CRYPTO: CRYPTOCURRENCY AND BLOCKCHAIN

THE FUTURE OF MONEY, PROPERTY, AND GOVERNANCE

JOHN COUSINS

INTRODUCTION

Bitcoin, cryptocurrencies,

You have heard about fantastic fortunes being made almost overnight.

blockchain, NFTs, DeFi, Web3,

You have heard about them but what do they mean and how will they impact your world. You may be wondering if this all is a fad or a bubble, or something more.

There is always euphoria and froth that accompanies big paradigm shifts. Remember the dotcom bubble? But there is much here that is serious change. Lots of early dotcoms went bust but the ones that provided real value and remain are the biggest companies in the world like Google, Amazon, Apple, and Facebook.

You can't unring the bell or put the toothpaste back in the tube. Talent and money are rushing into this space. There will be massive innovation and the winners will add incred-

ible value to our lives. And add incredible value to many investment portfolios.

Futurist Alvin Toffler once said,

> "The illiterate of the future are not those who can't read or write but those who cannot learn, unlearn, and relearn."

It's time to become savvy and literate in this new world. That's what this course is about. You don't have to be technical but you do need to be curious.

Let's get started!

CHAPTER 1

CRYPTO OVERVIEW

WE ARE GOING to cover a lot of revolutionary concepts in this book. These concepts are all interrelated. The challenge is where to start.

This chapter is going to be a quick overview of the main topics to get an idea of landscape.

Then I will have chapters on all the different concepts in more detail.

Think of cryptocurrencies, blockchain, NFTs, DeFi, as the internet of money. These things streamline the concept of money like email streamlined sending a letter.

So what is money?
- Medium of Exchange
- Store of Value

• Unit of Account. Accounting ledgers of debits and credits.

Crypto is about offsetting the debasement of fiat money.

Bitcoin is a distributed ledger.

Cryptocurrencies can be divided into Bitcoin, Ethereum and the major altcoins. We will discuss them and their differences in detail.

All of it is riding on the blockchain. Blockchains can be thought of as another layer on top of the internet. Like the web is a layer on top of the internet. This is all made possible by the internet and computers.

SO, WHAT IS A BLOCKCHAIN?

It is a sequential log of events or data that is tamper proof. It is a time stamped append only log.

Blockchains are secured by cryptography, which is communication in the presence of third parties or adversaries. It's how we make secret codes.

The data in a blockchain can be value like Bitcoin or the data can be computer code like smart contracts.

DEFI

DeFi is a new plumbing of finance that addresses some of the problems with CeFi. Remember the 2008 financial meltdown? Or ever hear of the Great Depression in the 1930s? Or inflation? DeFi seeks to remedy the structural risks and fragility of the financial system.

WHAT IS FINANCE?

Finance is moving money and risk through a network: the economy. Intermediaries like commercial and investment banks and credit card companies take fees to move money and risk around. DeFi aims to reduce these fees substantially which makes business and our consumer transactions cheaper and frictionless.

NFTS

NFTs non fungible tokens use blockchains and crypto to create digital property. Digital property rights are a very powerful innovation. The internet has had difficulty creating property rights for art, music, writing and lots more. Now creatives can own their work and create a profitable living online.

WEB3

Web3 is the next generation of the web. It is an idea for a new iteration of the World Wide Web that incorporates decentralization based on blockchains and addresses the issues of bad behavior and clickbait based on advertising models and incentives. Web 1 was read only and web2 is

interactive like social media. You can create content, but you can't own it and profit from it. Web3 isn't based on monetizing your personal data. In Web2 you are not the customer, you're the product.

DAOS

DAOs are an innovation riding on blockchains that are a new way to organize like a corporation or a government. The corporate structure of organization spurred capitalist economic growth through the 20th century. DOAs are the next evolution in organization and governance.

———

CHAPTER 2

LET'S START AT THE BEGINNING.

"It doesn't matter if you're a beginner or an expert as long as you're on the path.

If a beginner is on the path, all they need is time.

If an expert is off the path, they won't be an expert for long."

EVENTS ARE MOVING SO RAPIDLY in the crypto space that legacy expertise is outpaced by innovation. This creates an environment where opportunities abound, but it also is an environment where learning, unlearning, and relearning reign. In this course, I will lay out the concepts and areas that are conceptually fundamental, but it will be up to you to keep current and dive deeper as things evolve.

SO HOW DID ALL THIS BEGIN?

A mysterious anonymous figure known as Satoshi Nakamoto started the whole crypto blockchain phenomenon in 2008. It is interesting to note that Apple unveiled the iPhone in June 2007and the smartphone and mobile revolution exploded.

Mobile adoption happened incredibly rapidly, and now almost everyone has a connected smartphone.

Blockchain and its applications, including cryptocurrency, have been slower to reach mainstream adoption because it's not intuitively or immediately relevant to everyday life. It represents a paradigm shift in how we think about money, banking, and governments. These are big concepts that are beliefs around don't change quickly.

It started a revolution built slowly among visionaries that could comprehend the implications and is now poised to transform how the world is organized and how value is created and stored.

Now blockchains, while still seminal, have matured enough to represent a revolution potentially more significant than the mobile revolution, and think about how that has changed our world.

.   .   .

The big event that happened in 2008 that precipitated the idea of cryptocurrency as a response was the Global financial meltdown. We experienced the fragility of centralized systems in finance like banks and insurance companies and were distraught by the concept of "too big to fail" and the bailouts. But what was the alternative? There wasn't one, and we felt trapped in a flawed system that ultimately rewarded reckless risk-taking and Moral Hazard.

MORAL HAZARD

The term moral hazard comes from economics. Moral hazard is a situation where an economic agent has an incentive to increase its risk exposure because it does not bear the total costs of that risk. For example, mortgage brokers and securitizing institutions are agents that get paid upfront on commission or year-end bonuses and offload risk on unsuspecting investors. Government bailouts incentivize this behavior by not letting the agents or their institutions suffer the consequences of their actions.

But if we didn't bail them out, the public would suffer immensely more. That is basically what happened in the US in the 1930s. The banks were allowed to fail, and the lender of last resort, the Fed, stood by and let capitalism work its consequences. Millions suffered, and the capitalist system's viability was profoundly questioned and challenged by alternatives like fascism and communism.

THE RIDDLE

The riddle was how to move money (value) peer-to-peer without a centralized trusted intermediary. Satoshi solved the riddle and published the white paper on Halloween 2008.

SATOSHI NAKAMOTO

Satoshi Nakamoto described Bitcoin as a peer-to-peer electronic cash system in his seminal white paper. The white paper laid out the idea of cryptocurrency and the underlying technology of blockchain.

It is a relatively short paper, nine pages, for its incredible impact.

Check it out, and don't be intimidated by the technical details. Here is the abstract at the beginning of the paper which summarizes its goals.

Bitcoin: A Peer-to-Peer Electronic Cash System
     Satoshi   Nakamoto
satoshin@gmx.com www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online

payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

There is a statue of Satoshi in a park in Budapest. Here is a photo of the statue with the two sculptors. Notice the vague features.

Satoshi Nakamoto Statue in Budapest

Satoshi Nakamoto, the pseudonymous creator of bitcoin, is now the 15th wealthiest person in the world. Nakamoto's net worth is estimated to be up to $73 billion, with crypto holdings in the region of 750,000 to 1.1 million BTC.

Satoshi Nakamoto is the name used by the person or persons who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original implementation. Nakamoto also devised the first practical

blockchain database application as part of the implementation.

Blockchain was co-invented in the early 1990s by Stuart Haber at Bell Labs. Bell Labs has been at the forefront of technological invention throughout the 20th century.

Another powerful part of this story is that this original computer code and implementation have not changed or been updated for the past more than a decade. As a result, it has been running Bitcoin flawlessly as it has expanded both in the number of coins issued, buying and selling transactions, and the value of each coin.

These are monumental accomplishments that many brilliant people have adopted, expanded, refined, and invested in to bring manifest the vast implications.

It seems like something out of a science fiction fantasy story. But this is the amazing reality!

CHAPTER 3

CRYPTOCURRENCIES

IT IS difficult to overstate the importance of controlling the money supply and the dangers and risks of mismanagement.

> "Give me control of a nation's money supply, and I care not who makes its laws."

Said Mayer Amschel Rothschild, founder of the Rothschild banking dynasty.

Crypto is about creating a math-based monetary and finance system that eliminates the risks of centrally controlled money supplies.

THE THREE ERAS OF CURRENCY

Chris Dixon, the venture capitalist said there are Three (3) Eras of Currency:

- Commodity Based (Gold)
- Politically Based (Dollar & Fiat)
- Math Based (Bitcoin & Crypto)

Crypto is about offsetting the debasement of fiat money. Government mismanagement of currencies can create hyperinflation and the rapid devaluation of the currency. Even the traditional growth model of inflation at a target of 2% devalues money like a melting ice cube.

Cases of hyperinflation are extreme but have existed throughout history and in countries around the world. And inflation is everywhere, and people will increasingly look for alternatives to government money now that such things exist.

THE THREE CATEGORIES OF CRYPTOCURRENCY

There are three categories of cryptocurrencies:

- Bitcoin
- Ethereum
- Altcoins

They are all called cryptocurrencies, but they differ in their functions and applications. They are all secured by cryptography on a blockchain.

Bitcoin is an asset; it is digital property. Ethereum is more generalized as its blockchain network is based on smart contracts. In addition, the Ethereum chain acts as a Turing complete distributed computer. Altcoins expand and refine both concepts.

