Cryptocurrencies, Blockchain Technologies & the Law

University of Houston Law Center
Prof. Charles D. Brown

Fall 2022

WEB 3
LAW CENTER

Introduction to Class

What have I gotten myself into?

Hello World! - Personal Introduction

Class Syllabus - Aspirational, Flexible, Fiction

Class Structure - Quiz, Technology, New News, Participatory Lecture

Assessments - 25% Quiz, 25% Participation, 50% Written Assessment

Participation - New News, Class Discussions, Prepared on Readings

Written Assessment - “Add something meaningful to the understanding or direction of Web3 law.”

Group or Solo, Practical or Academic, Published or Presented (or Both)

My Web3 Story

Class Introductions

WEB 3
LAW CENTER

Next: What is a blockchain?

Background and Technological Primer

Reading Assignment: FW Chap. 1 & 2

Industry Assignment: Find some method of staying current with the state of the blockchain space. Some ideas include Google Alerts, Twitter follows, Apple News Interests. Read a few articles and be prepared to discuss with the class.

You should be able to explain what makes blockchain unique and why those unique characteristics are so important.

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

I will be out of town for the week of September 19th. We will have a guest lecturer (Susan Lindberg) who will cover SEC securities regulation and NFTs.

Assignment:

Sections 3 and 5 from

https://www.americanbar.org/content/dam/aba/administrative/business_law/buslaw/committees/CL620000pub/digital_assets.pdf

WEB 3
LAW CENTER

Housekeeping

Securities (9-19):

SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

In the Matter of Erik T. Voorhees, File No. 3-15902, Release No. 9592 (June 3, 2014) https://www.sec.gov/litigation/admin/2014/33-9592.pdf

U.S. Securities and Exchange Commission, Statement on digital asset securities issuance and trading (Nov. 16, 2018) https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading

L. Schneider, Oranges are not securities and neither is SOL, Crowdfund Insider (July 12, 2022) https://www.crowdfundinsider.com/2022/07/193572-oranges-are-not-securities-and-neither-is-sol/

NFTs (9-21):

W. Entriken, D. Shirley, J. Evans, N. Sachs, EIP-721: Non-Fungible Token Standard (Jan. 24, 2018) https://eips.ethereum.org/EIPS/eip-721

D. Van Boom, Seth Green Loses $200K Bored Ape Yacht Club NFT in Phishing Scam, CNET, May 18, 2022. https://www.cnet.com/personal-finance/seth-green-loses-200k-bored-ape-yacht-club-nft-in-phishing-scam/ See also story in Wired, https://www.wired.com/story/seth-green-bored-ape-nft-stolen/

Global Blockchain Convergence, A “Sensible” Token Classification System,

available at https://novuminsights.com/post/sensible-token-classification-system/

WEB 3
LAW CENTER

Tech Note

Discord

Discord is a communications platform that serves as the default community manager for most NFT/DAO projects.

The Web3 Law Center is just now starting a discord server. Please follow the link, create an account, and join the Web3LC server.

https://discord.com/invite/AC8BceyU

WEB 3
LAW CENTER

News Note

Alphabet (Google) Invests $1.5 Billion in 4 NFT/Crypto Companies

Fireblocks

Dapper Labs

Voltage

Digital Currency Group

What does an investment of this size tell us about the future of this technology? Keep in mind, they spent between $400 and $800 million on Google Glass.

WEB 3
LAW CENTER

What is a blockchain?

WEB 3
LAW CENTER

What is a blockchain?

Background and Technological Primer

Blockchains are decentralized databases, maintained by a distributed network of computers.

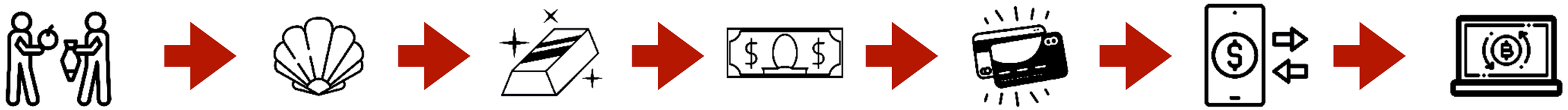
What is a database?

What is a computer?

WEB 3
LAW CENTER

What is a blockchain?

What is money?



