Crypto Applications: 2020–2025

SPEAKER
Balaji S. Srinivasan, Nakamoto.com
Important Disclosures

The views expressed here are those of the individual AH Capital Management, L.L.C. ("a16z") personnel quoted and are not the views of a16z or its affiliates. Certain information contained in here has been obtained from third-party sources, including from portfolio companies of funds managed by a16z. While taken from sources believed to be reliable, a16z has not independently verified such information and makes no representations about the enduring accuracy of the information or its appropriateness for a given situation.

This content is provided for informational purposes only, and should not be relied upon as legal, business, investment, or tax advice. You should consult your own advisers as to those matters. References to any securities, digital assets, tokens, and/or cryptocurrencies are for illustrative purposes only and do not constitute a recommendation to invest in any such instrument nor do such references constitute an offer to provide investment advisory services. Furthermore, this content is not directed at nor intended for use by any investors or prospective investors, and may not under any circumstances be relied upon when making a decision to invest in any fund managed by a16z. (An offering to invest in an a16z fund will be made only by the private placement memorandum, subscription agreement, and other relevant documentation of any such fund and should be read in their entirety.) Any investments or portfolio companies mentioned, referred to, or described are not representative of all investments in vehicles managed by a16z, and there can be no assurance that the investments will be profitable or that other investments made in the future will have similar characteristics or results. A list of investments made by funds managed by Andreessen Horowitz (excluding investments for which the issuer has not provided permission for a16z to disclose publicly as well as unannounced investments in publicly traded digital assets) is available at https://a16z.com/investments/.

Charts and graphs provided within are for informational purposes solely and should not be relied upon when making any investment decision. Past performance is not indicative of future results. The content speaks only as of the date indicated. Any projections, estimates, forecasts, targets, prospects, and/or opinions expressed in these materials are subject to change without notice and may differ or be contrary to opinions expressed by others. Please see https://a16z.com/disclosures for additional important information.
About

Balaji S. Srinivasan (@balajis)

CTO, Coinbase

ANDREessen HORowitz

General Partner, a16z

Counsyl

CTO & cofounder, Counsyl
Sold to Myriad for $375M

BS/MS/PhD EE, MS ChemE
Taught Stanford MOOC to 250k+
History
Concepts
Applications: 2020
Applications: 2025
What is Bitcoin and why was it invented? We can get there in four steps.

1. PHYSICAL CASH
   A hands B cash. B knows A no longer has it.

2. NAIVE DIGITAL CASH
   A sends B serial numbers. A still has a copy!

3. CENTRALIZED DIGITAL CASH
   C is a bank. It is trusted to debit A & credit B.

4. DECENTRALIZED DIGITAL CASH
   C is replaced by miners updating blockchain.
Then, Blockchain

The fundamental innovation behind Bitcoin. A blockchain is a tamper-resistant database for storing things of value.

Individual ‘transaction’ events

NEW BLOCK of transactions includes a security ‘hash’ of the previous block.

BLOCKCHAIN

new blocks are added approximately every 10 minutes.

Multiple computer ‘mining’ servers check the validity of the blocks in the chain. The quickest to check the latest block, gets payment.

Successful transactions

BLOCK Validated as ‘honest’ part of the chain

REJECTED
Next, Ethereum


Here’s an example of a script in Bitcoin:

```
OP_DUP OP_HASH160 62e907b15cbf27d5425399ebf6f0fb50ebb88f18
OP_EQUALVERIFY OP_CHECKSIG
```

And one in Ethereum’s Solidity:

```
contract Simple {
    function() {
        var two = 1 + 1;
    }
}
```
From 2017-2018, the ICO Boom and Bust.

Like dotcom boom, many won't work but some will.
Simultaneous disruption of VC, SWIFT, crowdfunding, cap tables.

2017–2018
From $XB to $YB to $ZB

2019–2020
Winter for price, summer for innovation?
History

Concepts: Technology

Applications: 2020

Applications: 2025
A blockchain is a database for storing things of value. Slower and less performant than centralized databases, their special property is tamper-resistant shared state in an adversarial environment. In other words: can't write to the DB and award yourself a million dollars. Or a million potions, or a million acres.

