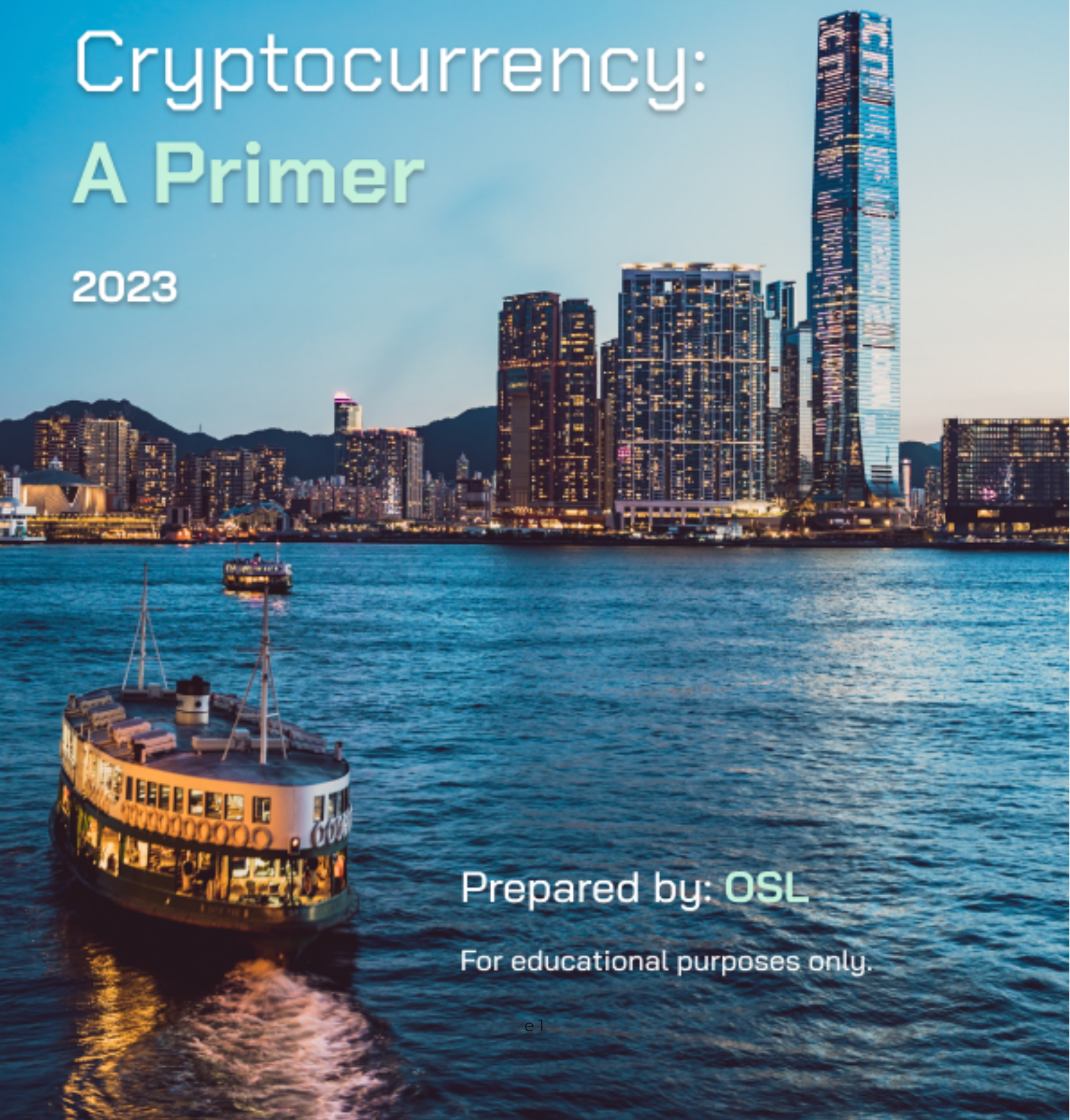
OSL

BC GROUP

Blockchain & Cryptocurrency: A Primer

2023



Prepared by: OSL

For educational purposes only.

Disclaimer:

All content and information contained in this guide is for informational and educational purposes only, and does not constitute financial advice or any offer or solicitation to offer or recommendation of any investment product. Furthermore, the content of the Services does not constitute an offer or invitation to subscribe for or purchase any securities, and shall form the basis of any contract or commitment whatsoever. While OSL strives to provide accurate general information, the information presented herein is not a substitute for any kind of professional advice, and you should always consult a professional for your particular needs and circumstances prior to making any professional, legal, financial or tax related decisions.

OSL | THE TRUSTED DIGITAL ASSET PLATFORM

Intro

"Crypto" can be intimidating.

It uses sophisticated technology that is not trivial to laypeople.

It converses in jargons, abbreviations and memes that deters outsiders.

It evolves rapidly and dynamically in the sense that new ideas and projects may appear every day, while existing ones may become irrelevant the day after.

Nonetheless, it is one of the most discussed topics nowadays, with the potential of being a contender to be one of the greatest inventions in the 21st century, among other possible candidates like smartphones and driverless vehicles.

And here you are, willing and ready to gain a better understanding of the topic.

The objective of this document:

- Readers at any level of proficiency in crypto will learn something new;
- Readers will be better equipped with relevant knowledge to invest in or utilize crypto products.
- Readers will enjoy this brief introduction into the world of blockchain technology and digital assets..

A Very Brief History of Bitcoin

It was the dawn of quantitative easing after the global financial crisis when the whitepaper of Bitcoin by Satoshi Nakamoto was published in October, 2008.

The idea was simple. As governments have full control of the monetary policy, Bitcoin provides an alternative to the fiat currency in the sense that its circulating supply and inflation rate are known and predetermined, and its governance is controlled not by a single authority, but a decentralized network of "validators" using the blockchain technology.

The decentralized nature of Bitcoin is probably also the reason why only few care about whether the true identity of Satoshi Nakamoto is a Japanese genius, a pseudonym of a group of people, or if he/she/they is/are even alive or not. There were attempts to invent virtual currency before Bitcoin, but the rise and fall of these pre-Bitcoin era virtual currencies depends on the rise and fall of the centralized company, organization or people behind them. That makes Bitcoin a little bit more unique than its predecessors.

That sounds promising. So why haven't we replaced all fiat currencies with a more superior alternative in the form of cryptocurrencies already?

Well, it is because decentralization comes with a cost, and sometimes that cost can be prohibitively high. Without going into the technical details here (yet), you can quickly come up with questions like: how do we agree on time and sequences of the communications? How do we come to consensus? How do we trust each other?

If the technology is centralized, then a single entity can call all the shots. However in a decentralized world, it is a different story.

Surprisingly (or not), the original whitepaper has already provided some groundbreaking solutions to these questions (and these solutions become the fundamental building blocks of blockchain technology we use today). Yet, naturally, every solution added makes the technology a tad bit less efficient, compared to the traditional, centralized solution.

Which brings us to the next topic: intrinsic value.

The Great Debate: Intrinsic Value

First of all, fiat currency, ironically, has no intrinsic value *by definition*. The term was used as opposed to the once popular gold standard (or silver standard) currency. Gold standard currency has intrinsic value, which is the value of the gold that mints the coins. It was the most common currency system until the 18th century, where governments started issuing paper notes as currency, with the understanding and trust that the governments will honor the value of the currency notes they print.

So arguing Bitcoin has no intrinsic value is nothing more than arguing fiat currency has no intrinsic value. And in some cases, people may even trust the governments less.

But we can go further to argue that Bitcoin and other cryptocurrencies *do* have intrinsic value.

The applications of blockchain as a distributed and decentralized technology have many benefits over the centralized version of these applications. ***If the benefits of using blockchain outweigh the associated costs, then such applications do have intrinsic value.***

Some of the benefits (of Bitcoin, but also of blockchain applications in general) include:

- **Portable**. 1 bitcoin weighs the same as 100,000 bitcoins.
- **Durable & Non-consumable**. No one can burn your bitcoins "just to send a message".[1]
- **Fungible**. The 1 bitcoin you own is the same as the 1 bitcoin that I own.
- **Divisible**. Bitcoins can be divided up to 8 decimal places.
- **Irreversible**. Once a transaction is confirmed, no one can alter the record ever.
- **High availability**. Thanks to the high redundancy of nodes in the decentralized network, the Bitcoin network has been functioning for 99.98% of the time since its inception.
- **Fast**. Time is relative (to banking transfers, for example). We will come back to that.
- **Pseudonymous**. While the wallet address is identifiable on the blockchain, there is no personally identifiable information attached to the address.

