.

Ethereum and Smart Contracts

Ethereum is an open source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality. It supports a modified version of Nakamoto consensus via transaction-based state transitions.

Ether is the cryptocurrency generated by the Ethereum platform as a reward to mining nodes for computations performed and is the only currency accepted in the payment of transaction fees.

Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes

Smart Contracts

The idea of smart contracts goes back to 1994, close to the dawn of the World Wide Web. That's when Nick Szabo, cryptographer widely credited with laying the groundwork for bitcoin, first coined the term "smart contract." At their core, these automated contracts work like any other if-then statements. They simply do it in a way that interacts with real-world assets. When a pre-programmed condition is triggered, the smart contract executes the corresponding contractual clause. Because smart contracts are computer programs, it is trivial to add more complex betting elements such as

odds and score differentials into the mix. While there are services today that can handle this sort of transaction, they all charge a fee. The key difference with smart contracts is that they are part of a decentralized system accessible to anyone, that doesn't require any intermediaries.

Some say the blockchain will be Civilization 2.0, and will change the way our world operates permanently, with clever cryptographic code and collaboration. A new trust protocol if you will, to build a better society. They say everything can be converted to digital and be bought and sold on a blockchain. The devil is always in the details, code is flawed, humans are all flawed, humans writing code has flaws, everything digital is hackable, so we shall see.

"Trust is the foundation of effective society." Don Tapscott, co-author of Blockchain Revolution

https://www.blockchain.com/
https://www.bitcoin.com/

Cryptography is the practice and study of techniques using math to secure communication in the presence of Global passive personal data adversaries like Facebook, Google, Microsoft, Apple, Amazon, and the NSA.

Merkle tree

In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.