EC10 Constituent Overview

June 2021

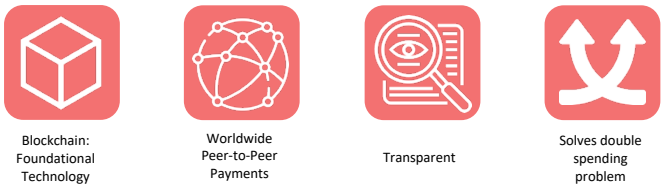
By Don Kruger

The EC10 bundle is South Africa's leading index tracking instrument of the cryptoasset sector. It offers exposure to the top 10 cryptocurrencies weighted by market capitalization, exclusive of Stablecoins. The following report provides an overview of the EC10 bundle constituents. The intention of this analysis is to enhance familiarity and stakeholder consensus of the innovative technology which underlies the EC10 bundle.

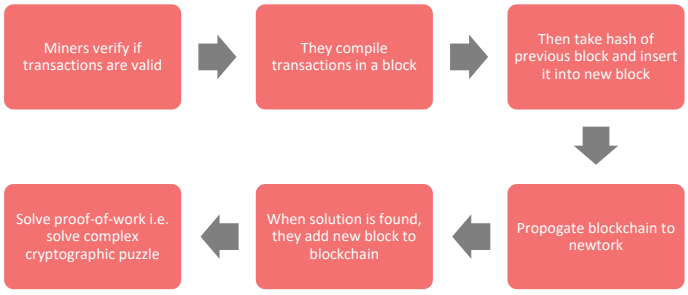
Bitcoin

Bitcoin (BTC) is the original cryptocurrency, which set the entire industry into motion. It was released as open source software in 2009 by a pseudonymous author, Satoshi Nakamoto[1]. It ushered a new era of decentralized finance and has since asserted itself as the top performing asset of the decade. It has challenged societal notions of money, weathered countless condemnation campaigns from the media, and earned itself the title "digital gold". Bitcoin famously brought distributed ledger technology, blockchain, into the fray. The primary appeal underpinning blockchain, and forthcoming altcoins in this overview, is that no central authority or server verifies transactions. Instead, blockchain validation procedures enable the legitimacy of payments to be verified by participants in the decentralized network itself. Miners participate in the blockchain and are fundamentally responsible for validating transactions. Bitcoin has a circulating supply of 18.6 million units, of which the maximum supply is 21 million units. Because Bitcoin is the first cryptocurrency, the transactional capabilities are relatively slower than most of the altcoins subsequently discussed. Namely, the Bitcoin network accommodates approximately 4.6 transaction per second[2].

Key Features



Bitcoin mining in a nutshell



Ethereum

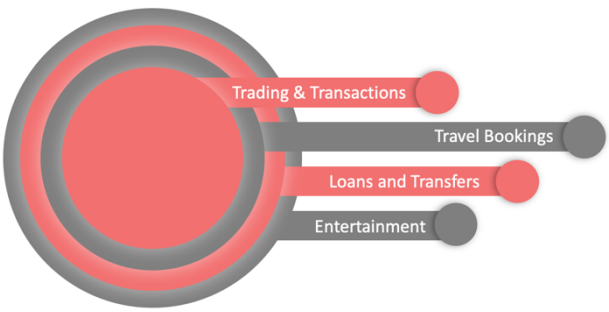
Ethereum (ETH) is the 2nd largest cryptocurrency in the EC10 bundle. ETH is an open software blockchain platform that enables developers to build and deploy decentralized applications. In the Ethereum blockchain, instead of mining for Bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Beyond being a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network. Ethereum is employed in a dedicated coding language called Solidity. Decentralized applications on the network are typically referred to as "dapps". Ethereum users pay fees to use dapps. The fees are called "gas" because they vary depending on the amount of computational power required. Ethereum distinguishes itself from Bitcoin as a programmable network that serves as a market place for applications such as financial services, games, social media, voting platforms etc. Some popular applications harnessing the ether network are Etheria[3], EtherTweet[4], RaidenNetwork[5], Tenx[6], and Gnosis[7] – all of which can be paid for in ETH and are safe from fraud, theft, or censorship. Promising developments in the ETH space have recently started gaining traction. Namely, Microsoft is in partnership with ConsenSys to offer Ethereum Blockchain as a Service (EBaaS) on the Microsoft Azure cloud. It is intended to offer Enterprise clients and developers a single click cloud-based blockchain developer environment.[8] Moreover, Advanced Micro Devices (AMD) and ConsenSys announced a joint venture to create a network of data centers built on the Ethereum infrastructure.[9] ETH has a circulating supply of 116 million units. The ETH system has an unlimited supply, but an annual maximum supply of 18 million units. While Bitcoin has a built in halving mechanism, Ethereum relies on EIPs (Ethereum Improvement Proposals) to control inflation. Ethereum is capable of processing approximately 20 transactions per second with an average confirmation time of 5 minutes.[10]