Cryptocurrencies are digital tokens that use cryptography (where the Crypto comes from in the name) to secure transactions and control creation of new tokens. Each transaction is encrypted and added to a ledger held over a distributed network of computers (the blockchain).

THE DEMATERIALIZATION OF THE GLOBAL MONETARY SYSTEM.

Cryptocurrencies are decentralized, meaning they are not controlled by governments or financial institutions. For example, Fiat currencies are money issued by governments. Cryptocurrencies are math-based money. Calculations are required, and computers must crunch numbers to validate transactions and issue coins or tokens.

Cryptocurrencies use blockchain technology, a decentralized public ledger that records transactions.

. . .

Bitcoin (BTC) and Ethereum (ETH) are the most prominent. They are used for payments, investments, and as stores of value. However, applications can use cryptocurrencies and blockchain technology for various other applications such as smart contracts, decentralized finance (Defi), supply chain management, voting and governance, healthcare records, and lots more. A new generation of creative applications and tokens are making novel and valuable use cases every day.

In the developed world, banking systems function relatively well, and the value of cryptocurrency and DeFi is not as immediately apparent. But billions of people are not banked and don't have access to the convenience and protection of their money that banks represent in doing transactions.

Also, countries suffer from high inflation where the local currency is eroding in value and hurting regular folks.

There is also value for businesses. Finance companies didn't design credit cards for the internet. Crypto transactions cost less and cannot be reversed in the way credit-card transactions can be. This tamper-proof quality is vital for firms selling to customers in countries known for credit-card fraud.

Trading coins and tokens aren't the important part. Look for projects that add real value and solve real problems in innovative ways. Look for utility and value-added by projects powered by tokens.

.   .   .

Tokens and blockchains that follow Ethereum's idea of a Turing complete blockchain capable of developing and supporting smart contracts create valuable use cases and solve real problems. Rather than use blockchain tech to power the tokens, these applications use the tokens to power the blockchain by incentivizing the validators.

It's not about just cryptocurrencies but projects built with cryptos. That's where the sustainable investment returns are to be found. They also make more sense as investments and aren't simply speculative objects.

INFLATION HEDGE OR TECH STOCK?

Whether cryptos are an alternative to gold, an inflation-fighting store of value, or a risk asset that behaves more like an emerging tech stock is a hot topic among investors. This is a key question now since increasing interest rates are wreaking havoc for growth stocks.

Proponents of Bitcoin believe that because of its finite supply and decentralized structure, policymakers are unable create and depreciate it like fiat currencies. By this logic, cryptos should be able to withstand inflation and preserve their buying power.

Meanwhile, skeptics point to Bitcoin's price activity, which suggests that this asset class is performing more like a tech stock than an inflation-fighting store of value, at least so far.

. . .

These competing forces and ideas will shake out over the next decade.

It is a good bet that Bitcoin, the founding cryptocurrency and largest by market value, is going to remain at the center of the crypto ecosystem.

Bitcoin as a store of value mechanism is referred to as digital gold. Let's take a look at gold next and its properties to get a better idea about what digital gold might mean.

CHAPTER 4

GOLD

ALL THAT SHIMMERS may not be gold (including gold)
   Is gold losing its luster as a store of value?

"We study history not to know the future but to widen our horizons, to understand that our present situation is neither natural nor inevitable and that we consequently have many more possibilities before us than we imagine." Yuval Noah Harari

---

Gold has been valued as a precious commodity for millennia. No wonder it retains consensus as a store of value. It has stood the test of time.

. . .

But gold has lost some of its investment allure.

It has been a less reliable hedge against inflation than inflation-protected Treasuries (TIPs). Moreover, gold is less exciting than Bitcoin as a store of value removed from the whims of governments and fiat currency mismanagement.

Inflation is surging, central bank money-printing has run amok, and political tensions between the world's powers intensify. These ingredients sound like the alarm bells for ardent believers in the long-term promise of gold. As a result, it is even tempting mainstream investors to increase their precious metal holdings. So why then did gold record its worst annual performance in six years?

Valuing gold poses problems because it is not an income-producing asset. It doesn't generate a stream of income, and the cash-flow models we have learned to determine whether assets are cheap or expensive can't be applied.

Demand for gold tends to be speculative.

The answer for investors would once have been clear. Overconfidence in the safety of paper money and govern-ment-issued bonds often leads to catastrophic breakdowns of financial institutions. The argument goes that gold, on the other hand, has stood the test of time. Only in 1863 did

the dollar become the United States' official currency. For millennia, people have valued precious metals.

However, gold's position as the last defense against currency manipulation is now being questioned. Bitcoin and other cryptocurrencies are becoming more mainstream as investment holdings. The asset class used to be too small to impair gold's demand. The two most popular cryptocurrencies, bitcoin, and ether, now have a combined market valuation of ten times what it was two years ago. Based on the World Gold Council's estimate of a little over 200,000 tons of gold above ground, that's about a tenth of the estimated $12 trillion in gold assets.

As Bitcoin increases in value at gold's expense as a store of value, gold may end up as an ornamental metal.

Bitcoin's volatility and extreme price swings may discourage more conservative investors for the time being. However, this does not have to be a show-stopper in the long run. For example, gold began its existence as a modern financial asset in the mid-1970s with episodes of high volatility. Furthermore, it took almost two decades for gold to become extensively owned by institutions in America after its ownership was made legal in 1974.

Gold has found itself in an uncomfortable situation, sandwiched between more solid, stable assets on the one

hand and more exciting, speculative crypto assets on the other.

Crypto, like gold, is built on a collective belief about its value. But so, to an extent, are all asset prices.

CHAPTER 5

THE CRYPTO ECOSYSTEM

WE HAVE A LOT TO LEARN, unlearn, and relearn.

Photo by NASA on Unsplash

Futurist Alvin Toffler once said,

> "The illiterate of the future are not those who can't read or write but those who cannot learn, unlearn, and relearn."

Now is one of those times when a new paradigm arises, and we can rethink how we want to live in relation to institutions, companies, money, and more. The future is here, and it is lumpy and not evenly distributed.

Take some time and focused effort to understand cryptocurrencies, blockchain, and smart contracts. The evolving crypto ecosystem is like personal computers in the '80s, the internet and web in the 90s, and mobile in the 2000s.

Entrepreneurs, economists, software engineers are diving in and creating apps that remove go-betweens, intermediaries, and friction. This disintermediation is the promise of blockchain and smart contracts. It is transforming industries like banking, insurance, gaming, corporations, online advertising, and the web.

Most times, the entrepreneurial spark comes from envisioning how the world could work versus how it does now. In other words, the opportunity to create something better comes from observing something broken or that doesn't work the way you believe it should.

.   .   .

The initial innovations and developments are centered around available activities ripe for disruption because they command outsize profits and operate inefficiently. For example, we can't make bank transfers on weekends, and they take several business days. Stock Markets only operate during weekday working hours. Visa and MasterCard make 60% profit margins. The list of inefficiencies, inconveniences, and outsize rents goes on and on.

Creating improvements in existing systems is called skeuomorphic applications. Steve Jobs coined the word skeuomorphic to explain the concept of taking a real-world application and creating a digital version that incrementally improves on the old way of doing things. Skeuomorphism makes objects familiar to users by using concepts they recognize.

The next step will be creating native applications. Native applications are only possible in the new environment. This step will be where entrepreneurs will release blockchain's immense potential value, and waves of adoption will occur.

We are still making skeuomorphic applications, but apps native to blockchain are evolving.
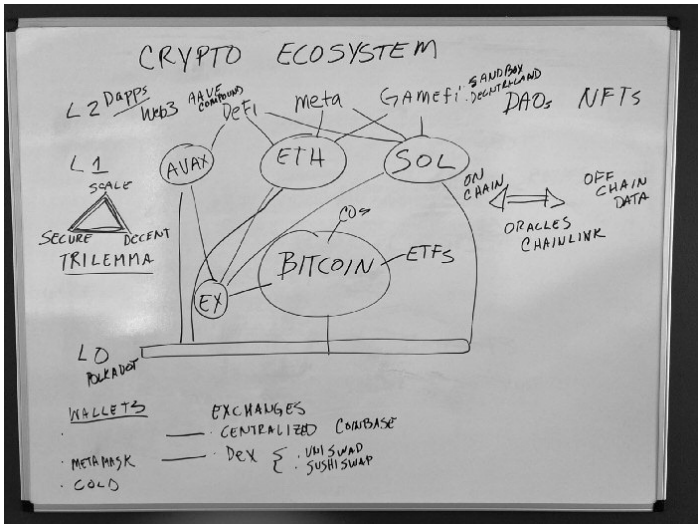
The Crypto Ecosystem

THE CRYPTO ECOSYSTEM CONTAINS:

Layer2 Dapps

- Metaverse: Facebook Meta, Microsoft, Google, Decentraland (MANA) and the Sandbox (SAND)
- Browsers: Brave Browser (BAT)
- DeFi. Lending: Aave, Compound,
- GameFi. Decentraland and the Sandbox
- Distributed Autonomous Organizations DAOs
- Non Fungible Tokens NFTs
- Web3

Layer 1 Blockchains Trilema Scale, Decen-

tralized, Security. Also, cost and speed constraints.

- Bitcoin
- Ethereum and Ethereum 2.0
- Avalanche
- Solana

Layer 0 Interoperability:

- Bridges
- Polkadot (DOT)

Tokens

On and off-chain integration. Oracles. Chainlink

IT STARTED WITH BITCOIN.