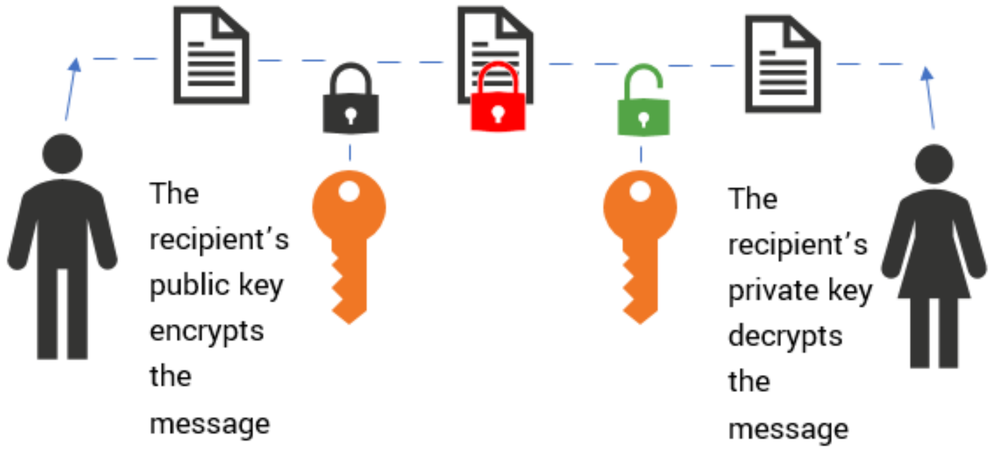
Tangible	→	Less Tangible
Anonymous	→	?
Free Movement	→	?

WEB 3
LAW CENTER

What is a blockchain?

The Encryption Side of Things

1976 - Public-Private Key Cryptography created a way around the shared key problem. Key-pair algorithms create authentication mechanisms that allow that are very, very difficult to break. Diffie and Helman's paper calls for the need for an open hashing model.



1989 - Ron Rivest developed the MD2 algorithm in 1989 it was the first to be widely used in open standards. One-way encryption. Takes a data string and converts it into a fixed string.

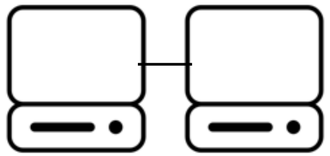
I love my dog. = BE6094D4C12DCE046608FA51F6A9158A
I love my dog! = BB0E53B3B3FE934D83BA8C87690CC7A4
My dog loves my wife. = ECDC4B093451417BE7E1440E36F9B490

WEB 3
LAW CENTER

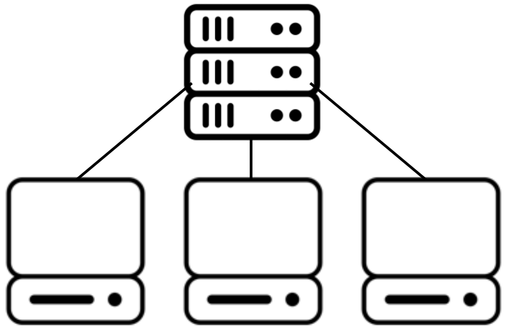
What is a blockchain?

Computer Networking

Pre-1964 - Computers lived alone. While there was terminal access, the computer was an isolated machine.



In August 1964, packet switching technology lays ground work for DARPA and later the internet. The goal was to protect information in the event of nuclear war.



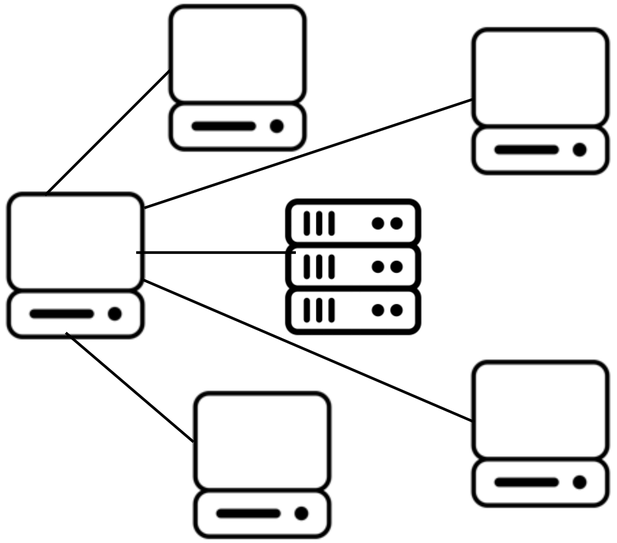
By the mid-1990s DARPA had evolved to become the commercial internet. Web 1.0 Under this client-server model, people went to websites and interacted with the pages served up by the web server. Here, the content creator owned the information, but the information is centralized and therefore vulnerable to security breakdowns, tech breakdowns, and censorship. Whether Google, Amazon, or the New York Times, Web 1.0 websites create content, own the content, and distribute that content (search results, stores, or news).

