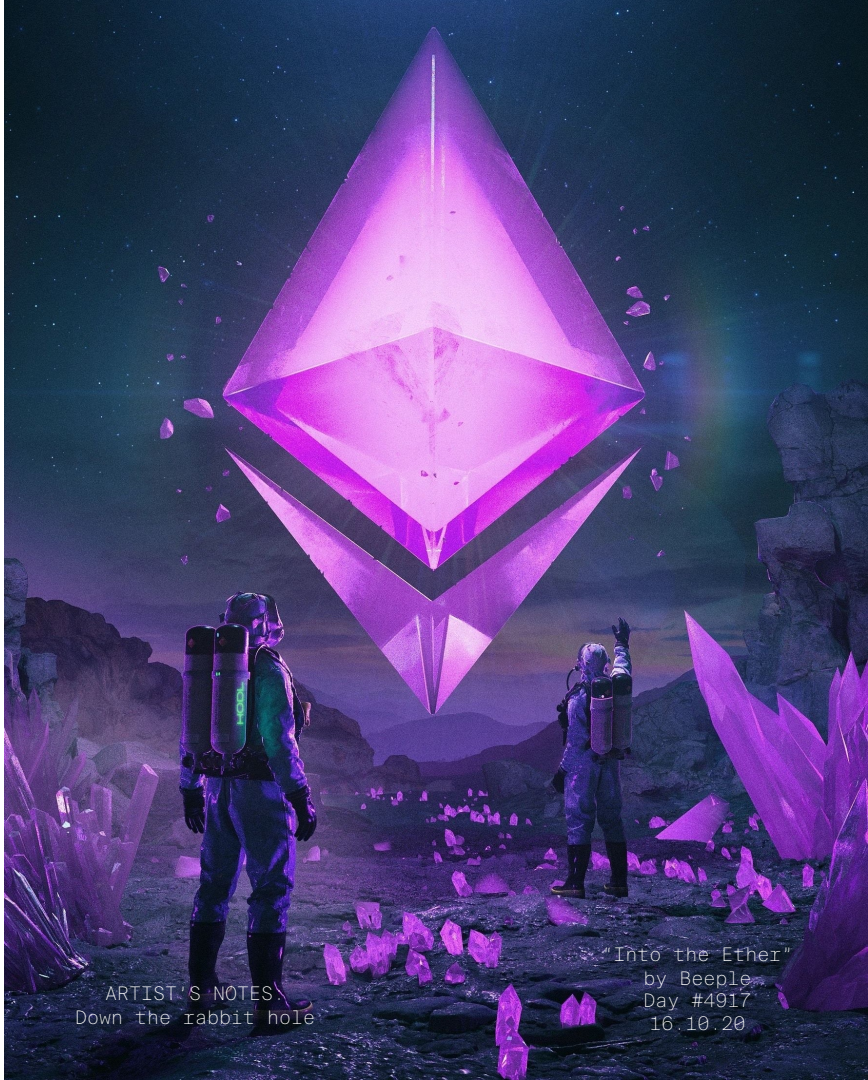
Crypto 101

September 2021

Kevin Lu & Andrew Yeo

AirTree



Disclaimer

The purpose of this presentation is to provide general information only, and nothing in it constitutes (i) an offer or disclosure document of any kind in relation to, (ii) a recommendation to buy, (iii) an offer to sell, (iv) a solicitation of an offer to buy, (v) advice in relation to or (vi) an endorsement of any securities, financial instruments, financial products, or financial services. An offer or invitation will only be extended to a person if the person has first satisfied AirTree that the offer or invitation would not require AirTree or its related entities to prepare a disclosure document or product disclosure statement (each as defined in the Corporations Act 2001 (Cth)) or equivalent document in other jurisdictions or require the Fund to be registered as a managed investment scheme under the Corporations Act 2001 (Cth).

To the extent permitted by law, none of AirTree, its related entities or their respective directors, officers, partners, employees, affiliates, shareholders or agents makes any representation, guarantee or warranty (express or implied) as to, or accepts responsibility for, the accuracy or completeness of the information contained in this presentation. None of AirTree, its related entities or their respective directors, officers, partners, employees, affiliates, shareholders or agents has any responsibility to notify any person of any inaccuracies or omissions in information contained in this document or to update this document in any way.

This presentation has been prepared without any knowledge or consideration of the investment objectives, financial situation, taxation position or other particular needs or requirements of any recipient and should not be relied on for the purposes of making any investment. Each of AirTree, its related entities and their respective directors, officers, partners, employees, affiliates, shareholders and agents disclaims to the fullest extent permitted by law all liability, direct or indirect, for any loss or damage suffered by any person (regardless of the basis on which such liability may arise, including out of negligence or otherwise) arising out of, or in connection with, any use or reliance on this presentation.

Contents

1. The basics

AirTree

Crypto was initially a response to the **flaws of global financial and government systems**

- **~20% of the world's GDP (US$16T)** is dedicated to moving money around.
- **>2B people unbanked** worldwide
- Money movement requires **trust of centralized third parties** who didn't prove so trustworthy in the GFC
- **Governments seizing assets/property in some countries**
- **Hyper inflation** – you can't always rely on government backed currency (e.g., Zimbabwe)
- (Large) funds are **not accessible** when banks are closed
- Cross-border transaction fees are **expensive**
- **Lengthy time** required to execute transactions

Crypto – refers to **digital currency** underpinned by cryptography and **blockchain** technology

Cryptocurrencies have these attributes

- universally accessible (with internet)
- cannot be faked
- the record of transactions is public
- cannot be altered retrospectively, and
- has limited supply (thus is deflationary)[1]

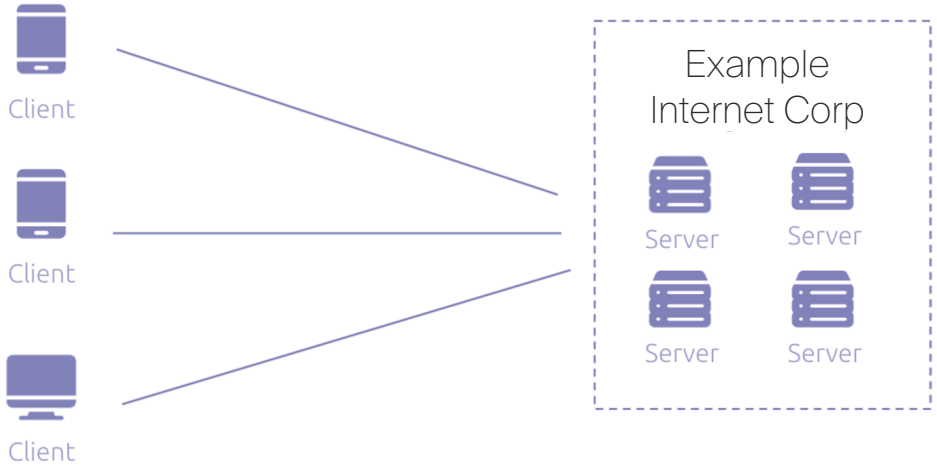
1. Not always the case

What is a **blockchain** ?

- **Level 1 - Basic explanation:** Think of it as an open list of data, shared by a network of people. New additions to the list needs to be validated by participants in the network. New additions cannot be changed once added. All the functionality of the list is secured by maths & computer science.
- **Level 2 - Geeky explanation[1]:** A virtual computer that runs on top of a network of physical computers that provides strong, auditable, game-theoretic guarantees that the code it runs will continue to operate as designed.

