The Origin and Evolution of Crypto-Currencies

By: Seoyoung Kim, Manager, Analysis Group
Sumon Mazumdar, Vice President, Analysis Group

Background

Since the mysterious Satoshi Nakamoto introduced the world's first crypto-currency, Bitcoin, in 2009, over 1800 other "crypto-currencies" (i.e., "digital assets", "tokens", or "coins") have been introduced, making some early adopters fantastically rich. Unsurprisingly, there have been cases of fraud involving crypto-currency schemes. While some believe Bitcoin may one day become a gold-like asset class worth trillions, others, like Warren Buffet, think Bitcoin is "rat poison squared."

Crypto-currencies are simply lines of code involving encryption technology that enable members of a permissionless, decentralized network to verify transactions using the cryptocurrency on the software's platform. Such transactions are recorded in a public electronic ledger (which may rely on "blockchain" technology) that is maintained by the decentralized network rather than a central authority or electronic clearinghouse. Bitcoin, for example, was designed to serve as a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution." Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) ("Nakamoto"). Thus, for example, today Bitcoins have been used to pay for real estate, art, wine, and even groceries.

In contrast, other coins (which are generally referred to as "utility tokens") are not intended to serve as peer-to-peer cash. Rather, much like arcade tokens that can be used to access rides in a theme park, these utility tokens are designed for use on a software platform that provides a specific good or service, e.g., to implement "smart contracts" (Ethereum), host data in the cloud (Filecoin), run online casinos (Sp8de), or improve digital advertising (BAT). Others are like traditional securities, giving the owner some cash flow rights in an enterprise. For example, tokens issued by Blockchain Capital, a venture capital fund that invests in the blockchain

technology sector, give the token's owner a share in the fund. Finally, some coins simply serve as a joke or political statement with no practical use case by design (e.g., the GotFomo (GTFO) coin is designed for those with the "fear of missing out" or "FOMO").

Notably, some utility tokens can be used immediately because the underlying platform is already operational. In other cases, a founding group of developers sell tokens to the public in exchange for some existing virtual currency to fund their platform's development (a process referred to as an initial coin offering or "ICO"). These tokens have no immediate functionality because the token's platform remains to be developed.

Federal regulators such as the Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission ("SEC") have emphasized that crypto-currencies must be properly regulated to protect consumers and investors from fraud and price manipulation. However, applying statutes written long before the "crypto" era to regulate a rapidly-evolving technology is challenging. We discuss differences among various crypto-currencies and the current regulatory views on these assets, which will likely evolve as the technology matures.

Money: From cows to Bitcoins

The functions of money

Bitcoin was designed to be a "peer-to-peer version of electronic cash;" i.e., a substitute for *fiat* money. To understand the revolutionary idea behind Bitcoin it helps to ask what exactly does the quotidian concept of "money" mean?

Loosely speaking, money refers to anything that can serve three functions: (1) a store of value, which allows consumers to save today and spend tomorrow; and/or (2) a unit of account that can be used as a common measure to price goods and services; and/or (3) a medium of exchange. *See* "*Virtual* Currencies: Key Definitions and Potential AML/CFT Risks," Financial Action Task Force, 2014 ("FATF"). Almost anything can serve as "money" by agreement within a community. Salt, squirrel pelts, tulip bulbs, cowry shells, and of course gold and silver coins have fitted the bill –no pun intended. Even today, cows serve as money in South Sudan. Non-

perishable metal coins, which are clearly better forms of money than cows or tulips, have been popular coinage for millennia. At some point, people deposited their clunky metal wealth in banks and used paper notes as a more convenient form of money. Importantly, early notes were issued by private banks rather than by a central bank and could be returned for the silver or gold coins deposits held in reserve for the issued notes. Eventually, this link was severed and *fiat* money (a country's currency, like dollar bills) was born.