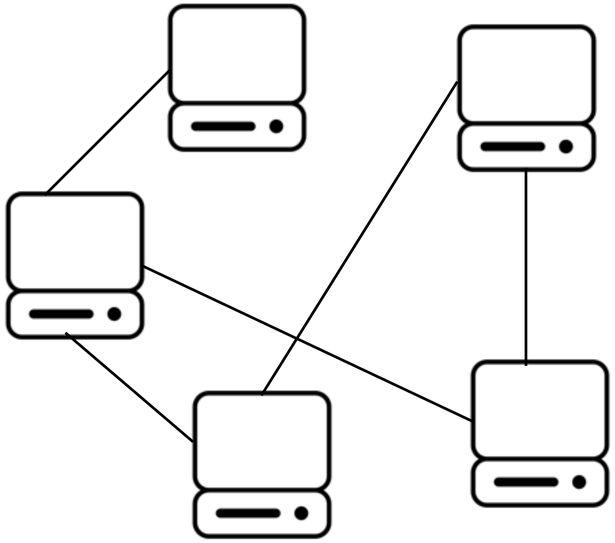
WEB 3
LAW CENTER

What is a blockchain?

Computer Networking

1999 - Napster introduces the world to peer-to-peer file sharing. Each computer acts as a node in the network and contains pieces of files that it serves up based on the file index contained on Napster's servers. Music copyright holders were not thrilled with the new technology, so they fight Napster, keying on the server.





2001 - After Napster pays the price for having a centralized index, BitTorrent and others distribute the index as well for a fully distributed file sharing system. Copyright holders are helpless. There is no one server to shut down. Distribution is now entirely global and decentralized.

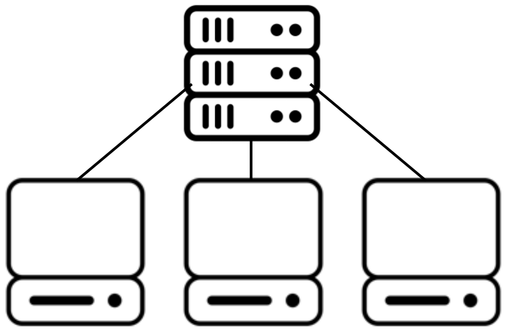
WEB 3
LAW CENTER

What is a blockchain?

Computer Networking

2003 - While the pirates are sharing music, movies, and more, the commercial internet remains in Web 1.0. But in 2003 with MySpace and 2004 with Facebook, the internet begins to change to Web 2.0. Here, the content creator uploads the content to a corporate server and the corporation monetizes it. YouTube, Instagram, Facebook, TicToc, and Yelp. All of these websites take content, monetize it, and pay nothing to the creator.

This consolidates money and power in the hands of those able to create and monetize the network effect.



If you are not paying for it, you're not the customer; you're the product being sold. - Andrew Lewis

WEB 3
LAW CENTER

What is a blockchain?

How do websites actually work?

Websites are viewed by browsers that interpret the computer language that the website is written in.

Client Side v. Server Side

Most of the information on the page is stored in a server-side database. For example, WordPress, the largest Content Management System on the Web.

So the large corporations that drive so much engagement off of other people's content are also capable of storing user information in their private databases and selling that information to others or displaying it (or censoring it) with little regard for the user's wishes.

WEB 3
LAW CENTER

What is a blockchain?

The Backdrop of the Blockchain Movement

The haves v. have nots. 1%ers. 2008 Financial Crisis.

Apple vs. Facebook, Small Business, Instagram, FBI, etc.

Hacking, shared data with 3rd parties, scraping data, invasive ads…

Social backlash, social censoring, opposing viewpoints.

Free speech, free expression, financial restraints.

Meme stocks, NFTs, HODL, and distribution of economic opportunity.

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

Written Assessment

- Mentors
- Tornado Cash and Regulation
- Work with the ADR team and generate work product from that.
- Privacy concerns with USDC and FedNow cash.
- Building an automated RSS feed or news feed for legal topics. Should be accompanied by an explanation of the categories and sources.