[1] The Dark Knight, 2008. Also interestingly, there is a mechanism in cryptocurrency that is called "burning" too, but we will leave it for later.

- **Permissionless & Censorship-resistant**. One does not need permission from anyone to use bitcoins, and on the other hand no one can stop anyone from using bitcoins.
- **Counterfeit-resistant**. There are many types of scams in the crypto world, however inserting a fake bitcoin into the circulation of the blockchain is virtually impossible.
- **Public & Transparent**. All Bitcoin transactions can be seen and verified on the blockchain.
- **Worldwide & Borderless**. As long as you have access to the internet, you are good to go.
- **Smart & Programmable**. They are not just a piece of paper, or a block of precious metal. For example, the total circulation of Bitcoin is programmed to a fixed and predetermined inflation rate.
- **Low transaction fee**. Transaction fee is relatively low compared to the traditional banking operations.
- **Decentralized**. Governance is not concentrated in the hands of a single or a few entities, indirectly creating check and balance across the ecosystem.
- **Scarce**. Bitcoin is programmed to have exactly 21 million units in circulation by the end of the mining cycles.

Some of the costs include:

- **Speed**. As we mentioned, speed of transaction time is relative.[2] We will come back to that, *relatively soon*.
- **Cost**. It costs more time, effort and resources to communicate or to make decisions in a decentralized setup.
- **Scalability**. The more decentralized the blockchain network is built, the more difficult it is to scale up.
- **Space**. Decentralized participants in the blockchain network implies multiple redundancy of data being stored. This requires more data storage than a centralized system.
- **Security**. One can scale up the network more efficiently or increase the speed of the network, at the expense of security measures. It is always a trade-off, and we will discuss the trilemma in a later section.
- **Interoperability**. There are many blockchains in the world of crypto. It takes additional effort to make a coin or token interoperable across different blockchains..

It is difficult, if not impossible, to quantify the benefits and costs here. However, in theory, **the difference between the sum of individual benefits of decentralized technology over centralized technology, and the sum of individual costs of**

[2] Albert Einstein, 1921.

decentralized technology over centralized technology, will be the intrinsic value of blockchain (even if it may not be a quantifiable, numeric value).

Some applications of blockchain technology may have a positive intrinsic value and prevail, and some may have negative value and eventually fail.

With that in mind, we rest our case on categorically calling out that "*crypto has no intrinsic value*" is nothing more than an incomprehension of how blockchain functions.

The Forgotten Debate: Market Value

It sounds trivial but it is still worth a short section to emphasize the difference between intrinsic value and market value.

Like many other asset classes, cryptocurrencies can be traded on open markets (both centralized exchanges and decentralized exchanges). Many factors can affect the market price at any given time on the market, most prominently the difference of expectations on future value.

While the intrinsic value may be intangible and difficult to quantify, it is rather a relatively objective value. However, when people buy a cryptocurrency or a digital asset[3] for investment purposes instead of its usage, they expect its future value will increase,[4] and this expectation can be subjective.

In stock markets, people often look at the price-to-earning ratio (P/E ratio) and other fundamental indicators to determine whether or not the current market price of a stock is undervalued or overvalued against its potential future value. Such indicators may not always be available to cryptocurrencies, and as a new technology as well as new asset class, the expectations of future value may vary a lot. This partly contributes to the high volatility of market value in cryptocurrencies.

Nevertheless, there are a number of other factors affecting the equilibrium of the market value of cryptocurrencies, including short term speculations, long / short trading, future / spot trading, triangular arbitrations, liquidity and other limitations in different exchanges and jurisdictions, breakthroughs in technological developments, market sentiments, social media trends, etc.

Neither intrinsic value nor market value is a superior idea to the other. Projects may fail to realize their full potential intrinsic value if they are severely undervalued in the market; projects may also thrill for a long period of time with inflated market values and the value becomes a self-fulfilling prophecy of its intrinsic value..

[3] We will use *cryptocurrencies* and *digital assets* interchangeably in this guide.
[4] Or if they are selling/shorting, they expect its future value will decrease. It is deemed to be understood, and we will try not to reiterate every time, when we talk about buying or selling.

What is Blockchain

Blockchain is no mystery. It is just a word invented for the decentralized and distributed ledger technology.

In order to truly achieve both the objectives of being decentralized and being distributed, there are a few innovative designs best explained (without involving the technical details) in a full analogy.

We will look into the analogy as a currency to start.

New Coin as Proxy to Store Value

Imagine a bunch of kids in school whose only source of currency is the pocket money from their parents each month. Apparently for the kids, that is not enough currency circulation for their daily use, for instance, to trade basketball or Pokemon cards, or to buy snacks off each other.[5]

Let's say they have decided to create a new kind of virtual currency called *Kidcoin*. In theory, the kids can use kidcoins to buy and sell (we will come back to how the kidcoins are being created). Alice can buy a Pokemon card from Bob and pay Kidcoins to Bob; and then Bob can buy some Cheetos crunchy cheese from Charlie using these kidcoins Alice just paid to him. They can optionally exchange kidcoins back to real money when their pocket money comes around by the beginning of each month as well. So far this is just a very simple credit book-keeping system.

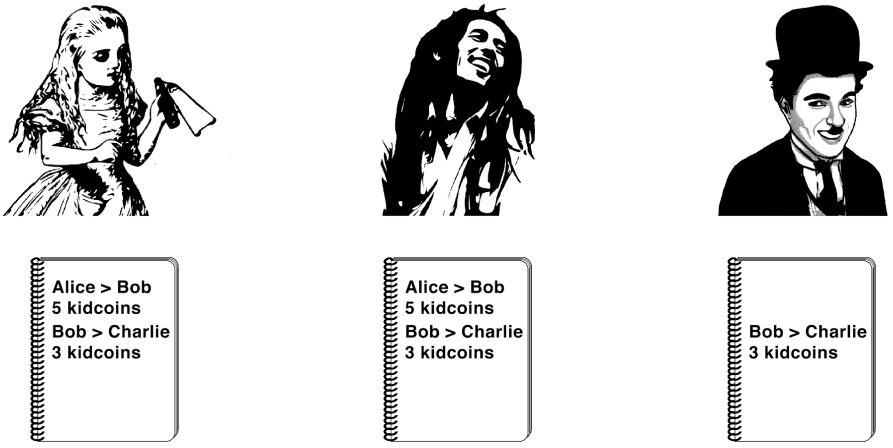
[5] Kids these days probably have smartphones and thus access to all forms of electronic payment services. Let's set the stage in the 1990s where smartphones are not a thing yet.

Distributed Ledger

There are no physical kidcoins circulating in the school, so they need a way to store and track Kidcoin transactions.

The question is, who should be responsible for keeping the transaction records (a.k.a. the ledger)? They may elect someone to do it, for example, the class prefects. However, some kids do not trust their class prefects (i.e. centralized intermediaries), as they may be absent from class and none can transact kidcoin on that particular day, or they may have malicious intent and falsify records.

An alternative solution is to have multiple, identical copies of the ledger, and all kids keep a binder notebook of these Kidcoin transactions. ***This resembles a network of peer-to-peer nodes in Bitcoin***. This helps solve the availability problem (as one or several individual kids absent from class will not affect the whole Kidcoin ecosystem), but not necessarily solves the issue of potential falsification of records by the record keepers. Separately, it also creates another problem of multiple copies of ledgers may not agree with each other (inconsistency in record keeping).

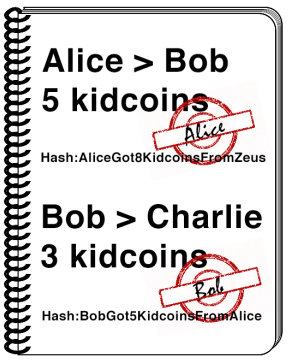


Temper-Proof

To prevent falsifications, the easiest approach is to have the payers of kidcoins undersign their own transactions. Using the previous example, Alice will sign the transaction to confirm the transfer of kidcoins from Alice to Bob is indeed valid and authorized by the payer, before Bob gives Alice the Pokemon card. Bob will then sign the transaction to confirm the transfer of Kidcoins from Bob to Charlie for the Cheetos, and so on.

