DECEMBER 17, 2024 • 11 MIN READ

Bitcoin and blockchain: a cheat-sheet for the crypto-curious

AUTHORS

Simon J.C. Williams

The breakthrough innovation of blockchain technology is that it brings provable scarcity and ownership to the digital realm for the first time, and promises to transform the internet economy from an ocean of “copy paste” overabundance to a new Web 3.0 characterized by ownership and value, where property rights are guaranteed by code rather than by courts. Bitcoin is emerging as the foundation of an alternative monetary system that separates money and State, a new investment category, and a pristine collateral asset based on its unique properties as a digital commodity and savings technology.

What you need to know

- With the U.S. Senate’s recent proposal of the BITCOIN Act of 2024[1] to formalize a strategic federal Bitcoin reserve, Bitcoin is poised for mainstream adoption in the role of providing a hard-money foundation and financial ballast in the face of escalating debt obligations and money-printing at the sovereign, corporate and individual levels.
- The Bitcoin network is the world’s largest and most secure supercomputer, stewarded over the internet by a decentralized hive-mind of participants across the globe.
- Bitcoin has reached an inflection point as an institutional-grade, capital asset digital savings technology by virtue of its unique properties of being a non-sovereign, censorship-resistant, hard-cap supply, global, immutable, decentralized, digital bearer asset and store-of-value[2].
- Blockchain technology replaces third-party intermediaries and custodians with a transparent, decentralized ledger that serves as a verified final arbiter of information and value.
- Blockchain acts as a digital deed of ownership and certificate of authenticity, recording the initial purchase of digital artifacts and all subsequent transfers in an unbreakable, immutable chain.
- Beyond Bitcoin, programmable blockchain networks like Ethereum and Solana have enabled “smart contracts”, which automatically self-execute transactions once specified conditions have been met. The ability to transact securely on a peer-to-peer basis, with near-instant settlement and no centralized intermediary, has unlocked new frontiers in capital formation and allocation, decentralized finance (DeFi) and decentralized physical infrastructure (DePIN) such as mobile and AI-inferencing network.

The blockchain innovation

The key innovation of blockchain technology lies in the novel way it records, stores and updates information.

Before blockchain, nearly every aspect of business and finance was controlled by trusted third-party gatekeepers and transacted on centralized databases, such as commercial and central bank ledgers, corporate filings databases, stock brokerage ledgers, DTTC, bond CUSIP numbers, Google Spreadsheets, land titles offices and healthcare databases. In order to process transactions like buying or selling shares, sending money or changing title on a deed, transaction principals must submit a request and pay a fee to the keeper of the database, who then records the transaction on their ledger. For example, when an e-transfer is sent from a bank account at one bank to another bank, the customer pays a fee and the two banks message each other to record the debit and corresponding credit in their respective ledgers.

Blockchain disintermediates the centralized database gatekeeper and enables individual stakeholders to transact directly in a cryptographically secure manner, where every transaction is recorded and added to a single, globally distributed ledger that lives on computer code running across the internet. Once the transaction has been added, it is permanently inscribed in the ledger, creating an immutable chain-of-history. This means that anyone with an internet connection can review and audit the entire database at any time, without seeking permission from anyone else to do so. However, the audit rights are read-only and cannot be altered. It has 24/7 uptime, meaning that it is accessible at any time, in contrast, for example, to a bank or stock exchange, which only transacts during business hours. This combination of features enables transparency, accessibility and near-instant settlement finality.

Digital scarcity and property rights

In the existing “Web 2.0” world, digital artifacts do not hold value without court-enforced IP rights because digital items can be reproduced *ad infinitem* at minimal cost. Digital assets like movies, songs, books, emails, digital art, mortgage records, and PDF scans of stock certificates can all be copy-pasted and sent to a million email addresses by a spam-bot. That same bot can then send those records to ten million addresses for the same negligible cost.

Blockchain acts as a digital deed of ownership and certificate of authenticity because it records the initial purchase of the original digital artifact on the blockchain, along with all subsequent transfers from inception up to the current owner, in a chain of record that cannot be forged or replicated. The current owner of the digital artifact can therefore prove its provenance and establish to the world his or her ownership because the digital DNA is immutably inscribed into the artifact itself and can be verified and traced by anyone.

Bitcoin

Bitcoin was the original conception of distributed ledger technology back in 2009. It is referred to as the ultimate “hard money” asset because its total supply is hard-capped at 21 million units or bitcoins, though each bitcoin is infinitesimally divisible to eight decimal places. It is this ultimate fixed supply that makes Bitcoin a “hard-money” deflationary asset, whose predominant use case is increasingly being espoused and adopted as a digital savings technology rather than a medium of exchange. This stands in contrast to traditional fiat currencies like the U.S. dollar, which continually lose their purchasing power over time as the money supply increases. For instance, since 2019 the purchasing power of the U.S. dollar has decreased by 20%, coincident with the issuance of an additional US$14 trillion in U.S. federal debt over that period. Total U.S. federal debt currently exceeds $36 trillion. Importantly, the rate of currency debasement through money printing cannot be known in advance because it is subject to the vagaries of political influence and monetary policy. By contrast, the fixed supply monetary policy of bitcoin is enshrined by code and cannot be changed: it will always be 21 million bitcoins, 19.9 million of which have been mined and are in circulation[3].

Given that Bitcoin is an open-source and permissionless system, anyone in the world with an internet connection can participate in the Bitcoin network.