WEB 3
LAW CENTER

Tech Note

GitHub

GitHub serves a number of functions for programmers.

1. File Storage - People working on software can store it here and access it from multiple locations with multiple device types.
2. Collaboration - People can access the source code, make changes, and then either continue with their fork or have the changes merged into the main branch.
3. Resume - When programmers want to show their work to potential employers, this is their resume.

What have you used it for?

WEB 3
LAW CENTER

News Note

Tether says it's not Freezing Tornado Cash Addresses Until Government Tells It To

8-8-22 - “Today, Treasury is sanctioning Tornado Cash, a virtual currency mixer that launders the proceeds of cybercrimes, including those committed against victims in the United States.”

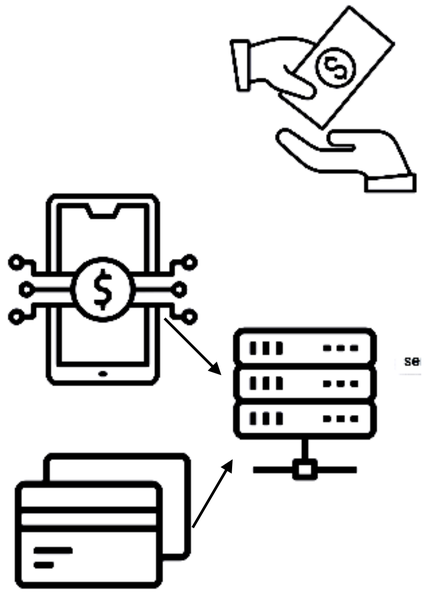
https://www.theblock.co/post/165513/tether-says-its-not-freezing-tornado-cash-until-government-tells-it-to

https://coincenter.substack.com/p/how-does-tornado-cash-actually-work?utm_source=substack&utm_medium=email

WEB 3
LAW CENTER

What is a blockchain?

Digital Currency and the Problem of Double Spending



If I buy something with cash, I cannot spend the same dollar again as it has been given to another person.

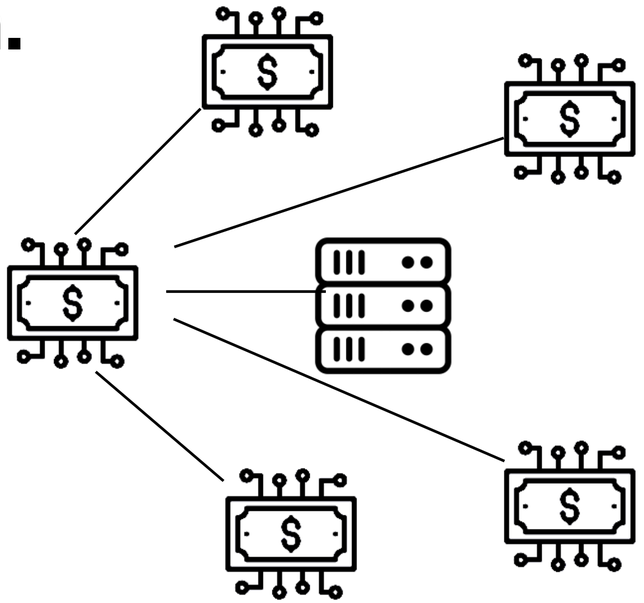
If I use digital currency or a credit card, the transaction must clear a central server (bank or credit card company) to verify funds and complete the transaction.

Without a central server, there is nothing to prevent a buyer from spending the same digital currency to purchase two different items.

WEB 3
LAW CENTER

What is a blockchain?

A blockchain is born. We call it Bitcoin.



In 1994, DigiCash is formed to allow anonymous cash transfers. But the ledger was on one server. Oops.

In 2008, “Satoshi Nakamoto” published a white paper that merged the ideas that we have discussed and, using a concept called blockchain, created a distributed, peer-to-peer cash system using a distributed ledger. Nakamoto called it Bitcoin. In 9 pages, Nakamoto changed the world.

WEB 3
LAW CENTER

What is a blockchain?

The Byzantine General's Problem

Several divisions of the Byzantine army are stationed just outside of an enemy city and are preparing for battle. Various generals can only communicate with each other via a messenger. They must agree upon a common course of action. However, we must assume that some generals are traitors who wish to prevent loyal generals from agreeing upon a common course of action. An algorithm is needed to ensure that a small group of traitors can't disrupt communications. To solve the Byzantine Generals problem, loyal generals need a secure way to come to agreement on a plan (known as consensus) and carry out their chosen plan (known as coordination).

