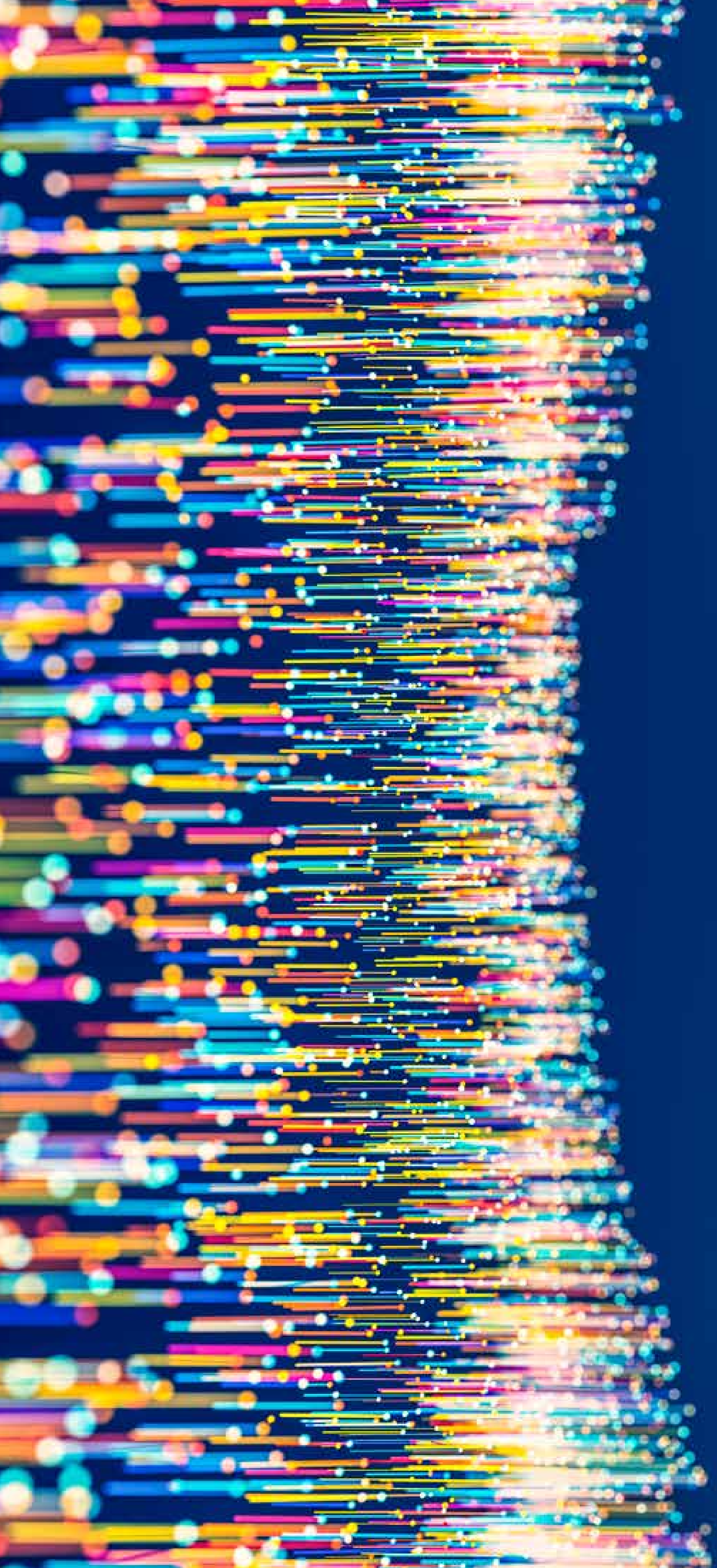


Paul | Weiss

Blockchain and Ethereum

The first paper in our series focused on cryptocurrencies and Bitcoin, examining how they function similarly and distinctly from traditional currencies. This paper, the second in our series, focuses on the distributed ledger technology known as the "blockchain," which many believe is a potentially groundbreaking technology with a multitude of applications outside of cryptocurrencies. This paper also discusses Ethereum, the most prominent platform for building blockchain-based applications.

Blockchain technology initially gained fame for its use in Bitcoin. Bitcoin was the first major digital currency network to use blockchain technology to facilitate digital transfers of value without a third-party intermediary. Bitcoin's rapid expansion and popularity brought blockchain into the public eye. However, blockchain's benefits, such as an immutable record, reliable time stamps and decentralized control, can extend to applications well beyond cryptocurrency.

