Cryptocurrencies: A Guide to Getting Started On

Crude Wealth LTD

COMMUNITY PAPER

Cover: Unsplash/EfeKurnaz

Inside: Unsplash/CallumWale; Unsplash/KrzysztofKowalik; Unsplash/NaomiHutchinson; Unsplash/JosueAs; Unsplash/RalphRavi; Unsplash/ChristianLue;

Contents

2

About Crude Wealth LTD

Crude Wealth LTD is a United Kingdom Company, Limited, located in the United Kingdom. Crude Wealth LTD is duely and verifiably registered under United Kingdom Investment Commission(UKIC). Crude Wealth LTD involved in Forex and Crypto currency Trading simultaneously. Crude Wealth LTD trading team consists of highly qualified analyst, analytical experts who by using their experience and latest software, are able to predict the movements in currency exchange & cryptocurrency market with best accuracy.

This company is managed by professional crypto currency trading experts with its vision and aim to help those willing to attain financial freedom but lack the technical know-how to achieve. We have perpetuated our vision to remain at the pinnacle of the crypto world through the opportunity offered to our distinguished clients.

2

Our Affordable investment plans

Starter Plan.

This plan is one of our amazingly affordable plans, which comes with a minimum investment of $200 and witha maximum investment of $499. This plan yeilds returns of up to 4.5%, in 5 days, That means you'll get 4.5% of your investment in a total of 5 days. To subscribe to this plan visit our website.

Professional Plan

The professional plan is an affordable plan, which comes with a minimum investment of $500 and witha maximum investment of $4999. This plan yeilds returns of up to 5.0%, in 5 days, That means you'll get 5.0% of your investment in a total of 5days. To subscribe to this plan visit our website at stockwealthinvestment.com.

Enterprise Plan.

The Enterprise plan is an affordable plan, which comes with a minimum investment of $5000 and witha maximum investment of $9999. This plan yeilds returns of up to 7.5%, i n 10 days,
To subscribe to this pla n visit our website at stockwealthinvestment.com.

2

Module 1 Plan

The module 1 plan is an affordable plan, which comes with a minimum investment of $1 0000 and witha maximum investment of $49999. This plan yeilds returns of up to 10.0%, in 28 days, That means you'll ge t 10.0 % of your investment in a tota l of 28 days. To subscribe to this plan visit our website
at stockwealthinvestment.com.

Module 2 Plan

The Module 2 plan, which comes with a minimum
investment of $50000 and with an unlimited maximum investment. This plan yeilds returns of up to 12%, in 28 days, That means you'll get 1 2% of your investment in a total of 28 days . To subscribe to this plan visit our website at stockwealthinvestment.com.

Executive summary

As cryptocurrencies transform how we trade, transact and interact online, it has become more important than ever for technology leaders to have experience with these innovations.

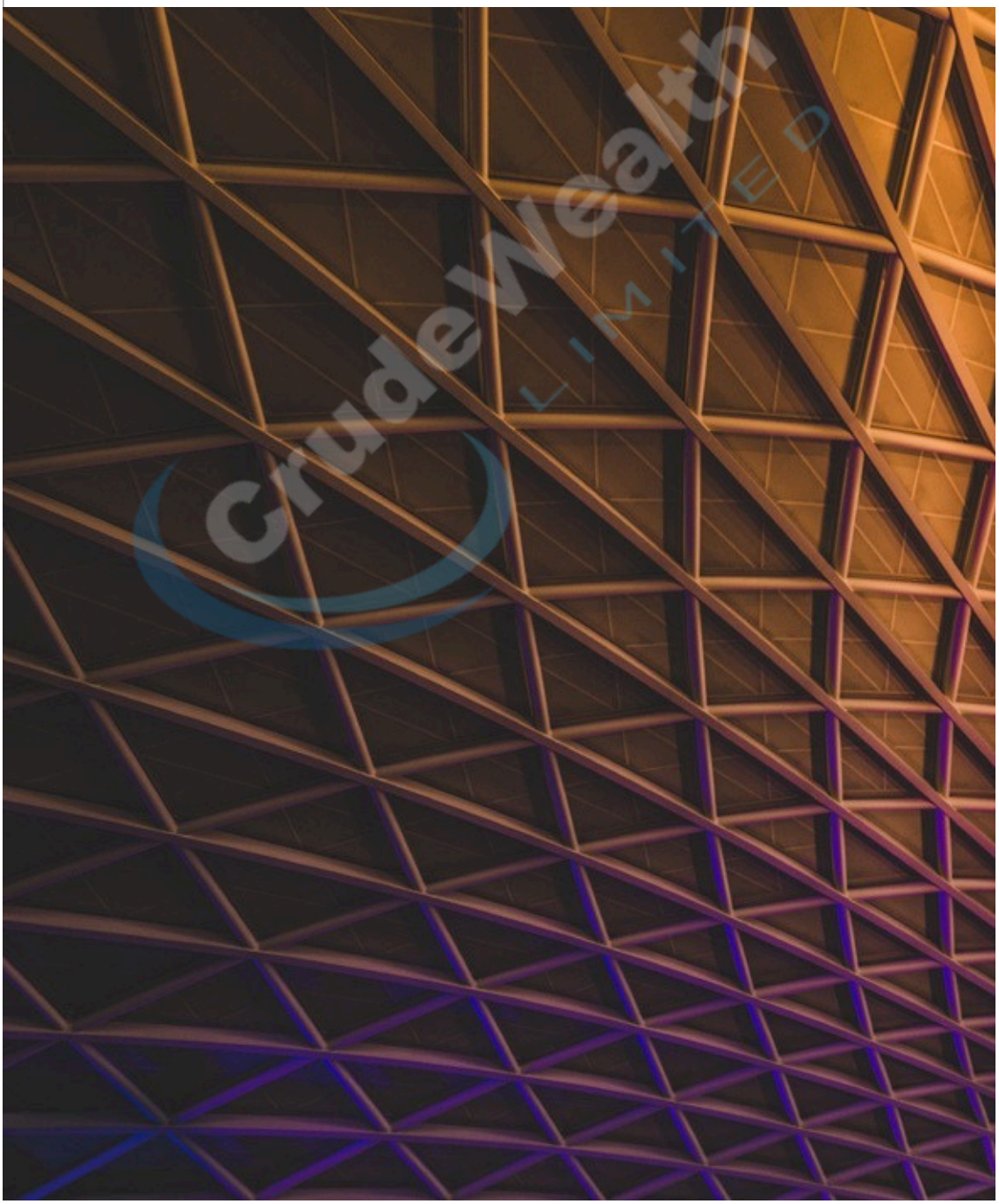
Since the creation of bitcoin in 2008, cryptocurrencies have been the subject of uncertainty, scepticism, hype and disillusionment. While still early as a technology category, cryptocurrencies are now maturing and have demonstrable utility.1 As of this writing, cryptocurrencies in aggregate are valued at over $2 trillion in market capitalization.2 Cryptocurrency-based lending applications and decentralized trading venues currently command $65 billion in on-boarded assets.3 Just in the first quarter of 2021, over $1 billion worth of digital collectibles and digital art traded hands, underpinned by cryptocurrency networks.4 This is not to mention the areas that are still in exploratory phases: community governance, file storage, and cross-border payments, among others.