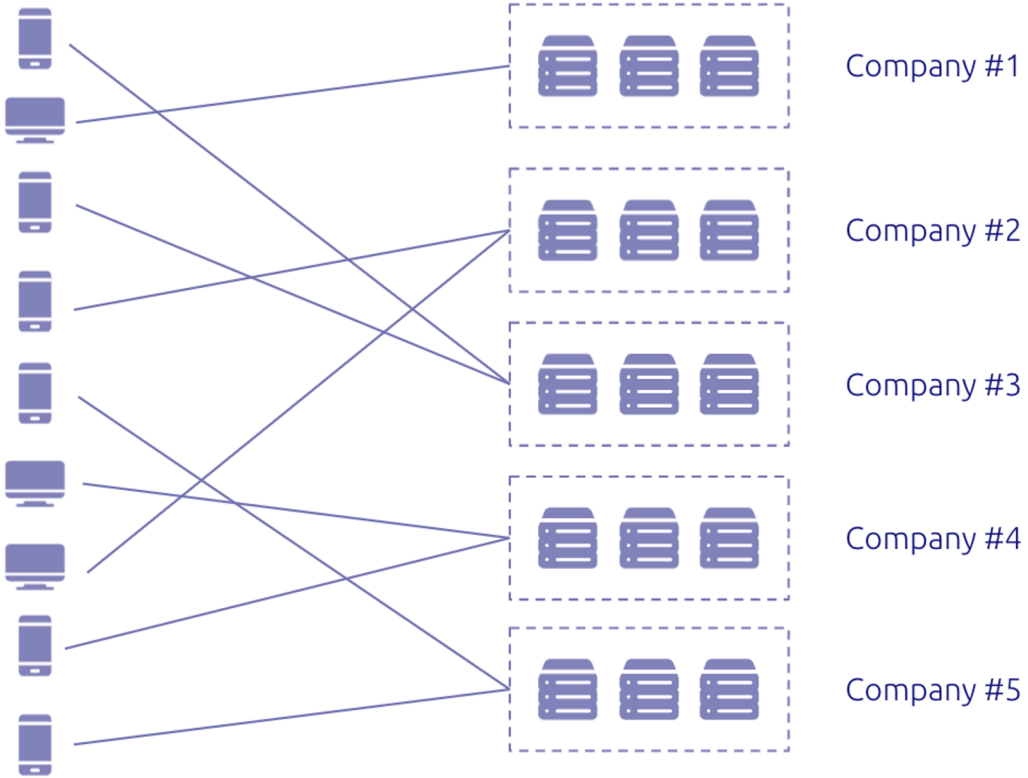
1. Simple definition of a computer: A system that can a) store data, and b) can perform operations on said data

Let's back track and look at **traditional client – server** architecture. Here, traditional servers are **closed systems** owned by a company.



Credits: Patrick Rivera

The internet is basically just a bunch of these **closed systems** interacting with each other



Credits: Patrick Rivera

There are **trade-offs** with the **traditional client-server** architecture

Pros

- Network effects
- Scalability
- Faster Iteration

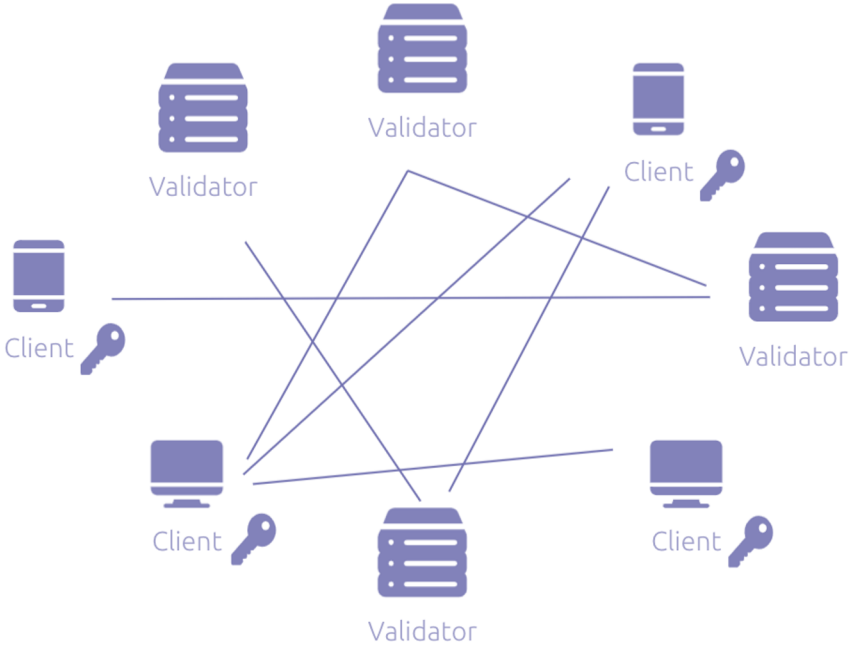
Cons

- Monopolistic behaviour
- Centralized control
- 3rd-parties need permission to integrate
- Single point of failure

Credits: Patrick Rivera

Now let's look at **decentralized architecture** & how it solves for client – server model issues

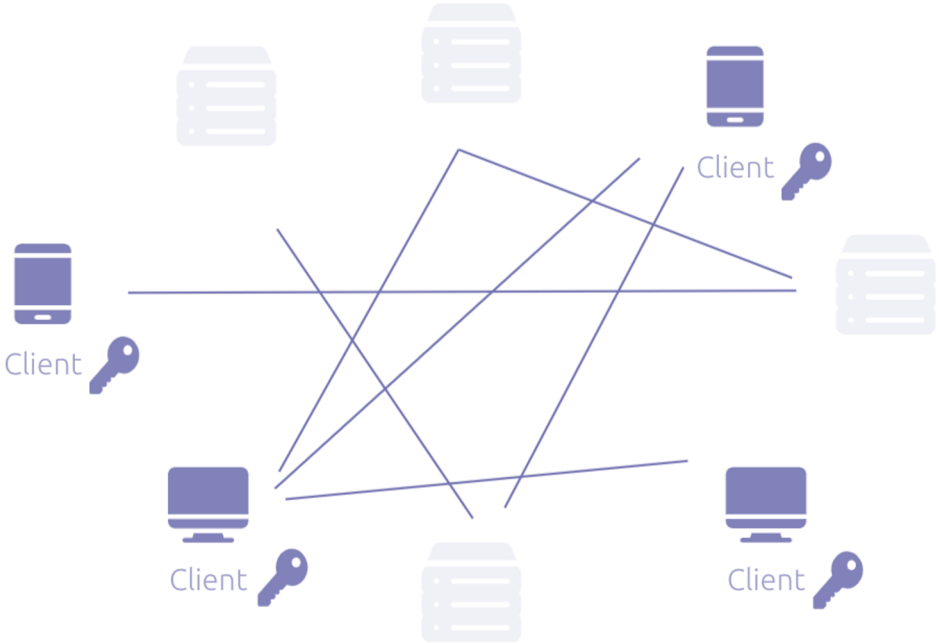
Blockchain are **peer-to-peer** networks



Credits: Patrick Rivera

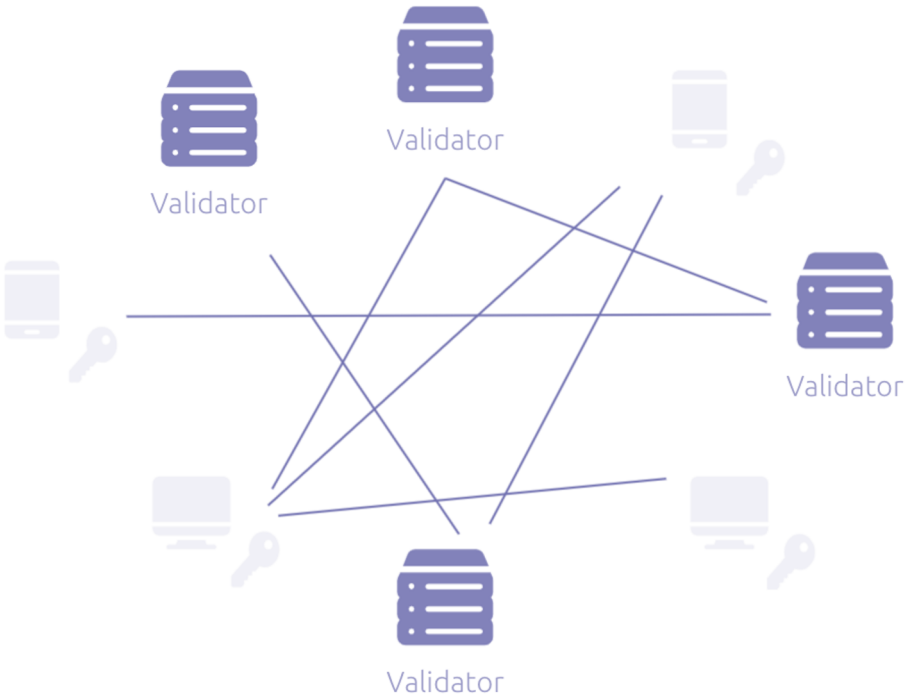
Clients can send, receive, and read transactions or information