Key Differences from Bitcoin

Binance Coin

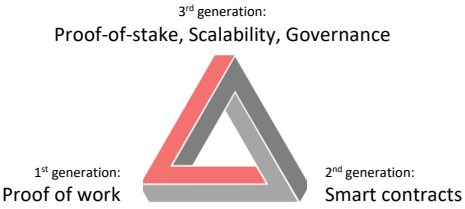
Binance Coin (BNB) is a cryptocurrency issued by the Binance exchange – the largest cryptocurrency exchange by trading volume. The BNB protocol has a strict maximum of 200 million tokens. Unlike Bitcoin and Ethereum, Binance uses one fifth of its quarterly profits, to repurchase and permanently retire ("burn") BNB coins held in the exchange's treasury. BNB was originally created as a utility token for discounted trading fees, but its modes of implementation have since promulgated to numerous applications, including payments for transaction fees , entertainment, travel bookings, online services, and financial services. This has ensued as a result of Binance launching the Binance Smart Chain for the development of decentralized apps. This dual-chain architecture has revolutionized how the Binance network processes transactions and substantially improved its scalability following the implementation. The transaction fees of the BNB network are notably lower than that of BTC and ETH, overcoming the primary limitations of the two largest cryptocurrencies in the EC10 bundle. The primary advantage of BNB is that it is underpinned by the world's largest crypto exchange, granting it a powerful intermediary capability between cryptocurrencies. The Binance exchange itself, advocates measuring the value of cryptoassets against BNB, instead of against the USD, for example. As such, the Binance platform has accommodated up to 1.4 million transactions per second using BNB as a medium of exchange.[11]

Primary Uses



Cardano

Cardano (ADA) is a proof-of-stake cryptocurrency. It has gained substantial traction since its entry into markets due to its intriguing peer-review infrastructure. Updates to the Cardano system are made through peer-reviewed scientific research and voted upon by a global community of academic researchers and scholars. The Cardano community asserts ADA as a "3rd-generation" cryptocurrency.



Cardano was developed to solve the 3 predominant issues of the former generations. Namely: scalability, interoperability and sustainability. 1st generation cryptoassets transfer and store virtual money, but are hindered by scalability issues (transactions per second, network bandwidth and storage). The 2nd generation of cryptoassets are underpinned by smart contracts but are similarly unable to address scalability obstacles. Cardano's Ouroboro system solves scalability through proof-of-stake (PoS), rather than proof-of-work (PoW) set forth by the BTC protocol. PoS offers enhanced efficiency because it doesn't allow all participants to mine new blocks, reducing global energy requirements. Instead, the PoS network elects' specific nodes to mine the next blocks. ADA solves the issue of large bandwidth requirements by sub-dividing the ADA network into silos using a technique called recursive internetwork architecture (RINA). Moreover, ADA resolves the problem of storage requirements through pruning, compression and partitioning.[12] Interoperability allows ADA to accommodate transactions between other cryptocurrencies. This essentially grants ADA the power to function as a cryptoasset intermediary operating as the "internet of blockchains". Stated differently, ADA is constituted by a blockchain protocol capable of interpreting other blockchains.

Governments and banks have historically shied away from cryptocurrencies because they don't adhere to customary financial regulations. Majority of cryptocurrencies lack the metadata necessary to determine transaction participants and the nature of such transactions. However, part of the crypto appeal is this very anonymity. The Cardano protocol, however, allows participants the discretion to attach metadata to transactions if they prefer to do so. Hence, accommodating the potential for institutional cooperation. Finally, ADA addresses the issue of sustainability through a treasury. The ADA treasury receives a micro-percentage of every transaction on the blockchain. The treasury itself is a special wallet not controlled by a central party. The treasury is built on a system which releases ADA to developers whom enhance the system's protocol through the peer-review voting system. To receive compensation from the treasury, developers have to submit a proposal to the ADA community describing the updates to the system, and how much ADA they require for the development. Hence, the community votes on ideas for which the treasury must fund. Over time the treasury model keeps Cardano sustainable by providing a continuous stream of funding that can be used to bolster research and improve the system.