As cryptocurrency matures, there has been increased interest from technology leaders in understanding this industry. While there is no shortage of content that exists explaining cryptocurrency technology and the promise that it holds, there is little reliable, practical guidance on where and how technology professionals can get started with getting hands-on with cryptocurrency.

This guide serves as a manual for corporate leaders, including, but not limited to, chief executive officers, innovation officers, chief information officers, product managers and other technology professionals. You should come away with an understanding of how to transact and trade cryptocurrencies, view and participate in the underlying blockchain systems, get started programming decentralized applications, engage in blockchain governance systems, reason about both privacy and scalability trade-offs among different cryptocurrencies, and research and consider relevant jurisdictional guidelines and regulations. The best way to be equipped to speak to, engage with and apply cryptocurrency to your life and your workplace is not to read about it, but rather to start working with it directly. The contents of this manual are your guide for doing so.

Note about scope: This guide speaks strictly to cryptocurrency – digital assets and digital infrastructure such as Bitcoin and Ethereum – that are open sourced and public. It does not address private or permissioned blockchains, or their related digital assets.

1 Getting started



1.1 Buying cryptocurrency

As you start your journey, you may be interested in acquiring cryptocurrency. We will walk through a few basic steps to follow in order to do this after considering the legality of cryptocurrency in your jurisdiction:

> Many institutions choose to rely on third parties, either exchanges or dedicated custodians, in order to hold their cryptocurrency assets.

Custody cryptocurrency To own cryptocurrency, you are required to have a "wallet". A cryptocurrency wallet is how coins and tokens are held or custodied.

There are a couple of options for "custody" of your assets:

– Third-party service: You may choose to hold your cryptocurrency with a third party, such as an exchange, which will provide the wallet for you. In this case, you should be aware that you are trusting the security of that exchange with your assets. If the exchange gets hacked, you may have little or no recourse. Generally, to set up a wallet with an exchange, you will need to set up an account using information, including your name, passport or ID number.

– Self-hosted: You may choose to self-host your wallet. If you go this route, you will bypass these identification requirements of third-party providers. You will also be taking the security of your assets into your own hands. Be aware that if you lose the necessary materials to access your wallet, you will have no recourse.

The type of cryptocurrency wallet that you will want will depend on the specific needs and features desired. Some cryptocurrency wallets only support specific cryptocurrencies or have limited functionality. This can sometimes mean a trade-off between security and usability. Major differences related to the custody of cryptocurrency include who has access to the private keys of the wallet, how often sensitive data is exposed to the internet, and the type of software or hardware that can be used in setup and maintenance.

Many institutions choose to rely on third parties, either exchanges or dedicated custodians, in order to hold their cryptocurrency assets. This gives them comfort that the ultimate responsibility around the security of their assets lies with a third party. However, this entails deep due diligence to understand the reliability, reputation and recourse provided by that exchange or custodian. Other institutions, particularly those with the requisite security know-how in-house, choose to self-host.

Custodying cryptocurrency is really about the secure custody of a private key, or a string of data akin to a password. Private keys may be represented as a binary code, QR code, mnemonic phrase or other formats. Private keys may be stored in software applications such as mobile apps or desktop applications (typically considered "hot" wallets as they are regularly connected to the internet) or on a specialized, separate hardware device not connected to the internet (also referred to as "cold" storage). There is also the possibility to use a multi-signature wallet, which requires multiple private keys to approve a transaction before assets are transferred (an m of n setup). In theory, this can increase the security of funds. There are pros and cons to each type of wallet with differing security, recovery methods and usability.5

Determine a method to acquire cryptocurrency

Once you have a wallet established, or a way to custody your assets, you will need to acquire your cryptocurrency. There are several methods and platforms to consider:

– Purchasing cryptocurrency as an individual: The most common route is to buy it via a centralized exchange.6 These exchanges serve as on- and off-ramps and charge fees (ranging from roughly 0.05-5.00%) on each transaction. Different jurisdictions have different exchanges providing liquidity.

– Purchasing cryptocurrency as an institution: You can use a centralized exchange, but often better liquidity and lower fees will be found via an over-the-counter trading desk. You can search for the competitors in these markets based on your jurisdiction.

– Alternative methods: Buying cryptocurrency is not the only way to own cryptocurrency. Other ways to acquire cryptocurrency include participation in the network (mining and staking), earning it (payment for work), airdrops (coins and tokens are randomly distributed to wallets), faucets (a way to collect small quantities of crypto for free), and more.

Taxation

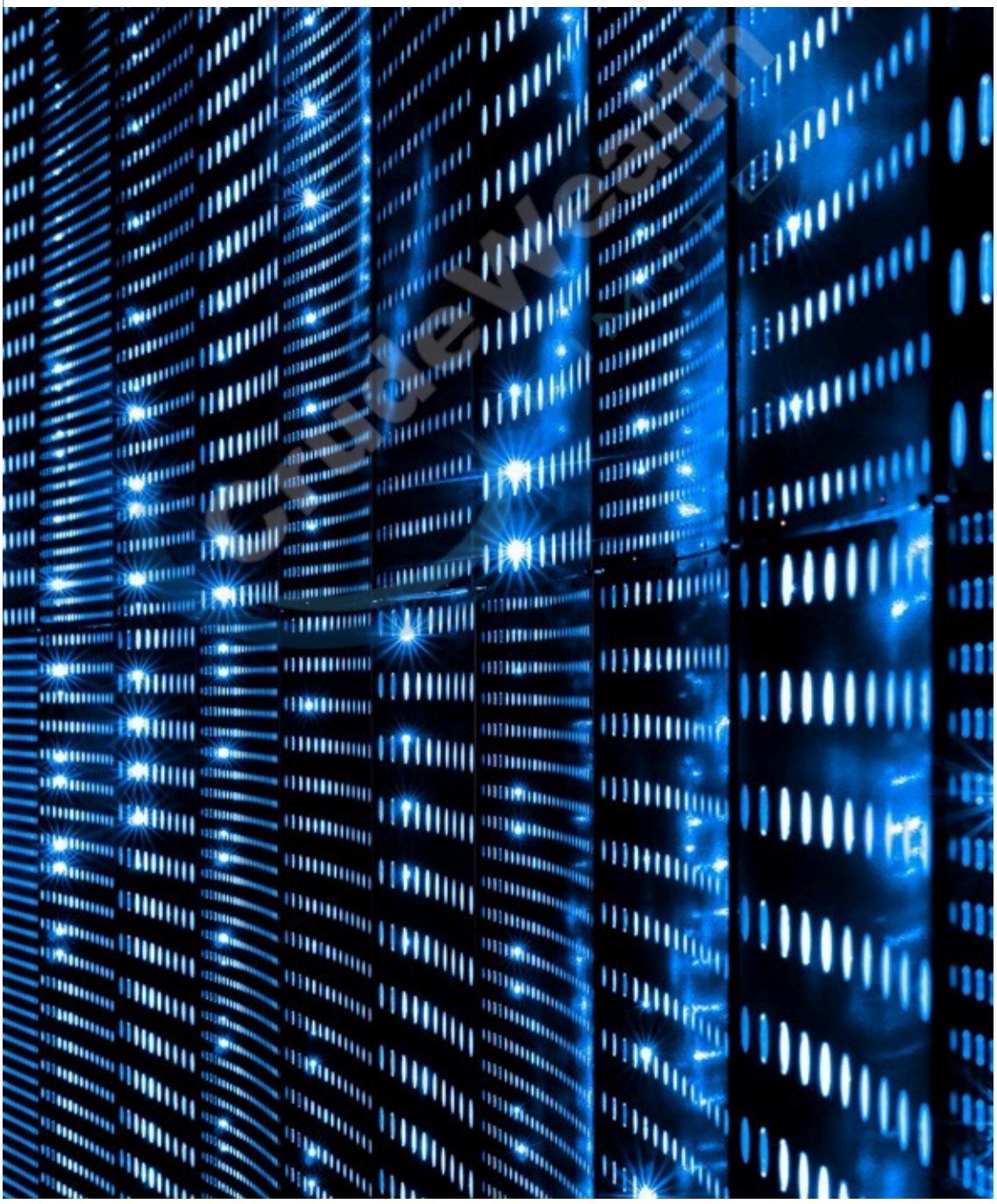
Each country taxes digital assets, including cryptocurrency, differently. Keep track of all cryptocurrency transactions to simplify your reconciliation process (when was the transfer made, in what amount, for what goods or services, etc.). Keep in mind that converting one cryptocurrency to another cryptocurrency (e.g. bitcoin to ether) may be considered taxable in some jurisdictions. Spending cryptocurrency to purchase small-value objects such as a coffee may also be taxable as it constitutes a sale of the cryptocurrency.