**CRYPTOCURRENCY**
Digital gold and cash.

**TOKENS**
Digital alternative to equity. Makes network effects tradeable.

**DIGITAL ASSETS**
Nonfungible scarce assets, from in-game items to real estate.

**IDENTITY**
Present proof of cryptoidentity to demonstrate that you possess an asset.
Bitcoin is a protocol. Payments are now packets.

Bitcoin and Ethereum are literally protocols in that one can open up Wireshark and see the raw packets that update the underlying blockchains.

It's fully packet-driven transmission of value without reference to a bank.
This means machines can now hold & send money.

A program can now have custody of funds so long as it has possession of private keys.

The internet allowed programs to autonomously communicate. Blockchain allows them to autonomously transact. A fundamental prerequisite for intelligent agents.
Blockchains have already 10X'd gold, SWIFT, crowdfunding

Is the blockchain creating real economic value? As shown, Bitcoin and Ethereum have already created quantifiable 10X improvements in multiple multibillion dollar sectors.

Deployment still ongoing, but innovation is real and quantifiable.

10X BETTER THAN GOLD
Bitcoin is infinitely lighter than gold. Faster to transport internationally, cheaper to custody.

10X FASTER THAN SWIFT
Ethereum clears in minutes in any country pair. SWIFT takes days.

10X LARGER THAN KICKSTARTER
Ethereum has shattered records, enabling 10X larger and faster internet crowdfunding.

10X FASTER THAN DELAWARE
Solidity means fractions of a second vs days to "incorporate". Smart contracts transform shareholder rights and governance.
Blockchains have already created many billion dollar entities

Are there any large businesses or organizations based on the blockchain?

Yes. Infrastructural entities in three major areas are in the billions: creators of new coins & tokens, miners, and exchanges.

**COIN FOUNDERS**
The engineers who create new coins and tokens have captured billions.

**MINERS**
The large miners who run server farms have captured billions.

**EXCHANGES**
The exchanges collectively have done many billions in revenue.
Blockchain means you have a choice of who to trust

It's not about "trusting no one", it's about having a greater choice of who to trust with custody of valuable assets.

Blockchains enable choice via fast, programmatic transfer of assets across international boundaries.

BEFORE: BANK
You had to store money at one of a few banks.

AFTER: BANK, EXCHANGE, OR YOUR COMPUTER
Now you can store it at the bank, at an exchange, or indeed on any computer.
Blockchains enable internet-scale cap tables

With tokens, organizations can now give users a piece of their "cap tables" in a programmatic way.

This is a completely new dynamic and will be widely adopted over the next ten years.

BEFORE: EXCEL
A few shareholders, managed centrally. No custody, poor visibility, limited liquidity till IPO.

AFTER: ETHERSCAN
Unlimited token holders for even a small startup. Internationally tradeable, transparent, and liquid around the clock from day 0.
Blockchain-first is the new mobile-first
Blockchain competitors are arising for many legacy businesses, and in some cases already taking significant share.

<table>
<thead>
<tr>
<th>Incumbent</th>
<th>Sample Blockchain Disruptor</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn</td>
<td>Earn.com</td>
<td>Social</td>
</tr>
<tr>
<td>Chase</td>
<td>Compound</td>
<td>Finance</td>
</tr>
<tr>
<td>PayPal</td>
<td>Bitcoin</td>
<td>Precious metals</td>
</tr>
<tr>
<td>AngelList</td>
<td>MobileCoin</td>
<td>P2P Payments</td>
</tr>
<tr>
<td></td>
<td>Coinlist</td>
<td>Messaging</td>
</tr>
<tr>
<td></td>
<td>Republic</td>
<td>Equity Crowdfunding</td>
</tr>
</tbody>
</table>

©2020 Andreessen Horowitz. All rights reserved worldwide.

