WHARTON FINANCIAL ANALYTICS

Data
Lab

# Crypto Investing

Michael R. Roberts

August 2022

Wharton
University of Pennsylvania

# About Wharton Financial Analytics

The **Wharton Financial Analytics** (**WFA**) initiative was created in 2020 for the purpose of empowering people to make better financial decisions through cutting edge research, innovative education programs, and industry engagement. In doing so, WFA serves the Wharton School, the University of Pennsylvania, and the broader global community.

For more information about Wharton Financial Analytics and its products and services, please visit our website at:
http://finance.wharton.upenn.edu/~mrrobert/
or contact
mrrobert@wharton.upenn.edu

Michael R. Roberts is the William H. Lawrence Professor of Finance at The Wharton School of the University of Pennsylvania. He developed this data lab solely for the purpose of class discussion. The lab is not intended to serve as an endorsement, source of data, or illustration of effective or ineffective decision making. Although based on real events and despite occasional references to actual companies, this lab is fictitious and any resemblance to actual persons or entities is coincidental.

Bill Dowling had spent the better part of his financial advisory career steering clients into traditional securities, namely stocks and investments. As the wealth of his clients grew so too did their expectations for investment returns. Many began pressing Bill for insights on alternative investments including private equity, venture capital, real estate, and cryptocurrency. In August of 2022, Bill believed it was time to investigate what role cryptocurrency should play in his clients' portfolios, and how exactly they should invest in this nascent asset class.

## Technology Background

To understand cryptocurrency, it is useful to have some context beginning with the underlying technology. One of the primary goals of cryptocurrency is reducing the cost of transactions by removing the middleman, e.g., bank, insurance company, government. Transactions are at the heart of cryptocurrency and are recorded in a ledger, which nowadays is synonymous with an electronic database. Transactions can include tickets sales (Guts), dating matches (Matchpool), product warranties (Waranteer), payments (Blockpoint), product status (IBM Blockchain), and insurance claims (Nationwide) among others. The names in parentheses are companies currently employing or testing blockchain technology in those spaces.

Broadly speaking, ledger systems come in multiple forms varying by (i) location and (ii) control.[1] Consider a bank that maintains records of customers' transactions – e.g., credit card, mortgage, and checking and savings accounts. The bank can maintain the ledger in one, centralized location, such as on its own servers. It could also outsource its IT needs to hosting services, such as Amazon Web Services, Google Cloud, or Microsoft Azure, in which case the ledger may by distributed across multiple servers located across the globe.

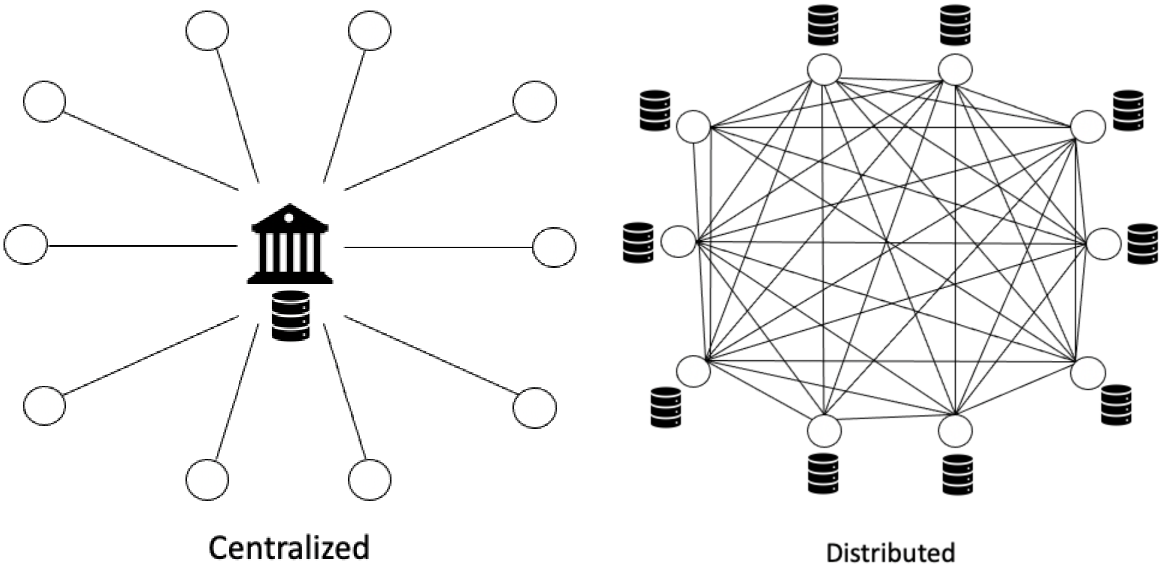
While physical location is important from a reliability perspective, arguably more important is control of the ledger. In both instances, the bank, and only the bank, can add, delete, or modify transactions. It is also the responsibility of the bank to maintain the accuracy of the ledger and that accuracy comes at a significant cost to the bank and, by extension, its customers. Finally, as a central authority