Dogecoin

Dogecoin (DOGE) is 1st-generation cryptocurrency originally created as a travesty of the crypto sector. As a fork of the source-code of Litecoin (LTC), it's first block was mined in December of 2013. The Dogecoin blockchain can process roughly 30 transactions per second. Notable features of Dogecoin, which uses a Scrypt algorithm, are its low price and unlimited supply. It has predominantly been used to tip content on Twitter and Reddit, but has since gained much attraction since its advocations from Elon Musk.[13]

Hash Rate Defined

Hashrate is a measure of the computational power per second used when mining. More simply, it is the speed of mining. It is measured in units of hash/second, meaning how many calculations per second can be performed.

Numerous Scrypt miners still prefer Dogecoin over other Scrypt PoW cryptocurrencies. Indeed, the Dogecoin hash rate is roughly 150 TH/s. This is just below the LTC hash rate of 170 TH/s, likely because Dogecoin can be merge mined with LTC, meaning miners can mine both cryptos simultaneously using the same work. Essentially, practically everyone who mines LTC chooses to mine Dogecoin as well, because merge mining Dogecoin increases profits.

XRP

Ripple is a technology that acts as both a cryptocurrency and a digital payment network for financial transactions[14]. Ripple's main process is a payment settlement asset exchange and remittance system, similar to the SWIFT system for international money and security transfers, which is used by banks and financial middlemen dealing across currencies. The token used for the cryptocurrency is pre-mined and utilizes the ticker symbol XRP. Ripple is the name of the company and the network, and XRP is the cryptocurrency token. The purpose of XRP is to serve as an intermediate mechanism of exchange between two currencies or networks—as a sort of temporary settlement layer denomination. Rather than use blockchain mining, Ripple uses a consensus mechanism, via a group of bank-owned servers, to confirm transactions. Ripple transactions use less energy than Bitcoin, can validate 1500 transactions per second, and cost very little, whereas bitcoin transactions use more energy, take longer to confirm, and include higher transaction costs. The XRP protocol does not accommodate mining.

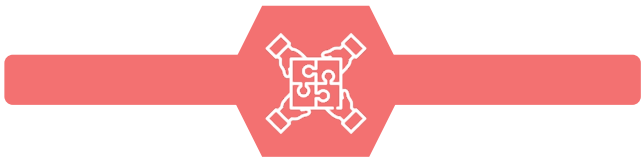
Key Differences from Bitcoin

Polkadot

Polkadot (DOT1) hosts a 3rd-generation blockchain protocol connecting multiple specialized blockchains into one unified network[15]. Polkadot shares many similarities with the interoperability of Cardano. Blockchains, by themselves, can only process a limited amount of traffic. Polkadot utilizes a sharded multichain network, meaning it can process many transactions on several chains in parallel, eliminating the bottlenecks that occurred on 1st-generation networks that processed individual transactions. This parallel processing power significantly improves scalability. Various chains connected to Polkadot are called "parachains" because they run on the network in parallel. When it comes to blockchain architecture, cryptocurrencies have varying features and characteristics. On Polkadot, each blockchain can have a novel design optimized for a specific purpose. That means blockchains can offer better services, while also improving efficiency and security by leaving out unnecessary code, with DOT1 as the middle man. Polkadot builds on what is called a Substrate development framework, which allows teams to develop and customize their projects harnessing various cryptoasset blockchains.

Therefore, networks and applications on Polkadot can share information and functionality like apps on a smartphone, without needing to rely on centralized service providers. Unlike previous networks that operated

largely as standalone environments. Polkadot offers interoperability and cross-chain communication. This opens supports new services and allows users to transfer information between chains. For example, a chain providing financial services can communicate with another that provides access to real-world data (known as an oracle chain).



3rd-generation cryptoassets harness upgrades to stay relevant and improve over time. However, upgrading conventional chains requires what are called "hard forks", which create two separate transaction histories that can splinter a community in two and often take months of work. Polkadot enables forkless upgrades, allowing blockchains to evolve and adapt easily as better technology becomes available from other blockchains.