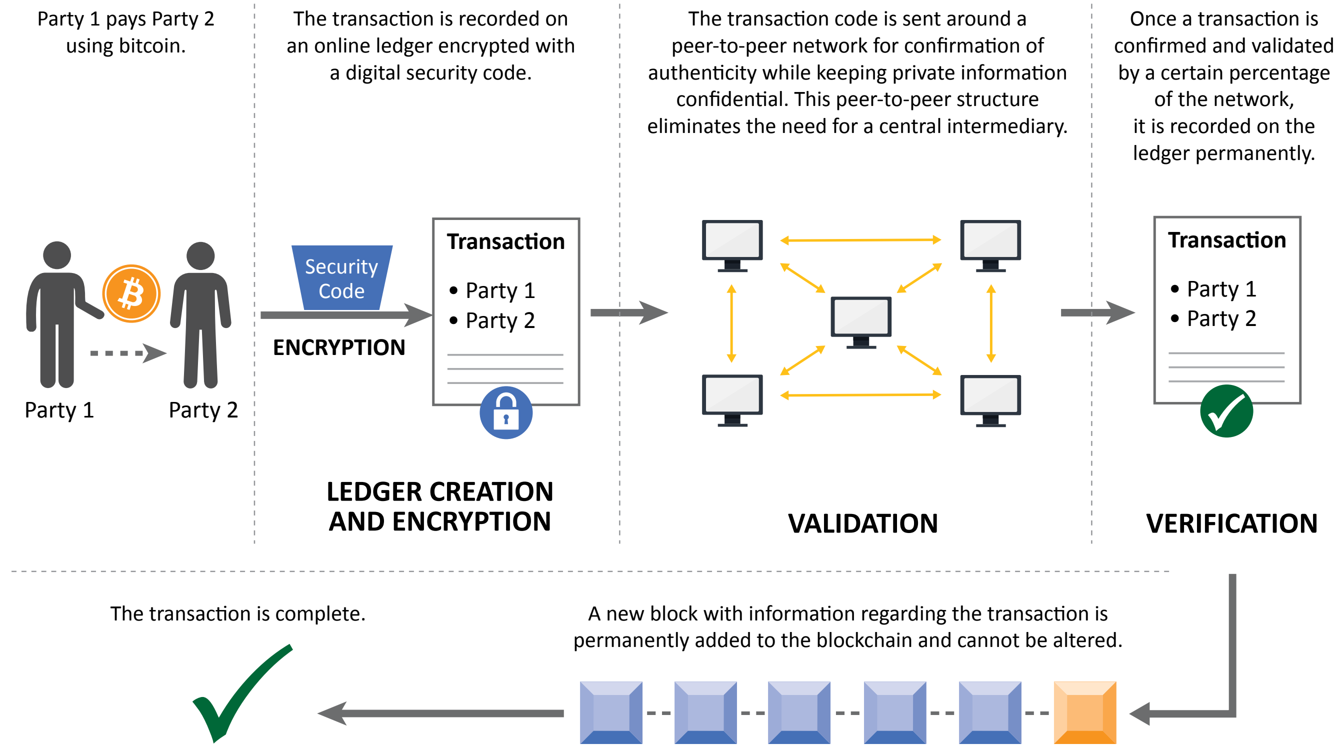
Blockchain

A blockchain is a cryptographically secured, distributed ledger that allows unfamiliar parties to transact with each other, without the need for a centralized third-party intermediary. Blockchains provide for security and transparency in peer-to-peer transactions between individuals or entities who do not otherwise know or trust each other. Blockchains can be thought of in the simplest sense as "global spreadsheets" that leverage large networks to record, verify and approve transactions.

Without a blockchain, electronic transactions would require intermediaries to ensure trust. That is, absent a secure ledger of transactions, a party could theoretically copy and spend the same digital asset multiple times — a phenomenon known as the

Blockchain (continued)

Blockchain Breakdown



Party 1 pays Party 2 using bitcoin.

The transaction is recorded on an online ledger encrypted with a digital security code.

The transaction code is sent around a peer-to-peer network for confirmation of authenticity while keeping private information confidential. This peer-to-peer structure eliminates the need for a central intermediary.

Once a transaction is confirmed and validated by a certain percentage of the network, it is recorded on the ledger permanently.

LEDGER CREATION AND ENCRYPTION

VALIDATION

VERIFICATION

The transaction is complete.

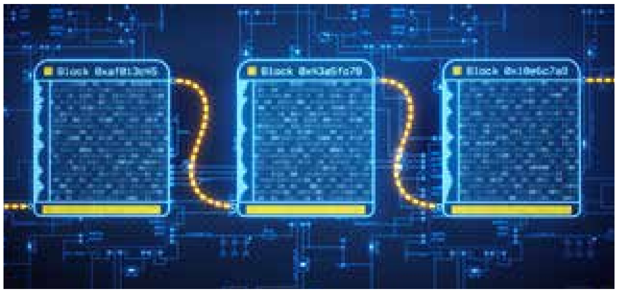
A new block with information regarding the transaction is permanently added to the blockchain and cannot be altered.