1.2 Making transactions

To make a transaction, you will need a few pieces of information. You will need access to your cryptocurrency. This involves having the information needed to access your funds via the third-party custodian, or having the private key to access the funds in your self-hosted wallet. You will also need the wallet address (or public key) of your counterparty. This might take the form of a string or QR code.

Once you enter the amount you are sending and the address of your counterparty, the system will sign your transaction with your private key (either done by you personally, or by the third party if you chose to use one), broadcast this to the network and show a unique code that represents the transaction called the transaction hash.

2 Exploring the blockchain



2.1 Block explorer

A block explorer – a website that tracks all the information inside the blockchain and shows it in intelligible form – is a useful tool for any blockchain user. It acts as a "search engine" for a particular blockchain, allowing users to verify transactions, or check the status of the network.

Most blockchains are transparent, meaning all details of each transaction are publicly broadcasted and recorded and allow for associated metadata to be queried via a block explorer. Traders can verify that transactions have gone through and finalized, agencies can audit and verify reported data, and law enforcement can trace the movement of funds. Individuals can also use block explorers to better understand the degree to which and how blockchains are being used.

2.2Pseudonymity vs anonymity

Most blockchains enable pseudonymity, but not anonymity, meaning they do not guarantee that a user will be unidentifiable.

Pseudonymity means that identities on the blockchain are not directly linked to real-world identifiers such as names, addresses, or identification numbers. When looking at a block explorer, you will not see names of individuals or institutions, but rather strings of data representing those holders' public key addresses. With enough effort, however, most of those addresses can be linked back to identifiers. This can be done via examination of on-chain activity, transaction histories and trails, and analysis of other data such as timestamps and IP addresses associated with transactions.

2.3 Privacy

> There are, however, a handful of privacy coins that enable private blockchain transactions.

As discussed earlier, most blockchains store data in a way that is publicly accessible at any time. There are, however, a handful of privacy coins that enable private blockchain transactions. Two of the best-known projects focusing on this use case are Monero (XMR) and Zcash (ZEC), a fork of the Bitcoin protocol that leverages Zero Knowledge Proofs (ZKPs) to maintain privacy. The basic idea behind ZKPs consists in allowing one party (a prover) to prove to another one (a verifier) the possession of a certain information without revealing that information.

Zcash incorporates transparent "t" and private "z" addresses for sending, receiving, and storing ZEC, thus offering four transaction types from which the user can choose. For example, a transaction facilitated between two "z" addresses is fully shielded. This implies only the fees paid and the occurrence of the transaction appear on the public blockchain, while the addresses, transaction amount and the encrypted memo field are not publicly visible. For auditing and regulatory compliance, Zcash users can use view keys to selectively share address and transaction information.

Monero, on the other hand, only offers fully private transactions. The Monero protocol maintains the privacy of its senders through ring signatures, which do not require a trusted party to perform a setup process. Ring signatures leverage private spend and view keys, as well as public addresses, to facilitate transactions while making it computationally impossible to determine whose key was used to sign. Additionally, stealth addresses guarantee the wallet address of the recipient is never publicly linked to any transaction. The public can nonetheless confirm the legitimacy of the transactions without de-anonymizing the participants through ring confidential transactions. Such privacy coins may face certain liquidity challenges because the current regulatory view on this feature is mixed, thus complicating their listings on exchanges.7

2.4 Running a node

Full nodes for any blockchain will place high demands on memory, storage and bandwidth.

Blockchains are decentralized, distributed databases. These databases are implemented in software and run on a network of nodes. Because cryptocurrency blockchains are permissionless and the code for popular nodes is open source, anyone can participate in the network by running a node.

Reasons for running a node may include:

- Providing a service to the blockchain network: Nodes receive transactions, check them against the rules of the protocol and relay them on to other nodes. A diverse and resilient set of nodes is integral to the health and security of the network.
- Benefits to the host: Running a node enables the individual or institution to interact directly with the blockchain database without relying on third parties. This may be of particular importance to those who place special value on privacy and security or developers building wallets, block explorers and working on chain analytics.

Running a full node entails downloading, validating, and hosting a full copy of the blockchain database of transactions, going back to the first transaction on the network. Archive nodes take this one step further, maintaining a full memory of the state of the blockchain for any given point in time. Light nodes, meanwhile, just store block headers, or abridged versions of the transactions in the chain. Light nodes are therefore reliant on full nodes for most data, but that data can be verified against the information contained in the block headers.

There are costs to running nodes. Full nodes for any blockchain will place high demands on memory, storage and bandwidth. All of this can become costly. Nodes generally need to be running for a minimum of six hours per day – and may take days to sync the entire history of the blockchain for the first time. The Bitcoin blockchain demands a minimum of 350 gigabytes of free disk space, 2 gigabytes of memory, and a broadband internet connection with an upload speed of at least 400 kilobits per second. Light nodes make fewer demands on memory and disk space (and can even be run on mobile phones) but are more reliant on network bandwidth.

To judge whether running a full or a light node may be of interest and in order to explore the first steps in doing so, consult the following resources:

- Bitcoin
  - Minimum requirements of a Bitcoin node
  - Bitcoin core
- Ethereum
  - Benefits of an Ethereum node
  - Light client
  - How to set up an Ethereum node

There are also third-party providers who offer node hosting services. This may be a more suitable path if you are with an institution, such as a financial institution, that does not have particular sensitivities around self-hosting and will not be developing applications, or tools that need to directly interact with the blockchain.