To simplify the story without going into the technical details, we will assume we have two magic processes. First, let's assume each signature can only be undersigned by the respective kid (i.e. other kids cannot forge signatures), while all kids can verify whether the signature is authentic or not. ***This resembles public key cryptography***. Let's call it "signature magic".

Second, in order to prevent kids from undersigning transactions of kidcoins they do not own, when they undersign a transaction, they also require to include a unique reference of a previous transaction record where they receive the kidcoins. These references can be easily verified by any and all kids in the notebooks. ***This resembles hash pointers***. Let's call it "hash magic".



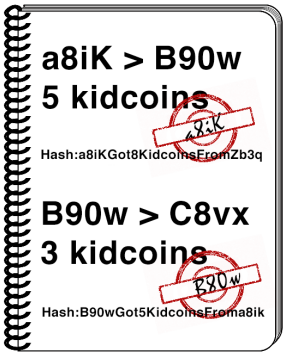
By now, every kid owns a binder notebook of Kidcoin transactions. Each kid will be responsible to make sure all transactions are valid by verifying the transactions' "signature magic" and "hash magic". To make things more efficient, they all go around to collect transactions from each other, and only publish them to other kids when they have a single full page of transactions, which ***resembles a block of transactions in blockchain***. Kids who receive the new page of transactions will then copy the page, and then append it to the end of their own binder notebook.

Anonymity

Imagine the kids do not want to disclose their names in the notebooks. Maybe they do not want others to know how much the Pokemon cards are worth; maybe they do not want the teachers to find out their names, in case they start looking into this little economic ecosystem.

What the kids can do is to use unique nicknames (pseudonyms) in the notebooks. They can undersign their own pseudonyms using the same "signature magic", in order to prove the ownership of the nicknames, and naturally, the ownership of the Kidcoins under the nicknames. ***These nicknames resemble public addresses*** *(or*

public keys) ***on the blockchain in Bitcoin***. The nicknames are public: every kid can send Kidcoins to any nickname; The signatures are private: only the kid with the correct signature can spend Kidcoins received by a particular nickname they own.



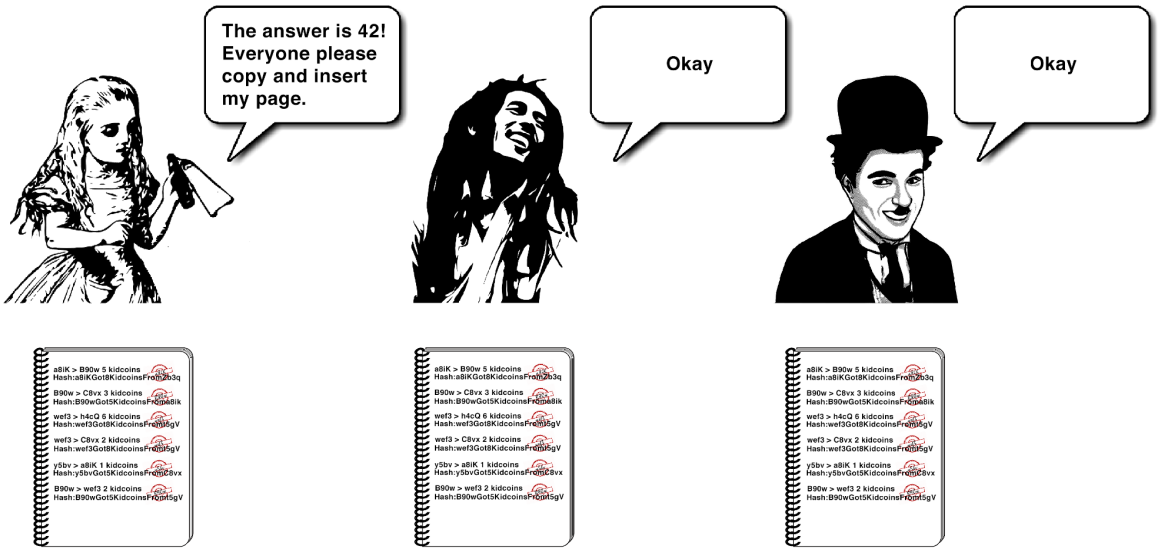
Distributed Consensus and Proof-of-Work

These kids now may gather transaction records at different paces. Occasionally, more than one of them may get a full page of transactions at the same time. And obviously, when Alice goes around the class and gathers transaction records, the page will be very different from the transactions Bob gathers. How can we decide which page goes to the binder notebook and starts propagating to the rest of the school?

One way to do it is to, again, get class prefects to decide. But then we go back into the problem of centralized authority. Another way is to completely randomize the decision of who gets to publish and append the next page. However, as Alice may physically be in Class A on the fifth floor of the school, and Bob may be in Class E on the second floor (***this resembles the real-life problem of physical locations of the nodes in a distributed network being far apart and inefficient in communication propagation***). How can they randomize something without a centralized authority, and communicate with each other which may suffer from a long delay?

The answer is to ask the kids to solve a very, very difficult mathematical equation. Without going into the details, let's assume that the answer of the question cannot be directly solved, but indirectly verified by feeding random numbers one at a time to the question to see if it is indeed the answer (brute force approach). In this case, the decision of who gets the right to publish the next page is not only probabilistic, but also proportional to how hardworking an individual kid is in solving the question. ***This resembles the proof of work*** *(using computing power instead of kids resolving math problems)* ***in the blockchain technology used by Bitcoin***.

Also, the mathematics question is set up in such a way that finding the correct answer is difficult, but verifying whether or not the answer is correct is easy and straightforward. That way, any kid can verify whether or not a particular kid does indeed find the solution.



Longest-Chain Rule and Confirmation by Probability

There is one more neat trick here. The mathematical equation is set up with the unique reference of the immediate previous page on the notebook. By solving the mathematical equation, you cannot alter the sequence of the current page with respect to its immediate previous page. And as the kid who publishes the previous page must have done the same to link with the previous-previous page, all pages in the binder notebooks in the circulations are verified, and linked together in sequence. Let's call it pagelink... or alternatively, blockchain.

What if Alice and Bob both have collected a full page of transactions, and solved the mathematical equation at the same time (or within a very close timeframe to each other)? Or worse, what if there is a malicious kid, Chuck, that intentionally attempts to append a page of transactions between two existing pages of transactions in the binder notebook?

Both scenarios can be resolved by agreeing among the kids that a new page can only be appended to the longest chain of pages already in the binder notebook. Let's say all kids have 30 existing pages, so the next new page will be the 31st page. Chuck wants to add a page between 23rd and 24th, and makes his page the "new"

24th page. Other kids will simply ignore him and continue to append pages from the 30th page onwards.

The situation with Alice and Bob is trickier. Both Alice and Bob genuinely want to append a page as the 31st page. Kids who are physically close to Alice will see Alice's page being valid and copy that into their own notebook. Kids who are around Bob will see Bob's page being valid and copy Bob's. Indeed, there is a temporary inconsistency within the school (i.e the blockchain network) that both versions of the 31st page are valid. It comes down to who solves the immediate next mathematical equation. If Dali, who has Alice's page as the 31st page, solves the question and appends his page as 32nd, it becomes the longest chain of pages. Kids who receive this confirmation will now be forced to abandon Bob's page like they ignore Chuck's page in the previous example, and build on Alice's and Dali's pages.

Hence, a transaction does not have a deterministic state of being confirmed or not. Instead, the more pages appended after the page where your transaction is recorded, the higher the probability your transaction is confirmed. Invalidating Bob's page does not imply that Bob has malicious intent per se. It only shows that the confirmation of transactions are probabilistic, and Bob only fails by chance. All Bob has to do now is to use Dali's page to solve the mathematical equation again, and append his page again when he solves it.

51% Attacks and Hard Forks

I hope you are still following the story nicely. The remaining topics should be fairly straightforward.