"double spending" problem. Blockchains address this problem by using cryptography to enable trustless, secure transactions through a distributed network, wherein all transactions are permanently and immutably recorded. That is, as soon as a digital asset, like a cryptocurrency, is exchanged from one person to another, that transaction is recorded in a blockchain, such that the first person is not permitted to spend the same asset a second time.

In short, a blockchain network functions as a distributed ledger that records and time-stamps all transactions ever made between participants on the network, with each new transaction immutably linked to the previous one.

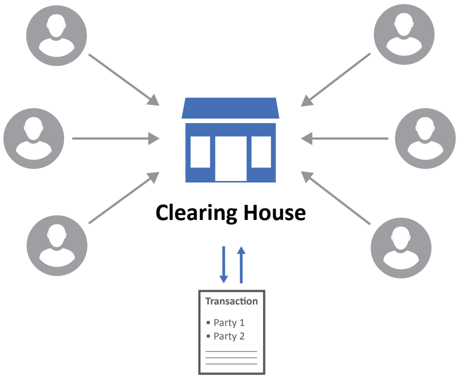
Certain defining characteristics of blockchains are:

- **Blocks**: The blockchain network verifies and clears all of the recent transactions, which are then stored in a "block" linked to the previous block. Each "block" in a blockchain consists of a certain number of those transactions. Each block builds off the previous block, creating a chain. Specifically, each block contains a cryptographic hash of every preceding block (see the *Cryptography* bullet below for more detail).

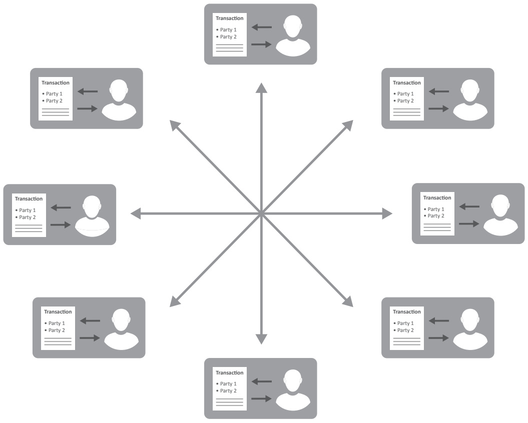


Blockchain (continued)

- **Distributed**: Blockchain is a distributed ledger, which means it is not stored in any one place and is not controlled by any one person or institution. Rather, it is stored and updated simultaneously on the servers or "nodes" that form a network.



Centralized Ledger



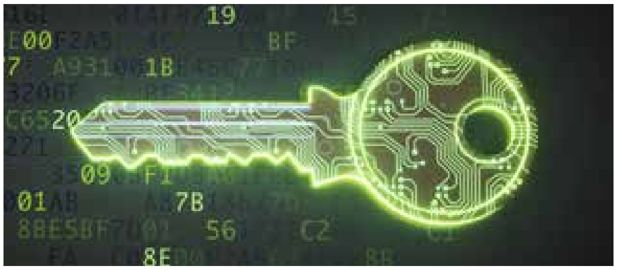
Distributed Ledger

- **Cryptography**: Blockchains use cryptographic hashing for security. These algorithms operate such that no two different inputs will ever return the same output, and even minor variations in the original input produce substantial differences in the outputs. As a result, experts believe that it is impossible to "hack" a blockchain to change the transaction history, using current computer technology.

- **Consensus Mechanisms**: Blockchain employs consensus mechanisms to verify the integrity and accuracy of each transaction. The exact mechanism varies depending on the architecture of the blockchain, but generally they rely on consensus of a majority of participating nodes on the network to verify transactions.

The most common mechanism to show consensus is called "proof of work," which involves a process known as mining. In "mining," volunteer participants compete to solve complex algorithms in order to verify each transaction on the blockchain. The first miner to solve the problem is declared the "winner" and receives new tokens as a reward.[1]

- **Permissionless vs. Permissioned**: Permissionless blockchains (like Bitcoin's) are open to the public (*i.e.*, anyone can download the blockchain, participate in transactions and/or run their own node). Permissioned blockchains are maintained by private entities and require permission to join. Facebook's proposed cryptocurrency Libra would initially operate using a permissioned blockchain with the goal of one day becoming permissionless. Initially, only members of the Libra Association Council would be able to serve as validator nodes for the permissioned blockchain, though users of Libra will still be able to use the Libra network and build products on it even in the permissioned state.[2]



Ethereum

Ethereum

The blockchain architecture that powers Bitcoin was only designed to work with cryptocurrency, and it was not designed to hold the large files required to support other types of transactions or transfers of content. In contrast, Ethereum uses a distributed filing system that allows documents and applications containing large amounts of data to be stored, encrypted, distributed and instantly accessed across secure networks. Thus, the Ethereum blockchain can support more complex transactions, such as the transfer of digital content, distributed applications and "smart contracts."