2.5Consensus mechanisms and mining

Consensus mechanisms are a critical function that secure permissionless blockchain ledgers and enable the characteristics of immutability and censorship resistance.

Proof of Work (PoW), the mechanism for Bitcoin, is perhaps the best known. PoW mining is the process of computers competing for a reward by executing a cryptographic mining algorithm to meet an output of a predetermined difficulty level. Bitcoin miners hash four inputs using the SHA- 256 cryptographic hash function: the transactions of a block; the hash of the previous block; the time stamp; and the nonce (a random number). If the output of this cryptographic function meets a certain difficulty level (i.e. a certain number of leading zero bits), the block is accepted by other nodes on the network and the miner is rewarded.

The culmination of mining results in the appending of new blocks to the blockchain. The newly appended blocks must adhere to the consensus rules of the Bitcoin network or will otherwise be rejected by nodes. The costliness of PoW mining means those who mine bitcoin, but act against the consensus rules of the network, lose significant sums of capital.

A deeper dive

- Difficulty: Because all miners are competing to append blocks to the Bitcoin network, the difficulty rises as more miners join and drops as miners fall. The difficulty adjusts every 2016 blocks (or every two weeks) and this process keeps miners finding blocks at a rate of roughly one per 10 minutes.
- Reward: When a block is successfully appended, a miner can send the first transaction to their own address (known as the coinbase transaction), which compensates the miner with a “block reward”. This block reward consists

> The key inputs to successful mining are low power cost and access to competitive equipment.

of newly issued bitcoin and all transaction fees from the mined block. The amount of newly issued bitcoin halves every 210,000 blocks, approximately every four years. The block subsidy originally started at 50 bitcoin (BTC) and currently is at 6.25 BTC mined approximately every 10 minutes, or about 900 bitcoin mined every 24 hours (as of April 2021). This algorithm ensures bitcoin is a scarce asset. When bitcoin first launched, for the first four years, approximately 7,200 bitcoin were mined daily.

– Hashrate: The speed of solving the cryptographic hash function is the hashrate; the total amount is the network hashrate. If one miner controls around 10% of the Bitcoin network hashrate, they can expect to mine roughly one in ten blocks, and more as their share of the network hashrate increases.

Attacking the network

To attack the network, a malicious entity would need to capture 51% of the hash power, allowing the entity to build a longer chain and double spend bitcoin, which they had previously used in a transaction. This would require convincing over 50% of miners to either sell or rent their hash power or someone with more hash power than the current total network hashrate.

Hardware Given the economic incentives, the mining industry is perpetually in an arms race to develop next generation hardware that increases hashrate output. Early bitcoin miners started with central processing units (CPUs), which evolved to graphics processing units (GPUs) and then field programmable gate arrays (FPGAs). But in 2013, single-purpose application specific integrated circuits (ASICs) optimized to hash the SHA-256 algorithm became prevalent. The difficulty level of bitcoin mining was pushed up significantly when ASICs were widely distributed to miners. The hashrate performance of ASICs and consequent difficulty jumps made all other hardware types obsolete. Other types of hardware are still used in the mining of other cryptocurrency protocols, especially those not based on SHA-256.

The key inputs to successful mining are low power cost and access to competitive equipment (ASICs, servers). To build a business of size and scale, particularly for the most popular/competitive cryptocurrencies like bitcoin, miners take on sizable risk in the form of upfront investment and capital expenditure in long-term power contracts, real estate, large volume mining equipment/ASICs, and energy efficient and temperature-controlled data centres to host the mining equipment. The upfront investment is often sized with certain assumptions about crypto market prices, which can be volatile and not guaranteed to materialize.

Given the statistics of success, miners frequently collaborate through participation in a mining pool. Participating in a mining pool enables a miner to have certainty of bitcoin mining rewards on a consistent schedule.

Despite the investment risk and challenges associated with industrial cryptocurrency mining, individuals can set up smaller scale mining operations to participate fully in cryptocurrency networks and may even discover more productivity by mining less mainstream and less competitive cryptocurrencies.

Getting started with PoW mining

– Acquire equipment: Selection of equipment depends on the triangulation of cost, availability, hashrate performance and power consumption. You may choose either a bitcoin- specific ASIC or hardware that can be used to mine multiple different cryptocurrencies, which have varying algorithms. While it may be difficult to procure equipment from manufacturers, there are secondary markets for used miners available for purchase. As the mining hardware can be loud and hot, often running more than one miner may require finding a data centre hosting location with a low cost of power – factors include the location, source of power (renewable energy based), cost per kilowatt (kWh), as well as whether or not the facility incurs additional costs like cooling requirements to ensure maximum efficiency of the miners.

– Select and contribute hashrate to mining pool: Once the hardware is set up, this can be helpful to ensure consistent returns. Factors to selecting a mining pool include cryptocurrency specialization, reputation, size of the pool and its overall percentage of global hashrate, fees paid to the pool and minimum payout sizes.

For alternative coins seeking a less power-intensive approach to securing the network than PoW mining, various consensus models have emerged such as Ethereum's move to Proof of Stake (PoS) and Algorand's Pure Proof of Stake (PPoS), which require miners to stake their native coins to become network validators, ordering transactions and creating new blocks driving all nodes to agreement on the state of the network.

In addition to less power usage, proponents for PoS suggest that barriers to entry are lower as specialized equipment is not required to mine successfully and as more network participants are able to mine with general hardware, the network composition may be more decentralized as well. However, there is some suggestion that PoS may lead to network mining inequality and may unfairly benefit well-resourced network participants since

their ability to mine successfully is directly related to the amount of native coin owned. PPoS seeks to address both PoW's energy consumption and PoS's miner inequity by enabling all network participants the opportunity to propose and validate blocks (with only the probability of mining successfully directly related to the amount of native coin owned). In selecting the consensus mechanism and mining protocol, cryptocurrency networks must trade-off between decentralization, scale and network security.

For more information on the evolution of mining and how to get started, visit:

- Evolution of Mining by Marshall Long, Tales from the Crypt
- Beginner's Guide to Mining, MasterDC
- Choosing a Mining Pool, Make Tech Easier
- Getting Started with Mining, Compass Mining
- Global Hash Rate, BTC.com
- Mempool & Transaction Fees, Mempool.Space
- How Blockchain Works, MIT

2.6 Energy consumption

> Permissioned blockchain improves efficiency and latency while also reducing energy consumption.

As explained above, in order to participate in PoW, significant computational energy is required. Upfront capital expenditure and ongoing electricity bills are costs of running a node to participate in PoW networks (e.g. Bitcoin). Energy consumption depends on the difficulty of the cryptographic puzzle to be solved by a mine in PoW. Nonetheless, the Cambridge Centre for Alternative Finance estimates bitcoin's total electricity consumption to be about 126.98 terawatt hours (TWh) per year.8

The proof-of-work scheme is thus compute-intensive and energy demanding, but it is key to addressing the double-spending problem and ensuring the security of the blockchain, as it costs money to attack the network. It is hard to mitigate the energy consumption of PoW blockchains because even if more transactions are added to one block, the cryptographic puzzle difficulty ultimately defines the amount of energy required to participate. In PoW blockchain, energy consumption correlates to market capitalization.9

Alternative consensus mechanisms such as PoS consensus and permissioned blockchain consensus consume less energy than PoW blockchains.10 PoS blockchains are a good alternative to PoW blockchains and entail a participant "staking" capital. This consensus mechanism consumes much less energy and provides adequate security. However, PoS consensus is less battle-tested than PoW so it cannot be said with full certainty that the PoS consensus provides the same security level as PoW.11 Permissioned blockchain improves efficiency and latency while also reducing energy consumption. Permissioned blockchains are especially suitable for public institutions aiming to decentralize some of their operations. However, they do not give the same flexibility when it comes to decentralization of participants.