Internet Computer

Certain critics, and participants in the cryptoasset sector argue cryptocurrencies are in fact not purely decentralized. This is because the internet we use today is controlled by a handful of organizations which all other crypto projects rely on for storage, computing and front-end user interfaces such as mobile applications and websites. The Internet Computer (ICP) aims to be the solution to this absolute decentralization obstacle, by creating a brand new decentralized internet, independent of the current internet infrastructure harnessed across the globe[16]. What sets ICP apart from other cryptoassets is that it aims to replace the entire internet stack, not just the application layer. ICP is maintained and developed by the "DFINITY" foundation. ICP is arguably the most sophisticated cryptocurrency development to date…

The inner-workings of ICP are not fully discussed in this overview, as it would require an extensive elaboration. The following, however, is intended to suffice as a high-level summary of the ICP technology. Direct participation on the ICP blockchain is permissioned, and requires standardized hardware provided by the DFINITY foundation. Development of ICP began with the release of "COPPER" which introduced a software developer kit for smart contracts coded in "Motoko" – a new programming language specifically created for the ICP. ICP accommodates the potential for a global application infrastructure completely online, and completely decentralized. In other words, if widespread adoption were to ensure, all application developed using ICP would essentially be web applications.

From a bird's eye view the ICP consists of series of data centers spread across the world. Each data center contains multiple nodes, whereby, nodes from multiple data centers are grouped together to form a subnet. Each subnet forms a proof-of-stake blockchain utilizing a novel consensus mechanism called "threshold relay". A subset of nodes in each subnet is selected to produce a block based on their staked ICP. Subnets are similar to the chains harnessed by Polkadot and Cardano. Subnets host the dapps running on ICP. Whereas regular cryptoasset dapps consist as a collection of smart contracts, each dapp on the ICP is made up of one or more "canisters". Canisters are a tortuous rendition of smart contracts. They can automatically create new versions of themselves on other subnets to support additional users, and can be leveraged by other developers building dapps. What sets ICP dapps apart from Ethereum dapps is that no fees are required for their operation. This is in stark contrast to other cryptocurrencies which require you to pay a network fee for every network interaction on their blockchains. The final major difference between ICP and other cryptoassets is that it requires an internet identify to access its blockchain facilities. This internet identify can be paired to your smartphone, computer or a secure USB key. A wallet address is automatically generated upon creation of an internet identify. ICP has an initial supply of 469 213 710 tokens. It has no maximum supply and imposes a diminishing annual inflation rate that starts at 10% and converges to 5% over time. In summary, ICP is a cryptoasset that allows users to participate in and govern the ICP blockchain. The network aims to help developers create websites, enterprise IT systems, internet services, and DeFi applications by installing their code directly on the ICP blockchain.

Uniswap

Uniswap (UNI) is an Ethereum-based automated market maker protocol that facilitates trades without the explicit need for a central administrator[17]. UNI sets itself apart from other cryptoasset exchange platforms by being completely decentralized and maintains liquidity by incentivizing users to contribute their assets to liquidity pools. Stated differently, UNI can be used as a technology to swap out other cryptoassets. Uniswap is the largest decentralized market maker for cryptoassets which challenges the Binance business model. Arbitrage trading is very common on the Uniswap platform. Arbitrage traders analyze multiple cryptocurrency trading platforms in order to find price discrepancies and then trade between platforms for profit until the price difference is eliminated. Uniswap has deployed a range of applications targeted at arbitrage traders, including analytics tools and token lists.

Bitcoin Cash

Bitcoin Cash (BCH) is the product of a Bitcoin hard fork which took place in August 2017. It was created to accommodate a larger block size compared to Bitcoin, allowing more transactions into a single block[18]. BCH and BTC share several technical similarities. Namely, they use the same consensus mechanism and have capped their supply at 21 million tokens. BCH transaction fees are much lower than BTC as the block space is not limited to the same capacity. Thus, BCH has scaled onchain allowing for extra block space accommodating greater adoption and lower fees while still retaining the original BTC attributes.

