JEFFERSON CAPITAL

"The issuing power should be taken from the banks and restored to the people to whom it properly belongs."

--Thomas Jefferson

Jefferson believed in limiting the power of financial institutions to influence the nation's economy. It is in this spirit that crypto-technology was invented, and that Jefferson Capital, long-only manager of crypto-asset hedge funds, was founded.

What is "crypto" technology? Why is it so significant? Twenty years ago, people asked the same questions of the Internet. A minority of people knew the answer—among them, Bill Gates, Jeff Bezos, and Eric Schmidt. They turned the Internet into a basic necessity for citizens of every developed nation on Earth (and made a fortune doing so). Today, those same individuals recognize the merits of blockchain technology, and foresee it becoming at least as significant as the Internet, if not dramatically more so.

Blockchain technology, the driving force behind cryptocurrency is a reimagining of digital databases that eliminates *all possibility of hacking or fraud*.

This point bears repeating: For the first time in the history of computer science, a digital format for storing and sharing information with 100% security and reliability is publicly available. This simple guarantee of data security opens the door to enormous possibility: Smart ledgers for automatically tracking energy consumption and production could replace state-sponsored monopolies. Smart records for shipping and freight could automate the most tedious and costly areas of international trade. Smart-yet-encrypted databases for healthcare could be combined with AI algorithms to automate medical research, dramatically improving diagnoses and advancing treatment methods without strictly compromising patient data.

The secret to a blockchain database's security is the logic of its design. Unlike traditional databases, Blockchain databases do not reside in servers, are not controlled via master-passwords, and do not require layers upon layers of state-of-the-art security.

Instead, they are:

1. Distributed: Stored not centrally but collectively, parsed across hundreds, thousands, or even millions of personal computers;

2. Encrypted: To participate in the network, a user creates a passcode, known as a "private key," known only to the user and to no one in the middle (as in traditional websites, i. e. Facebook, Amazon, etc);

3. Updated in real time, at all times, via a constant channel of communication, between a significant majority of users' computers.

These features allow a database of information to be managed and controlled automatically, with absolutely no possibility of tampering by a malicious party. With these features in mind, avid programmers can program blockchain databases to perform specific functions, or to enforce certain permissions (instead of majority rule, for example, a government might build its own blockchain on the premise of

"rule by authorized parties.")

This, in and of itself, is of obvious value. Google, Amazon, Oracle, and Goldman Sachs are a few examples of the entities currently seeking to implement Blockchain technology into their businesses.

Beyond the invention itself, however, is a far larger market implication of its use: A decentralized, tamperproof database can, in principle, be used to verify transactions between individuals—playing the role of "trusted third party" –*for free*.

Consider how much of the market is dominated by companies of some form or another whose business models can be effectively summarized as that of the "transaction enabler": They enable the goods from a buyer to reach a seller, and take a fee for doing so. Producers make less than the god is actually worth, and consumers pay more.

Paypal. iTunes. Amazon. Companies following this model often titans of industry.

On a tamperproof Blockchain database, the Blockchain can provide the same service these companies provide. Better still, a Blockchain would charge no middleman fee—Party A and Party C transact directly—provided only that they transact using a digital unit of value, compatible with that Blockchain's database.

This unit of value is called a "token" or "crypto-currency."
By issuing its own units of value, a unique Blockchain database can thus transact any good, asset or service, with all the nuances required for that specific transaction being programmed directly into the currency itself.

"Currency" is thus a bit of a misnomer; these are not competitors to the dollar but vehicles for it. Instead of currencies, these are better thought of as *digital assets*—purpose-built for the transaction of a *real* asset.

Blockchain-based digital assets open the door to another interesting opportunity, one that is still as-yet not widely understood: The ability to store and trade securities over a blockchain network, via a digital asset class commonly referred to as "security tokens."

In 2017, a plethora of digital assets were created by startup enterprises, hoping to cash in on investor euphoria about this unprecedented technological revolution by offering digital assets through unregulated IPOs called "Initial Coin Offerings," and declaring that these digital assets were not security tokens—that they were "utility tokens," backed not by the value of a company but merely by demand for a particular good, service, or commodity. This period from mid-2017 to early-2018 has become known in blockchain circles as "the ICO Craze" or "the ICO Bubble."

SEC chair Michael Clayton famously said at the time: "I have yet to see a single ICO that should not be classified as a security."

Since then, however, the SEC has also famously declared that Bitcoin and Ethereum would *not* be considered security tokens. Why the difference? What, exactly, is a security token, and what makes it different from a utility token? This distinction is further explored in our Security Token two-pager.