[1] For more details, see Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework, Bank for International Settlements (2017); Oracle Blockchain Services Quick Start Guide, Robert van Molken (2018),

responsible for the accurate recording and maintenance of transactions, banks require a great deal of trust among their customers.

However, a bank is just a middleman, hence the label intermediary. The bank stands between parties making transactions to ensure the delivery of funds. When an individual wants to pay a company for goods and services, they might write a check to the business. The check-writer's bank debits the individual's checking account, and the business' bank credits the company's account. That is, banks update their respective ledgers for the individual and the company. This centralized control is illustrated in the left panel of Figure 1 in which the bank sits in the middle and its customers are represented by the individual nodes.

**Figure 1. Centralized and Distributed Ledger Systems**

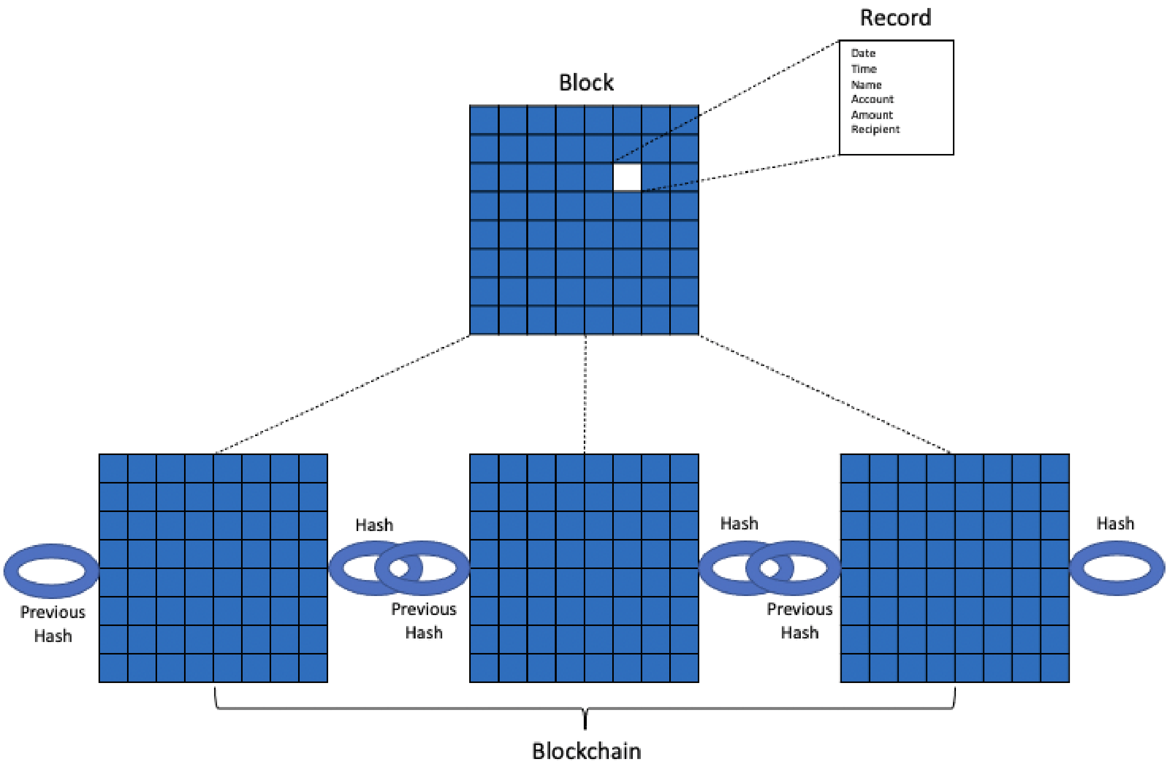


Distributed ledger technology (DLT) eliminates the need for a central authority, the bank in this case, and is illustrated in the right panel of Figure 1. A distributed ledger is a database that is shared across a network and maintained by multiple parties, as opposed to a central authority. For example, rather than each bank having their own ledger for their customers, the same distributed ledger could reside on all banks' servers. Or, as we'll see, the ledger could even reside on every individual's computer thereby eliminating the need for banks altogether.