It is very difficult to prove the authenticity of a message without a central coordinating authenticator.

WEB 3
LAW CENTER

What is a blockchain?

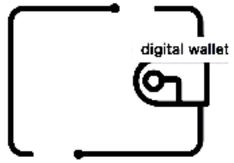
How Bitcoin Creates BFT (Byzantine Fault Tolerance)

They use a proof-of-work chain to solve the problem. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work. - Satoshi Nakamoto

WEB 3
LAW CENTER

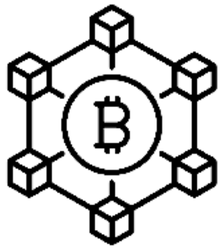
How does a blockchain work?

Perfect trust in an anonymous and hostile environment.



Public-Private Key - Commonly known as a wallet.

Bitcoin is sent from one wallet to another wallet.

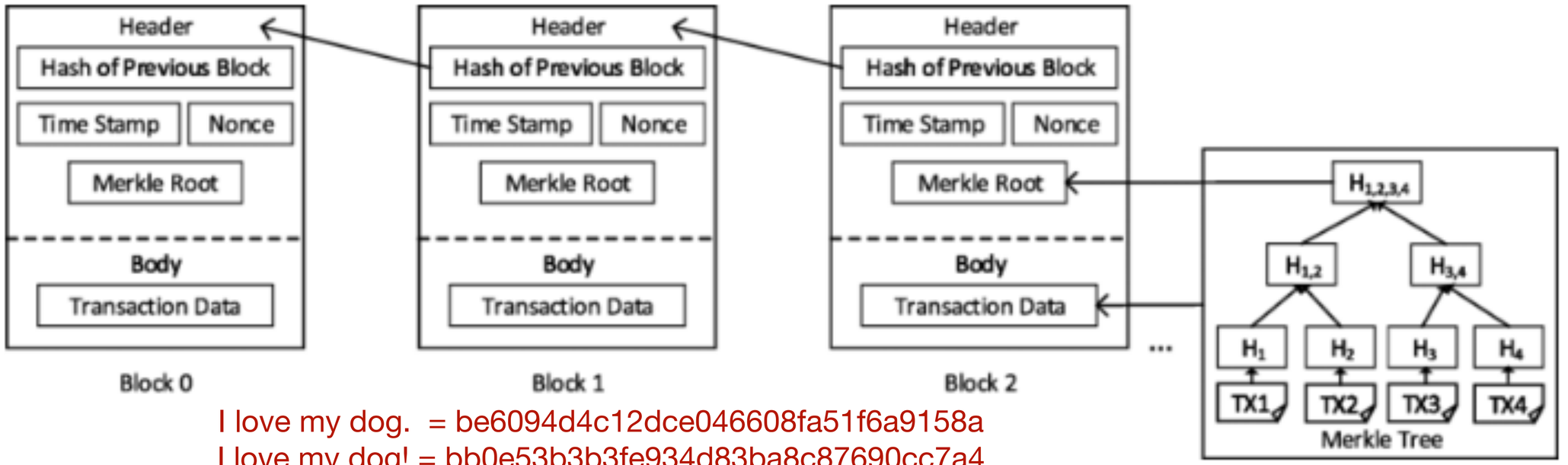


The transaction is validated and the balances in each ledger are edited.

WEB 3
LAW CENTER

How does a blockchain work?