There is still criticism that Bitcoin will go to zero because it has no inherent value. For example, it doesn't have gold or diamonds backing it up, and no governments say they will exchange crypto for their fiat currencies.

But gold and diamonds are not inherently valuable. We value them because they are rare, and we find them attractive. However, you can't eat them, wear them, or build with them.

. . .

The original cryptocurrency bitcoin is now considered digital gold. Bitcoin is a store of value with some beneficial characteristics because it is uncorrelated with the fiat currency economies.

Ethereum was the first successful attempt at expanding the functionality provided by a Turing complete blockchain to provide usefulness across multiple domains. However, its success uncovered some rate-limiting issues as it has scaled up in popularity and use cases.

The Ethereum blockchain was, until recently, the unquestioned hub of smart-contract-based activity. It was developed in 2015 as a more general-purpose bitcoin alternative.

The database connected with Bitcoin keeps the information about transactions in the associated cryptocurrency, proving who owns what at any given time.

More information, such as computer code, is stored in the Ethereum blockchain. An application that developers can program in code is guaranteed to work as intended, eliminating the need for a middleman. However, much as Ethereum improved bitcoin, it is currently being supplanted by newer, more advanced technologies. The battle recalls the battle between computer operating systems.

.   .   .

Now the second generation of token-driven blockchain companies aims to solve these issues creatively and focus on particular use cases to be efficient and compelling. These address problems in the original blockchains and address issues in the traditional financial ecosystem.

A leading indicator value of a cryptocurrency is how many developers are actively involved in developing on its chain. GitHub repositories and activity is a way to gauge this activity as a proxy of interest and value in the token.

This approach brings real underlying value to these tokens and projects.

I see the promise and practical benefits, and I want to share what I am discovering. I am just a few steps ahead of what I'm reporting, and I'm quickly learning more every day. Like the adage about the person with only a fourth-grade education when asked, "what are you going to do with a fourth-grade education?" replied, "teach third grade."

Here are some of the more exciting tokens and blockchain projects filling these needs and creating new opportunities as the crypto ecosystem evolves, develops, and fills out. Check them out and DYOR: Do Your Own Research.

- Avalanche AAVE
- Chainlink. LINK
- Polkadot. DOT

- Solana. SOL
- Polygon. MATIC
- Brave Browser. BAT
- Uniswap

Blockchains are secured by cryptography. Bitcoin and Ethereum use Proof of Work as their consensus mechanism to solve cryptographic math problems in a decentralized way. Decentralization means lots of nodes (computers) providing cryptographic computation services in exchange for the possibility of getting paid. Only the winner, the first to correctly solve the math problem, gets paid with proof of work. This winner take all scenario is inefficient and unfair and is a function of the price remaining high enough to attract and incentivize miners.

But this model of decentralized and distributed computational resources not controlled by a central authority or central computer or centralized cloud points to a more general benefit that didn't exist before the internet and now blockchain and tokens. Blockchains can act like a big worldwide computer (Turing complete) incentivized to do work and allocate resources through tokens. Turing completeness through smart contracts was the significant innovation of Ethereum.

The history of modern computing is a constant struggle between decentralizers and recentralizers. In the 1980s the shift from mainframes to personal computers gave more power to individual users.

· · ·

Blockchains invert the traditional relationship between hardware and software.

The significant issues to keep in mind about how different blockchains and tokens fit into the ecosystem surround these concepts:

- Decentralization
- Scale. Size and speed
- Security
- Consensus mechanism
- Transparency

DAOs with AI guidance might overcome partisanship and other organizational and governmental frictions and disfunction.

Trading coins and tokens aren't the important part. Look for projects that add real value and solve real problems in innovative ways. Look for utility and value-added by projects powered by tokens.

Tokens that follow Ethereum's idea of a Turing complete blockchain capable of developing and supporting smart contracts are where the use cases are. Rather than use blockchain tech to power the currency, use the currency to power the blockchain.

. . .

It's not about just cryptocurrencies but projects built with cryptos. That's where the best returns are surfaced. They also make more sense as investments and aren't simply speculative objects.

Identify and research the infrastructure companies and all the other plumbing and picks and shovels of the industry.

Bitcoin is different. It is digital property. Bitcoin is protection from the struggle between deflationary and inflationary forces in the world's economies.

Software is eating the world. Technology makes things cheaper, more powerful, and dematerializes objects like cameras, film, mail, fax machines, recording studios, and tons more. This deflationary process undermines central banks and their managed inflation target of 2% to spur growth in the economy.

Technology makes things cheaper. Deflationary. Our current system is based on prices going up for growth — inflationary based on credit. The two approaches are opposed and are in a titanic struggle.

CHAPTER 6

LEDGERS MATTER

BLOCKCHAINS ARE a mechanism to store transactions.

Photo by Jeremy Bezanger on Unsplash

Blockchains and Bitcoin can seem so challenging and technical but its really built on an old system of debits and credits in a bookkeeping ledger.

Blockchains are a double-entry ledger system like double-entry bookkeeping, which is the basis of accounting.

Accounting is actually quite brilliant and there is a good argument that it spurred the Renaissance and thus the modern world.

But that's a story for another post. Suffice it to say one of the greatest thinkers and writers **Johann Wolfgang von Goethe** called double entry accounting,

> "among the finest inventions of the human mind."

I bet he would get a kick out of blockchain and distributed ledgers secured by cryptography and invented in anonymity.

Double entry bookkeeping was the intellectual achievement of the 14th century that created the banking dynasties that fueled and financed the Renaissance.

. . .

The distributed ledgers of blockchains are its latest incarnation. It is the basis of banking and financial markets and business.

The blockchain can act as a payment system. A payment system is a method to amend and record changers in ledgers for money.

Coins and tokens are used as money in crypto on a blockchain.

Ledgers Matter

THE CHARACTERISTICS OF A GOOD LEDGER ARE:

- Immutable and tamper-proof
- Time-stamped. When transactions take place.
- Document the counter-parties to transactions
- Accuracy

In our current banking, we make deposits and withdrawals. We use debit and credit cards to record the ledger activity. We also use checks to record a transaction.

The salient information on a check is:

- Date (timestamp)
- Signature
- Payer and payee

- Account number and routing number
- Amount

This information is what is stored in the blockchain to record each transaction.

CHAPTER 7

DX UX

DEVELOPER INTERFACE (DX) AND USER INTERFACE (UX)

Photo by Sigmund on Unsplash

WE ARE all familiar with how important it is for an app, phone, website, or any consumer-facing product or service to have a good user interface.

It is also critical for platforms to design a good development interface to attract and retain developers and coders to create applications for the platform.

The more valuable and innovative applications, the more users gravitate to that platform. As a platform becomes more popular, this acts as a flywheel to attract more developers and users into its orbit. The network effects of more users increase the value of the platform.

A leading indicator of the value of a cryptocurrency is how many developers are actively involved in developing on its chain. Therefore, the crypto network that draws the top developers to create apps will generate network effects and become the ultimate victor.
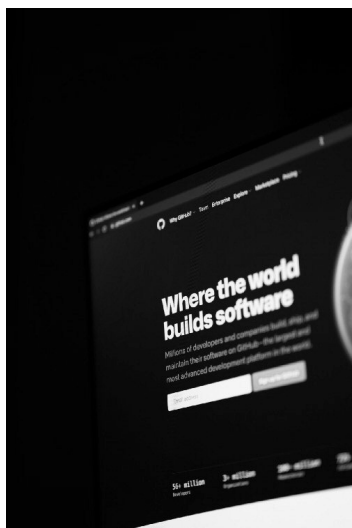
Photo by Mohammad Rahmani on Unsplash

The number of **GitHub** repositories and activity is a way to gauge this activity as a proxy of interest and value in the token.

Creating an interface and programming that is comfortable to developers is critical in attracting the best developers.

CHAPTER 8

WHAT IS A BLOCKCHAIN?

BLOCKCHAIN TECHNOLOGY IS the underlying infrastructure of cryptocurrencies.

Photo by Launchpresso on Unsplash

Blockchain is a shared database that differs from traditional databases in how data is stored. Information is kept in blocks, which are cryptographically linked together.

. . .

Blockchains are a form of ledger that is managed collectively by its power users rather than centrally by a single entity like a bank controls all of its customers' accounts.

As new data is generated, it is entered into a new block as it arrives. When the block is filled, it is chained to the previous block, forming a chronological data chain.

Blockchains may hold various data, but the most popular application has been as a transaction ledger.

Blockchains are deployed in a decentralized manner, meaning that no single person or group has oversight. Instead, all the users collectively do this through consensus.

Decentralized blockchains are immutable, meaning that the data cannot be changed. This tamper-proof quality means that transactions are forever recorded and transparently accessible to everybody.

A blockchain is a distributed database. It's a decentralized ledger in which data is stored in digital blocks. Once a block is confirmed valid and added to the chain, the chain can't be altered. Thus, blockchains offer transparent public records of unchangeable data.

Photo by David Pupaza on Unsplash

Many different blockchains feature varying degrees of decentralization, efficiency (speed and ability to scale), and security. In addition, many have their native cryptocurrency or tokens. Ether, for instance, is a cryptocurrency based on the Ethereum network, and bitcoin is the currency built on the Bitcoin blockchain.

Some Altcoins are built on top of the Ethereum blockchain, these are called Layer 2 altcoins, and some are built on their own proprietary blockchains and have properties that expand and refine Ethereum.

