MERKLE TREE

CAPITAL

Investor Guide
To Cryptocurrency

The Crypto, or Digital Asset, ecosystem has been growing rapidly since its inception early in 2009 when the Bitcoin Network software was released, and Satoshi Nakamoto mined the first block (known as the genesis block).

The genesis block contained a text message "The Times 03/Jan/2009 Chancellor on the brink of second bailout for banks" a reference to the intended purpose of bitcoin, an alternative monetary system that is not beholden to banks, governments, bankers (central or otherwise) or the inherent risk of a fractional banking system which had just been laid bare in the 2008 Global Financial Crisis.

While the primary use case was transactions, bitcoin is a peer-to-peer payments system with store of value / scarcity qualities similar to a commodity like gold, new cryptocurrency projects like Ethereum took this a step further, adding smart contract functionality to a blockchain.

Bitcoin is both a payment network, like SWIFT (only faster, cheaper and more secure) and a currency like USD (only it can't be censored or manipulated by a government or central bank) where bitcoin the currency is moved around the Bitcoin Network. Ethereum is often described as a planetary virtual computer, a simple analogy would be it's a platform, like iOS or Android, it can host applications supporting ecommerce, IOT, supply chain solutions and gaming, to name a few, but instead of your data being hosted (and harvested) by big tech companies it is stored on a network of decentralisd computers and protected by cryptography.

What is a Merkle Tree?

A Merkle tree, is a data structure used in cryptography and computer science, it is an imperative component of blockchain technology, ensuring the secure and efficient verification of data.

At a high level, this guide will:

1. Provide an Introduction to Blockchain, Distributed Ledger, Cryptocurrency and Smart Contract technologies.

2. Provide examples of current use cases and the industries they are distrupting.

3. The investment opportunity and introducing cryptocurrency to a balanced portfolio.

Introduction to Blockchain, Distributed Ledger, Cryptocurrency & Smart Contract technologies

There can be some confusion between the technologies that support crypto and some scepticism of crypto currency itself. They are all just technology-based software, much like sending an email, they can be used to send digital payments, instantly and free. Email allows us to send information, cutting out the time and cost of the postal service by removing the intermediaries and their expensive infrastructure. Blockchain technology allows for lower-cost, seamless payments, by cutting out the existing banking infrastructure.

Blockchain

Blockchain is type of ledger underpinned by a specific technology. Blockchain creates an unchangeable (immutable) ledger of records enabling everyone involved in a transaction to know with certainty what happened, when it happened, and confirm other parties are seeing the same thing without the need for an intermediary providing assurance, and without a need to reconcile data afterwards. Blockchains may be centralised (controlled by a single entity) or distributed (controlled by a network of participants).

How does blockchain technology work?

The user requests a transaction > A block which represents the transaction is created > The block is broadcasted to all nodes of the network > All nodes validate the block and transaction > The block is added to the chain > The transaction is verified and completed

Distributed Ledger Technology

Distributed Ledger Technology (DLT) enables the secure functioning of a decentralised digital database. Distributed networks eliminate the need for a central authority to keep a check against manipulation.

DLT allows for storage of all information in a secure and accurate manner using cryptography. The same can be accessed using "keys" and cryptographic signatures. Once the information is stored, it becomes an immutable database and is governed by the rules of the network.

The very nature of a decentralised ledger makes them immune to cyber-crime, as all the copies stored across the network need to be attacked at the same time for the attack to be successful. Additionally, the simultaneous (peer-to-peer) sharing and updating of records make the whole process much faster, more effective, and cheaper.

Cryptocurrency

Combining the two above technologies requires an incentive for the decentralised participants to act in good faith towards the database, which is where cryptocurrency comes in. Participants in the network can run nodes (storing a record of all transactions) and receive details of each new transaction to be added as the next block in the blockchain. A reward of cryptocurrency is issued to the node that produces the next block. A majority of nodes must agree the block is accurate i.e. does not include fraudulent transactions, this process of validation is called consensus, once achieved work starts on the next block.