Transactions include transferring cryptocurrency (e.g., bitcoin) or assets between client x and client y



Credits: Patrick Rivera

Validators check that transactions are correct by solving cryptographic (math) problems which use computer power. Consensus between validators is needed for transactions to be recorded on the blockchain. Validators receive rewards like bitcoin for their work

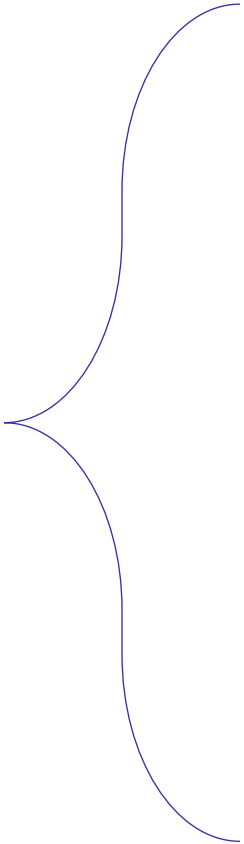


Credits: Patrick Rivera

Consensus refers to when most validators agree on the right transactions to add to the blockchain ledger. The most common consensus methods are **Proof of Stake** and **Proof of Work**

	Proof of work	Proof of stake
Energy consumption	High	Low
Participants	"Miners"	"Stakers"
Reward selection	To add new blocks, miners compete using their computer's processing power to solve difficult math puzzles	Creator of a new block is randomly chosen among stakers by an algorithm. Amount staked increases chances of selection
Validation	All miners compete to solve cryptographic puzzle to validate the transaction	Set validators participate in a consensus algorithm to vote on the next block to be forged
Rewards	The first miner to solve the puzzle is given a reward for their work	No block reward. The randomly selected staker takes the block's pooled transaction fees
Protocol	Bitcoin, ethereum	Algorand, Tezos

There are **trade-offs with decentralised** architecture as well



Pros

- Decentralized governance
- No single point of failure
- Each client node owns their data
- Global access
- 3rd parties can integrate w/o permission

Cons

- Challenging to scale
- Security bugs are near impossible to revert
- Proof of work consensus consumes a lot of energy (but Proof of Stake solves this)

Credits: Patrick Rivera

2. Story of webs and waves

AirTree

Let’s start with the era of the **webs**

Web 1.0 (1993 – 2002)

- Static websites
- Portals
- Directories
- Email/Chat
- Physical goods marketplaces
- Low bandwidth
- Limited hardware

Credits: Patrick Rivera

Web 2.0 (2002 - 2018)

- Social
- Mobile
- Cloud computing and SaaS
- Gig economy marketplaces
- Centralized web

Credits: Patrick Rivera

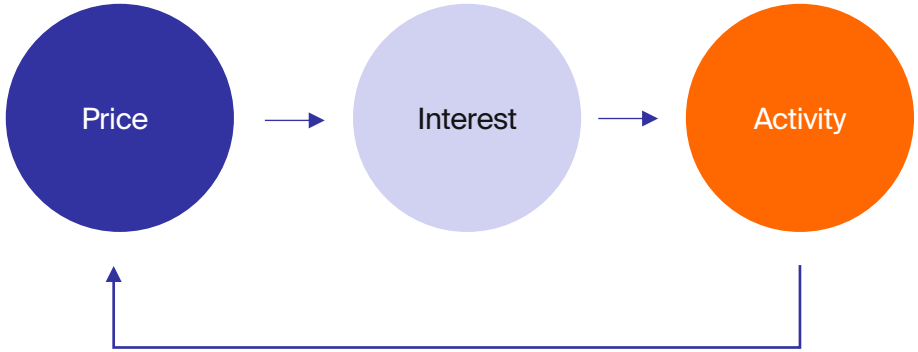
Web 3.0 (2018 - ?)

- Decentralised web + in-built payment rail
- Smart contracts
- DeFi
- NFT standards
- Metaverses
- Decentralised Autonomous Organisations (DAOs)

Web 3.0 is Crypto

- Decentralizing control and reducing intermediaries
- Using technology to help the disadvantaged
- Fixing what's wrong with the internet and finance today

Crypto's story has played out in 4 waves, each with similar underlying dynamics:

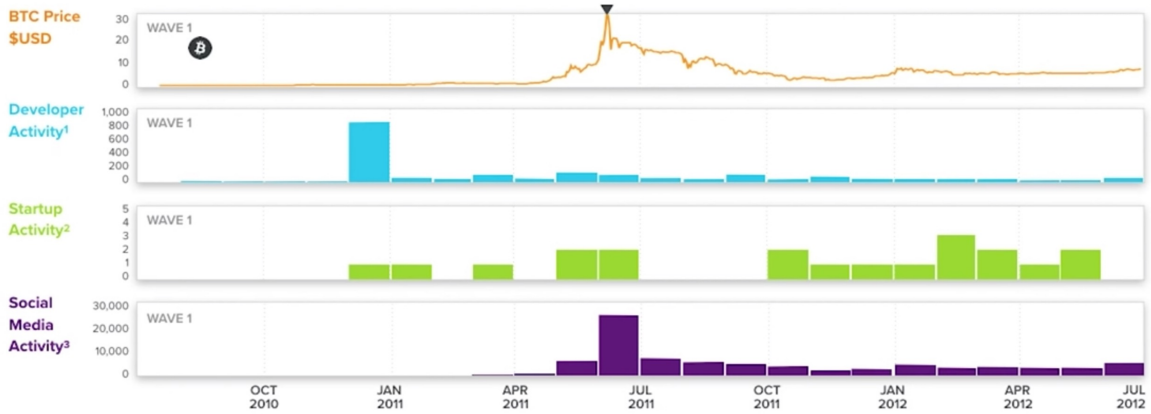


Source: a16z, AirTree Ventures analysis

Wave 1: (2010-2012)

- Bitcoin
- Miners
- Centralised exchanges

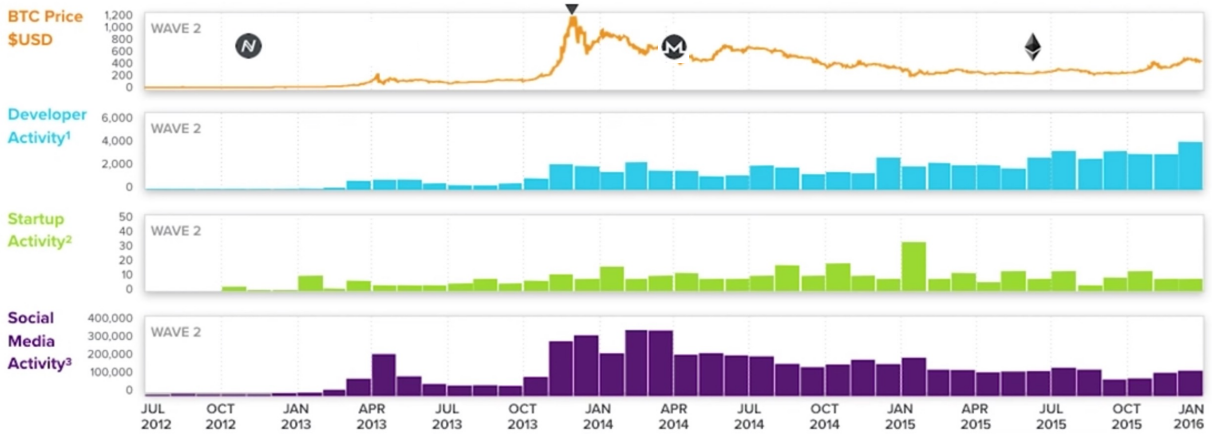
  (Coinbase, Mt Gox, Kraken)
- Focus on wallet technologies