If the school has 100 kids keeping records on their notebooks, and 51 or more kids now gang up together[6] and want to disrupt the operations with malicious intent, they can in theory do so. Chuck can now insert a page between 23rd and 24th like we mentioned earlier, and have all these naughty kids following Chuck's page until it becomes the longest chain, effectively voiding all the transactions in the original 24th to 30th pages. This allows Chuck or others to "double-spend" the coins they have previously spent.

What if the other 49 kids do not agree with these naughty kids, and collectively decide to follow the original chain (Alice's) instead of the malicious chain (Chuck's)? In that case, it becomes a hard fork on the chain. They become two separate and exclusive chains that go separate ways from a common root. These two groups of

[6] Technically speaking, you only need 51% of the computing power, not 51% of the total number of nodes.

kids will maintain their notebook records separately, and the kidcoins will not be interchangeable between the two groups.

Hard forks do not have to come with malicious intent though. People may have different ideas about how the tokens should operate, and disagreeing parties may go separate ways from an agreed point (block) onwards.

Incentivization of Node Running and Mining

So far, we assume that kids receive pocket money from parents, and Kidcoin is being used as a "credit" system so that they can convert back to real money by the beginning of each month. We also assume that there is a way to control the creation process of Kidcoin. We can tackle these two questions in the following case.

Edgar and Friedrich are new kids joining the school. Sadly they do not have any pocket money. However, Edgar is very good at math, and Friedrich has a lot of Pokemon cards. In reality, not all the kids want to keep track of the transactions on the notebook or do the math (that is a lot of effort). They are happy to rely on the fact that if there are enough kids in the school to maintain the records for them, they can trust these kids collectively, and their kidcoins can be used as per usual.

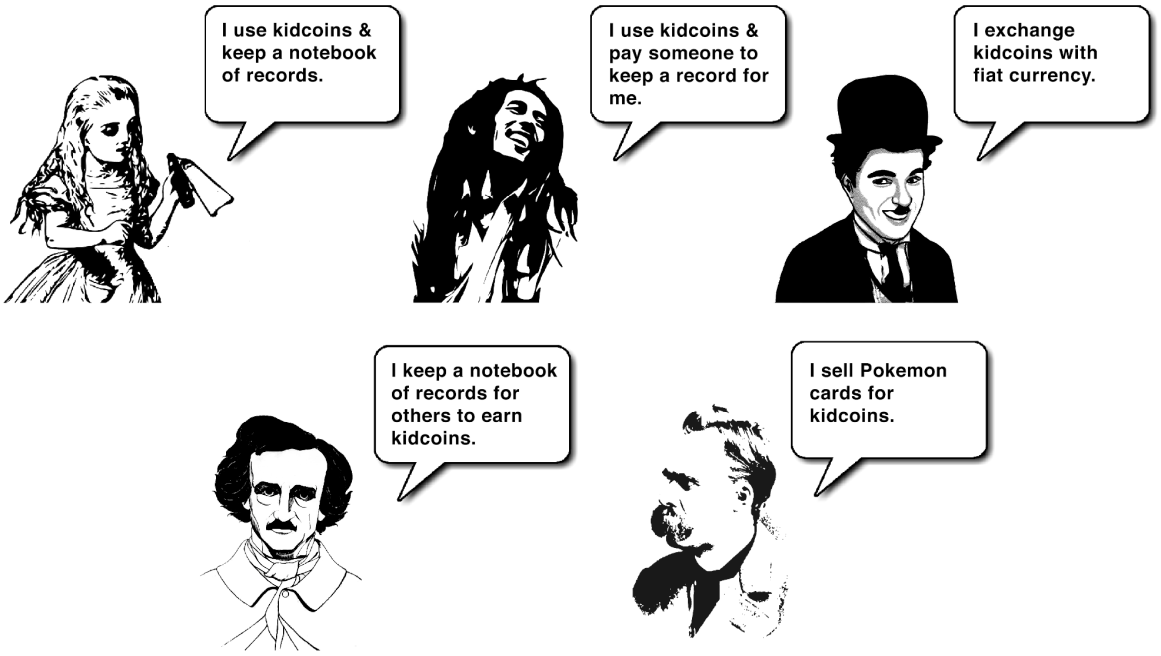
In order to incentivize a subgroup of kids to continue maintaining the notebook of transactions, they are rewarded in two ways. First, they receive a small transaction fee. It is a negotiable amount agreed between the kid who wants to transact, and the kid who maintains the notebook. If a kid wants a confirmation sooner (gets to an earlier page of transactions), they may pay a higher transaction fee. ***This (loosely) resembles the gas fee in blockchain transactions***.

Second, among all the kids they agree that whoever successfully solves the mathematical equation and appends a new page, in that particular page they can add a unique transaction that pays the solver a certain amount of Kidcoins out of nowhere. For example, a page contains 99 transactions from general usage of Kidcoins, and one transaction that creates 25 Kidcoins and transfers to the solver of the mathematical equation. ***This resembles Bitcoin mining***.

Further to this, to prevent an infinite amount of kidcoins being created, the reward will be halved approximately every 4 years. This "halving sequence" becomes a geometric series with finite sum, so the sum of all kidcoins will be predictable and limited in some distant future.

Now, Friedrich can sell his Pokemon cards, pay a kid who maintains a notebook a small transaction fee to have the record confirmed and validated, and receive kidcoins in return. Similarly, Edgar has nothing to sell, but he can maintain a

notebook and help other kids transacting kidcoins, and earn kidcoins from transaction fees and mining. No fiat currency is involved from Edgar's and Friedrich's perspective. These kids can eventually evolve into different roles ***resembling different roles in the crypto ecosystem like miners, validators, users, project developers, exchanges, etc.***



Variations and Evolutions

The great thing about blockchain is you can always create a new chain and program it differently to suit your use cases and needs. We will continue the discussions in later chapters.

Usage and Storage

Blockchain is Your Oyster

The concept of blockchain starts off as a technology to support a very particular use case: digital currencies. However, it has quickly evolved into other applications, most notably as a foundation of smart contracts.

In the following chapters, we will discuss how smart contracts on blockchain can help enforce the terms and conditions in the contracts without a central authority. We will talk about stablecoins as a USD equivalent of cryptocurrency and we will discuss crypto exchanges, both centralized and decentralized.

The Curious Case of Asymmetric Keys

Before we talk about how we can use cryptocurrencies, let's talk about how we can store them.

Due to the nature of asymmetric cryptography (or public-key cryptography) used in blockchain, the concept of cryptocurrency storage can be quite different from the equivalent in fiat currency. Specifically, one does not store the cryptocurrency, but only stores the private keys.

In the world of cryptocurrency, the concept of ownership is split into two: **public key (or public address) is your right to receive or earn, and private key is your right to send or spend**. Every transaction of all private-public key pairs are public, verifiable, non-repudiable and available forever on the blockchain, so there is no need (or, impractical) to store the *balance* in individual wallets.

Your balance is the net sum of all your transactions.

One can always generate the corresponding public key from the private key, but engineering the private key from a known public key is extremely improbable[7] (hence, *asymmetric* cryptography). Hence public keys can be shared to whomever you want to receive payments from, and it has little to no consequence if you accidentally lose your public key, or disclose it to the public[8].

Private keys, on the other hand, are never meant to be shared or disclosed. And as we mentioned, **there is no concept of right to own, only the concept of right to send or spend**. And as blockchain is decentralized, you cannot submit documents to any authority to prove your ownership of a private key and "reclaim" it. If a private key is lost or forgotten, then no one can ever spend the cryptocurrency balance; if a private key is mistakenly shared or disclosed, then whoever possesses the private key has the equal right to spend the balance, depending on who commits and confirms the transaction on blockchain the quickest.

Wallet Types

Hot Wallet & Cold Wallet

There are, generally speaking, three types of wallets: hot wallet, cold wallet and exchange wallet.

A hot wallet is the wallet that connects to the internet to transact. It can be in the form of a web-based wallet, mobile app, or desktop wallet. They are all almost always online. It is like your actual leather wallet in your bag or in your backpocket.

A hot wallet is often exposed to the whole world. Pickpockets can easily steal money from your leather wallet and equally, hackers can easily exploit your hot wallet. It is not meant to hold your pension fund or life savings, but just enough petty cash for day to day usage.