Note: Nodes maintain the latest record of the Bitcoin network and consistently verify and approve new transactions. They also ensure that everyone is following the rules set forth by the network.

Smart Contracts

Smart contracts are self-executing digital agreements that enable two or more parties to exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the need for a third party.
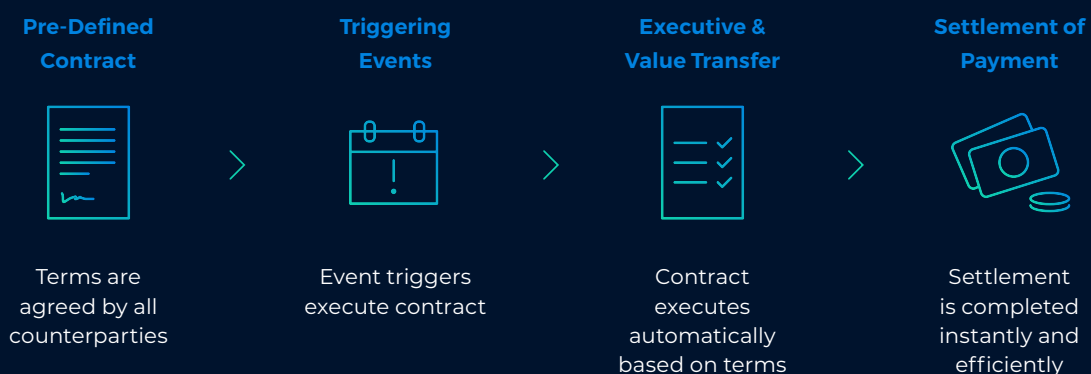
Smart contracts deployed to blockchains render transactions traceable, transparent, and irreversible.

Similar to a transfer of value on a blockchain, deployment of a smart contract on a blockchain occurs by sending a transaction that includes code for the smart contract. That transaction must then be included in a block that is added to the blockchain, at which point the smart contract's code will execute to establish the initial state of the smart contract.

This allows for new use cases like Decentralised Finance (DeFi), Web3, The Metaverse and NFTs to be added to a blockchain and managed via smart contracts.

Note: smart contract transactions generated $10bn in fees on Ethereum alone in 2021.

How Do Smart Contracts Work

Pre-Defined Contract

Terms are agreed by all counterparties

Triggering Events

Event triggers execute contract

Executive & Value Transfer

Contract executes automatically based on terms

Settlement of Payment

Settlement is completed instantly and efficiently

So, why use Cryptocurrency?

Traditional transactions are complex and costly:

- Prone to human error or fraud — each participant has its own separate ledger.
- Inefficient — intermediaries are needed for validation.
- Frequent delays & losses — paper-based and data stored locally by each party.

Cryptocurrency as a solution:

- Peers have a single shared ledger — once the transaction is validated, the record is permanent, secure and immutable.
- A smart contract — code running on top of a blockchain that contains a set of rules under which the parties mutually agree — eliminates the need for third parties.
- Owner of the transaction has the power to move anything of value freely and instantly without intermediaries.
- Eliminates or reduces paper processes, the need for intermediaries, speeds up transaction times and increases efficiencies and transparency.

Current Use Cases

Blockchain technology is emerging as a game-changer for multiple industries, including healthcare, education, real estate, supply chain & logistics, and IoT (Internet of Things). The list is constantly expanding as the power of this transformational technology is explored by more and more industries. A few established examples include:

Global payments Network

The Bitcoin Network is the world's first public payments infrastructure. Existing payments infrastructure like, VISA or SWIFT, are private networks that extract value from every payment (often around 3%), which currently equates to around $2Trn per annum in fees. This represents a huge pro-ductivity gain for the global economy, cutting out the old, expensive, slow payments infrastructure in favour of free, instant, immutable payments.