Transactions on blockchains are finalized only when a new bundle of transactions, called a block, is accepted by the

network. Adding blocks takes around ten minutes on Bitcoin and 13 seconds on Ethereum. Newer blockchains are designed to address speed and expense issues related to handling large-scale use cases and competing with financial entities like Visa and NASDAQ in transaction volume and speed.

These newer blockchains and their attendant altcoins are called third-generation blockchain platforms; Bitcoin is the first generation, and Ethereum is the second generation.

Blockchain technology enables peer-to-peer transfer of digital assets without an intermediary. This disintermediation is disruptive to the banking and financial industry, which traditionally has held our transaction ledgers since the Medici in Renaissance Florence. That banking revolution fueled the renaissance. So how will this innovation transform our world in the future?

The record of cryptocurrency transfers on a blockchain cannot be altered or hacked. It is stored across multiple computers in a distributed network system secured by cryptography. With cryptocurrencies and blockchain, transactions are transparent and cannot be manipulated.

Blockchains are databases distributed over many computers and kept secure by cryptography.

. . .

Bitcoin is a cryptocurrency that acts as digital property and is a store of value. Bitcoin is referred to as digital gold. Ethereum is a blockchain network that acts as a Turing complete computer system using smart contracts built in a coding language called Solidity. Bitcoin and Ethereum differ in how their blockchains record events in the database. Bitcoin is a transaction ledger. Ethereum is a balance ledger.

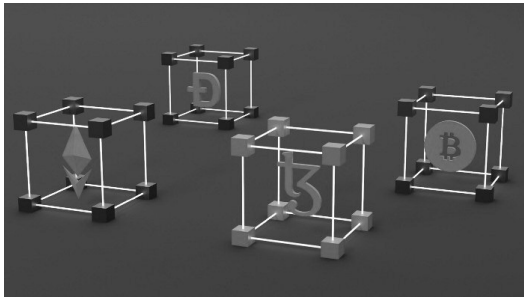Third-generation Altcoins expand and refine both concepts.

Photo by Shubham Dhage on Unsplash

So, what is a blockchain?

Blockchains are databases distributed over many computers and kept secure by cryptography.

A blockchain is a sequential log of events or data that is tamper-proof. It is a time-stamped append-only log. Append only means you can't go back and change transactions already recorded.

.   .   .

Blockchains are secured by cryptography. Cryptography is the science of communication in the presence of third parties or adversaries. It's how we make secret codes. For example, the Enigma machine was the Nazi cryptographic device that they thought was tamper-proof and that the Poles and English decoded.

The data in a blockchain can be a value like Bitcoin, or the data can be computer code like smart contracts as in the Ethereum chain.

We know what a ledger is from accounting. A ledger is a log that records all the transactions of an entity like a company and uses double-entry accounting of debits and credits.

For every asset transaction, one account gains (debit), and one account is reduced (credit), and vice versa for liabilities. If this is confusing, take my accounting course.

In traditional accounting, there is one set of books, the ledger. A Blockchain is a distributed ledger where all the nodes or computers have a complete set of books and verify through consensus when a new block of transactions is recorded.

.   .   .

It has taken seemingly long to adopt because blockchain is an exponential technology. Those usually tend to trend up very slowly at first and then accelerate at an astonishing pace.

It seems long, but it has only been a little more than a decade since Bitcoin was invented. It is now a digital network with a value of over $1 trillion. Only four other companies, all essentially digital networks, are valued over $1 trillion: Amazon, Apple, Microsoft, and Facebook.

All four took way longer than a decade to reach that value threshold.

Crypto and blockchain are also so different and new that it is challenging to get our minds around the concepts and applications at first.

There have also been some epic speedbumps and screwups along the way, like the early failure of crypto exchange Mt. Gox and the nefarious activity of the Silkroad trading website.

BLOCKCHAIN IS A SOLUTION THAT ADDRESSES A BIG PROBLEM.

The idea of money created and transacted on blockchains came about in the aftermath of the 2008 financial melt-

down and crisis. It is essentially a response to fixing a fragile system that incentivizes risky behavior.

The concept of Moral Hazard is from economics. It describes a situation where an economic actor has an incentive to increase its exposure to risk because it does not bear the total costs of that risk. For example, moral hazard is a fundamental problem of "too big to fail" financial institutions like investment banks that bonus individuals for risky trades and investment practices.

There is also Counterparty risk and other risks. For example, money printing by governments to pay debts in devalued currency, inflation, and other risks created by centralized financial control systems are addressed by blockchain-based cryptocurrencies.

Besides addressing risky behavior, the crypto ecosystem aims to reduce costs. The financial system represents 7.5% of economic activity, and transaction fees are generally 2–3% and take more time than is necessary. Credit card companies enjoy 60% gross profit margins. These are excess rents that are ripe for disruption.

The anonymous Satoshi Nakamoto penned the Bitcoin white paper that started it all. Still, Satoshi didn't invent blockchain technology, although Satoshi codified the most compelling use case, so far, for blockchain.

. . .

In 1991, scientists at Bell Labs conceived blockchain as a research project. The blockchain concept predates Bitcoin, which was first implemented in 2009. For blockchain technology to work in practice, it needed the internet to become mature.

Blockchains like Ethereum and Bitcoin run as layers on top of the internet.

Blockchain technology also needed computer hardware and software to develop the speed and capacity to handle the storage and cryptographic number-crunching requirements.

SECOND GENERATION BLOCKCHAIN: ETHEREUM, TURING COMPLETE, AND SMART CONTRACTS

The benefit of implementing a blockchain like Ethereum is that it functions equivalent to a new type of computer. A physical computer stores data and manipulates it using a set of instructions known as a program. These criteria are known as "Turing Complete" after Alan Turing, who first defined a computer's fundamental criteria. A Turing-complete language (also called a universal language) is one where you can compute anything that any other computational method can compute.

Photo by Kanchanara on Unsplash

A blockchain can operate as a Turing complete computer distributed over many connected computers. This world-wide computer is the revolutionary concept behind smart contracts and Ethereum.

Smart contracts can execute any contractual condition or function. Furthermore, they are Turing-complete, meaning that they use programming languages with conditional statements and conditional branching. These programming languages have "if, then, else" and can replicate any computer logic.

The Ethereum blockchain, like a virtual computer that runs on top of a network of actual computers, provides a mechanism to store and execute data. As a result, the computer will continue to function as intended and will not be controlled by the whims of a central organization.

DECENTRALIZATION

A person or organization controls every computer outside of a blockchain. That entity can change their mind. This control sometimes operates at the physical hardware level. Apple, in many ways, retains broad authority over the devices it sells through its ability to push software updates like how it neutered Facebook's trackers. More importantly, this applies across all web pages and applications. For example, each time someone logs on to Facebook, they rely on server farms run by Facebook hosting its service. Companies can change the software as they wish by controlling the hardware.

However, the relationship is flipped on a blockchain: the software regulates the hardware and may make commitments. In addition, **blockchain-enabled computers can make guarantees**. A central controlling agent can't tamper or change the game's rules. This arrangement removes or at least drastically reduces counter-party risk.

If you have ever dealt with making a claim to an insurance company, you know what counter-party risk is.

KEY TAKEAWAYS

- Blockchain is a shared database that differs from traditional databases in how data is stored. Information is kept in blocks, which are cryptographically linked together.

- New data is entered into a new block as it arrives. When the block is filled, it is chained to the previous block, forming a chronological data chain.
- Blockchains may hold various data, but the most popular application to date has been as a transaction ledger.
- Blockchains are deployed in a decentralized manner, meaning that no single person or group has oversight, all users collectively do.
- Decentralized blockchains are immutable, meaning that the data cannot be changed. This tamper-proof quality means that transactions are forever recorded and transparently accessible to everybody.

CHAPTER 9

THE BIG PICTURE AND IMPLICATIONS.

QUESTIONS ASKED THE WRONG WAY

Photo by Ana Municio on Unsplash

DISCUSSIONS ABOUT CRYPTO can devolve into superficial speculation about trading coins and guessing trends on price. Still, crypto is about big ideas and questions that challenge our thinking, beliefs, and assumptions about modern life.

Learning about it not only helps us navigate the future but widens our horizons and helps us understand that our present situation is neither natural nor inevitable and that we have many more possibilities before us than we imagine.

Blockchain and its applications like Cryptocurrency, NFTs, DeFi, Metaverse, and DAOs reside in a conceptual space that intersects political science and governments, technology, Finance and business, money and value. It is at the intersection of Economics, Finance, Technology, and Cryptography.

As Marc Andreessen said,

> "Crypto represents an architectural shift in how technology works and therefore how the world works."

Marc invented the web browser, so he has seen this type of paradigm shift before.

. . .

Crypto is fascinating because it makes us question many basic assumptions about how a society functions and transacts.

Crypto is about big ideas that only now are practical because the technology has sufficiently advanced to implement them. It is challenging us to shift the fundamental organizing principles of our societies.

By revisiting and questioning our fundamental beliefs, we have an opportunity to add a new layer to make the world of humans function better, fairer, and more efficiently.

We have social problems that seem intractable, impossible to solve.

> "Problems that remain persistently insoluble should always be suspected as questions asked in the wrong way." — Alan Watts

Crypto forces us to revisit our assumptions and beliefs and ask new questions.

It holds huge promise for the developing world and for the billions of people who are unbanked.

. . .

Crypto is also about offsetting the debasement of fiat money. Government mismanagement of currencies can create hyperinflation and the devaluation of currency. Even the traditional growth model of inflation at a target of 2% devalues money like a melting ice cube.