A cold wallet is usually disconnected from the outside world and the only way to attempt to hack it is to have physical possession of the wallet. It is most often in the form of a hardware wallet, or in the early days of the crypto world, a paper wallet. It is like a safe in your house.

---

[7] We have carefully avoided the word "impossible" here. Yet, if the public-key cryptography technology is being compromised, it will mark the end of modern digital security and, unironically, modern economy.

[8] You cannot deny receiving cryptocurrency from anyone who possesses your public key. Does not sound *too* bad, but there are occasions where scammers would send scam coins to random public addresses hoping the address owners would pick up and proceed. It is called *dust attacks*.

The risk of the money getting stolen from your safe is much lower if you are being careful. As long as you do not lose or give away your key or password of your safe, this is probably the safest way to store any substantial amount of funding. **Simply put, the difference between a hot wallet and cold wallet is the connectivity to the internet.**

	Hot Wallet	Cold Wallet
Characteristics	Connected / "Online"	Disconnected / "Offline"
Examples	Web-based Wallet Mobile App Wallet Desktop Wallet	Hardware Wallet Paper Wallet Air-gapped Computer Wallet

Custodial Wallet vs Non-Custodial Wallet

There are people who strongly believe that **"not your (private) keys, not your coins"**. So it is only fair to also classify wallet types by looking at who is holding the private keys.

A custodial wallet is where your private keys are being managed and controlled by someone else, usually your "custodian". It can be an exchange, a broker, or a custody service platform. It is a bit like valet parking: you give the car key to the valet, assuming that they will take good care of your key *and* your car.

A non-custodial wallet (or sometimes referred to as a "self-custody" wallet) is where your private keys are being managed and controlled solely by yourself. Naturally, you are solely responsible for the safekeeping of your keys. If you lose them, they are gone forever.

Exchange Account

Now let's add (centralized) exchanges into the mix.

As an exchange needs to store its users' virtual assets, the exchange in turn has a choice to use a hot storage, cold storage, or a combination of both.

The same pros and cons are still applicable. A hot wallet vault is always connected to the internet and ready for transactions. A cold wallet vault is safer and less easily exploitable by hackers, but it is operationally less efficient than a hot wallet vault.

From the user's perspective, an exchange account is just like a bank account.

An (centralized) exchange account is almost always custodial, where the exchange or its custodian will help manage your private keys. The tricky bit is, exchanges may

not hold your money in a separate wallet address from others. Instead, they often aggregate all client assets (and sometimes, house assets as well) under the same wallet addresses, so when people buy and sell on the exchange, it is merely an internal book and record change but not an actual on-chain transaction. This arrangement helps the exchanges save time (block confirmations) and money (on-chain transaction fees).

However, it takes away many advantages of using blockchain technology. For example, transactions will no longer be irreversible, public and transparent, and the availability will be at the discretion of the exchange. The practice of putting everything under the same wallet addresses also raises security concerns and questions, especially in circumstances like private key loss due to data damage or hacks. Moreover, in an increasing number of jurisdictions, there are regulatory requirements to segregate client and house (in this case, exchange) assets.

The concept of exchanges' custody services divides the opinions in the crypto community. After all, many people who invest in crypto have a strong distrust of banks and governments and strongly prefer a decentralized model, so why would they jump right back into centralized exchanges?

On the other hand, actions speak louder than words. There are hundreds of billions worth of cryptocurrency stored on crypto exchanges. Storing your money in a reputable exchange is probably as safe as storing it in your own cold wallet. Additionally, some exchanges may provide insurance coverage on their custody services, which offers an extra layer of protection over self-custody.

Neither approach is absolutely risk-free, so it is always wise to do your research on the profiles and reputations of the exchanges, and to put your eggs in different baskets.

Exchange Standalone Wallet

To make this conversation even more confusing, exchanges often extend their product and service offerings by supporting standalone exchange wallets. They are under the brand name of the exchange, but may or may not be integrated with the exchange platform, thus they can be custodial or non-custodial, depending on how it is designed.

It is best summarized as follows:

	Connectivity	Private Key Ownership
Hardware Wallet	Cold	Non-custodial
Mobile / Desktop / Web Wallet	Hot	Non-custodial
Exchange Account	Exchange may store the keys in hot and/or cold storage	Custodial
Exchange Standalone Wallet	Hot	Can be custodial or non-custodial

Medium of Exchange

Bank transfers and stock settlements take days.

Credit cards and contactless e-payment services take seconds.

Cryptocurrency transactions on blockchain sit *awkwardly* in the middle of taking minutes.

So when we talk about cryptocurrency as an investment instrument, it is great that it trades 24/7 and settles round the clock, without having to worry about non office hours, weekends and bank holidays. But when we talk about cryptocurrency as a day-to-day medium of exchange, it is impractical to buy a coffee and then wait 20 minutes for the confirmation of the transaction.

The problem has worsened in the years of exponential growth in adoptions worldwide, and the scalability of the Bitcoin blockchain unable to keep up with the volume growth. Satoshi Nakamoto probably never expected such a degree of success.

Another issue with Bitcoin as a medium of exchange is that Bitcoin is still experiencing bouts of very high price volatility, and no one knows what the fair and stable value of Bitcoin will finally settle at. This actually deters people from using bitcoins as a medium of exchange, as they use it as a store of value instead, very much like gold.

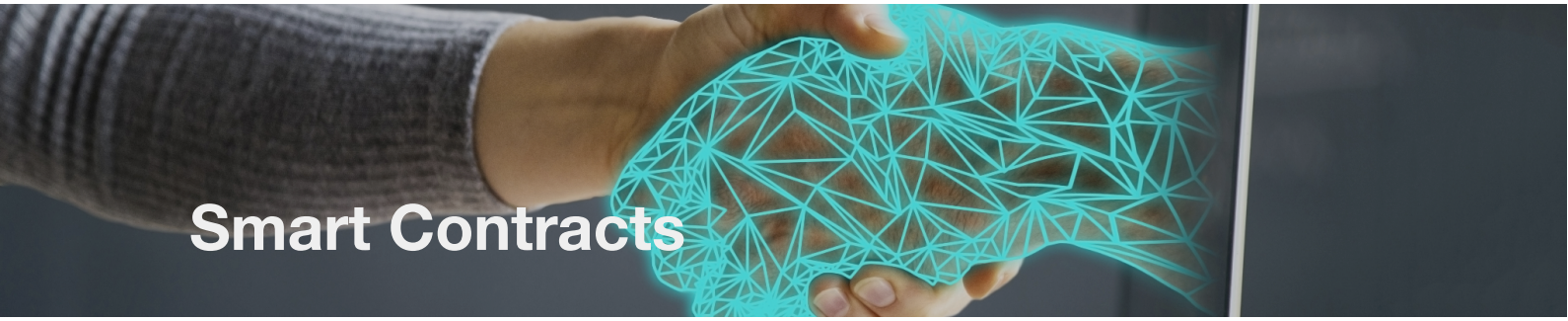
The scalability of transaction volume and speed is being tackled in a few approaches. First, there are a few attempts to improve the scalability of the blockchain itself. However, the solutions may not always be universally supported and accepted; disagreeing parties have parted ways in the form of hard forks as a result. Bitcoin Cash, Bitcoin Classic, Bitcoin Gold, Bitcoin SV, Litecoin, etc. are all results of hard forks from the Bitcoin blockchain. You can imagine these hard forks are like branches of a tree, and they are all coming from the same trunk.

While these Bitcoin-forks have different levels of success, they have never overtaken Bitcoin's overwhelming dominance, so the issue remains.

Another approach is a scaling solution on top of the original blockchain, which in Bitcoin's case, is called the lightning network. The lightning network is often called a layer 2 solution, which processes microtransactions of Bitcoin between two parties almost instantaneously by making these transactions off-chain. These microtransactions between two parties can keep accumulating until the amounts are net-settled on-chain.

The lightning network seems to be the leading solution to resolve the Bitcoin scalability issue right now. Small merchants (e.g. cafes) can use the lightning network to improve transaction speeds and reduce transaction fees, while the merchants can then transact in larger amounts with the crypto exchanges to settle on-chain.

But none of these can solve the fundamental issue of Bitcoin being an asset with a highly fluctuating value.