Did you know

Visa and Mastercard are partnering with different cryptocurrency providers to roll out payment services that point to the Bitcoin Network rather than the convoluted multi-intermediary systems that they set up in the 1940s?
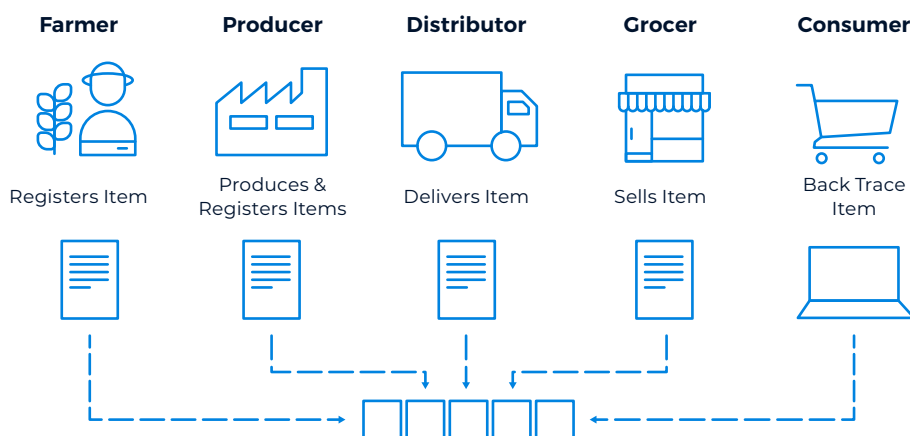
Merchant Payment Flow – Traditional vs Blockchain

Traditional
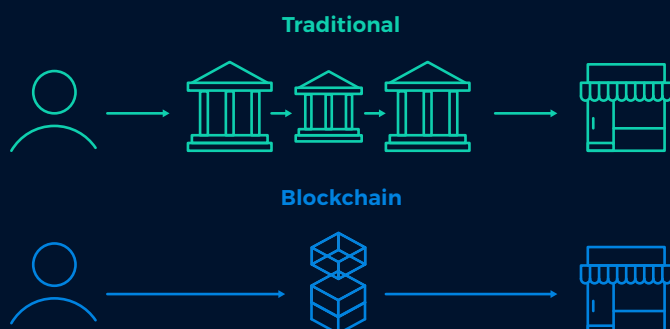
- 2-3 days to settle payment
- Multiple intermediaries
- 3% transaction fee

Blockchain

- Instant settlement of funds
- Blockchain payment rails
- 0% transaction fee

Supply chain optimisation

Blockchain can help participants record price, date, location, quality, certification, and other relevant information to more effectively manage the supply chain. The availability of this information within blockchain can increase traceability, lower losses from counterfeit and gray market, improve visibility and compliance over outsourced contract manufacturing, and potentially enhance an organisation's position as a leader in responsible/ethical manufacturing (the EU is increasingly turning to blockchain for proof of provenance and ESG certification).

Farmer	Producer	Distributor	Grocer	Consumer
Registers Item	Produces & Registers Items	Delivers Item	Sells Item	Back Trace Item

Shipping companies are using blockchain to manage freight tracking, providing buyers, sellers, and officials with a mechanism to track goods shipped around the world. Products traveling across borders may require review and approvals from up to 30 parties before arrival, creating a large amount of paperwork and creating opportunities for fraud at multiple points in the process—leading to billions of dollars in maritime fraud each year. Blockchain can reduce administrative and logistics timelines in shipping by more than 85 percent.

Banking the unbanked

Nearly 2 billion people on the planet do not have access to a bank account, the Bitcoin Network, via scaling solutions like the Bitcoin Lightening Network, are changing this. Now anyone with a phone (which most of this cohort have) can now be included in the financial system, they can send, receive and save money like everyone else. In fact, the Central African Republic is following in the footsteps of El Salvador, which adopted Bitcoin as legal tender last year.