Sources: Chris Dixon (a16z), data from Github, Pitchbook, Twitter and Subreddits

Wave 2: (2012-2016)

- Ethereum started which gave birth to **smart contracts**
- Mt.Gox Hack (2014)
- Developer activity kicked off and sustained despite price declines

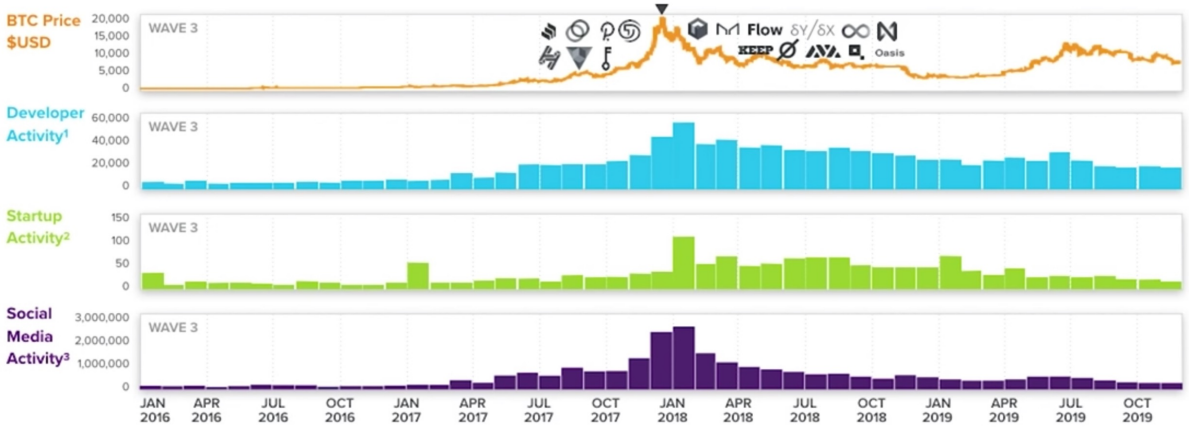


A Smart Contract is a programmatic agreement to exchange goods, services, or money that will automatically execute, without third party oversight, so long as established criteria are met. This allows agreements between parties to be executed without a central authority or legal system. It also enables things like trading of crypto assets or liquidations of loan collateral to happen autonomously without intermediaries.

Sources: Chris Dixon (a16z), data from Github, Pitchbook, Twitter and Subreddits

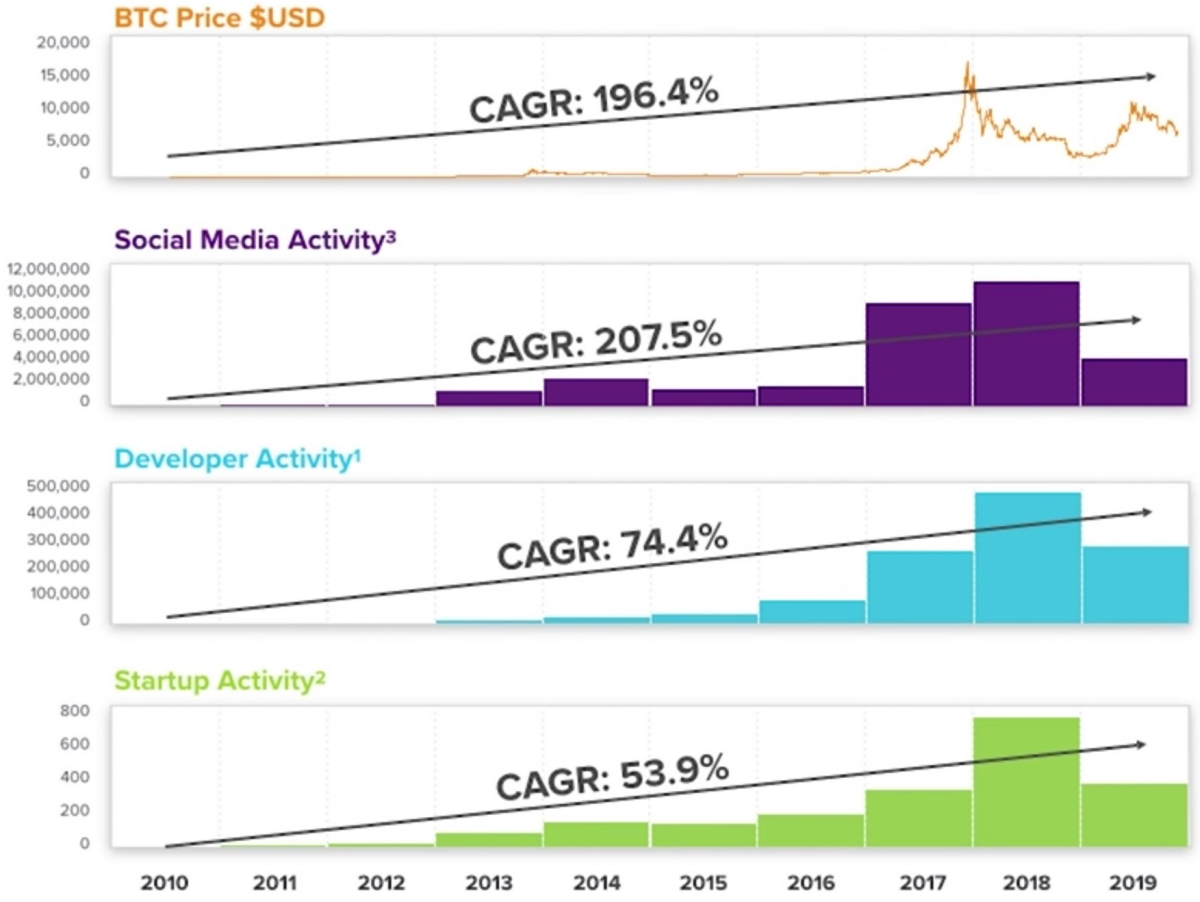
Wave 3: (2017-2019)

- Start of DeFi (Maker)
- New focus on interoperability
- ICO mania
- NFTs and gaming
- Crypto winter
- Birth of stable-coins



Sources: Chris Dixon (a16z), data from Github, Pitchbook, Twitter and Subreddits

Putting the 3 waves together, we see consistent growth driven by a **feedback loop** between **interest** & **innovation**



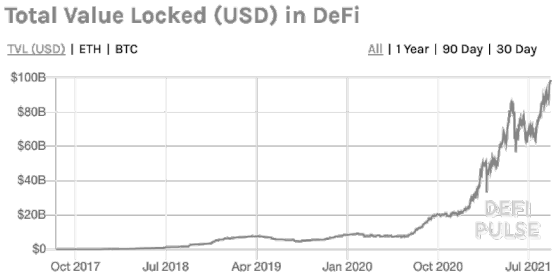
Sources: Chris Dixon (a16z), data from Github, Pitchbook, Twitter and Subreddits
CAGR: Compound Annual Growth Rate

Wave 4: 2020-?