Thus, when a user is participating in a blockchain network, they should assess what the economic benefit is of choosing a specific type of consensus mechanism and ensure the energy consumption is weighed sufficiently against benefits.

3 Programmability

3.1 Ethereum

> Ethereum is the first, and most widely used, blockchain that allows for the development of programmable applications.

Ethereum is the first, and most widely used, blockchain that allows for the development of programmable applications which operate on its network. It was inspired by Bitcoin and was publicly launched in 2016.

There are a few key components to Ethereum and similar programmable blockchains:

– A smart contract is code on a blockchain that executes when predefined conditions are met. For example, one could write a programme permitting payment of $10 for a specific digital audio file, but only if transferred before a certain date. Because this code is publicly auditable and verifiable, it allows strangers to have the trust to transact without the involvement of any third parties. Contrast that with today where a handful of third parties operate behind the scenes: a platform ensuring rights ownership, the bank ensuring a buyer has funds and the database which hosts the file.

– Solidity is Ethereum's high-level programming language for coding smart contracts, which are then recorded and executed on the Ethereum blockchain.

– Ether (ETH) is the native currency used to pay for transaction fees. Running and verifying smart contracts requires energy and computing resources. ETH is the native token that pays network nodes for their resource contributions (and therefore provides an incentive for other nodes to participate).

– Decentralized applications (abbreviated as "dApps"), in turn, are programmes that use blockchain-based data and smart contracts, rather than centralized databases and computing environments.

Therefore, what may sound like an arcane innovation – smart contracts recorded on a public ledger – has the potential to enable entirely new ways of interacting on the internet. For example, users can have full control over their own data and use a smart contract to require payment for access to that data. This inverts ad-based internet monetization, where platforms sell user data to advertisers and share little if any profit or control with users. In addition, a blockchain is by nature a globally synchronized database stored across many computers rather than servers owned by the few. This makes it more difficult to curtail access or alter data according to national origin or other motivations.

Programmable blockchain infrastructure is an area of robust technical innovation and competition among numerous protocols in an effort to increase the speed, capacity and security of distributed infrastructure to compete with the performance of centralized internet infrastructure.

To get started with Ethereum, visit Ethereum.org.

3.2Languages and reference implementations

Different blockchains use unique languages and reference implementations – each with its own set of attacks and defences. Among the most common languages used for blockchain are C++, Solidity, Java, JavaScript and Python.

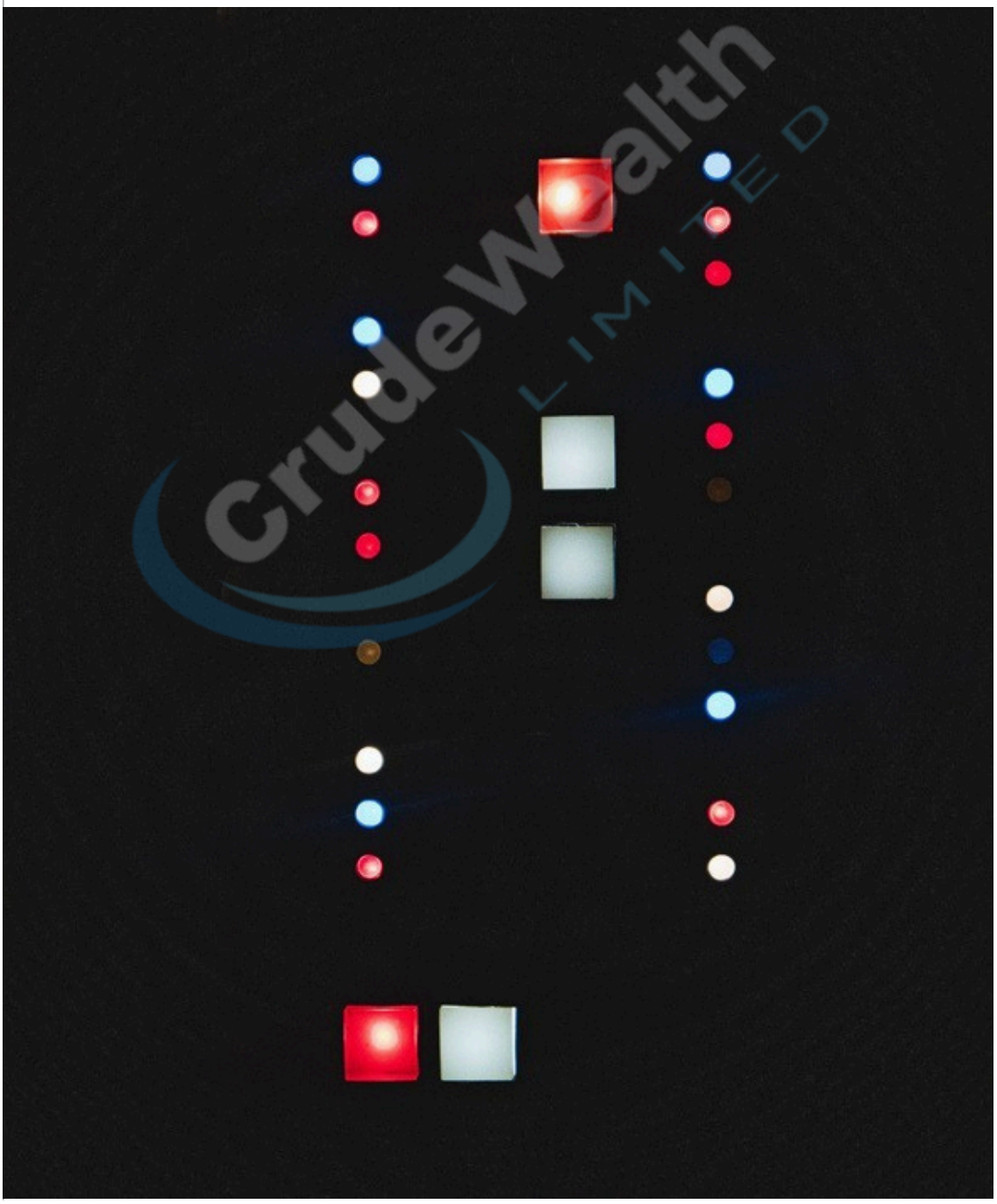
Taking the example of the Ethereum blockchain discussed above, we will examine challenges, types of languages and verifications. Exploitations emerge when there is an error in the smart contract code; it arises when developers fail to identify code errors in the decentralized application. Examples include re-entrancy, smart contract overflow/underflow, short address attack, delegate call, default visibilities, transaction ordering dependency and timestamp dependence. The listed attacks can allow attackers to drain smart contracts or manipulate smart contract vulnerabilities to favour them.