Because the remaining un-mined supply of bitcoin (about 1.1 million bitcoins) is issued programmatically, based on a four-year halving cycle, the price of bitcoin is driven almost entirely by demand. A fixed-supply monetary base harkens back to the pre-Bretton Woods era, when the U.S. dollar was pegged to—and exchangeable for—physical gold, which indirectly brought other currencies, exchanging their own money for U.S. dollars, onto the gold standard. However, the total supply of gold on Earth is unknown and also somewhat elastic: higher gold prices incentivize more gold mining, which increases the circulating supply and applies downward pressure on the price per ounce. By contrast, bitcoin's absolute scarcity makes it rarer than gold and therefore a harder money.

Bitcoin as pristine collateral and a digital commodity

Bitcoin's properties of monetary hardness, divisibility, auditability, transferability, immutability and 24/7 tradability on a liquid market make it highly optimized for loan collateral. It can also be automatically liquidated from digital escrow with smart contract logic when loan-to-value ratios or other contractual parameters are breached. There are already several companies, including Toronto-based company Ledn, that provide loans backed by Bitcoin or Ethereum[4].

Following on the heels of the recent U.S. election, corporate working capital facilities that are partially or fully collateralized with bitcoin sub-facilities may begin to proliferate in the U.S. under the incoming administration given its stated pro-innovation and pro-crypto policies[5]. If so, Canada may follow the U.S. market in this regard. Bitcoin is also the collateral foundation for the emerging decentralized finance space where capital pools are aggregated and then allocated to borrowers through a decentralized exchange (i.e., without the involvement of an intermediary bank or company).

Smart contracts

The first second-generation blockchain-based network, Ethereum, took the blueprint for Bitcoin blockchain software and made a few tweaks to make it programmable, then later changed the consensus mechanism—how new transactions are recorded to the ledger—from proof-of-work (requiring energy) to proof-of-stake (requiring capital). The Ethereum blockchain protocol allows for the development of self-executing "smart contracts"—namely, the ability to automatically execute transactions without the need for institutions or courts to enforce their terms.

Unlike Bitcoin, whose use-case as "digital gold" is uncontested, Ethereum has dozens of other smart contract competitors vying for market share as "digital oil" or "world computers". Some of the main use-cases for smart contract blockchains are as follows.

- **Tokenization of real-world assets**. Stocks, bonds, treasuries, mobile networks, title deeds, mortgage records, government IDs, REITs, and concert tickets are some examples of real-world assets that can be represented on a blockchain and traded 24/7 without fees or intermediaries. Tickets for Taylor Swift's next concert tour will likely be distributed as NFTs on blockchain, where the ability to transfer tickets can have certain parameters and attributes pre-programmed into them: for example, they might include stipulations that the tickets cannot be sold for more than 20% of the original price, that a 5% royalty is automatically paid to Taylor Swift, or that the NFT holder unlocks perks like early download rights to Taylor's next album drop. The tokenization of financial assets like private credit and treasuries is expected to jump from US$12.5 billion to US$50 billion by end of 2025.

- **Stablecoins**. Stablecoins are a type of cryptocurrency that is designed to maintain a fixed value over time, with its value pegged to a specific real-world currency. There are nearly a trillion dollars of USD-denominated stablecoins in circulation from the top three issuers: Tether, PayPal and Circle. Anyone can send as little as $1 or as much as $10 billion (or more) anytime, anywhere in the world, at near-light speed with negligible transaction costs. This contrasts significantly with the time delay for ACH and SWIFT transfers, especially for international transfers and over non-business day periods.

- **Decentralized Autonomous Organizations**. These are a new, digital incarnation of corporations that subsist on blockchain rails. Members can organize and govern themselves, vote on taking certain actions, raise and deploy capital, or carry out other functions. An example could be a global DAO established for the purpose of investing in luxury waterfront buildings around the world, which democratizes investment geographically and socio-economically.

- **Zero knowledge proofs**. ZK proofs are a cryptographic method used to prove knowledge about a piece of data, without revealing the data itself. For instance, a banking client using a ZK proof would be able to provide proof of the amount of money in their bank account without revealing any other identifying information about themselves, such as the amount of their mortgages or where they live. Similarly, investors and corporations can use ZK proofs to prove that they are accredited investors, without revealing their actual net worth and bank balances/stock holdings.

- **Integration with AI**. AI inferencing requires tremendous computing power, which has massive CapEx barriers to entry given the cost of NVIDIA's H100 chips. Helping to lower those barriers are a number of blockchain networks that are pooling distributed computing power from thousands of dispersed computers and focusing them on AI inferencing or video rendering tasks. An example is Bittensor, whose stated purpose is to democratize the field of AI by creating a platform for numerous decentralized commodity markets or "subnetworks" united under a single-token system where participants are paid in cryptocurrency. Beyond that, the proliferation of AI agents—autonomous systems designed to complete repetitive tasks—requires 24/7, permissionless access to trusted information and money to carry out their functions. Blockchain provides the rails for transferring both money and information to AI agents and will be integrated into products like Tesla's fully autonomous RoboTaxis and their humanoid Optimus robots, anticipated to be rolled out in 2025-26. Both classes of robots will be funded with cryptocurrency (likely stablecoins) and will be able carry out tasks for the human owner such as buying groceries, booking travel, employing copy-trade investment strategies, and operating autonomous vehicles.

Conclusion

Blockchain technology has unlocked a new investment category in digital assets like Bitcoin, Ether and Solana, and its properties as a global database are changing the financial and informational infrastructure upon which individuals and businesses transact. Given that blockchain protocols can be legally characterized as commodities, securities or currencies depending on their properties, the regulatory landscape for this emerging industry is complex and continues to evolve.

FOOTNOTES

To discuss these issues, please contact the author(s).