Did you know

In Africa there are services that can send and receive bitcoin via SMS?
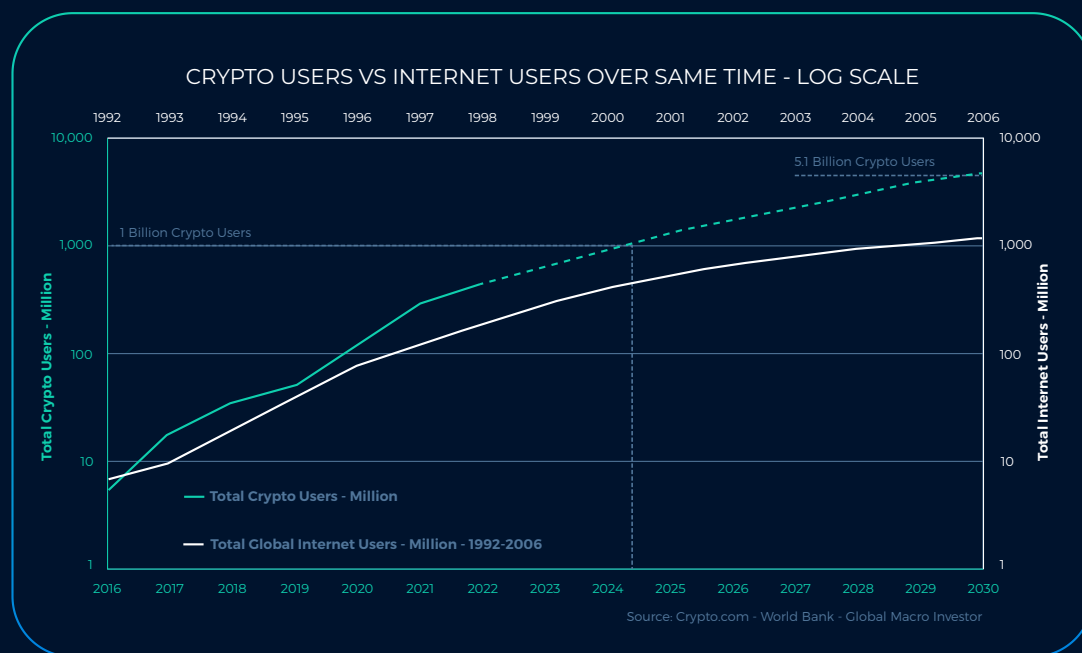
Cloud data storage

Relying on centralised data storage has a major shortcoming: it's hard to systematically verify the integrity of the stored data. As it stands today, the Filecoin network is a peer-to-peer version of Amazon S3 that regularly verifies the storage of data. Filecoin uses storage deals priced based on supply and demand dynamics. Instead of a fixed pricing structure it is frequently cheaper, faster and more secure than its centralised competitors, AWS, Google Cloud and Microsoft Azure.

Currently, there are about 25,000 transactions on the Filecoin blockchain per day and in total there is about 127 pebibytes (1PiB equals 1,125,900 gigabytes) worth of data stored on it. In terms of total capacity, Filecoin developers say that the network is currently at around 10% of AWS' storage capacity.

Cryptographically hashing data in Filecoin's Inter-Planetary File System and storing it with a Filecoin miner costs less than 1% of the storing fee for the same amount of data on AWS.

The Investment Opportunity

Crypto is growing at 113% per year in terms of users. Even if it slows down to the 63% growth rate of network adoption the internet saw at the same stage, it will lead to 4bn users by 2030 or earlier. This is approximately 20 times the number of users that are using blockchain technology today.

CRYPTO USERS VS INTERNET USERS OVER SAME TIME - LOG SCALE

Source: Crypto.com - World Bank - Global Macro Investor

The first new asset class in 150 years?

As an asset that exists purely in digital form, cryptocurrency is fundamentally different from all other major asset classes.

Cryptocurrency has weaker correlation to traditional asset classes than most other assets typically sought out for their diversification. Although volatility is notably high, crypto's low correlation profile means it has the potential to enhance long-term risk-adjusted returns when added to a diversified portfolio.

Legendary value and macro investors like Bill Miller (former chairman of Legg Mason), Paul Tudor Jones (Tudor Investment Corporation), Ray Dalio (founder of Bridgewater Associates) and Stanley Druckenmiller (founder of Duquense Capital) have all person-ally allcated to crypto assets and are all strong proponents of the sector. Ray Dalio believes ALL investors should have an allocation to crypto assets, suggesting a 2% allocation would be reasonable.