Another goal is to replace intermediaries like global banks and tech platforms with software built on top of networks that direct the value they generate back to the users who own and run them. This evolution could go a long way to combatting misinformation and clickbait driven by advertising models of revenue generation. With Web3, we can ditch the ad-based business model and build a better web.

Chris Dixon says, "Web3 combines the decentralized, community-governed ethos of Web1 with the advanced, modern functionality of Web2". Sounds good.

Only puny secrets need protection. Big secrets are protected by public incredulity.

Our current ideas and beliefs, and assumptions surrounding money, corporations, the role of governments and artists, are deeply embedded in our psyches and not easy to change. It's like the matrix. We think money, banks, governments, and fiat currencies are natural laws. But it's all human constructions and supported by collective agreement.

. . .

There are a lot of topics to cover in the crypto ecosystem and they all require an open and curious mind to entertain.

Crypto is a paradigm shift. A paradigm shift is a concept introduced in the book The Structure of Scientific Revolutions by Thomas Kuhn. In the book Kuhn proposes that progress isn't steady but goes in fits and starts as we try to hold on to outdated models and resist new ones. Think about Copernicus and the Earth not being the center of the universe. Crypto represents a similar paradigm shift in our thinking about how money, governments, and commerce function.

The future is here but it's lumpy and uneven and not evenly distributed. Stay tuned.

CHAPTER 10

SATOSHI'S DREAM CHILD

INFLATION IS EVERYWHERE, *and people will increasingly look for alternatives to government money.*

Photo by Илья Мельниченко on Unsplash

It has taken me more than a decade to digest just how ingenious Bitcoin is. Its like when you first go to a foreign country and realize how many things you took for granted are just socially accepted conventions. Bitcoin, cryptocur-

rencies and blockchain are like that for rethinking money, property, governments, and lots more.

Bitcoin was first.

Bitcoin is the first cryptocurrency. It was created in 2009 under the alias Satoshi Nakamoto by a person or group of persons. Twenty-one million bitcoins can ever be issued, and around 19 million are already in circulation.

Bitcoin is the only economic entity where the supply is unaffected by the demand. Bitcoin's hard cap is set at 21 million coins. Bitcoin's block reward is paid out to miners who secure the bitcoin blockchain. and

Bitcoins can be issued to anyone with a powerful computer: it mints them by solving complicated mathematical problems. The problems are automatically made harder to ensure that the overall supply of Bitcoins cannot grow too fast.

Bitcoin is traded and exchanged online, with transactions cryptographically authenticated and stored on the blockchain.

Shortly after the currency launched in 2009, articles spread around the internet saying that Bitcoins would protect wealth from hyperinflation and that early adopters would make a fortune.

Bitcoin was the first practical cryptocurrency to work and gain traction. However, many earlier attempts failed because the technology wasn't there yet, and they lacked one or another of the critical components that made bitcoin work.

Bitcoin has a predictable supply. There is a limit on how many bitcoins will ever be created. Twenty-one million bitcoins will be made, of which 19 million have been created. Bitcoin value, like gold, is governed by scarcity.

The bitcoin protocol is based on:

- *Peer to peer networking*
- *Proof of work consensus mechanism*
- *Public key cryptography*

A pair of keys known as a public key and a private key (a public key pair) are associated with an entity that needs to authenticate its identity electronically using public-key cryptography. Each public key is made public, but the private key is kept private.

The generation of such key pairs depends on cryptographic algorithms based on mathematical problems termed one-way functions.

Photo by Bermix Studio on Unsplash

Public key cryptography is how cryptocurrency wallets work and store our crypto assets. Keep your private key information in a safe place. Don't share your private key as then that person has access to your storage, and don't lose your private key information. There are many stories of

people who forgot their private keys and can no longer access their cryptocurrency. There is a famous saying,

"not you key not your coins."

Bitcoin is a mechanism to store transactions. It is a transaction ledger as opposed to a balance ledger like Ethereum.

It is a double-entry ledger system like double-entry bookkeeping, which is the basis of accounting.

Double-entry bookkeeping was the innovative technology of the 15th century that helped finance and usher in the renaissance. It is the basis of banking and financial markets and business.

The bitcoin blockchain is a payment system. A payment system is a method to amend and record changers in ledgers for money.

Bitcoin's proponents cite its limited supply and decentralized nature as protection from policymakers and central bankers printing up more and depreciating it like fiat currencies. For example, since March of 2020, the Federal Reserve has issued 40% of all US dollars ever created. That is a very significant increase in the money supply.

Photo by Blogging Guide on Unsplash

Bitcoin is supposed to weather inflation and retain purchasing power. But unfortunately, inflation is everywhere, and people will increasingly look for alternatives to government money.

But crypto skeptics point to Bitcoin's price action that suggests this asset class is acting more like a tech stock than an inflation-fighting store of value.

Time will tell.

CHAPTER 11

THE ELYSIAN FIELDS OF ETHEREUM

COULD *we be on the threshold of techno utopia?*

Photo by Iñaki del Olmo on Unsplash

If the implications of blockchain's potential come to fruition and create a juster, fairer society, the innovations baked into Ethereum will be thought of as the inflection point.

Blockchain's potential to facilitate more than payments

became more apparent with the creation in 2015 of the Ethereum blockchain. The Ethereum blockchain stores and records lines of computer code, including entire programs, which are visible to all.

This innovation enables the creation of smart contracts. Smart contracts are self-executing agreements in which a chain of actions follows when certain conditions are met. These are automatically enforced and tamper proof.

This math-based tamper-proof quality removes third-party and counterparty risks.

You must pay a fluctuating "gas" fee in ether to verify a transaction on the Ethereum network. That is the incentive like Bitcoin's miner payments. Gas fees fluctuate based on the network traffic and capacity.

The Ethereum blockchain is designed to store lines of code. It and others like Cardano and Avalanche, issue and use their own tokens. Ethereum's is called "ether." Cardano's is called "ada" and Avalanche is named "avax".

Ada is a nod to the proto-computer scientist Ada Lovelace who created the first computer in the 1850s with Charles Babbage. She was the daughter of the famous poet Lord Byron.
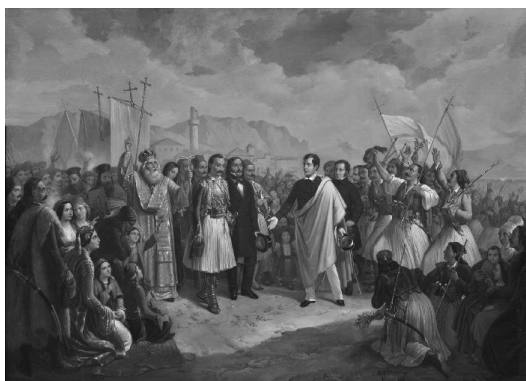
Photo by Europeana on Unsplash

Cardano is also a reference to a famous mathematician Gerolamo Cardano. These references point to the math-based nature of cryptocurrencies.

Think of money as having three eras through history as we have evolved. The first is commodity-based currencies like gold and silver. The second is government-based fiat currencies like the dollar, euro, and yen. Governments and guns back these fiat currencies. The third era we entered a decade ago is math-based currencies: cryptocurrencies.

Ethereum is the second generation of blockchain. Bitcoin was the first and is based on using the blockchain as a transaction ledger for digital property. Ethereum built on expanding the applications that could reside in a blockchain to include computer code in the form of smart contracts.

The Ethereum blockchain acts as a Turing Complete distributed computer. A Turing Complete computer is considered a machine programmed to carry out arithmetic or logical operations automatically.

Photo by Mauro Sbicego on Unsplash

Implementing a blockchain is beneficial because it functions comparable to a new type of computer. A physical computer stores and processes data using a set of instructions known as a program. These criteria are known as being "Turing Complete" after Alan Turing (of Enigma code cracking fame), who first defined the fundamental criteria of what a computer is. A Turing-complete language (also called a universal language) is one where you can compute anything that any other computational method can compute.

Smart contracts can execute any contractual condition or function. Furthermore, they are Turing-complete, meaning that they use programming languages with conditional statements and conditional branching. These programming languages have "if, then, else" and can replicate any computer logic.

Blockchains like Ethereum and Bitcoin run as layers on top of the internet.

Photo by NASA on Unsplash

The Ethereum blockchain, like a virtual computer that runs on top of a network of actual computers, provides a mechanism to store and execute data. As a result, the computer will continue to run as designed and intended.

Every traditional computer is controlled by a person or organization that can change their mind. These proprietary chokepoints are sometimes evident at the physical, hardware level: Apple, in many ways, retains broad control over the devices it sells through its ability to push software updates like how it neutered Facebook's trackers. More importantly, this applies across all web pages and applications. For example, each time someone logs on to Facebook, they rely on the servers the company runs to host its website. By controlling the hardware, companies can change the software as they please.

On a blockchain, though, this relationship is inverted: the software governs the hardware and can make guarantees. Computers controlled by blockchain technology are, in Mr. Dixon's words, "computers that can make commit-

ments." A central controlling agent can't tamper or change the game's rules. This arrangement removes or at least drastically reduces counterparty risk.

If you have ever dealt with making a claim to an insurance company, you know what counterparty risk is.

Ethereum's Turing complete blockchain concept has spurred the development of innovative applications, including decentralized finance (DeFi), decentralized autonomous organizations (DAOs), nonfungible tokens (NFTs), and a slew of layer 2 and third-generation blockchains.