When an individual wants to pay a company, the two parties can do so directly through the DLT. What ensures the validity of the transaction is the use of cryptographic tools and consensus among the members on the network. Exactly why other members on the network would want to investigate other transactions will become clear below.

Blockchain is one type of distributed ledger in which transactions are stored in discrete units or "blocks" that are encrypted and linked or "chained" together; hence the name.[2] Figure 2 presents a visualization of a blockchain.

**Figure 2. Blockchain Visualization**



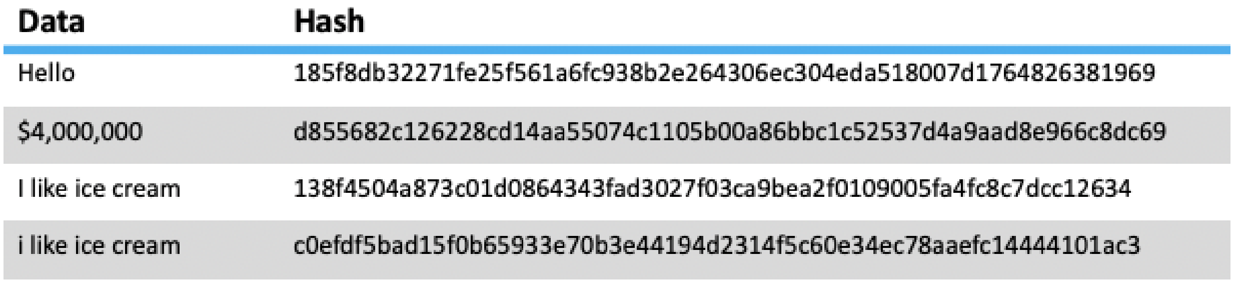
The basic unit of a blockchain is a record containing information about a transaction. Continuing with the bank example, a record of a credit card charge could contain information about the cardholder (name), the merchant (name, address, phone), the date and time of the transaction, and details of the transaction itself (money transacted, specific good or service exchanged, warranty information, etc.).

[2] Other types of distributed ledgers include hashgraph, directed acyclic graph (DAG), holochain, and tempo.

The record is checked by "nodes" – other individuals – on the network to ensure that the transaction is valid.

If valid, the record is added to a block. Each block is identified by a unique code called a hash. Hashing refers to the transformation of a string of arbitrary length into a string of fixed length. Table 1 illustrates how hashing works using a few examples. Despite appearances, the number of characters in each hash is identical (64). Notice that even slight changes in the data – the last two rows – results in dramatically different hashes. From a security standpoint, hashes are very useful because it is virtually impossible to reverse engineer the original data from a hash. In addition to the hash identifying the block, there is a hash identifying the previous block. Hence, the blocks are ordered.

**Table 1. SHA-256 Example Hashes**



| Data | Hash |
|---|---|
| Hello | 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969 |
| $4,000,000 | d855682c126228cd14aa55074c1105b00a86bbc1c52537d4a9aad8e966c8dc69 |
| I like ice cream | 138f4504a873c01d0864343fad3027f03ca9bea2f0109005fa4fc8c7dcc12634 |
| i like ice cream | c0efdf5bad15f0b65933e70b3e44194d2314f5c60e34ec78aaefc14444101ac3 |

As new records are validated, they are added to a block. When filled with records, the block is appended to the end of the block chain. Importantly, the block chain is immutable. Existing records cannot be modified. Any errors in a block can only be rectified by adding new records to the chain. Additionally, blocks cannot be inserted anywhere in the chain. They can only be appended to the end of the chain. Thus, a blockchain is an ever-growing, permanent database of transactions that lives on multiple computers – nodes – on a network.

## Cryptocurrency

Cryptocurrency is digital money analogous to traditional currency like the U.S. dollar or the Euro. As of June 2022, there were more than 19,000 different cryptocurrencies in existence. Unlike the U.S. dollar or Euro, cryptocurrencies are not managed or maintained by a central authority like a government. Additionally, transactions in cryptocurrency avoid the need for financial intermediaries like a bank. Rather, cryptocurrencies can be transacted directly between parties and rely on cryptographic proof instead of trust in a central authority. In addition to removing the government and financial intermediaries from transactions, cryptocurrency allows for anonymity between transaction parties who can be identified by numeric keys as opposed to names, addresses, etc.