In particular, two common applications are smart contracts and decentralized applications or "Dapps." Both are explained below.

- **Smart Contracts**: The Ethereum blockchain supports "smart contracts," which can have broad functionality and utility. Smart contracts are digital agreements that use a blockchain to secure, execute and enforce agreed-upon contractual terms between parties. For example, a music streaming service that operates on a blockchain could require that all artists seeking to include their musical works in the streaming service enter into a smart contract with the streaming service. The smart contract would contain self-executing code that pays the artist a royalty every time a third-party user streams the artist's music. This is thought to increase efficiency by cutting out the middleman and provide for near-instantaneous payment directly from the listener to the artist.[3]

- **Dapps**: Ethereum enables users of the Ethereum network to develop decentralized applications known as "Dapps." In this way, Ethereum can function as a blockchain-based "app store" where anyone can publish their applications, without relying on a centralized intermediary to function.[4] Ethereum also powers the Ethereum Virtual Machine, which enables the development of Dapps.

Ethereum (continued)

- **Ether**: Ethereum also supports its own cryptocurrency, called Ether. Ether often ranks as the second or third most widely used cryptocurrency after Bitcoin.[5] Quick figures of Ether are provided to the right.

Quick Figures of Ether
(as of June 10, 2019)[6]

Value:
$187

Market Cap:
Over $20 billion

24-hr Trading Volume:
Over $7 billion

Conclusion

In conclusion, blockchain technology has great potential to revolutionize a variety of industries. Those who saw this potential early on sought to capitalize on it through initial coin offerings, or ICOs, many of which were launched by building Dapps on the Ethereum network. Through ICOs, ICO promoters were able to raise enormous sums of money promising incredible returns due in large part to the potential of blockchain technology. However, regulators quickly put a damper on the wave of ICOs that have hit the market in recent years, as we discuss in our third and final paper in this introductory series.

[1] *See Proof of Work vs Proof of Stake: Basic Mining Guide*, <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake> (last visited Nov. 27, 2018).

[2] Libra White Paper*,* <https://libra.org/en-US/white-paper/> (last visited August 14, 2019).

[3] *See How Do Ethereum Smart Contacts Work?*, <https://www.coindesk.com/information/ethereum-smart-contracts-work> (last visited Nov. 27, 2018); *see also* Sherman Lee, *Embracing Blockchain Could Completely Change The Way Artists Sell Music and Interact with Fans*, Forbes, Apr. 25, 2018, <https://www.forbes.com/sites/shermanlee/2018/04/25/embracing-blockchain-could-completely-change-the-way-artists-sell-music-and-interact-with-fans/#5ec967541a25b> (last visited Nov. 27, 2018).

[4] *See What is a Decentralized Application?*, <https://www.coindesk.com/information/what-is-a-decentralized-application-dapp> (last visited Jan. 17, 2019).

[5] *See* Esther Kim, *Ripple (XRP) Overtakes Ethereum as Second Biggest Crypto By Market Cap*, Nov. 15, 2018, <https://bitcoinist.com/ripple-xrp-price-ethereum-btc-price> (last visited Nov. 27, 2018).

[6] CoinMarketCap, <https://coinmarketcap.com/currencies/ethereum> (last visited June 10, 2019).

Our Team

Corporate

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

Manuel S. Frey
212-373-3127
mfrey@paulweiss.com

David S. Huntington
212-373-3124
dhuntington@paulweiss.com

Raphael M. Russo
212-373-3309
rrusso@paulweiss.com

Jonathan H. Ashtor
212-373-3823
jashtor@paulweiss.com

Litigation

Susanna M. Buergel
212-373-3553
sbuergel@paulweiss.com

Jessica S. Carey
212-373-3566
jcarey@paulweiss.com

Roberto Finzi
212-373-3311
rfinzi@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Roberto J. Gonzalez
202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

Karen R. King
212-373-3784
kking@paulweiss.com

Associates Jacobus J. Schutte, Anastasia V. Peterson, Marisa Seiss, Andrew J. Heffler, Deniz Gurbuz, Patrick R. Kessock and Apeksha S. Vora contributed to this white paper.

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

www.paulweiss.com