THE ALTERNATE UNIVERSE OF ALTCOINS

POWERING DEFI, Web3, and the Metaverse.
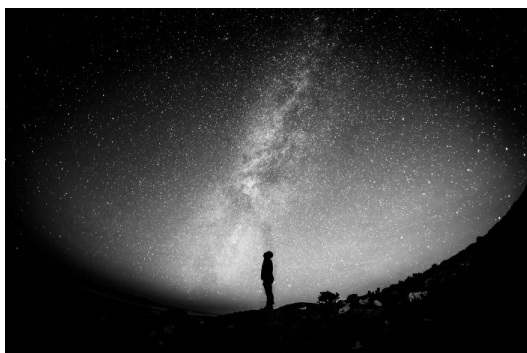
Photo by Greg Rakozy on Unsplash

Altcoins refers to any cryptocurrency that's not bitcoin or ether.

Cryptocurrencies and blockchain technology are

changing the world. But to understand their potential, you need to look past currencies like Bitcoin and Ethereum and towards projects that use cryptos to power decentralized applications (dapps) and decentralized finance or "Defi" products. These new tokens act as incentives and payments for service in these new applications.

Trading crypto can be lucrative and new dispassionate, self-learning trading engines powered by AI are fascinating and exciting. But a sole focus on tokens trading alone is missing the point of crypto. Smart contracts that are essentially computer programs that power decentralized applications and how they are used within projects are the most important use case.
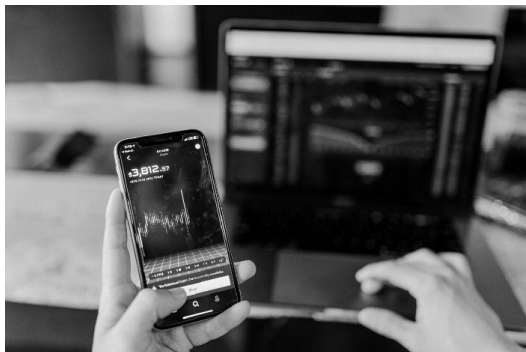

Photo by Austin Distel on Unsplash

Trading coins and tokens isn't the important part. Look for projects that add real value and are solving real problems in innovative ways. Look for utility and value added by projects powered by tokens.

Tokens that follow Ethereum's idea of a Turing complete blockchain can develop and support smart contracts. Rather than use blockchain tech to power the currency, they use the currency to power the blockchain.

There are altcoins and dapps that ride on top of the Ethereum chain. That structure is called layer 2. And there are projects that are built on their own unique blockchain called third generation (Bitcoin is the first generation and Ethereum the second.)
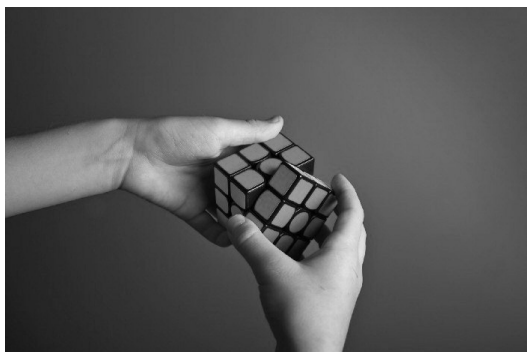
Photo by Olav Ahrens Røtne on Unsplash

A new trend is what's called interoperability, which means where you can migrate from one blockchain to another seamlessly and quick. We are seeing a new ecosystem develop with a new generation of tokens and applications in what is known as the zero layer, the layer underlying the layer one blockchains and interconnecting them.

Photo by Aleksandr Barsukov on Unsplash

There are also bridges being built between different blockchains.

It's not about just cryptocurrencies, but projects and applications built with cryptos on blockchain application layers. These decentralized applications (dapps) also make more sense as investments and aren't simply speculative objects.

Seek out in research the infrastructure companies and the exchanges and all the other plumbing and picks and shovels of the industry.

Here are some to check out and do your own research:

- *Solana* (*SOL*)
- *Avalanche* (*AVAX*)
- *Polkadot* (*DOT*)
- *Chainlnk* (*LINK*)
- *Cardano* (*ADA*)
- *Aave* (*AAVE*)

- *Decentraland* (*MANA*)
- *Polygon* (*MATIC*)
- *Cosmos* (*ATOM*)
- *Algorand* (*ALGO*)

CHAPTER 13

CEX OR DEX? CRYPTO EXCHANGES

EVERYBODY INTO THE POOL!

Photo by Shubham Dhage on Unsplash

HOW DO WE ACTUALLY BUY AND SELL, AND TRADE CRYPTO?

We do it on an exchange.

Photo by Kelly Sikkema on Unsplash

HOW ARE THE PRICES OF CRYPTOCURRENCIES DETERMINED?

Markets are price discovery mechanisms. Exchanges access markets where buys, sells and trades are made to determine an asset's price.

Crypto exchanges trade 24/7 every day, unlike stock exchanges which run during working hours Monday-Friday and are closed on weekends and holidays. There are two main kinds of exchanges for crypto: centralized and decentralized.
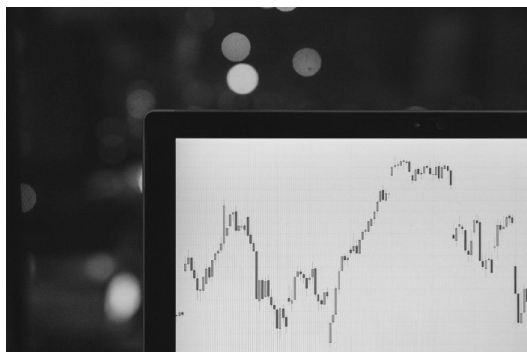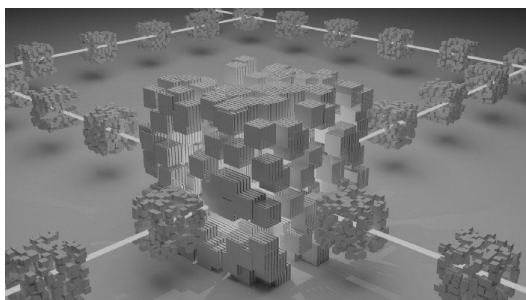
Photo by m. on Unsplash

Order matching, the ability to match buyers with sellers, is a crucial difference between CEX and DEX.

Centralized exchanges (CEXs) are easy to use and come with an attached wallet to store your assets. A CEX is operated by a company that owns it in a centralized way. CEXs offer enhanced liquidity, the ability to exchange one currency for another in a speedy and low-cost manner through deploying their capital and assets, and market makers that have order books and actively trade.

Decentralized exchanges (DEXs) work with no human intermediaries. Some DEXs are governed by a decentralized autonomous organization (DAO) where the holders of the DAO coin vote on decisions relative to the running of the DEX. DEXs trade with a programmed protocol based on functionality programmed on the blockchain in smart contracts.

Photo by Shubham Dhage on Unsplash

Order matching liquidity in a DEX is achieved through a liquidity pool that balances out buy and sell orders. A liquidity pool is a bundle of cryptocurrency assets that are held in a smart contract and can be used for exchanges. Investors lend their crypto to the pool in exchange for a portion of the transaction fees generated by the trading. The underlying smart contract will deliver a "liquidity pool token" representing the liquidity provider's stake when they add their tokens to the pool. They also get a cut of the fees paid by traders who utilize the pool, which is proportional to the value of the liquidity they have risked.

DEFI AND REGULATION

Without identification checks, converting traditional money into tokens is often challenging. Most firms that trade dollars for ether or bitcoin do "know your customer" checks. **(KYC)** checks intended to deter money laundering (AML) anti-money laundering. Yet the fact that anyone can quickly move tokens around once in the on-chain world has raised

legitimate fears about how criminals will use DeFi to launder and move dirty money.

Photo by Samuel Schroth on Unsplash

REGULATORY UNCERTAINTY AND RISK

Financial intermediaries are expected to be on the alert for questionable transactions by regulators, but DeFi rejects this responsibility. In America, for example, the attempt to add a seemingly minor provision to regulate the business in an infrastructure bill was ill-received by the DeFi movement. Fierce opposition to regulation adds to the sense that it is working against the public interest. It may enhance regulators' determination to stifle flows into the on-chain world.

CEX

Centralized exchanges are the easiest to use because their user interfaces are familiar and easy to use.

Popular Centralized Exchanges

- **Binance:** Binance was founded by Changpeng Zhao, known as CZ, a developer who had previously created high-frequency trading software for stock traders.
- **Coinbase:** Brian Armstrong is the founder and CEO. Bilaji Srinivasan is the former CTO and one of the smartest people you will ever meet (check out his two podcast episodes with Tim Ferris for a mind-expanding experience). Coinbase is a Public company.
- **FTX:** Sam Baack Fried is the founder and CEO. FTX specializes in derivatives and leveraged products.
- **Gemini:** Cameron and Tyler, the Winklevoss twins, own Gemini. The company's name is the Zodiac sign of the twins. They are world-class athletes and best known for accepting a $65 million settlement of a lawsuit against Mark Zuckerberg over Facebook.

The founders and CEOs of these four CEXs are all billionaire personalities in the crypto world.

DEX

Decentralized exchanges, or DEXs, operate decentralized or without any interference from third-party control. This form of exchange allows users to conduct peer-to-peer transactions or trade cryptocurrencies with others without entrusting their cash to a third-party custodian or intermediary.

DEXs use AMMs automated market makers to remove

some frictions from trading. An automated market maker (AMM) is a process that enables automated trading to offer liquidity to the exchange in which it operates.

WHAT IS AN AMM?