A common critique of Bitcoin (and Gold) by institutional investors is the lack of yield, however Etheruem's move to proof of stake (POS) means the number 2 crypto asset now offers a yield of around 4.5%. Note all other major blockchains (with the exception of Bitcoin) run on POS and also offer a yield (and use a fraction of the energy for the ESG constrained).

Where does it fit in a portfolio?

Fidelity surveyed over 1,000 institutional investors mid 2022, 81% of respondents view digital assets as having a role in their portfolio, with 35% of the total preferring to allocate from an independent allocation bucket and 34% preferring to allocate from alternatives and a further 11% allocating from their real assets bucket.

The features top of mind when considering how to allocate were; high potential upside, innovative technology play, enabling de-centralisation, free from government intervention, uncorrelated to other assets macro/inflation upside and participation in DeFi and yield opportunities.

Morningstar explored the risk equation for adding crypto to a 60/40 portfolio allocating from equities and from bonds, with bitcoin allocations of 1% and 2% having 9% and 24% contributions to gross risk respectively but more importantly a de minimis change to overall portfolio volatility and unsurprisingly marginally less risk when funding the allocation from equities as opposed to bonds. At a 5% allocation the Sharpe ratio is doubled, but allocation beyond 10% see a significant uplift in overall volatility.

Our calculations, represented in the chart below, confirm small allocations can have a significant impact enhancing a 60/40 portfolio, we allocated pro rata from both buckets with the 5% allocation resulting in annualised performance 300% higher at a cost of just 7% more volatility.

Year	BTC ROI	ETH ROI
2021	57%	404%
2020	303%	465%
2019	87%	-8%
2018	-72%	-82%
2017	1295%	8985%

	Cumulative	Annualised
0% Crypto	5.7%	1.1%
1% Crypto	9.3%	1.8%
2.5% Crypto	14.9%	2.8%
5% Crypto	24.1%	4.4%

DIGITAL ASSETS IN A 60 / 40 PORTFOLIO - CUMULATIVE RETURNS

— 1% Crypto   — 2.5% Crypto   — 5.0% Crypto   — 0% Crypto
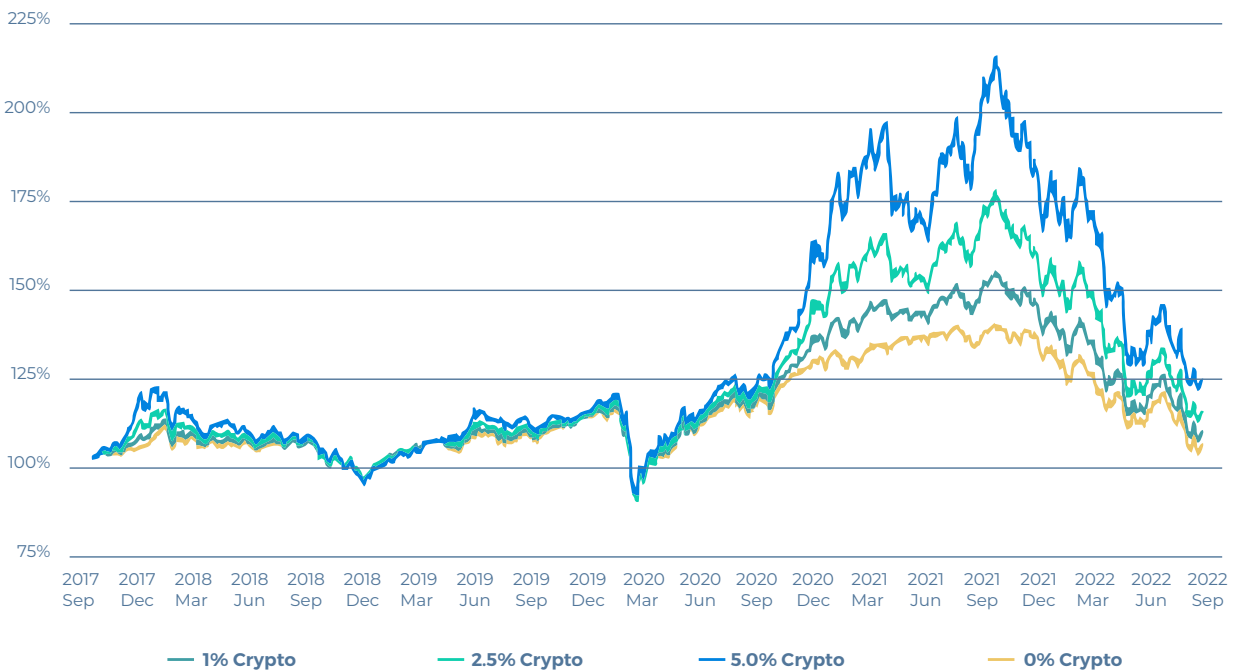
About the Directors