Seeds planted in the 2017 wave are seeing mainstream adoption, two main use cases being:

1. DeFi & Stablecoins

This takes crypto beyond just being a currency, enabling financial services (insurance, loans, exchanges, derivatives) in a decentralized manner. Emergence of scalable and fast L1 and L2 chains, and stablecoins have boosted DeFi adoption



Key Projects:

USD Coin

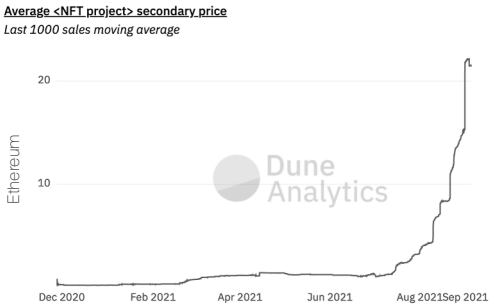
Compound

UNISWAP

SOLANA

2. NFTs & Gaming

Files that live on a blockchain that can prove ownership of an asset, hugely beneficial to the issue of attribution in the world of art and gaming.



Key Projects:

TOP SHOT

AXIE INFINITY

Sources: DeFi Pulse, Dune Analytics, AirTree Ventures analysis

From the **outside**, it looks like crypto is just **cycles of speculation**

But **insiders** realize each cycle brings the capital needed to invest in **critical infrastructure**

Critical Infrastructure already built:

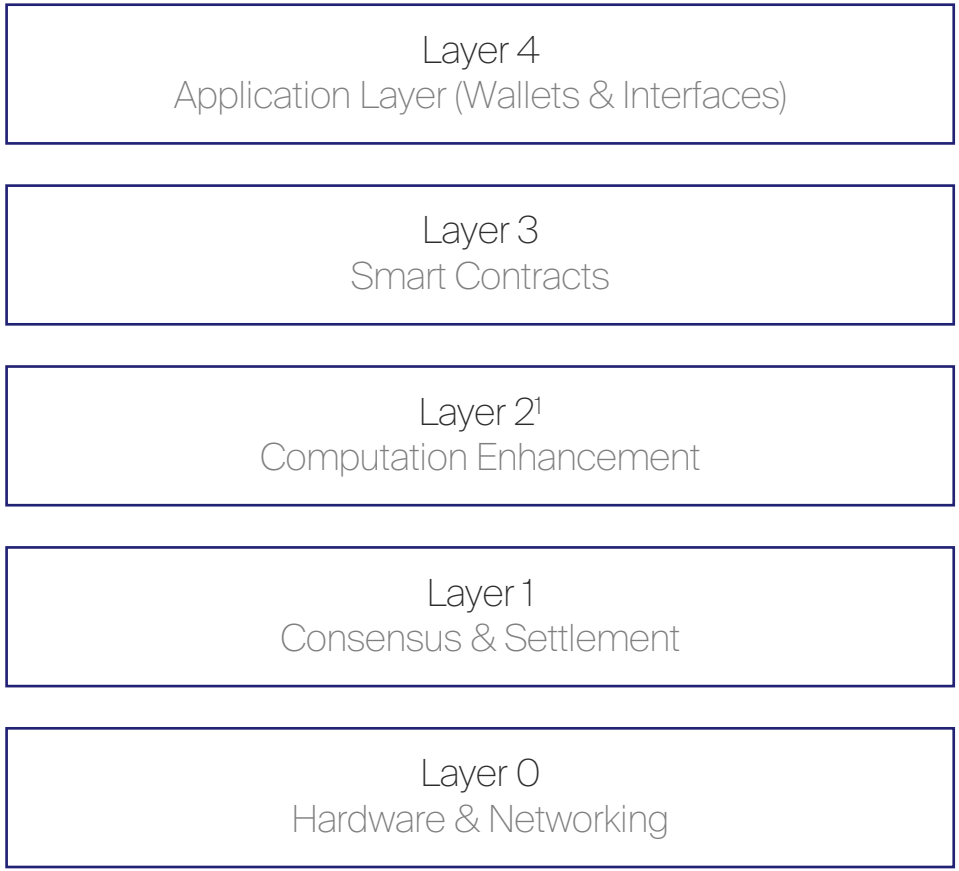
- ✓ Layer 1 blockchains (e.g., Ethereum, Solana)
- ✓ Developer tools
- ✓ Decentralized exchanges
- ✓ Smart wallets
- ✓ Storage protocols
- ✓ Stablecoins
- ✓ Lending protocols

Credits: Patrick Rivera

3. Taxonomy of crypto land

AirTree

There are 5 layers to a virtual blockchain computer



1. Only applies to earlier Proof of Work L1 chains like Bitcoin and Ethereum. Does not apply to new iterations of chains like Solana, Avalanche and Algorand which are scalable and fast

L1 - L3 are at the heart of crypto, being the key points of value aggregation[1]

Layer 4
Application Layer (Wallets & Interfaces)

NBA TOP SHOT

Layer 3
Smart Contracts

MAKER
Borrowing, saving crypto

UNISWAP
Decentralised exchange

Layer 2
Computation Enhancement

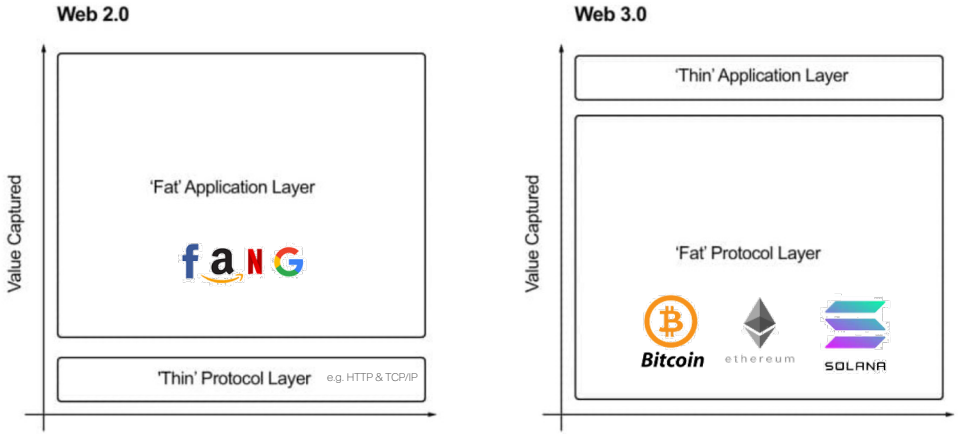
Matic zkSync OP
Enable greater network transaction speed

Layer 1
Consensus & Settlement

Bitcoin ethereum SOLANA

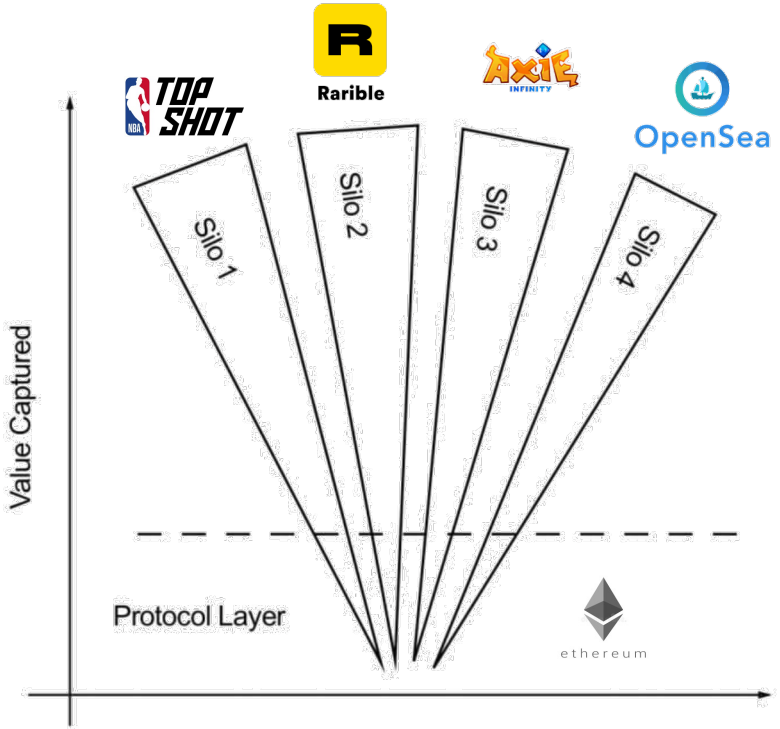
Layer 0
Hardware & Networking

Initially we thought most of the value in web 3.0. would be captured in L1 (Fat Protocol Thesis)[1]