AMM systems took off after Shearson Lehman Brothers and ATD first implemented them in the early 1990s. Before their invention, order books were managed by humans who manually initiated trades meant to enhance the market's liquidity.

This strategy contributed to some market slippage and slowness in price discovery. Market makers have also been accused of market manipulation. When they were first launched, AMMs remedied all of the problems that human market makers had produced. These systems are now being used in blockchain-based decentralized exchanges.

The traditional order book is replaced on AMM-based decentralized exchanges by liquidity pools that are funded on-chain for both assets of the trading pair. Investors contribute liquidity by staking their coins, and they receive passive income on their deposits via trading fees based on the percentage of the liquidity pool they offer.

One decentralized exchange that has implemented an AMM is Uniswap. Uniswap is an Ethereum-based decentralized exchange that allows users to supply liquidity to earn passive income or exchange between various assets.

A big difference from CEX and important to sophisticated users, DEXs allow users to retain control of their wallet's private keys. Here are some of the biggest decentralized exchange cryptocurrencies.

SushiSwap (SUSHI)

Sushiswap seeks to broaden the AMM and introduce

unique features not previously seen on Uniswap. It launched in September 2020. Its native coin is used to compensate users for their share of the network's fees for transactions that take place in its liquidity pool.

Curve DAO Token (CRV)

Launched in January 2020, Curve is a decentralized exchange for stablecoins that use the AMM to manage liquidity. In addition, it launched a DAO (decentralized autonomous organization) that has CRV as its in-house token.

Loopring (LRC)

It is an open protocol for developing decentralized crypto exchanges that was launched in August 2017. Loopring's stated purpose is to bring the finest of both centralized and decentralized exchanges together.

PancakeSwap (CAKE)

It is a DEX for swapping BEP20 tokens on Binance Smart Chain that was launched in September 2020. Users of PancakeSwap trade against a liquidity pool using an AMM model. Users that put money into the pool receive LP (liquidity provider) tokens in exchange.

Stellar (XLM)

Stellar allows money to be transported and stored, and it was launched in 2014. Its original purpose was to increase financial inclusion, but today its top priority is to help financial firms communicate with one another via blockchain technology. In addition, its native token helps to make the trading of assets less expensive.

Uniswap (UNI)

Uniswap, launched in November 2018, allows for automatic DeFi token trading. Uniswap's goal is to make token trading automated and completely open to all token holders.

Uniswap's governance token was intended to cement Uniswap as a publicly-owned and self-sustaining infrastructure while carefully protecting its autonomous properties, according to the company.

SUMMARY

Exchanges are the on-ramp to crypto investing and trading. Check out their websites and explore their features and functionality. Don't forget your water wings if you decide to dive into a liquidity pool!

CRYPTO GLOSSARY

BLOCKCHAIN **and cryptocurrency phrases you need to know**

Blockchain technology is now widely used. Bitcoin has become well-known, and financial institutions are taking notice and investing in cryptocurrencies or allowing their customers to do so. Meanwhile, NFTs have attracted a lot of media attention.

Despite all of the hype, blockchain technology remains a mystery. It's understood chiefly by technologists and developers, many of whom were early adopters of cryptocurrencies like bitcoin and Ether, and it can be intimidating for the average person.

An alphabetical vocabulary of blockchain words is provided below for your convenience. It's not a complete collection of

terminology and phrases, but it covers the essentials to get you started in better comprehending the space.

AIRDROP

When a corporation distributes bitcoin or an NFT directly into your wallet, it is known as an airdrop. Instead of an IPO, blockchain services will issue a token and distribute it to people who have previously utilized the service. Issuers can do this for various reasons, including pure marketing. Airdrops promote awareness of a token that others can then invest in or give governance tokens for a decentralized autonomous organization (DAO).

APING

To "ape" into something is to invest recklessly in the hopes of short-term profit. Of course, everyone knows scams abound, and careful investors research a cryptocurrency or NFT project to ensure its legitimacy. But, on the other hand, to "ape" into a project is to see its value increasing and speculate into it, hoping for the best.

ALTCOIN

Any cryptocurrency that's not bitcoin or Ether.

BINANCE

Binance is one of the world's biggest cryptocurrency exchanges, where people buy and trade cryptocurrencies.

BLOCKCHAIN

A distributed database is a blockchain. To put it another way, it's a decentralized ledger that stores data in digital blocks. Parties cannot change a block once it has been mined and put to the chain. As a result, blockchains provide public records of immutable data.

Decentralization, efficiency, and security levels vary widely among blockchains. Many of them have their native coin or tokens. Ethereum, for example, is a cryptocurrency based on the Ethereum blockchain.

BITCOIN

Bitcoin was the first cryptocurrency to be developed on the blockchain. It was founded in 2009 under Satoshi Nakamoto's pseudonym by a person or group of persons. However, only 21 million will ever be produced, with approximately 19 million already issued.

BURNING

When cryptocurrency is sent to a wallet that can only receive it and not transmit it, it is "burned." Burn mechanics often cause a deflationary impact: the fewer tokens in circulation, the scarcer the ones investors hold become. If Demand stays constant, scarcity of supply drives price higher. At least that is the theory.

BUY THE DIP

Buy the dip refers to buying more of an asset after its price has dropped. A bitcoin holder, for example, might "buy the dip" if the price drops $5,000.

CANDLESTICKS

Green and red bars, referred to as "candlesticks," appear on cryptocurrency graphs that show price movement. Green bars indicate price increases, while red bars indicate price decreases.

COLD WALLET

A cryptocurrency wallet that is not linked to the internet is known as a cold wallet. These are considered safer and less prone to scams.

CROSS-CHAIN

Cross-chain is the ability to send data, tokens, or assets from one blockchain to another. Cross-chain is different from multichain services built to work on multiple blockchains.

CRYPTOGRAPHY

Cryptography is a form of information encryption, where data can only be unencrypted with a key. For new blocks to be mined and validated, several blockchains use proof of work protocols that rely on solving challenging cryptography riddles with powerful computers.

CRYPTOCURRENCY

A cryptocurrency is a native token on the blockchain. Cryptography secures blockchains, hence the "crypto" in the name. With each new block mined, a new unit of cryptocurrency is usually created. Each new block of Ethereum mined, for example, rewards the miner with two ether tokens as compensation.

Tokens are a sort of cryptocurrency. Their native blockchain is what distinguishes them. Other tokens are created utilizing blockchain-based platforms and apps built on top of a layer 1 blockchain, whereas cryptocurrencies are incorporated into a blockchain protocol.

DAPPS

Dapps is short for "decentralized apps."

DAO

A DAO is a decentralized autonomous organization (DAO) that makes decisions by consensus. All governance token holders get a vote in the organization's decisions. The solution with the most votes is the DAO's course of action. For example, consider a decentralized investment bank where, instead of fund managers making investment choices, governance token holders vote on how monies from the fund's treasury are invested.

DECENTRALIZED EXCHANGE

Decentralized exchanges, or Dex, are used to buy and trade cryptocurrencies. Unlike centralized exchanges, these use peer-to-peer transactions that circumvent any centralized authority. Uniswap and Sushiswap are Dexs.

DEGEN

Similar to aping, and short for "degenerate." Investing in anything without completing due diligence is referred to as a "degen play" or "becoming a degen."

DEFI

"Decentralized finance" is abbreviated as "Defi." DeFi refers to any financial tool that leverages blockchain technology to bypass middlemen institutions, such as a smart contract or a decentralized autonomous organization (DAO).

DYOR

Short for "Do Your Own Research." Which is excellent advice.

ETHER

Ether is the token mined on the Ethereum blockchain. Ether is second only to bitcoin in terms of market capitalization, although it is a considerably more widely used cryptocurrency. Most altcoins are based on Ethereum and are hence connected to it. In addition, most NFTs are also built

on Ethereum, which is why Ether is the dominant token used in NFT trading.

ETHEREUM

Ethereum is a competing blockchain to bitcoin. It's intended to take the blockchain technology pioneered by bitcoin's developers and apply it to more advanced financial tools such as smart contracts.

FLASH LOAN

Flash loans are a DeFi tool that allows for loans without collateral. You can borrow money to buy an asset with a flash loan, but only if the asset can be purchased and the interest paid back in the same block.

Flash loans use smart-contract technology and programming.

FUD

Short for "fear, uncertainty, and doubt." FUD can be legitimate, like people airing concerns about a token or NFT project's security or legitimacy, or tactical, as in an organized campaign that encourages people to sell, lowering an asset's price.

GAS

The cost of using the Ethereum network is measured in gas. Every transaction necessitates the payment of a gas fee, which varies according to how busy the blockchain is. Prices usually range from $50 to $500 per transaction.

However, they can rise dramatically during periods of high network traffic.

GOVERNANCE TOKEN

Governance tokens are digital assets that grant their owners voting rights over a project. Also, see DAO.

GWEI

GWEI expresses the cost of gas. Gas will be inexpensive when the GWEI is below 50 and expensive when it is above 100, as a general approximation.

HODL

A purposeful misspelling of "hold " used to encourage investors to hold onto their tokens.

LAYER 1 AND LAYER 2

If you're interested in cryptocurrencies, you've probably heard about Layer 1 and Layer 2. Layer 1 refers to the blockchain architecture itself, while Layer 2 refers to the architecture developed on top of layer 1.

Take Ethereum's high gas costs, for example. Adopting proof-of-stake techniques to make the Ethereum blockchain more efficient is a layer 1 solution. A layer 2 solution is an exchange built on top of Ethereum that uses smart-contract technology to allow gas-free, carbon-neutral trading.