Defences have been made on Ethereum through analysis of smart contracts to mitigate attacks, including: Slither, a static analysis framework for smart contract code; MythX, a security analysis service that scans Ethereum Virtual Machine (EVM) based smart contracts for vulnerabilities; and Mythril, a security tool that analyses smart contracts written by Solidity. Various other types of smart contract languages have been created, such as Vyper, which was designed to be more simple, secure and easier to audit than Solidity, Psamathe, Casper, Simplicity and IELE.

Formal analysis and verification of compilers further assists resistance to attacks on Ethereum, done by giving a formal model of the program-to-verify, either by a manual construction in a language which can be interpreted by theorem provers such as Coq or Isabelle, or by a translation of the source code to some intermediate verification language (IVL) such as Boogie. Formal verification can provide the highest level of confidence about the correct behaviour of smart contracts.

Different smart contract languages each have unique vulnerability vectors. Tools for analysing bugs in blockchain languages are still nascent and research is ongoing.

4 Governance



> Governance activities include making decisions, resolving conflicts and making changes to the protocol.

While "corporate governance" refers to how corporations are managed, software protocols generally have varying governance structures that are very different from traditional corporations. Governance activities include making decisions, resolving conflicts and making changes to the protocol. Having a governance system in place is important to mitigate risk and ensure functionality and operational success. "Decentralized governance" refers simply to frameworks that function by way of multiple community participants governing transparently, without one centralized authority with exclusive hierarchical power over these activities.

Within decentralized governance, there exists a spectrum of arrangements. On one end, developers relinquish considerable control to token-holders. This often takes the form of establishing a decentralized autonomous organization (DAO) to run the protocol without input or interference from the team that led the software development of the protocol. Such an approach may result in too little leadership and slow down decision-making. Another version of decentralized governance might allow developers to implement code which is then voted on by token-holders. A final common version features developers that implement code and make a wide range of decisions, while reserving other decisions or override rights for token-holders.

There also exist a variety of voting arrangements. Two common mechanisms are:

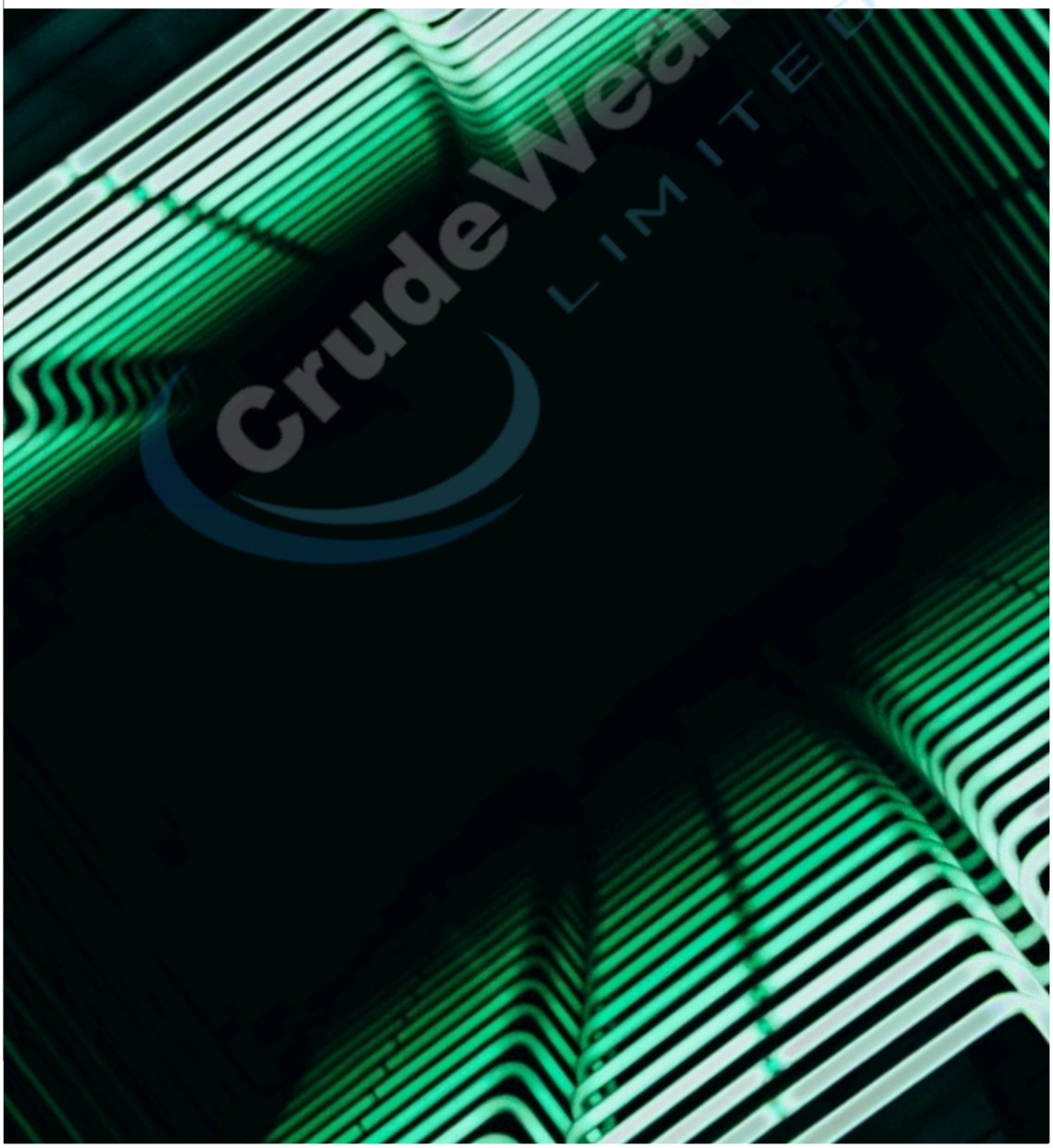
- One token, one vote: Allows for token-holders to express opinions through their tokens with one token allowing one vote. Thus, those with larger token holdings possess a larger share of voting power. Many protocols allow delegation of tokens for voting purposes so that token-holders can combine votes.

- Quadratic voting: Allows token-holders to express both direction of preference and degree of preference through allocation of votes. Quadratic voting can lead to smaller holders having relatively more say than they would under a one token, one vote model.

To learn more about governance of open source projects and to get involved in cryptocurrency governance, you may get started with these resources:

- A guide to open source project governance models, Redhat
- Leadership and Governance, Open Source Guides
- Decentralized Network Governance: Blockchain Technology and the Future of Regulation, Andrej Zwitter and Jilles Hazenberg
- Governance on Ethereum, EtHub
- What is Ethereum Governance? Complete Beginner's Guide, Unblock
- Tally
- 0x Governance

5 Throughput and scalability



Scalability is a comparative term within blockchain technology, most notably for assessing throughput. Throughput approximates the number of transactions that can be processed per second. However, with many new and innovative blockchain technologies and underlying protocols, throughput is just one factor to consider in assessing the overall scalability of a network. The following outlines the throughput of various networks and provides resources for learning more about their scalability features.