Ethereum - One Chain to Rule Them All?

Ethereum does not position itself as a currency like Bitcoin.

Ethereum is built as a **general purpose smart contract platform**. As we have described in an earlier chapter, blockchain is a decentralized, distributed ledger. Bitcoin is merely one of the many applications of blockchain.

Smart contracts are contracts programmed on blockchain, so they consist of the same characteristics of blockchain: decentralized, irreversible, anonymous, transparent, etc. And instead of just sending and receiving tokens, smart contracts allow any combination of transactions with different conditions and complexity. Essentially, you can create borrowing and lending agreements, futures and options contracts, leverage products, bonds and notes, and virtually any financial instruments that have ever existed in modern society, as long as they are programmable into the blockchain.

It is worth reiterating that Ethereum and Bitcoin are two very different products with very few similarities except their dominance in market capitalization terms. To compare Ethereum with Bitcoin is like comparing Google to the US dollar. Having said that, it does not imply that Ethereum has no competition in the market.

Proof of Work

You may have heard of these terms: proof of work and proof of stake.

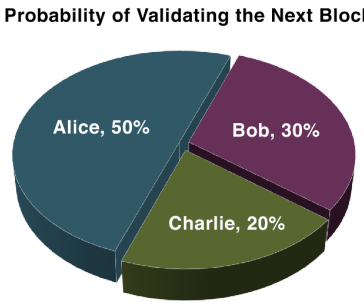
Going back to our Kidcoin example, kids need to compute a very difficult math question to get a say on who gets to insert a new page. It is not too far off from reality. This is essentially the ”proof of work “ mechanism to determine who gets the right to validate the next block.

However, the difficulty of the math questions needs to be continuously adjusted in order to have a constant and controlled inflation of circulation. As more and more participants try to solve the math questions, the more likely they are to be solved sooner (just Probability 101), and so more rewards are being distributed to the

solvers in a fixed period of time. If the math questions are being solved quickly enough, the increase in the supply of coins could crash the coin's economy, which is obviously very undesirable.

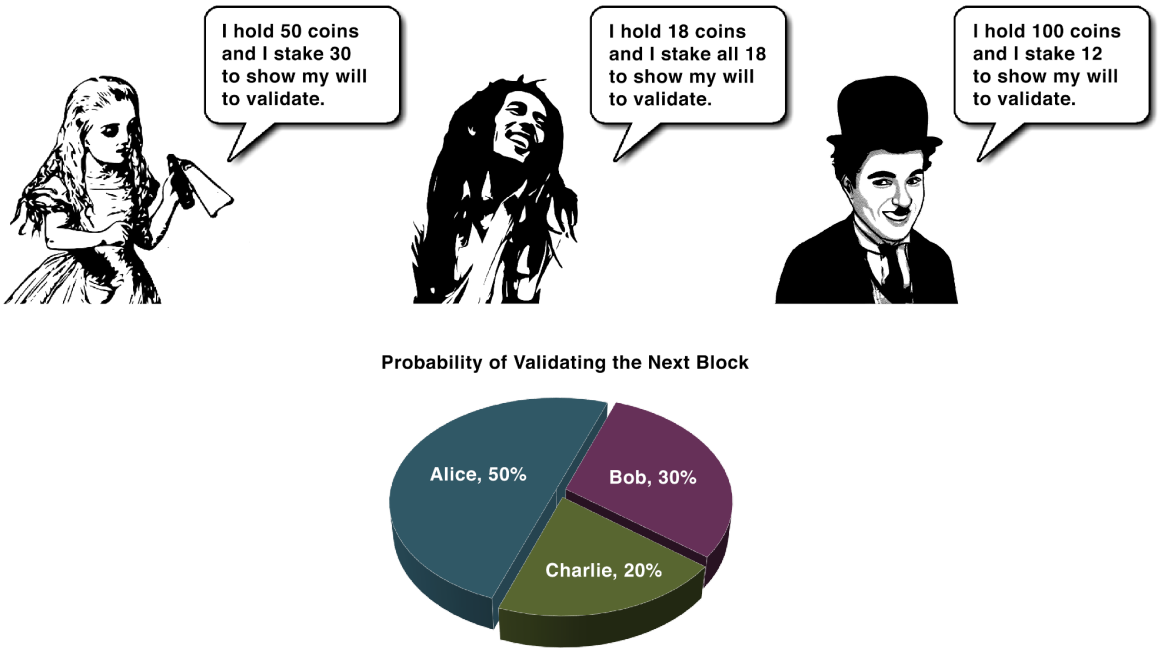
As a result, the difficulty of the math questions has been adjusted upwards massively. It is so difficult that those solving the equations need to purchase a lot of computing power and consume a lot of electricity to solve the questions. They are also known as the miners.

Proof of work mining is considered to be inefficient. Miners spend capital to buy racks of servers, pay exorbitant electricity bills, and solve very difficult math problems that are not even beneficial to the field of mathematics. The "proof of work" essentially becomes a "proof of electricity". The environmental impact of how Bitcoin is being mined has become a major factor making institutions hesitant to invest in cryptocurrency.



Proof of Stake

How about if miners just spend the money directly to "buy" the rights to validate a block? Well, that is the premise of "proof of stake": validators can hold coins to prove their "stake" in the ecosystem, and in turn they have a chance to validate a block (the staked coins will be locked up for a period of time, so it will not be the same validator with a large "stake" who keeps validating block after block).



You can see the resulting probability is largely the same, yet we cut off all the intermediate cost and inefficiency of servers and electricity.

Proof of work and proof of stake have their own pros and cons, which we will not discuss here. What you need to know is, Ethereum has successfully moved from proof of work to proof of stake, while Bitcoin is staying on the proof of work mechanism with no current plan to change the consensus mechanism just yet.

As a by-product of the change of consensus mechanism, validators started offering a yield to borrow Ether from long term holders to increase their "stakes", while the validators can earn a profit from the difference between the transaction fees gathered from users, and the yield payable to holders. ***This yield earning exercise is also known as staking***.

Layer 1 Solutions - Who is the Ethereum Killer?

Ethereum is not the only smart contract platform.

Vitalik Buterin, the cofounder of Ethereum, first proposed the trilemma of blockchain developments. **A blockchain can only achieve two of the three factors at a given timeframe: being scalable, being secure and being decentralized**.

While Ethereum is now generally considered fairly secure and decentralized, it suffers a similar scalability issue as Bitcoin as it has been growing exponentially. The time to take the Ethereum blockchain to confirm a block of transactions may take hours at worst, and as users fight to get their transaction confirmations on the chain first, they drive up the transaction fee (also known as gas fee) as well.

This provides a window of opportunity for other smart contract competitors entering the market. Binance Smart Chain, Solana, Fantom, Avalanche, Tron are some examples.[9]

Most of these smart contract platforms aim to improve either transaction speed or lower transaction fees. And as you may suspect, some of them sacrifice decentralization or security aspects as the trilemma hypothesizes, which these vulnerabilities have shown to be prone to hacks or exploits.

We are not going to talk in detail about the individual smart contract platforms here. Essentially, they all build their own different ecosystems, and are standalone from each other to some degree.

A good example is iOS and Android - They are two different mobile phone operating systems. The development frameworks, userbases, characteristics, etc. have their similarities and differences. If you develop a mobile app on iOS, you probably need to put in additional effort to develop it on Android. And some mobile apps may even be exclusive to either operating system.

So all these platforms are competing on not only the circulation of capital and userbases, but also the number of applications built on their chains.

An ecosystem.

We do not know what the final picture of the smart platform race will look like. It may become a monopoly but with dominance cycles (e.g. social media platforms

[9] Some newcomers may have joined the competition, and some examples listed here may have become irrelevant depending on how far you are from the latest update of this deck. After all, product life cycles in this space are very fast-paced.

or browsers); it may become a duopoly (e.g. iOS/Android or Macintosh/Windows); it may even evolve into something else that makes the competition among smart contract platforms irrelevant.

Layer 2 Solutions - Scale Up

Similar to Bitcoin and its scaling solution lightning network, Ethereum has its scaling solution too to help tackle the network congestion, and these solutions are often called layer 2 solutions.