Definitions

Altcoin	An altcoin any cryptocurrency except for Bitcoin. "Altcoin" is a combination of two words: "alternative Bitcoin" or "alternative coin".
Block	A block is a single digital record created within a blockchain. Each block contains a record of the previous block, and when linked together these become the "chain".
Blockchain	Blockchain is a digital recording, used to prove that a group of people came to an agreement about something. Blockchain records are permanent and secure, preventing manipulation.
Cryptocurrency	A cryptocurrency, also known as 'crypto', is a type of currency that is transferred via a blockchain. It uses strong cryptography to secure the transactions, that usually have value. While traditional fiat currencies are subject to counterfeiting, this is not possible in a cryptocurrency. Bitcoin is still the most valuable cryptocurrency.
DApp	DApp is short for 'Decentralized application' that relies partly on blockchain for its functionality. They are different than 'Smart Contracts' because it can be interacted with. It does not need to have a financial function. Dapps can be created using common programming languages like Javascript, PHP or C#. At the time of writing, most Dapps are using the Ethereum blockchain.
DeFi	DeFi is the abbreviation of 'Decentralized Finance'. It can be defined as a new financial ecosystem consisting of various financial tools, apps and services utilizing blockchain technology. It's an umbrella term for all these projects combined and is growing daily. Examples of DeFi functionality are banking services in the form of stablecoins, decentralized exchanges, derivatives, prediction markets, or lending and borrowing systems. The last one can be either peer-to-peer or with a pool. It is a combination of replicating products and services in the traditional finance industry as well as innovative new ones only possible with blockchain technology.
Exchange	An exchange is a place where you can buy and sell different kinds of cryptocurrencies and tokens. These coins can then be deposited back to a wallet, which supports the coin. Sometimes it's also possible to convert it to dollars.

Gas	Gas' or 'Wei' is used to execute a transaction on the Ethereum blockchain. The 'gas' that is used can be seen as 'fee' for the 'miners. The more 'gas' you set, the faster your transaction will be completed. Because of the higher reward, more miners will be incentivized to process the transaction earlier.
Hard Fork	A hard fork is a major change in the Blockchain protocol. A hard fork requires all nodes to upgrade to the latest version of the protocol software. Usually, there is a transition period where the miners can show their support of the hard fork. Once a date is set via a specific block number, everybody will need to have updated their software by that time. The ones that fail to upgrade could cause a chain split. The chain with the highest number of nodes or hash rate will be seen as the original chain.
Mining	Mining is also known as 'Cryptocurrency mining' or 'Cryptomining'. It is a process where blocks are added to a blockchain by solving a mathematical puzzle. The block can also contain transactions on that blockchain and will then become verified and immutable. Depending on the blockchain, mining can be done with a CPU, GPU, specialised hardware or a combination of all.
Proof-of-stake (PoS)	The Proof-of-Stake (PoS) consensus algorithm is introduced as an alternative to Proof-of-Work (PoW) without the energy-consuming aspect. In the case of PoS the creator of the next block is randomly chosen based on a combined selection of age and wealth, where the wealth is the 'stake' or amount of cryptocurrency that has been put to work. This is done by having it in an unlocked wallet for staking. The staking can usually be done on a VPS or computer at home.
Proof-of-work (PoW)	The Proof-of-Work (PoW) consensus algorithm successfully came to life with the introduction of Bitcoin in 2009. It is the algorithm that is used to confirm transactions and the creation of new blocks in a blockchain. Specialised devices, computers or graphic cards can be used to do calculations. In PoW a new block is created or found by solving a mathematical puzzle. The process of trying to solve that puzzle is called mining. The miners are working hard and usually consuming a lot of energy to find the solution to the puzzle. This is basically where the definition 'Proof-of-Work' comes from.
Smart contract	A smart contract came to existence with the launch of the Ethereum blockchain but has nowadays also been replicated in different forms on other blockchains. It can be seen as a protocol or computer program that is meant to autonomously and automatically execute pre-defined commands based on relevant events. The goal of this technology is to automate events and reduce the need for trusted third parties. This technology can be used for various purposes like the creation of tokens, facilitating DeFi, prediction markets and more. Oracles enable the usage of real-world data in smart contracts. The possibilities of this technology are endless.
Wallet	A 'wallet' is a place to store cryptocurrencies encrypted. There are several variants, such as a paper wallet, hardware wallet or software wallet. Each coin has one or more supported wallets.

References

1. 2. 3.
4. 5. 6.
7. 8. 9.
10. 11. 12.
13. 14. 15.
16. 17. 18.