Algorand

Algorand is an open-source, permissionless, PPoS blockchain protocol. The network enables traditional finance and decentralized financial businesses to build decentralized applications. Algorand allows for 1,000 transactions per second with a ledger close time of approximately five seconds. The following resources are available to learn more about scalability on Algorand:

- Website: https://www.algorand.com
- Developer docs: https://developer.algorand.org/docs
- GitHub: https://github.com/algorand

Cardano

Cardano is an open-source PoS blockchain network and smart contract platform that aims to provide multiple features through layered design and modularity. It allows for 257 transactions per second. The following resources are available to learn more about scalability on Cardano:

- Website: https://www.cardano.org
- Developer docs: https://docs.cardano.org
- GitHub: https://github.com/input-output-hk

Celo

Celo is a mobile-first, open-source, PoS blockchain network. Their tech stack and suite of financial tools are designed for smartphone users to send, receive, and store money. Celo has a ledger close time of approximately five seconds, with 1000 transactions per second. The following resources are available to learn more about scalability on Celo:

- Website: https://celo.org/
- Developer docs: https://docs.celo.org/v/master/developer-guide/overview/introduction
- GitHub: https://github.com/celo-org/celo-monorepo

XRPL

The XRP Ledger (XRPL) is a global open-source public blockchain that focuses on payments as a use case. XRP boasts 1,500 transactions per second, costs $0.0003 per transaction and settles in 3 seconds. The following resources are available to learn more about scalability on XRPL:

- Website: https://xrpl.org
- Developer docs: https://xrpl.org/docs.html
- GitHub: https://github.com/ripple/rippled

Solana

Solana is a PoS blockchain network, with a focus on scale for mainstream adoption modelled after mobile broadband data services and hardware. It enables fast transaction times with the ability to scale as usage of the protocol grows without relying on Layer-2 systems or sharding.12 The following resources are available to learn more about scalability on Solana:

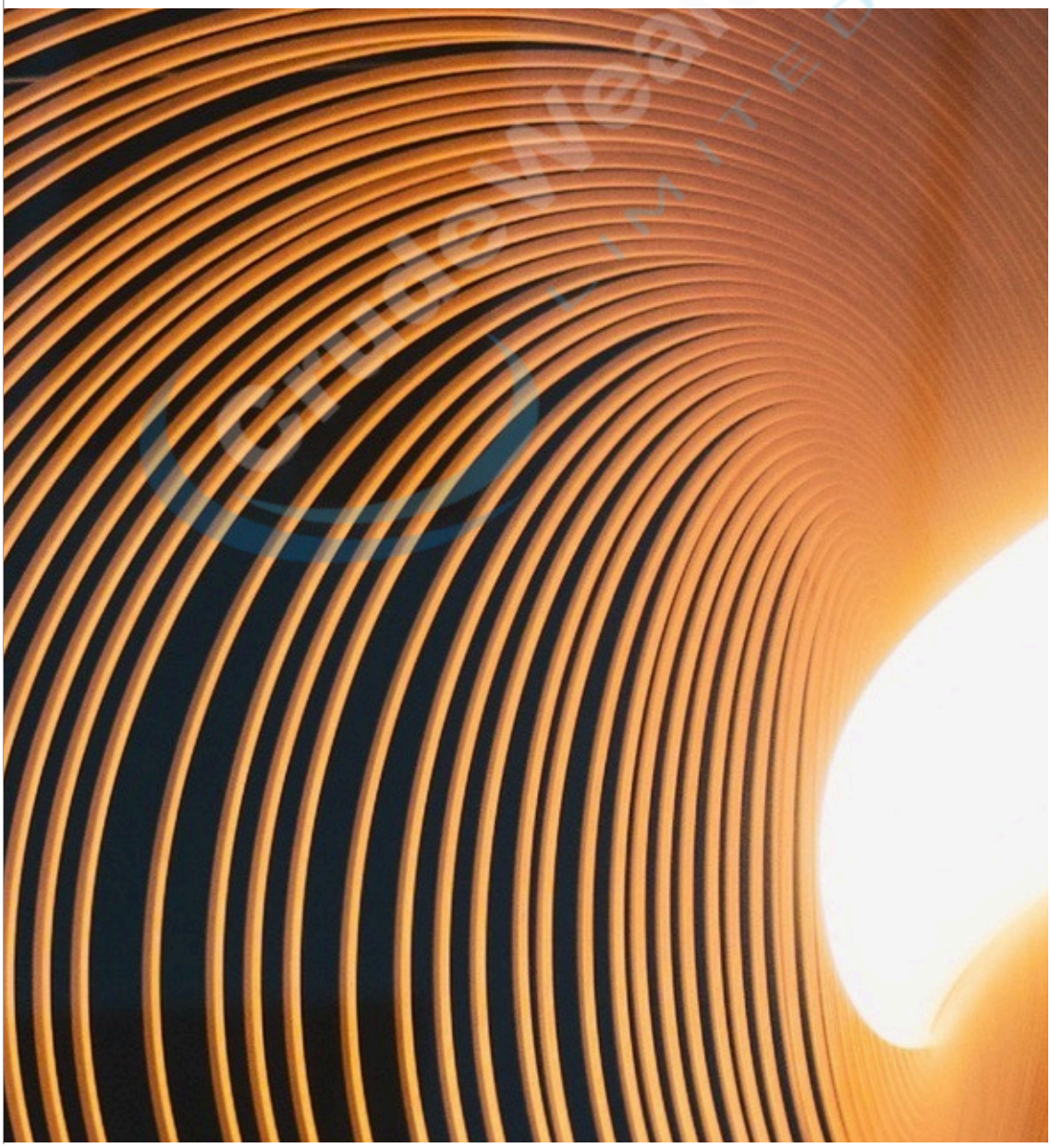
- Website: https://solana.com
- Developer docs: https://docs.solana.com
- GitHub: https://github.com/solana-labs/solana

Stellar

Stellar is a global, public blockchain network built for interoperability between traditional and digital financial infrastructure, most notably for cross-border payments. Stellar's ledger limit is currently set at 1,000 operations per ledger. With ledgers closing approximately every 5 seconds, that's a limit of 250 transactions per second. The following resources are available to learn more about scalability on Stellar:

- Website: https://stellar.org
- Developer docs: https://developers.stellar.org/docs
- GitHub: https://github.com/stellar

6 Compliance and regulatory considerations



Regulation and compliance requirements related to financial crime are particularly relevant.

Those who wish to use or interact with cryptocurrencies must keep several legal, regulatory and compliance considerations in mind.

Overview of considerations

First, given nascent technologies, there is still a lot of debate around taxonomy and classifications. This has significant implications across policy and regulation including, but not limited to, taxation, consumer protection and even which regulators are relevant within the space.

Regulation and compliance requirements related to financial crime are particularly relevant, with Know Your Customer (KYC), Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) schemes at the centre of many national and international policy and regulation decisions related to cryptocurrencies. In an attempt to prevent financial crime and illicit activity, identification is often a core component, which may be at odds with cryptocurrencies' pseudonymity. In an attempt to reconcile the gap, some policy-makers and regulators have imposed identification requirements for service providers, such as exchanges.