LIQUID MARKET

A liquid market is one with many buyers and sellers, allowing buy and sell orders to be fulfilled almost instantly. NFT markets are not liquid, whereas some cryptocurrency markets are. Legitimate cryptocurrencies can be bought or sold at any time, but NFT traders must publish an item for sale and wait for a buyer to purchase it manually.

MAINNET

Developers will put a blockchain protocol launching for public use in the Mainnet. Mainnet is distinguished from a testnet, which is more like a beta launch of a blockchain protocol for troubleshooting.

MEMECOIN

Many cryptocurrencies are designed to be useful or fulfill a specific function. Memecoins are entirely speculative assets with no potential of usage. The most well-known is Dogecoin, but there are a slew of others.

METAMASK

Metamask is an online, browser-based digital wallet used primarily for transactions on the Ethereum blockchain.

MINING

Mining is how transactions are verified and blocks are added to a blockchain. Mining typically involves powerful computers solving complex cryptography problems. And

more importantly, this is how new cryptocurrency enters the market. For example, when a new bitcoin block is mined, approximately six bitcoins are minted and issued.

MINING RIG

A mining rig is a powerful computer setup for mining cryptocurrencies.

MINING FARM

A mining farm is a warehouse or room of mining rigs that operate mining cryptocurrencies.

MINT

Minting a cryptocurrency means verifying information and lodging it as a block on the blockchain.

Buying an NFT from its creator during a public sale is the same as minting it.

MULTICHAIN

A Multichain app or service is built to work across various blockchains. This isn't the same as cross-chain apps and services developed to send data or assets from one blockchain to another.

NFT

NFT stands for non-fungible token. A token that is not fungible represents the unique private digital property. These are digital deeds that prove a digital asset's owner-

ship. NFTs are currently linked with art, although they can certify ownership of any digital asset.

OFF-CHAIN/ON-CHAIN

Something that exists on a blockchain is referred to as on-chain. While something that does not exist on a blockchain is referred to as off-chain. So, for example, cryptocurrency is on-chain money, and fiat currency is off-chain money.

OPENSEA

OpenSea is the largest NFT marketplace.

PLAY TO EARN (P2E)

Play-to-earn P2E games are blockchain integrated and reward players with an in-game cryptocurrency. Players can then exchange in-game cryptocurrencies for bitcoin or Ether.

PROOF OF WORK

Proof of work (POW) is a mechanism for consensus that adds blocks to a blockchain. POW requires miners to solve complicated cryptographic puzzles to validate new blockchain transactions, which demand large amounts of energy from powerful mining rigs.

POW is safe and decentralized, but it's inefficient and unfair to the operators that don't win. Nevertheless, it's how bitcoin's and Ethereum's blockchains operate, although

Ethereum will soon shift to the more efficient proof of stake.

PROOF OF STAKE

Proof of stake is a new consensus technique that enables for significantly more efficient block mining. Cryptocurrency holders can use POS to validate new blocks and add them to the appropriate blockchain.

Validators do this by staking their cryptocurrency, and when a randomized algorithm chooses their stake, they get to validate a new block. For validating, they'll get a reward in the form of more cryptocurrency. As a result, the more cryptocurrency a user has staked, the more likely they are to be chosen to validate a new block.

Proof of stake rewards those who stake their cryptocurrency over a lengthy period of time, whereas proof of work rewards those who have invested the greatest computer power to solve a cryptographic challenge. Both have their pros and cons.

PUMP AND DUMP

Pump and dump techniques include inflating the Demand for a product in order to get others to buy it and raise the price. Pump and dump operators then sell their assets at a high price, causing the market price to plummet.

These scams also exist in traditional markets like stocks on the OTC market. Pump and dump are more common in

low liquidity micro-cap cryptocurrencies because trading makes price manipulation easier.

RUG PULL

Rug pulls occur when a cryptocurrency's originator disappears, taking the funds with them. "Rug" is a synonym for "scam."

SATOSHI NAKAMOTO

Satoshi Nakamoto is the pseudonymous and anonymous creator of bitcoin. The original white paper explaining the need for decentralized finance and explaining how bitcoin works was signed by Satoshi Nakamoto. No one knows who Satoshi is. It's been speculated that Satoshi Nakamoto might be several people working together.

SEED PHRASE

You'll be given a 12-word seed phrase when you create a cryptocurrency wallet. You'll need to enter your seed phrase every time you log into your wallet on a new device. Never tell anyone your seed phrase. Anyone who knows your seed phrase can take your crypto-assets.

SHARDING

Sharding distributes network load across a blockchain, processing more transactions per second (TPS). TPS sounds dry, but it's crucial. Ethereum will integrate sharding next year as part of 2.0, making using it cheaper and much less environmentally damaging.

SILK ROAD

The FBI shut down Silk Road, an illicit online market, in 2013. However, because bitcoin was a popular payment method for the site's illegal commodities, it was where many individuals first learned about cryptocurrencies.

SMART CONTRACT

A smart contract is a computer program on a blockchain that automatically executes when specific criteria are satisfied. For example, if Wallet A sends 0.08 ether to Wallet B, Wallet B responds by sending NFT C to Wallet A. They're most typically used to automate transactions, but they can also be utilized for more advanced applications like flash loans.

STABLECOIN

Cryptocurrencies that are tied to the US dollar or another fiat currency are known as stablecoins. Tether and USDC are two examples. Their goal is to allow cryptocurrency traders to store their tokens in a crypto ecosystem without having to worry about the price volatility of bitcoin and Ether.

STAKING

Some cryptocurrencies allow you to stake tokens in exchange for a percentage of that total paid out at regular intervals for the duration of the stake. For example, Token X may provide a 10% monthly return on any stake of more

than 5,000 tokens. So in that example, you would put down 5,000 tokens in exchange for 500 Token X each month.

Staking is a passive income investing strategy: In the above situation, it could take ten months to recoup the initial 5,000 tokens. After that time, each monthly payment of 500 Token X would be pure profit (assuming the value of Token X remains steady).

Bitcoin does not offer staking. Nor does Ethereum, though Ether eventually will when it adopts the proof of stake mechanism.

TLT

Short for "think long term."

TOKEN

Tokens are blockchain assets. Cryptocurrencies like bitcoin, for example, are a form of token. Other forms include governance tokens, which give the bearer voting rights in a DAO or service, and utility tokens, which offer access to a service based on the number of tokens held.

UTILITY TOKEN

A utility token is designed to perform a specific function. These can be for access to a game, service, or application. Filecoin is an example that grants access to blockchain-based digital storage, and Chainlink, which connects smart-contracts of off-chain data types.

VAPORWARE

Vaporware is a product or service that has been promised but never delivered. The word first gained traction in the late 1990s during the first internet boom, and it has recently resurfaced because of some dubious cryptocurrency inventors.

VITALIK BUTERIN

Vitalik is the creator and visionary of Ethereum.

WALLET

You can keep your bitcoin and NFTs in cryptocurrency wallets. These wallets can be hot or cold, i.e., browser wallets that are connected to the internet or hardware wallets that are not. Wallets have the ability to read and write, allowing them to receive data and serve as an online signature or ID.

WEB3

According to blockchain enthusiasts, Web3 is the next iteration of the internet. From the beginning of the internet until roughly 2005, Web1 was a read-only internet. The term "Web2" refers to the emergence of creators who create material and upload it on the internet. Web3 will be a blockchain-based internet. Imagine owning your social media postings in NFTs, utilizing Ether as a worldwide currency, and using your wallet as a form of identification instead of an email and password combination.

WHALE

A whale is someone with significant holdings of cryptocurrency.

WHITE PAPER

A white paper, sometimes known as a "whitepaper," is a type of informational document produced by a company or non-profit organization to promote or highlight the benefits of a solution, product, or service that it offers or promises to offer. For example, most blockchain platforms have a white paper that describes what they are trying to accomplish and how.

WAGMI

WAGMI is short for "we're all going to make it."

John Cousins is the founder of Tetraktys Global.

Tetraktys Global seeks to continuously produce high-quality trading signals (alphas) through our proprietary research platform **Alpha-Bets**. We develop and deploy

systematic investment strategies focused on market inefficiencies across a variety of asset classes and global markets.

John is an author of over 20 books, blogger, podcaster, online course creator, investor, inventor, entrepreneur and musician.

John began his career, after graduating from Boston University and MIT with degrees in Media Studies and Electronics, working for one of the great early Silicon Valley tech firms: Ampex. He then spent a decade in Manhattan working for ABC Television as a systems engineer designing and building facilities for the network and managing programs for sports and news; big spectacles like the Olympics and political conventions.

John then received his MBA from Wharton. He has since taken two companies public as CFO and CEO and has had 15 years experience as a public company CFO and ten years experience as a public company CEO. John has been involved in many start up and public company financings and deal making. He has founded numerous startups in alternative energy, life sciences, and technology. His career shifted to teaching at numerous universities in US and internationally in the past ten years. His company MBA ASAP delivers digital content on business topics via eBooks, paperbacks, audiobooks, podcasts and online courses.

- Connect with me on twitter: @jjcousins
- Subscribe to my podcast MBA ASAP
- Subscribe to my YouTube channel MBA ASAP
- Check out my blog posts on Medium

- Kindle, paperback, audio books at Amazon and Audible
- Check my online courses at Udemy.com
- Connect with me on LinkedIn
- Get the free eBook Understanding Financial Statements at MBA-ASAP.com
- Sign up for my email list at www.MBA-ASAP.com