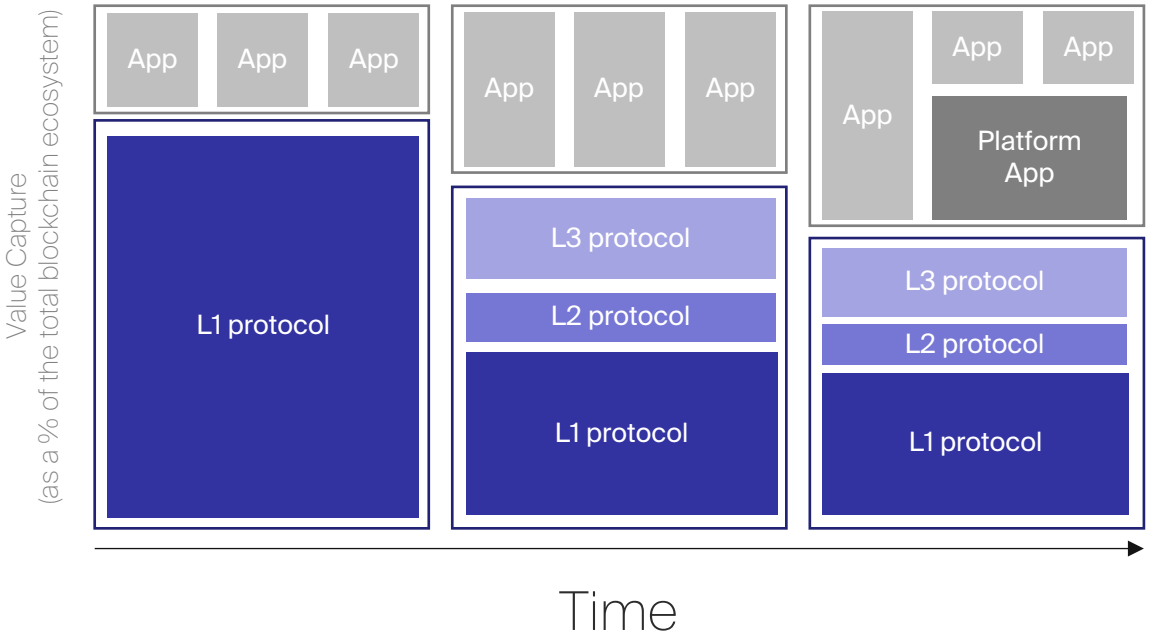
1. Joel Monegro (ex USV) – originally published the thesis in 2016

But we realized we can draw a protocol-application boundary at any level of abstraction[1]



1. Jake Brukman (CoinFund)

Longer term, we see **composability** being a key theme, particularly in **DeFi**, which may mean more value, **more evenly distributed**[1]

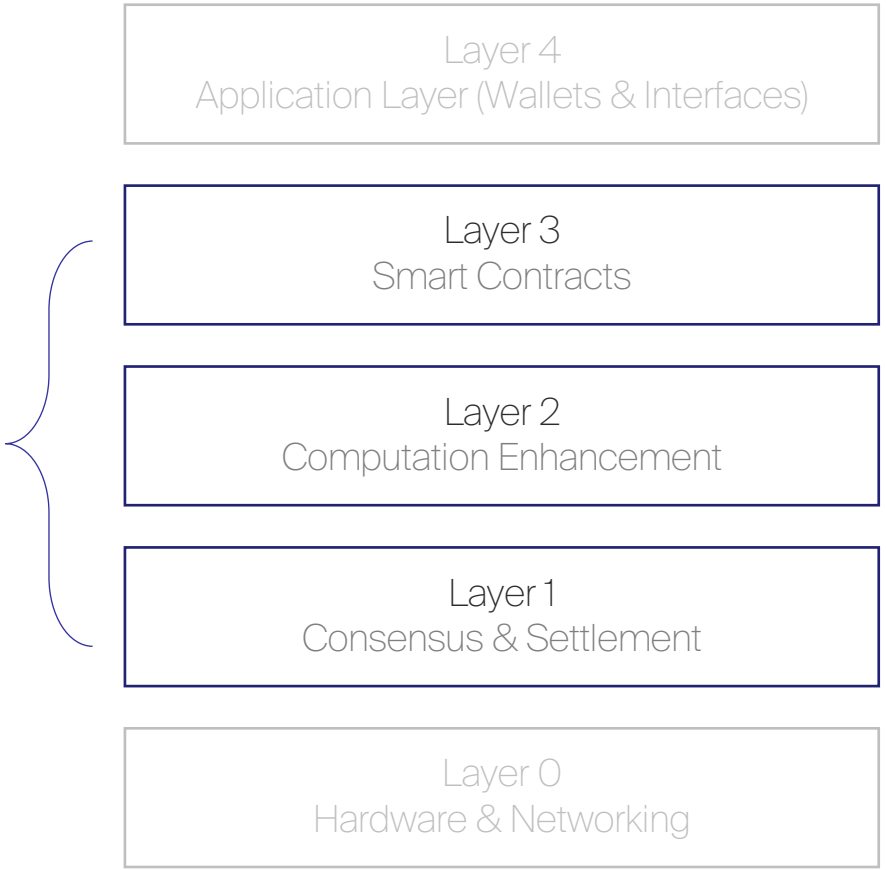


1. Johnson Nakano (CoinMonk)

4. Crypto Business Models

AirTree

Let's **focus on L1 – L3** that make crypto possible, L0 & L4 have more traditional business models



Source: a16z, AirTree Ventures update

Value capture at L1 & L3 are instances of **multi-sided platforms**

What is a multi-sided platform?

- Common ground that enables interaction between different types of participants to create value

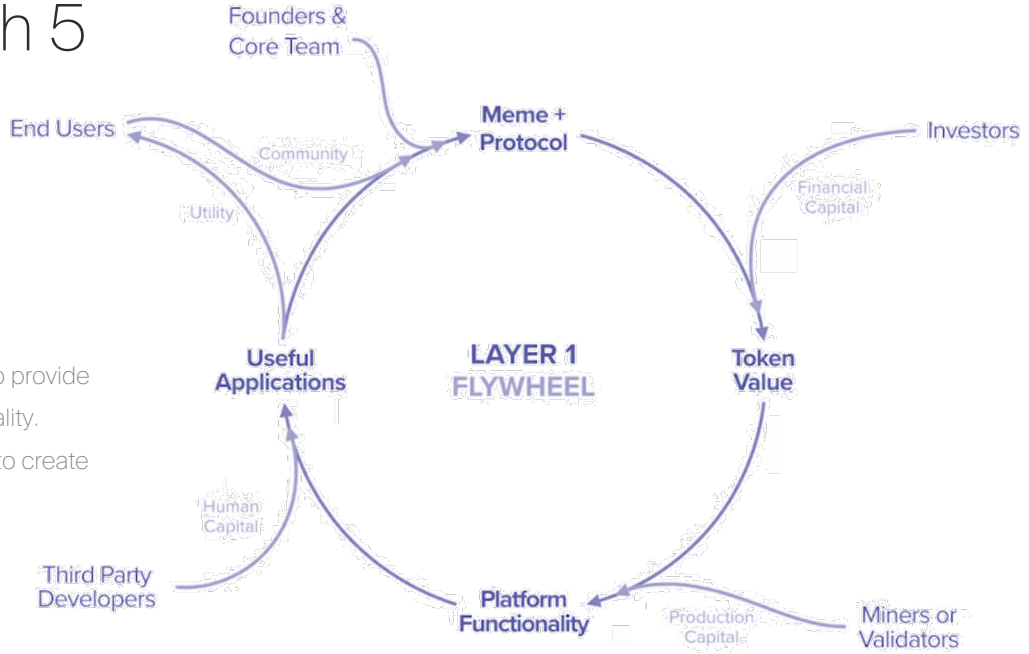
Examples:

1. Bazaar - where merchants meet villagers
2. Uber – where drivers meet riders
3. App Store – where developers meet users

Source: a16z, AirTree Ventures update

L1 blockchains are generally multi-sided platforms with 5 participants

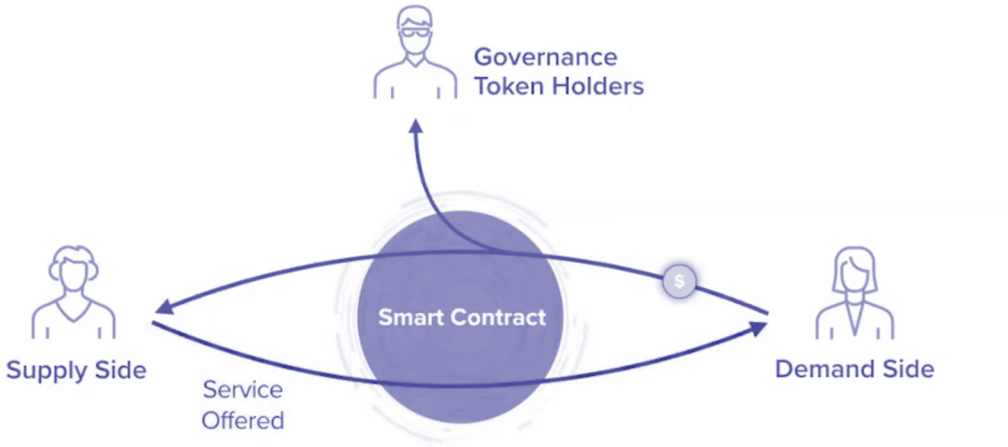
1. Founder & Team build protocol
2. Investors may help fund project
3. Protocol generates some initial token value
4. Once token value exists, it creates incentive for validators to provide computational resources for platform security and functionality.
5. Once platform exists, 3rd party developers are incentivised to create useful applications (Layer 4)
6. Which bring utility to end users
7. As a result, community begins to form and grow
8. Which reinforces the protocol/token value



Source: Ali Yahya (a16z)

Core Layer 3 Business Model

- Smart Contract exists in the middle
- Supply side provides/offers service
- Demand side pays for service
- Protocol Governance Token holders captures a small share of the revenue
- All in a way which is automatic, no intermediary/middle person



Source: Ali Yahya (a16z)

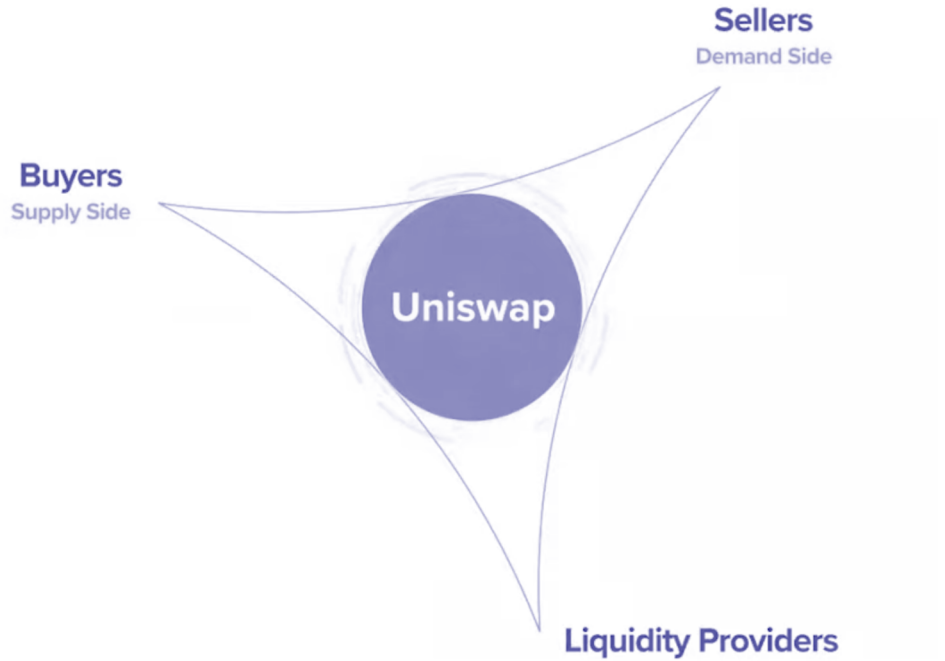
Case Study: Maker (L3)

- Ethereum based multi-sided platform with 5 participants, split into 2 halves, one half offers a stable coin, the other facilitates loans.
- Loan half: Composed of the Lender and Borrowers
- Stable coin 'DAI' half: As a result of the lending activity (capital from lenders, and collateral from borrowers), a stable USD pegged crypto currency is produced. Collateral providers receive a stability fee that continuously accrues as interest. Fees vary based on collateral provided, and range between 1%-9% p.a.
- Keepers: Guardians of the network to ensure the network is financially sound.
- MKR Holders: Serves as both governance (making sure parameters of the network are sound, and risk is managed), and mechanism for financial capital to enter the network

Source: Ali Yahya (a16z)

Case Study: UniSwap (L3)

- Uniswap: Ethereum based decentralised exchange platform with 3 sides. Was designed to function as a public good.
- Buyers and Sellers trade on the platform (just like they would on Coinbase or Binance)
- Liquidity providers park their crypto assets (e.g., BTC, ETH, DAI) in Uniswap liquidity pools in exchange for fees (~0.3% per transaction). This allows buyers and sellers to always trade with the pool rather than needing to wait for a counter party to match their order.



Source: Ali Yahya (a16z)

5. Regulatory responses to date

AirTree

Most of the western world is moving towards **favourable crypto regulation**

Source: Elliptic

Key regulatory tension points globally

1. **Crypto's definition, particularly in being viewed as a security.**

   - Crypto can be classed as for personal use or as a security. If crypto is deemed to be a security, this creates a reporting burden for projects. In the US, Safe Harbor proposals and The Howey Test help crypto projects test if their tokens qualify as a security or investment contract

2. **Decentralized exchanges and Know Your Customer (KYC)**

   - Exchanges need to KYC/AML, but there are many areas of the world where KYC and AML infrastructure is not developed, preventing access to financial systems. Embedded in crypto beliefs is global indiscriminate access, which goes against the KYC/AML measures of traditional finance

3. **Banning Crypto entirely to prevent capital flight**

   - This is largely only the case in countries with totalitarian regimes.

Source: Brian Brooks – Chief Legal Officer (Coinbase)

Latest developments

1. **U.S. Infrastructure Bill (August 2021)**

   - Bill passed which broadened the definition of broker to include cryptocurrency developers, protocols and miners who will be required to report customer info to the Internal Revenue Service (IRS).

   - An attempted amendment to distinguish developers had majority support but was vetoed. Definitional issue remains, framework not workable let alone enforceable. More work needs to be done before laws are legislated in circa 2023

2. **China Crackdown heightened (June 2021)**

   - China's ban on crypto miners and exchanges have been going on and off since 2018. It has been in part to stop capital flight, and in part to lower carbon emissions from Bitcoin mining. China's Bitmain supplies 65% of world's mining rigs. Miners like Bitmain have been transferring rigs out of China and are moving to Kazakhstan, Mongolia and the US.