Current state of regulation

In the past, regulation of blockchain and cryptocurrencies has lagged behind, as regulators globally have found it difficult to regulate a technology that is borderless. To date, there has been no internationally coordinated regulation of blockchain and cryptocurrencies, though international bodies such as the Financial Action Task Force, Financial Stability Board, International Organization of Securities Commissions and Bank of International Settlements have been working towards international standards and guidance in service of this aim.

Globally, there has been a spectrum of responses to cryptocurrencies. Some have banned cryptocurrencies entirely, while others are adopting novel models such as sandboxes to better understand the technology and how to regulate it.

Some jurisdictions are consolidating regulation towards blockchain and cryptocurrencies. For example, the European Union (EU) announced their Markets in Crypto Assets (MiCa) proposal, its response to the emergence of crypto-assets. With MiCa, the EU is examining the effect of blockchain in financial markets and assessing how to mitigate typical crypto-asset risks such as fraud, cyberattacks and market manipulation. This type of cross-border regulation is positive reinforcement towards the potential of blockchain and cryptocurrencies. Whereas it is a positive sign, there is still some uncertainty about blockchain's immutable property complying with the EU General Data Protection Regulation (GDPR).

As cryptocurrencies are still an emerging financial instrument, regulation is constantly evolving. Therefore, it is recommended to consult with your appropriate jurisdiction for updated regulation before starting a blockchain or cryptocurrency project. A forthcoming publication from the World Economic Forum's Global Future Council on Cryptocurrencies will provide guidance on global cryptocurrency regulation.

To learn more about policy, regulation and compliance, consult the following resources:

- State of Crypto Newsletter, CoinDesk
- Virtual Currency Report (and associated tracker), Perkins Coie
- Global Standards Mapping Initiative, Global Blockchain Business Council and World Economic Forum
- Crypto Regulation Blog, Elliptic
- Coin Center
- Chamber of Digital Commerce

7 Conclusion

This manual represents only the first steps of getting started working with cryptocurrency.

The processes, considerations and resources imparted in this guide only skim the surface of the opportunities that exist in working with cryptocurrency. Indeed, one of the key challenges of putting this guide together came down to the need to be fastidious about what to include.
As you continue to explore the cryptocurrency ecosystem, you can engage more broadly by experimenting with or using open blockchain protocols not mentioned here. You can also engage in more depth, diving further into the possibilities around programmability, governance and scalability.

No matter what your reason for using this guide, it is critical to understand these technologies, their trade- offs and implications, and how they might be leveraged to transform industries. The best way to be prepared to speak to these subjects, advocate for sensible approaches to the new technology, and build products is to develop a first-hand understanding of cryptocurrency systems.

We encourage you to open your computer and get hands-on with everything that has been covered here and see for yourself the promises, and indeed the limitations, of this technology.

Contributors

Subject lead

Jill Carlson
Co-Founder, Open Money Initiative, USA

Co-authors

Marvin Ammori
Chief Legal Officer, Uniswap, USA

Denelle Dixon
Chief Executive Officer, Stellar Development Foundation, USA

Christina Lomazzo
Innovation Fund Lead, United Nations Children's Fund (UNICEF), New York

Lily Liu
Co-Founder, Aiden Health, USA

Christine Moy
Managing Director, Global Head of Liink and Blockchain, J.P. Morgan, USA

Sebastian Serrano
Chief Executive Officer, Ripio, Argentina

Arianna Simpson
Partner, Andreessen Horowitz, USA

Mariana Gomez de la Villa
Program Director, Distributed Ledger Technology, ING, Netherlands

Council manager

Clarisse Awamengwi
Project Specialist, Blockchain and Digital Assets, World Economic Forum

Reviewers

Marwan Al Zarouni
Chief Executive Officer, Dubai Blockchain Center, United Arab Emirates

Sebastian Banescu
Senior Research Engineer, Quantstamp, USA

Ben Borodach
Vice-President, Strategy and Operations, Team8, USA

David Carlisle
Director, Policy and Regulatory Affairs, Elliptic, USA

Matthew Davie
Chief Strategy Officer, Kiva, USA

Sumedha Deshmukh
Platform Curator, Blockchain and Digital Assets, World Economic Forum

Evgeniia Filippova-Karlusch
Associate Professor, Management Center Innsbruck, Austria

Brad Garlinghouse
Chief Executive Officer, Ripple, USA

Ashley Lannquist
Project Lead, Blockchain and Digital Assets, World Economic Forum

Jose Fernandez da Ponte
Vice-President, Blockchain, Crypto and Digital Currencies, PayPal, USA

Sheila Warren
Deputy Head, Centre for the Fourth Industrial Revolution Network, World Economic Forum

Yan Xiao
Project Lead, Digital Trade, World Economic Forum

Endnotes

1 World Economic Forum, Crypto, What Is It Good For? An Overview of Cryptocurrency Use Cases, 2020, http://www3.weforum.org/docs/WEF_Cryptocurrency_Uses_Cases_2020.pdf.

2 Coin Market Cap, 28 April 2021, https://coinmarketcap.com. DeFi Pulse, 28 April 2021, https://defipulse.com.

3 The Block, Weekly Trade Volumes of NFTs, 28 April 2021, https://www.theblockcrypto.com/data/nft-non-fungible-tokens/nft-overview/weekly-trade-volume-of-nfts.

4 Find an Ethereum Wallet, https://ethereum.org/en/wallets/find-wallet; Choose Your Bitcoin Wallet, https://bitcoin.org/en/choose-your-wallet.

5 You may also consider wallet providers including, but not limited to, MetaMask, Casa and MyCrypto. Monero is currently working to ensure its own liquidity through the Bitcoin–Monero cross-chain Atomic Swap.

6 Cambridge Bitcoin Electricity Consumption Index, https://cbeci.org. Many critics and sceptics focus on the energy consumption of PoW blockchains, and as noted, the energy required is significant. However, it has been found that energy consumption in Bitcoin is still below that of gold mining (around 131.9 Twh) and the banking system as a whole (around 140 Twh); Wintermeyer, Lawrence, "Bitcoin's Energy Consumption Is A Highly Charged Debate – Who's Right?" Forbes, 10 March 2021, https://www.forbes.com/sites/lawrencewintermeyer/2021/03/10/bitcoins-energy-consumption-is-a-highly-charged-debate--whos-right/?sh=54d6ec457e78.

7

8

9

10 Sedlmeir, J., Buhl, H.U., Fridgen, G. et al. "The Energy Consumption of Blockchain Technology: Beyond Myth." Business & Information Systems Engineering, vol. 62, 2020, pp. 599–608, https://doi.org/10.1007/s12599-020-00656-x.

11 Borzi, E. and Salim, D. "Energy Consumption and Security in Blockchain", KTH, School of Electrical Engineering and Computer Science (EECS), 2020, http://ur n.kb.se/resolve?ur n=ur n:nbn:se:kth:diva-285901.

12 Sharding is a technique whereby a blockchain network splits its database into smaller partitions known as "shards" for the purpose of scalability. Each shard stores its own distinct data and enables more transactions to be processed per second.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org