The most notable scaling solutions are Polygon, Arbitrum and Optimism.[10] We do not intend to deep-dive into layer 2 discussions. There are several approaches to help scale up Ethereum network's capacity, and it may be able to challenge the trilemma in the long run to have a scalable, secure, and decentralized solution in the future.

It is also worth noting that those layer 1 competitors built much more recently than Ethereum have learnt the lesson from Ethereum's problem, and have more innovative and efficient blockchain mechanisms. So you do not usually hear about layer 2 scaling solutions being a big focus for them.

Cross-chain Interoperability

Efforts are being made to explore the possibility to bridge different chains too, which is a very important topic in the crypto world: interoperability. This can be achieved at different levels.

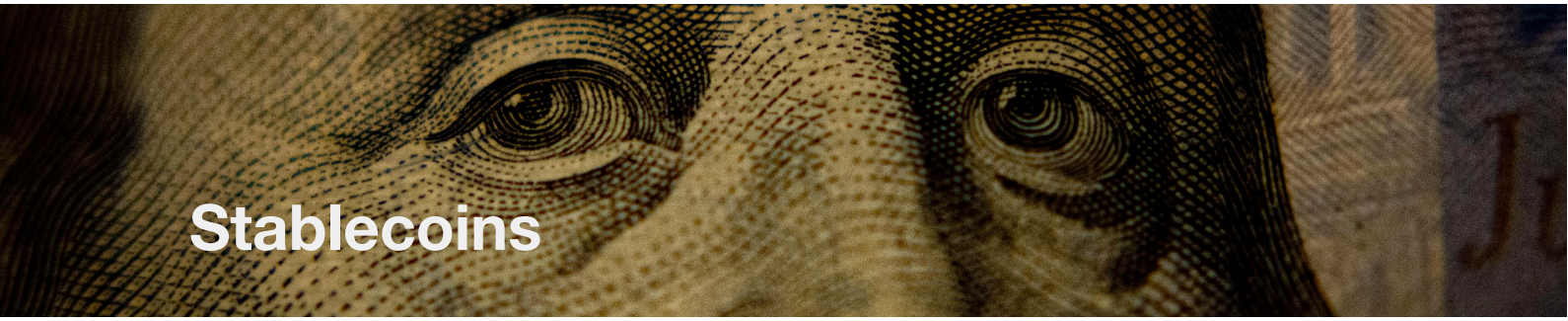
Application level: Applications can be built to be either chain-agnostic, or interoperable in as many chains as possible. As an analogy, you can access your Gmail service in virtually any mobile device and any browser with a similar user experience.

Development level: Development tools and "building blocks" are now available for applications to be developed and deployed in multiple chains.

Token Level: Tokens can be wrapped into another "synthetic token" that has the same value as the original token, yet can circulate on a different chain. For example, Bitcoin (BTC) can be wrapped into Wrapped Bitcoin (WBTC), which then can be used on the Ethereum network.

[10] Again, these solutions may come and go. It is understood that no additional footnotes will be made on the possible evolution of the ecosystem rendering some examples given irrelevant.

Chain Level: Chains can be bridged by bridging protocols and exchanges of tokens can be done regardless of the native chains they are on.



Stablecoins

In the earlier chapter, we talked about why Bitcoin's price swings may deter people from using it as a medium of exchange. If you recall the (in)famous first real-world purchase using Bitcoin, you'd agree with me here. A 19-year old California student, Jeremy Sturdivant, paid 10,000 bitcoins back in 2010 for two delivered Papa John's pizzas worth ~30 USD at the time, but worth millions of dollars now.[11] Nobody wants to be in Jeremy's seat, and luckily stablecoins can solve this problem and save you from splurging millions on 2 slices of pizza.

Stablecoins, as its name suggests, is a type of cryptocurrency without the relative volatility with its value being pegged to another asset such as fiat, commodities, treasuries, or even other cryptocurrencies. It acts as a bridge between the volatile cryptocurrencies and real-world assets. There are different types of stablecoins, some are backed by assets in a reserve which can range from commodities, fiat, commercial paper or even other cryptocurrencies; Others use algorithms to stabilize their value.

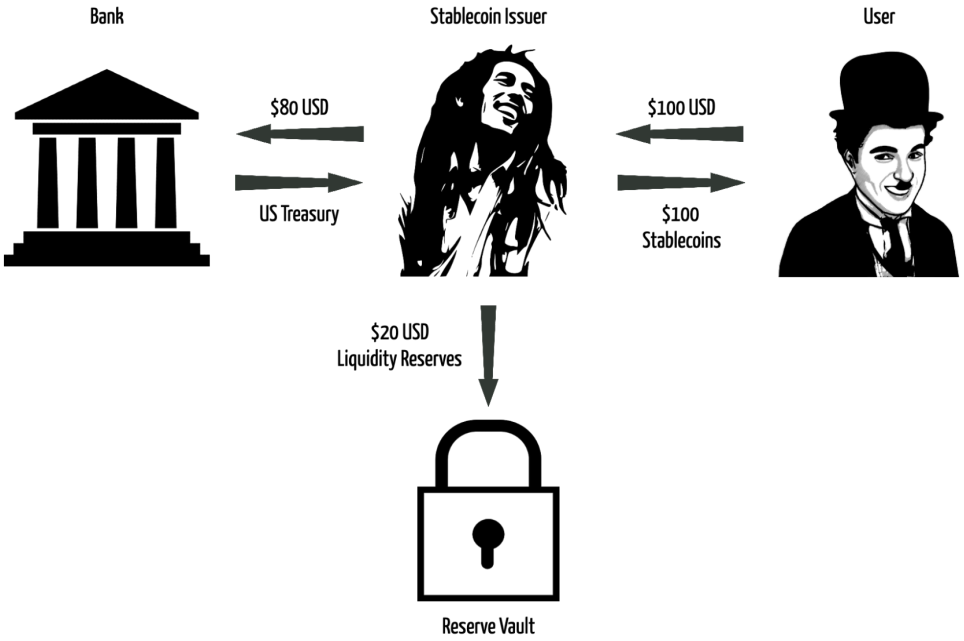
Fiat-backed Stablecoins - The Dollar is Still King

This is the most straightforward version of stablecoins. To make the value of the coin stable, the coin issuer will use the funding they receive from issuing the stablecoins to buy fiat or fiat-equivalent of risk-free products as a reserve to back the stablecoin's value. For example, a USD-pegged stablecoin will buy US dollars or US Treasury Bills. The issuers earn interest from the reserves in order to keep up the operations.

It is worth noting that the top fiat-backed stablecoins all claim to be fully backed 1:1. It is however not (yet) a mandatory requirement to be fully collateralized, just like many governments do not have full reserves for all money supply in circulation. But being fully collateralized is the most straightforward way to give users confidence in the liquidity of the said stablecoins.

[11] You can check the Bitcoin Pizza Index online to see the actual value now.

Most notable examples of fiat-backed stablecoins are USD Coin (USDC) and Tether (USDT).



Stable, but for Whom?

With no surprises, regulations will likely be a big theme for stablecoins in the near future across the globe. The fact that stablecoins (particularly the USD-pegged ones) directly impact the money market and influence the efficiency of monetary policy make them the primary targets for regulators. It is not an uncommon commentary from regulators that stablecoins "pose systematic risk to the traditional financial system which may potentially undermine the greater economy".

Bringing more scrutiny to the space is not necessarily a bad thing. Government regulations, if done right, can in fact help facilitate stablecoins or crypto to gain mainstream adoption, by offering greater transparency through eliminating bad actors and filling in that gap between traditional finance and decentralized finance.

Exchange Tokens

Cryptocurrency exchanges are platforms that facilitate the buying, selling and exchanging of cryptocurrencies (and in some cases, between fiat currencies and cryptocurrencies).

As the crypto industry matures and becomes more competitive, crypto exchanges have started offering tokens as a "loyalty program" for their users. These crypto exchange tokens are also digital assets, and in essence can be bought and sold similar to all other cryptocurrencies.

Centralized Exchanges (CEX) Tokens

CEX tokens are generally used within the respective exchanges to facilitate trading or other operations. Exchange token holders may have access to fee discounts, staking rewards, or trading pairs that provide better liquidity. The primary objective is often to incentivize users to retain their funding in their exchange. The price of these tokens are often tied to the performance of the exchange and to the number of exchange users.