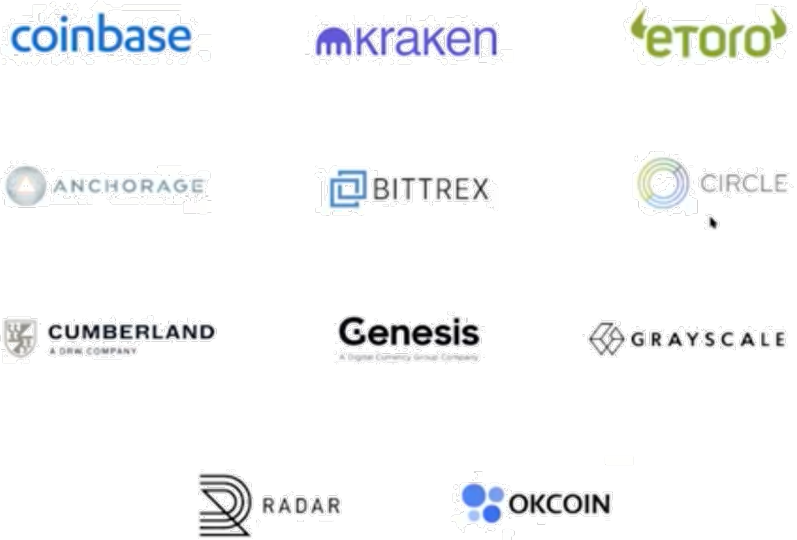
3. **El Salvador's world first adoption of Bitcoin as legal tender**

   - In June 2021, President Nayib Bukele said he will make BitCoin legal tender in El Salvador, touting its potential to help Salvadorians living abroad send remittances home.

Sources: WSJ, Financial Times, Coindesk, Reuters, Forbes

Crypto Rating Council:

Group of 11 institutions that have come together to provide risk-based scoring of crypto tokens



CRC have put together a 36-question scorecard framework to determine whether something is a security or not, and the riskiness of new crypto projects

Source: Brian Brooks – Chief Legal Officer (Coinbase)

Australia has **largely been crypto friendly** (besides Libra), and is consistently consulting with industry to evolve policy

- In Australia, cryptocurrencies are treated as property and subject to capital gains tax - previously was subject to double taxation under GST
- Since 2018, all crypto exchanges in Australia must register with the Australian Transaction Reports and Analysis Centre (AUSTRAC) - in compliance with AML/CTF 2006 Part 6A (Anti-Money Laundering and Counter-Terrorism Financing Act 2006).
  - This rule requires entities acting as exchanges, or providing registrable exchange type services to identity and verify their users, maintain records and comply with AML/CTF reporting obligations
- Since May 2019, ASIC updated regulatory requirements for both ICOs and cryptocurrency trading
- Select Committee on Australia as a Technology and Financial Centre has launched new rounds of consultation to review the policy and provide consistency across a federal level
  - One option is extending the nation's fintech sandbox to include crypto projects. This approach has been favoured in the FCA in the U.K. and the recently introduced fintech sandbox in Spain
- Currently there is not yet a position on whether a "Governance Token" constitutes a security. The token framework needs to be updated to distinguish between Governance and Utility tokens
- Tax Treatment – if a crypto currency is held as an investment, investors are to entitled to the personal use asset exemption, but if crypto is held for more than 12 months, investors may be entitled to CGT discount to reduce a capital gain at disposal. See here for more detail

Sources: Comply Advantage, ATO, Coindesk.

6. Differences in investing in crypto vs regular start-ups

AirTree

Token vs Equity

Regular Startups

- Invest in equity, which increases in value as the cash flows and impact of the business increases. Equity represents share of ownership in an entity
- Often has investor protections e.g., pro rata rights and liquidation preferences
- Equity pool is illiquid until liquidity event which is typically 4+ years from investment
- Includes ESOP, a stock option pool reserved for staff and hires used to incentivize staff
- Equity is held by investors and staff
- Ownership stake can be diluted but pro-rata rights protects from dilution
- Organization is governed by a central board and management

Crypto startups

- Invest in either Equity or Tokens but tokens are more common, highly volatile and liquid
- Token value and economics vary but simplistically, token value increases with usage of the product/Dapp/protocol and high demand for the token relative to supply. Two types of tokens:
  - Governance token gives holders voting rights to make changes to the project. Analogy in equity is voting shares
  - Utility tokens enable you to use, buy or earn in the product e.g., Axie Play to Earn, DeFi rewards
- Equity protections and liquidity are similar to normal startups, but should provide rights to tokens (not necessarily pro-rata)
- Tokens are split by 'circulating supply' and 'non circulating'. Circulating tokens are liquid in the secondary market. 'Non circulating' are reserved or have vesting periods before they are liquid
- Projects typically incentivize staff and community with tokens
- Tokens are held by investors, staff, treasury, users and the community. Projects reward active contributors with more tokens over time meaning passive investors are diluted over time
- Projects are increasingly transitioning to Decentralised Autonomous Organisations (DAOs), which is governed by code that can only be changed via governance token holders voting on community proposals

Difference in terms

Regular Startups	Crypto startups

• **Investor protections:** Includes pro-rata rights, ROFR and liquidation preferences	• **Investor protections:**
	  • Equity: similar to regular startup but need to ensure pro-rata rights to tokens
	  • Tokens: Not yet market standard to have pro-rata rights to each new token issuance. No liquidation preferences

• **Investor liquidity:** preference shares typically issued at time of investment. Liquidations typically happen 4+ years after investment at time of IPO, M&A or secondary sale	• **Investor liquidity:**
	  • Equity: similar to left but also includes conversion to tokens upon DAO transition
	  • Token: 2-3 year vesting period with 6-month cliff and monthly vesting to avoid token dumping

• **Employee stock and option vesting:** typically 4 year vesting, 1 year cliff	• **Employee vesting:**
	  • Equity: similar to startup but uncommon
	  • Token: similar vesting to investors above

• **ESOP:** Typically 10% of total capitalization is set aside for staff options which is topped up in each fundraising round	• **Core team tokens:** Typically 30 %+ of max token supply are set aside for core team and hires, and community

Source: AirTree Ventures, Modern Finance

Valuation Methods

Regular Startups	Crypto startups

• Comparable multiples for enterprise value
  • Revenue multiples for SaaS
  • FUM multiples for investment tech
  • EBITDA/CM multiples for later stage scaleups
	• Comparable multiples for token market capitalisation
	  • Revenue multiple
	  • Total Value Locked multiple for DeFi
	  • Treasury reserve multiple
	  • Community size multiple

• Entry price based on % stake, exit revenue and valuation scenarios. "What you need to believe to return the fund analysis"	• The importance of % ownership of tokens in circulation for fund return outcomes is TBD but scenarios around future token supply increases and expected token market cap can help determine required % stake upon investment

Appendix: Glossary & Resources

AirTree

Crypto Jargon & Resources

Key resources for full in depth glossary:

- Decryptionary.com
- Coinmarketcap.com

Learning resources:

- Decrypt
- A16z Crypto Canon
- Coinbase Learn

- **Smart Contracts:** Smart contract is defined as an programmatic agreement to exchange goods, services, or money that will automatically execute, without third party oversight, so long as established criteria are met.
- **Mining:** Mining is defined as the process of using computer power to solve a complex math problem, review and verify information, and create a new record of transactions to be added to the blockchain.
- **Stable Coin:** A cryptocurrency with extremely low volatility, sometimes used as a means of portfolio diversification. Examples include gold-backed crypto – or fiat USD pegged crypto
- **Tokens:** A digital unit design with utility in mind, providing access, governance and use of a larger crypto economic system
- **Staking:** Participating in a proof-of-stake (PoS) system to put your tokens in to serve as a validator to the blockchain and receive rewards
- **Zero Knowledge Proof:** In cryptography, a ZKP enables one party to provide evidence that a transaction or event happened without revealing private details of that transaction or event
- **Scaling problem:** the limitations of a blockchain's transaction throughput and ability to have fast and low cost transactions. I.e. Bitcoin processes 1 transaction per 15mins. Solana can do 50k per second.
- **Gas:** A term used on the Ethereum platform that refers to a unit of measuring the computational effort of conducting transactions or smart contracts, or launch Dapps in the Ethereum network. It is the "fuel" of the Ethereum network.

End.

@airtreevc

medium.com/airtree-venture

www.airtree.vc