Anatomy of a Block



I love my dog. = be6094d4c12dce046608fa51f6a9158a

I love my dog! = bb0e53b3b3fe934d83ba8c87690cc7a4

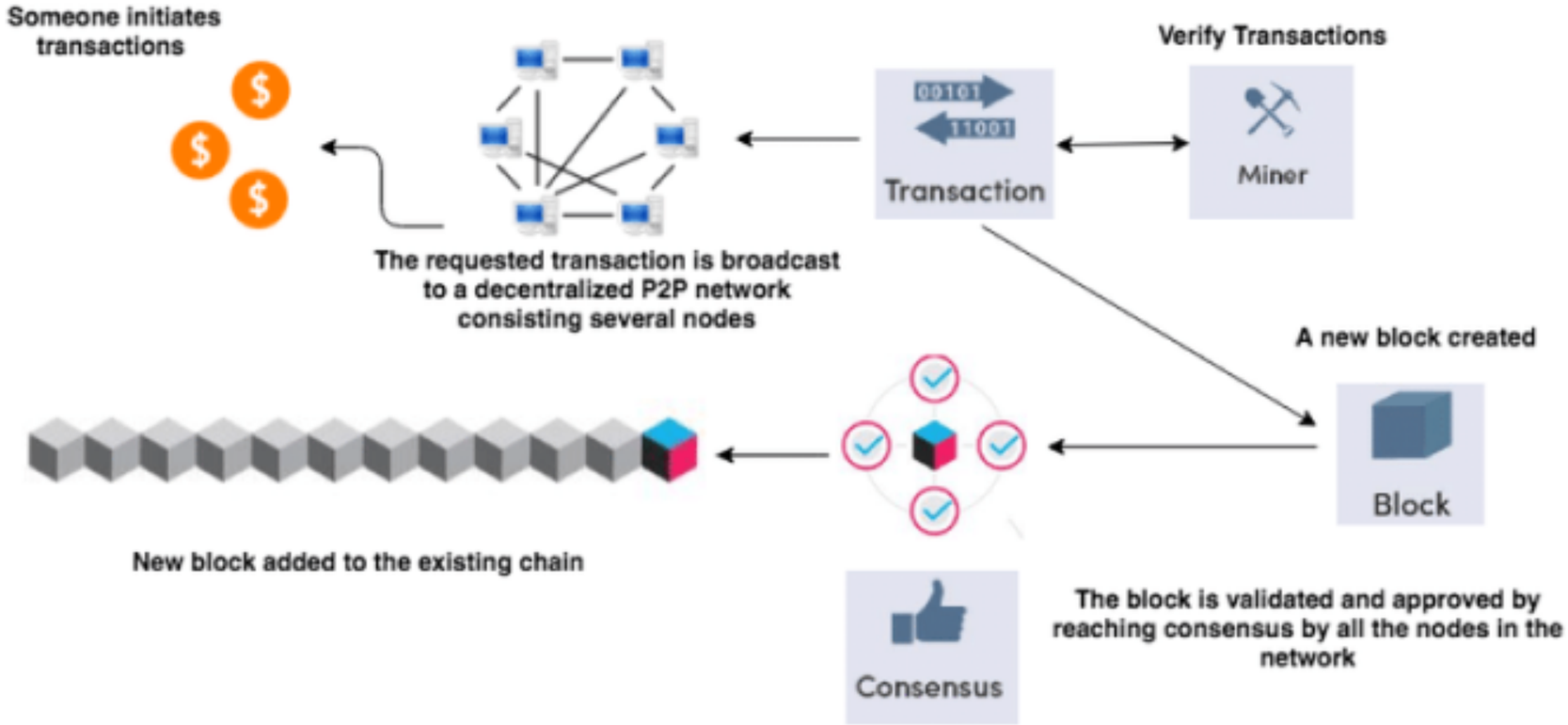
be6094d4c12dce046608fa51f6a9158abb0e53b3b3fe934d83ba8c87690cc7a4 = 3aebd55e6bf738c2c6483ada58dd01b7

Blockchain for Dynamic Spectrum Management - Scientific Figure on ResearchGate.

WEB 3 LAW CENTER

How does a blockchain work?

Nodes, Mining, and Distribution



Functional diagram of a Blockchain network - Scientific Figure on ResearchGate.

WEB 3 LAW CENTER

Characteristics of Blockchain

For better or worse.

Disintermediated.

Transnational.

Resilient.

Resistant to change.

Nonrepudible.

Pseudonymous.

Transparent.

WEB 3
LAW CENTER

Characteristics of Blockchain

For better or worse.

Incentivization and Cost-Structures (PoW, Bounties, Gas)

Consensus (PoW, PoS, Delegated PoS)

Autonomous Software

WEB 3
LAW CENTER

Blockchain Use Cases

What is the point of all of this?

Smart Contracts (with and without an Oracle)

Transaction Register

Store of Value

Bored Apes

Authentication

Democratic Entities

What else?

WEB 3
LAW CENTER

Next: What is a blockchain?

Background and Technological Primer

Reading Assignment: FW Chap. 3

Industry Assignment: Find a couple of good explanations of how blockchain works. The goal is to put together a library from reputable sources that meet people at multiple entry points. These links will be entered on the quiz sheet.

By the end of the next section, you should have an understanding of how blockchain technology is used to create a “currency.”

WEB 3
LAW CENTER

Blockchain as a cryptocurrency.

WEB 3
LAW CENTER