Fiat money is not convertible into gold or silver and has no intrinsic value. It serves as money simply by government fiat and because people collectively trust the issuing government's authority and ability to maintain the currency's value. Transactions in fiat money are recorded by banks, and its supply is maintained by the government or its central bank. Thus, fiat money's use rests critically on the trust that its users place on the issuer's ability to maintain that value and its acceptance as a medium of exchange. People may abandon a currency in favor of a more stable alternative such as the US dollar (de facto "dollarization") if they lose trust in a central authority's ability to maintain its currency's value (e.g., if counterfeit bills are rampant or the government prints too much money to meet its expenses and hyperinflation follows).

Unlike fiat money, virtual currency doesn't have legal tender status in any jurisdiction and isn't guaranteed by any jurisdiction. Instead, it serves as money "only by agreement within the community of users of the virtual currency" (FATF). Thus, the revolutionary idea behind Bitcoin, the first official cryptocurrency, was to do away with the trust-based system required for fiat money transactions. Instead, as the pseudonymous Nakamoto described in a whitepaper posted to an obscure cryptography listserv on November 1, 2008, Bitcoin, was designed to serve as a digital currency, whose transactions are recorded on a public blockchain-based distributed ledger, "allowing any two willing parties to transact without the need for a trusted third party."(Nakamoto)

Bitcoin and the original blockchain

Past efforts at introducing a digital currency had envisaged that a digital clearinghouse would maintain a real-time ledger of all transactions in that currency to ensure that the same unit was

not spent multiple times (the "double spending" problem). Notably, Bitcoin's protocol does not require a centralized clearinghouse to maintain a real-time ledger of all transactions or a central bank to maintain the money supply. Instead, a Bitcoin transaction (i.e., the exchange of Bitcoin between two parties) is broadcast to the entire decentralized network for verification, and "miners" (i.e., nodes or computers within the network) compete to solve cryptographic puzzles involving data from the most recent transactions. The safety of the Bitcoin blockchain is predicated on the complexity of these puzzles, which are computationally expensive to crack but easy to verify once solved. Once a solution is found, broadcast, and verified by other members of the network, the current block of transaction records is closed and added to the chain of prior recorded blocks of transactions on the public digital ledger. Confirmed Bitcoin transactions are virtually irreversible and permanent.

Bitcoin payments are borderless and censorship-resistant because no one party can deny a valid transaction. The permissionless ledger is shared, updated and monitored by everyone and controlled by no one. In short, Bitcoin provides a disintermediated payment network outside the purview of a banking system. Furthermore, instead of a central bank creating money, the Bitcoin protocol is designed to create new Bitcoins to reward miners for their verification efforts in accordance with Bitcoin's open-source algorithm. The maximum circulating supply of Bitcoins is fixed by design to be 21 million, and the number of Bitcoins a miner receives for creating a new block is programmed to be progressively smaller as the circulating supply increases. Nakamoto himself verified the first block in January 2009, receiving 50 newly generated Bitcoins in exchange. Since then, the reward per block has dropped to 25, then to 12.5, with the next drop (to 6.25) anticipated in approximately two years.

The success of such an open-source software project depends on its popularity. Initially, the bitcoin community was limited, consisting of a small group of enthusiasts who wanted to promote the idea of a disintermediated virtual currency. One coder in New England bought 10,000 bitcoins for $50 and created a site called the Bitcoin Faucet where he distributed the Bitcoins for free. A farmer in Massachusetts named David Forster began accepting Bitcoin as payment for alpaca socks. On May 22, 2010, Laszlo Hanyecz, a Florida programmer, paid 10,000

Bitcoins to have two Papa John's pizzas delivered (at the time, Hanyecz sent the Bitcoins to a volunteer in England, who then called in a credit card order). Since then, Bitcoin's value has risen astronomically, albeit accompanied by significant volatility, and it has increasingly become an acceptable form of international payment by individuals and businesses. Nonetheless, Bitcoin has still not become a universal digital currency for several reasons. Its price volatility makes it an impractical store of value and unit of account. Moreover, it is not yet widely accepted in every country and even banned in some, making it impractical for businesses to rely entirely on Bitcoins. Use of some conventional "hard" currency in addition to Bitcoins for international payments then continues to expose a business to foreign currency risks. Despite these shortcomings, Bitcoin's early success has been unprecedented. Today, Bitcoin's market cap is approximately $128 billion, and Hanyecz's pizza purchase for 10,000 Bitcoins would be worth about $75 million.