Ryan McMillin

B.Comm, CPA, Grad Dip Applied Finance & Investment

ryan@merkle.com.au
0455 319 994

Ryan is an investment professional with 20 years of experience in asset management split between Australia and the U.K. Ryan is a specialist in product development, strategy and structuring having designed and successfully launched over 100 funds in 10 jurisdictions which have raised billions and won multiple awards. Ryan is also a qualified accountant with experience in portfolio construction, fund operations, risk management and compliance. Ryan has worked at several global asset management firms including at BlackRock, GAM, Coutts & Co., AMP Capital and RBS Investment Bank, winning awards for product design and development and creating many industry firsts like creating the first risk premia funds offered to retail clients in the Europe.

Dean Serroni

B. Computing, PMP
dean@merkle.com.au
0438 466 164

Dean is a technology leader with over 20 years of experience in technology transformations, consulting leadership and entrepreneurship. Dean spent the first part of his career delivering technology implementations, primarily in the financial services sector, before taking on leadership roles at a range of consulting firms. While building and successfully exiting a tech startup over the past decade, Dean became exposed to the cryptocurrency ecosystem and developed his skills as both an investor and industry contributor. Through his involvement in cryptocurrency Dean established a passion for this nascent space and felt compelled to become more deeply involved. Merkle Tree Capital was born.

If you are interested in assisting to increase awareness of the digital assets space, or have any further questions on blockchain technology or digital assets, we welcome your call and involvement.

Additional reading:

- Blockchain Technology and what it means to be Trustless

- Blockchain in the Real Estate Industry. Part 1: Investment Vehicles

- Applying traditional risk management practices to a crypto portfolio

Additional resources can be found on the Insights section of our website at https://merkle.com.au/

Disclaimer

Merkle Tree Capital Pty Ltd is a Corporate Authorised Representative (CAR) of Boutique Capital Pty Ltd (BCPL) AFSL 508011, CAR Number 001293010.

This document contains general advice only and has been prepared by Merkle Tree Capital Pty Ltd (CAR) for individuals identified as wholesale investors for the purposes of providing a financial product or financial service, under Section 761G or Section761GA of the Corporations Act 2001 (Cth).

The information herein is presented in summary form and is therefore, subject to qualification and further explanation. The information in this document is not intended to be relied upon as advice to investors or potential investors and has been prepared without taking into account personal investment objectives, financial circumstances or particular needs. Recipients of this document are advised to consult their own professional advisers about legal, tax, financial or other matters relevant to the suitability of this investment service.

The investment summarised in this document is subject to known and unknown risks, some of which are beyond the control of CAR and their directors, employees, advisers or agents. CAR does not guarantee any particular rate of return or the performance of the Fund, nor does CAR and its directors personally guarantee the repayment of capital or any particular tax treatment. Past performance does not guarantee future performance.

This document is informational purposes only and is not a solicitation for units in the Fund. Application for units in the Fund can only be made via the application form, in conjunction with the Fund's Information Memorandum, which should be read thoroughly.

All information provided herein is qualified in its entirety by reference to such documentation.