Digital Gold: A Primer on Cryptocurrency

Douglas R. McKay, MD, MBA, FRCSC¹
and Daniel A. Peters, MD, MBA, FRCSC^{2,3}

Plastic Surgery
2018, Vol. 26(2) 137-138
© 2018 The Author(s)
Reprints and permission:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/2292550318777228
journals.sagepub.com/home/psg

Many have heard the term cryptocurrency but few understand what it means. Bitcoin, Litecoin, Ethereum, and many more are all examples. It's a little overwhelming and it's very easy to get swamped in jargon. This is an attempt to explain the what, the how and the why with respect to these new forms of currency. The zealots believe these will upend the economy and the naysayers expect them to fizzle. Only time will dictate their significance, but the underlying technology is likely here to stay.

What Is Money?

We all know what money is in practice but a well-articulated definition does not come easily. Finding a consistent definition to reference is equally challenging. Without an understanding of the money we currently use, we are unable to tackle the fresh approach cryptocurrencies bring to the table. When in doubt, we refer to the Oxford English Dictionary. Here, money is defined as a current medium of exchange in the form of coins and banknotes. This is a good place to start, but there is some nuance with respect to value and accounting that we must also ferret out.

An agreed-upon value and a ledger tracking an exchange are imperative when considering the definition of money and sadly there are many different subtypes. For simplicity's sake, we will only consider 2 broad categories as we get to know our history: commodity money and fiat money. *Commodity* money is a value of exchange based on a resource that has other uses and an intrinsic value. Think gold. Anyone who needs a refresher can look back through our recent publications on the history and role of gold in the economy. *Fiat* money is a form of currency without intrinsic value but that carries value set by a government and supported by those involved in its exchange. It is distrust in the centralized nature of these fiat currencies that spawned the growth of cryptos.

We Need to Decentralize Man!

Those who created cryptocurrencies were philosophically opposed to the centralized origins of money. Where fiat money can be created by a government, the amount of a

given cryptocurrency that enters circulation is known at the outset. Think back to the monetary stimulus packages during the recent economic crisis where the Federal Reserve created money by adding value to account balances. Even an event where a cryptocurrency can be created or brought into existence is defined at the outset by the original algorithm.

The idea of a digital cash system wasn't a new one. Many had tried and failed to create a centralized system to facilitate the exchange of digital cash, but Bitcoin broke the mold and succeeded by breaking away from centralized oversight. The creator of the currency believed that only through decentralization could digital cash succeed. As an interesting aside, no one actually knows who invented Bitcoin, although he or she uses the pseudonym Satoshi Nakamoto.

The lack of a centralized body or authority to validate transactions presented a problem. Think of paying a bill online as an analogy. This requires centralized oversight to document that the transaction has happened and store the change in a ledger balance as a credit and debit for both parties. Decentralizing digital cash posed a significant problem with respect to documentation. The ingenuity of the cryptocurrencies lies in the way that transactions are tracked and validated.

Blockchain

In a decentralized system, the oversight must be done by the members of the network. Think economic communism with shocking wealth disparity. Cryptocurrencies are exchanged

¹ Division of Plastic Surgery, Department of Surgery, Queen's University, Kingston, Ontario, Canada

² Division of Plastic Surgery, Department of Surgery, University of Ottawa, Ottawa, Ontario, Canada

³ Telfer School of Management, University of Ottawa, Ottawa, Ontario, Canada

Corresponding Author:

Douglas R. McKay, Department of Surgery, Queen's University, Hotel Dieu Hospital, 166 Brock Street, Sydenham 3 S3023, Kingston, Ontario, Canada K7L 5G2.

Email: doug.mckay@utoronto.ca

through a peer-to-peer network, and the system ensures and documents consensus for any given exchange.

For any given coin held by the network, there is an ever-growing chain of code that tracks the transactions executed by the coin. Each block has a record of the transaction, a timestamp of when the transaction occurred, and a pointer, commonly called a hash, directed and linked to the previous block in the chain. The information is encrypted, hence crypto and is confirmed and distributed to the users of the entire system. Once a transaction has been validated and linked in the chain, it cannot be modified without changing every other link in the chain.

Consensus is a crucial concept for cryptocurrencies. The entire network must agree upon and be made aware that a transaction has occurred and that information must be safeguarded. Confirmation is equally crucial. But who out there takes care of every transaction within the system? Enter the miners.

What Is a Cryptocurrency Miner?

Within the decentralized system, it is the public at large who protects the integrity of the transactions through encryption, adds a timestamp, validates transactions and creates global consensus. The public does this on their own computers, supporting the notion that the system is in the hands of the people. The communities executing this work are known as miners. It's an analogy to those who once ferreted out gold and the other precious metals used in the first commodity-based money systems.

Once a coin has been exchanged, the documentation of that exchange must be confirmed and shared with the entire network to make it irrefutable. Miners compete to document and encrypt the transaction in exchange for a digital coin. It's really like solving a puzzle for a prize.

The Particulars of Mining

If a miner successfully submits a block, they are rewarded with Bitcoin and a transaction fee. In the case of Bitcoin, the value of the prize has been algorithmically predetermined at the outset of creation and is falling in value. The current prize for adding a block is 12.5 Bitcoin. When Bitcoin is trading around US\$17 500 a coin, this is almost a US\$150 000 reward for

adding a block. Sounds spectacular right? Where can I sign up? The problem lies in your chances at success.

As the popularity of Bitcoin mining has grown so has the technology and the number of participants. In fact, mining has engendered an entire secondary industry within the micro-chip- and computer-processing world where companies compete to create computer equipment that mines rapidly. Computer equipment, electricity, and heat are all costs that play into a miner's bottom line. The individual stands almost no chance at consistently adding blocks and joins pools that share costs and rewards.

Where there is an opportunity for profit, one will find a business. Professional mining outfits seem to be here to stay. These companies raise capital, purchase computing power, and enter the chase. Iceland has become the cryptocurrency mining capital of the world for 2 reasons: cheap and abundant power and cool air. Electricity in Iceland is generated at geothermal stations driven by volcanic activity. It is clean and abundant. It's also naturally cold there, minimizing the investment required to cool the servers while they work.

What's Next for Cryptos and Blockchain?

No one really knows what the future holds. The zealots believe this is the dawn of a new era and the surface has barely been scratched. The naysayers predict systemic collapse citing that a monetary system unsupported by tangible assets or a government endorsement is destined to fail. There is no unifying consensus on taxation across countries, but Bitcoin certainly got a leg up this year when it started to trade on the Chicago Board of Exchange. Like any other commodity, one can now buy futures in Bitcoin. Regulation is required as a monetary system without oversight can lend itself nicely to criminal activity.

Even if the currency tanks and disappears, blockchain is likely here to stay. It's a game changer with respect to data encryption with unlimited applications. In our world, blockchain lends itself beautifully to medical charting. Each event is added and encrypted and only the patient can share a key that allows access to the chain. It is a fascinating technology whose development and influence on the economy will be fun to follow.