Utility tokens

Today there are over 1800 different crypto-currencies (or digital "tokens" or "coins") with more than one being created daily of late. Many are traded on crypto-exchange platforms across the world, and cryptocurrencies' total market capitalization now exceeds $350 billion.

Some (e.g., Litecoin and Bitcoin Cash), like Bitcoin, are designed to also serve as electronic cash, albeit faster than Bitcoin. Most, however, are not intended to serve as virtual money or as a global medium of exchange. For example, so-called utility tokens are designed for use (to pay for goods or services) on a particular platform, e.g., transactions on Ethereum (another blockchain-based platform) are powered by its native token, Ether. Specifically, Ethereum facilitates the creation and implementation of "smart contracts," which automatically verify and enforce a series of pre-designated rules without manual parsing and execution. Thus, Ethereum "allows individuals and companies to do much more than just transfer money between entities." *Blockchain: A Very Short History Of Ethereum Everyone Should Read*, Forbes, Feb. 2, 2018.

A popular example of a smart contract is an ICO, a crowdsale mechanism that a founding group of developers can use to raise funds to pay for the development of a new platform. Developers use a smart contract on the Ethereum blockchain to create a new cryptographic token for their ICO's investors. These investors send funds (i.e., Ether) to a smart contract address, which, upon verification of funds by the Ethereum network, distributes an equivalent value in the new token which has no immediate functionality until the platform is developed. Compared to traditional funding, developers can raise money at warp speed through an ICO – for example, in the Basic Attention Token ("BAT") ICO, developers raised $35 million in only 30 seconds. ICOs have allowed blockchain-related projects to raise at least 3.5 times more capital than through venture capital funding since 2017, according to a March 2018 techcrunch.com article.

Given Ether's success and popularity, it has also become an acceptable *general-purpose* virtual currency, *i.e.,* a medium of exchange for payments that do not explicitly involve the use of Ethereum's platform other than to verify and validate the transaction. For example, one can buy products on overstock.com using a credit card, or Ether or Bitcoin.

CFTC and SEC's perspectives on crypto-currencies

Overall, not all coins are created alike, and cryptocurrencies can differ vastly in purpose. Some, like Bitcoin, serve as a virtual currency, designed to be a general purpose digital payment system. The CFTC treats virtual currencies like a "commodity" that falls under its purview according to the Commodity Exchange Act (CEA). We discuss the CFTC's recent regulatory actions to protect consumers from fraud and price manipulation related to virtual currencies in a companion article.

In contrast, utility tokens are intended as a medium of exchange for use on a *particular* platform (either immediately or at some point in the future), rather than as general purpose electronic cash. While such tokens may not be considered virtual currencies (thereby exempting them from the CFTC's scrutiny), they may be viewed as "securities" and subject to SEC oversight. As SEC Chairman Clayton noted, "[m]erely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security. Tokens

and offerings that incorporate features and marketing efforts that *emphasize the potential for profits based on the entrepreneurial or managerial efforts of others* [the "Howey Test" from *SEC v. W.J. Howey Co.,* 328 U.S. 293 (1946)] continue to contain the hallmarks of a security under U.S. law." Chairman Jay Clayton's Testimony on *Virtual Currencies: The Roles of the SEC and CFTC*, United States Senate, Committee on Banking, Housing, and Urban Affairs, Feb. 6, 2018. The SEC's actions related to utility tokens has garnered significant public attention lately. Regulatory agencies' views about crypto-currencies continue to evolve as does this technology, which is still in its infancy.