There is no physical currency associated with cryptocurrency, which is more accurately described as a set of rules for maintaining a distributed ledger. The job of the computers on the cryptocurrency network is to maintain the ledger by validating transactions and "mining" new blocks to be added to the block chain. As mentioned above, transactions are validated by nodes on the network – the circles in the distributed ledger system of Figure 1. Once validated, miners aggregate transactions – a few thousand – into a block by performing complex computations called "proof of work." Once completed, the block is added to the blockchain and the network updated. Anyone can see the Bitcoin blockchain at Blockchain.com.

While there are many cryptocurrencies, Bitcoin was the first and is, arguably, the most popular. Bitcoin was invented in 2008 by Satoshi Nakamoto (likely a pseudonym).[3] As of August 2022, Bitcoin had a market capitalization in of over $467 billion, which is measured as the total dollar value of outstanding coins. (Coins is of course a metaphor.) This is nearly double that of the next largest cryptocurrency, Ethereum, and seven times that of the third largest, Tether.

## Investing in Cryptocurrency

There are several options for investing in cryptocurrency.

- Centralized exchanges, such as Coinbase or Binance, allow buyers and sellers of cryptocurrency to trade directly.
- Decentralized exchanges are a lower fee.
- Brokers such as Robinhood and SoFi insulate investors from some of the complexity associated with direct trading on an exchange.

[3] See "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, by Satoshi Nakamoto.

- Peer to peer transactions.

There are risks unique to investing in cryptocurrency. Cryptocurrencies are unregulated by central entities and therefore enjoy none of the security benefits enjoyed by stocks, bonds, or other currencies. Cryptocurrencies can, and have been, hacked, leaving investors with little recourse.[4] Cryptocurrencies can also simply be discontinued, eliminating the value of any holdings. Finally, transactions in cryptocurrencies rely on "keys," which can be thought of as passwords. Lose your key, and you lose access to your cryptocurrency.

Alternatively, one can gain exposure to cryptocurrency risk while avoiding the risks of holding actual cryptocurrency. Investors can purchase stock in companies with business dealings in the cryptocurrency space. For example, Coinbase Global Inc. runs a large cryptocurrency exchange. NVIDIA Corp produces graphics cards that are used in mining cryptocurrency. Riot Blockchain Inc. mines Bitcoin blockchain. Exchange traded funds (ETFs) are another alternative available to investors. Some ETFs are portfolios of companies exposed to cryptocurrency risk, like those just mentioned. Other ETFs attempt to replicate cryptocurrency risk by engaging in derivative (futures) transactions.

## Bitcoin

Bill decided he would concentrate his efforts on Bitcoin, given its popularity and track-record. His goal was to provide a report for his clients detailing the role Bitcoin could play in their portfolios and the attendant risks. Because his he and his clientele were not particularly tech-savvy, he also wanted to explore ETFs as a potential investment vehicle. So, he downloaded the data detailed in the Appendix and set off on advising his clients.

[4] Several blockchains have been hacked resulting in significant financial loss. Some of the largest include Wormhole in February 2022 ($325 million), Mt. Gox in February 2014 ($470), Coincheck in January 2018 ($532 million), Ronin Bridge in May 2022 ($540 million), and Poly Network in August 2021 ($611 million).

# Appendix

**Data filename: 20-crypto-investing-mva.csv**

| Position | Variable | Data Type | Description | Source |
|---|---|---|---|---|
| 0 | date | date | Calendar date - end of month | Ken French |
| 1 | stock | float | Value-weighted return to all NYSE, NASDAQ, and AMEX listed stocks. | Ken French |
| 2 | bond | float | Vanguard Total Bond Market Index Fund | Yahoo! Finance |
| 3 | btc | float | Bitcoin USD (BTC-USD) | Yahoo! Finance |
| 4 | rf | float | 30-day Treasury bill yield | Ken French |

**Data filename: 21-crypto-investing-etf.csv**

| Position | Variable | Data Type | Description | Source |
|---|---|---|---|---|
| 0 | date | date | Calendar date - end of month | Yahoo! Finance |
| 1 | bito | float | ProShares Bitcoin Strategy ETF | Yahoo! Finance |
| 2 | xbtf | float | VanEck Bitcoin Strategy ETF | Yahoo! Finance |
| 3 | btc | float | Bitcoin USD (BTC-USD) | Yahoo! Finance |

Wharton
University *of* Pennsylvania
FINANCIAL ANALYTICS

**Wharton Financial Analytics**
The Wharton School, University of Pennsylvania
3620 Locust Walk, Suite 2461
Philadelphia, PA 19104

To connect with Wharton Financial Analytics, contact
**mrrobert@wharton.upenn.edu** or visit **http://finance.wharton.upenn.edu/~mrrobert/**