Some notable CEX tokens include the now notorious FTX Token (FTT), Binance Token (BNB), Crypto.com Token (CRO).

The sheer size and influence of these exchanges have seen some of them expanding the development of these exchange tokens into their own layer 1 chain solution, and subsequently building an entire ecosystem on them. Binance, for example, has created Binance Smart Chain[12] which has resulted in numerous applications spawning, and users of these applications have to use BNB tokens to pay transaction (gas) fees.

[12] They have since changed the chain's name to BNB Smart Chain as an attempt to distance the ecosystem from the Binance brand name. BNB now stands for "Build and Build", which is awkward enough to make most market participants happy to stick with Binance Smart Chain.

Governance Tokens & Utility Tokens

Governance Tokens

Governance tokens are tokens being used as **a proxy of votes to govern the directions of the underlying project**. Governance tokens are not necessarily an exclusive concept to other token types we have discussed. Any token can also be a governance token if the corresponding voting mechanism is implemented.

Most crypto projects, despite being decentralized in nature, are often initiated by some core project members and developers. The organizational structure, and hence, its governance, indeed varies from project to project. Some governance tokens are created with very little power on the directions of the project, while other governance tokens may have the power to completely dissolve the project and request the project owners to return the remaining funding to the users. Tokens can also be programmed to have different tiers that carry different voting weightings or even veto powers.

As you can see, community governance does not necessarily imply a full liberal democracy in the modern world. At best, it resembles most closely to voting rights by the shareholders of listed companies.

Utility Tokens

Utility tokens are the opposite concept of governance tokens. They are being earned or spent as part of the application of the project, without the power to influence the project's directions.

A project is free to use a single token as their governance *and* utility token. However, there are several advantages to using a "dual-token" system.

The most important advantage is that project owners can control the circulating supply of governance tokens to a limited number, while giving themselves the freedom to increase the circulation of utility tokens (or to make the supply unlimited). This way, one can scale up the project easily, without worrying about the governance rights being diluted.

Other Crypto Products

In this section, we cover some digital asset products which may become more relevant as the digital asset marketplace matures.

Security Token Offerings (STO)

Security Token Offering (STO) is a type of public offering in the form of tokenized digital securities. Unlike initial coin offerings (ICO), which are usually classified as utility tokens, STOs have been classified as securities, and are under the regulations and supervision of regulators around the world, typically those governing securities. In particular, STO is regulated by the Securities and Futures Commission in Hong Kong. Only licensed digital trading platforms can carry licensed activities like dealing in STO.

Exchange Traded Funds (ETF)

A cryptocurrency exchange traded fund (ETF) is an investment fund that tracks the price of a single cryptocurrency or a basket of digital assets. This allows investors to get exposure to digital assets without having to buy them directly. The two most common types of cryptocurrency ETFs are physical backed ETFs and derivatives backed ETF.

Physical backed ETFs involve the investment firm managing the fund that buys cryptocurrencies or stocks in companies that invest in crypto or related companies involved in the underlying blockchain technology development. Investors can buy shares in the ETF, giving them indirect investment return to the underlying assets the investment firms invested in.

The adoption and approval of Bitcoin ETFs, especially Bitcoin spot ETFs, have been under the spotlight in recent years, as such ETFs will provide the general public the accessibility to invest in Bitcoin, using traditional financial markets as the channel bridging two worlds.

Regulations

It is only fair to wrap up this guide with a more imminent subject that may dictate the directions of the crypto industry: Regulations.

Many who believe in the ideals of crypto are often those who lean away from central establishments and authorities, given the decentralization nature of crypto and blockchain. However, in practice, it is almost inevitable to introduce some degree of regulations (and other involvement of centralized authorities) if the crypto ecosystem is set to integrate with the rest of the financial system in the world.

For instance, one wants to buy bitcoins with US dollars. Bitcoin may be unregulated in some jurisdictions, but US dollars are quite comprehensively regulated almost everywhere. On the other hand, one probably does not want to have their P2P or daily transactions being monitored and regulated (e.g. keeping records of your ID and proving the ownership of funds buying a coffee should be deemed to be extensive and unnecessary). So it is, as always, a question of where we draw the line.

Let's break the discussions down to regulation types and product types.

Regulation Types

Many regulators across the globe have either enacted regulatory schemes for dealing in digital assets or are on the brink of doing so. The following are some of the common requirements that the regulators are focussed on:

AML / CFT

These are the common 3-letter acronym laws or policies you may have heard before.

- **Anti-Money Laundering (AML)**. Guidelines and procedures for institutions to prevent and to detect the proceeds originated from illicit activities being disguised as legitimate funds.

- **Combat / Counter Financing of Terrorism (CFT)**, or sometimes Counter-Terrorist Financing (CTF). Guidelines and procedures for institutions to prevent and to detect the use of funds, to support terrorist activities.

As you can deduce from these short descriptions, these are holistic laws and regulations being enforced across the whole financial system. Leaving any hole in any asset class will render the laws less effective.

Segregation of Client Assets

As we mentioned in the earlier chapter, many jurisdictions, particularly in the securities industry, require institutions (usually brokerage firms) to hold client assets in a separate account from the institution's own assets. Such segregation protects the client assets from potential loss in the event of the institution's insolvency, essentially isolating the investment risk of the clients and of the institutions.

Obviously, unregulated crypto exchanges have had very little incentive to follow this rule as aggregating client and house assets in the same wallet addresses reduces transaction time and cost. However, this segregation requirement will become the most pressing demand not only from regulators but also from end users in the near future, especially in light of the spectacular failures (FTX, Terra Luna, to name a few notable examples) we have seen in 2022.

Travel Rule for Crypto

Travel Rule is one of the implementations to enforce AML / CFT policies. It requires crypto exchanges to obtain and pass on certain customer information to the next exchange or digital asset service provider when transmitting the customer's assets. The rule was introduced by the Financial Action Task Force (FATF).

Coin Purity Check

Coin purity check is not necessarily a well-adapted rule worldwide yet, but it is nevertheless another implementation to enforce AML / CFT policies, thanks to blockchain technology. As blockchain transactions are mostly publicly available and each token can be uniquely identifiable, one can trace any deposit of funds on blockchain to see if these particular coins have ever interacted with suspicious wallet addresses that have previously been associated with illicit activities[13].

[13] We have simplified the discussion here ignoring the existence of privacy coins and privacy exchanges.

A “score” of coin purity can be assessed and assigned. If a token has a low coin purity score, the recipient may wish to decline the deposit from the originator, and potentially follow up with other actions, including reporting to law enforcement.

Product Types

The debates of regulations on each individual product can easily expand into their own essays. We will try to keep this brief and explain the complexity of each.

Bitcoin

Being the oldest cryptocurrency, Bitcoin is naturally the one being most matured towards regulations. In many jurisdictions, laws pertaining to cryptocurrency are often “borrowed” over from existing laws of other asset classes.

For Bitcoin, the debate centers on how to classify it: is it a currency, a security, a commodity, or even a separate new asset class? Based on the answer, it may be governed by a different regulatory body, a combination of different authorities, or even a brand new authority specifically for virtual assets.

Ethereum and other Altcoins

The more we go down the list by market capitalization, the more diverse the list becomes: different natures, usages and designs that regulators need to decide whether or not to categorically group all cryptocurrencies into a single asset class, or if they have to come up with a new set of criteria to attempt to qualify these assets..

Stablecoins

Regulators pay more attention to stablecoins than other cryptocurrencies, as stablecoins are a direct competitor to a nation’s fiat currency, and may potentially impair the efficiency of a government’s monetary policy.

The focus with stablecoins is often on the issuers, particularly how they manage their reserves: Are they required to be fully backed 1 to 1? Are they allowed to reinvest their reserves, and to what extent? How do we handle crypto-backed stablecoins or algorithmically-pegged stablecoins?

CEX / DEX

Regulations revolving around centralized exchanges and brokerage firms seem to be the most matured in crypto space.

On the other hand, decentralized exchanges are permissionless by design. This poses a great challenge to regulate these platforms, as it is virtually impossible to conduct the same level of KYC as traditional financial institutions.