Any Andreessen Horowitz investments and portfolio companies described or referred to above are not representative of all investments in vehicles managed by the firm and there can be no assurance that the investments described are or will be profitable or that other investments made in the future will have similar character or results. See Important Disclosures at the outset for more information.
And more is coming soon

Next: collectibles, identity, distributed databases, marketplaces, DNS/protocols, browsers, and decentralized cloud.

<table>
<thead>
<tr>
<th>Incumbent</th>
<th>Sample Blockchain Disruptor</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAGIC: The Gathering</td>
<td>CryptoKitties</td>
<td>Collectibles</td>
</tr>
<tr>
<td>Facebook Login</td>
<td>BOX</td>
<td>Identity</td>
</tr>
<tr>
<td>WIKIPEDIA: The Free Encyclopedia</td>
<td>0</td>
<td>Distributed databases</td>
</tr>
<tr>
<td>airbnb</td>
<td>OpenBazaar</td>
<td>Marketplaces</td>
</tr>
<tr>
<td>DNS Domain Name System</td>
<td>ens</td>
<td>DNS</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>MetaMask</td>
<td>Browsers</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>Filecoin</td>
<td>Decentralized file storage</td>
</tr>
</tbody>
</table>

©2020 Andreessen Horowitz. All rights reserved worldwide.

Any Andreessen Horowitz investments and portfolio companies described or referred to above are not representative of all investments in vehicles managed by the firm and there can be no assurance that the investments described are or will be profitable or that other investments made in the future will have similar character or results. See Important Disclosures at the outset for more information.
Blockchains break network effects

Why? Because token upside is inversely proportional to network effect.

You can now give early adopters an equity-like stake in the network to reward them for inviting others.
Blockchains transform social networks

From liking and poking to buying and earning. The next 10 years of social networks will involve real value being sent over the edges.

BEFORE: LIKE, POKE, MESSAGE
Have fun online, or waste time. The last 10 years of social networks.

AFTER: PAID DMS, SURVEYS, TASKS
Reply to messages and complete tasks for digital currency. The next 10 years of social networks.
Blockchain is a partial move away from cloud towards privacy

Users are learning to keep their private keys local and private.

Private keys are an anchor that will lead to other data also being encrypted and moved locally, out of the cloud and onto devices.
History
Concepts: Community
Applications: 2020
Applications: 2025
A blockchain's value derives from its community

Recall our point about how "blockchains scale cap tables". The holders, devs, miners and other community members agree between themselves on mechanisms of value transfer.

The price is how they interface with the outside world.
As context, three random people are *not* economically aligned

Each of them can lose or win on their own, independently, without any impact on the others.
A blockchain community is *economically* aligned

If the price goes up, they all benefit together and can become millionaires. If the price goes down, or the blockchain is attacked in some way, they also all lose.

If they are holders, none of them can win unless they all win.
In the slippery slope, one person's rights can be eroded without others facing immediate consequences.

In the crypto cliff, to abrogate one person's rights means you are economically damaging many others at the same time.

Blockchains thus take us from slippery slope to crypto cliff

**BEFORE: DNS SEIZURE**
Someone loses a lol.cat domain, but you keep your .com domain.

**AFTER: ENS SEIZURE**
To seize someone's .ens domain in the same way means interfering with the Ethereum blockchain.
Thus, a *monetary* incentive to defend another's rights

Because of the crypto cliff, everyone speaks out at once if there is the attempt to attack the blockchain that binds the community together.

BEFORE: SLIPPERY SLOPE
Someone loses a lol.cat domain, but you keep your .com domain.

AFTER: CRYPTO CLIFF
To seize someone's .ens domain in the same way means interfering with the Ethereum blockchain.

©2020 Andreessen Horowitz. All rights reserved worldwide.
As such, blockchains allow for experiments in self-governance

With blockchains, any sufficiently large group of people can choose a mechanism to wholly or partially govern their economic life in the cloud.

This has been a fascination from people of all political stripes, from the Paris Commune to Galt's Gulch.
Blockchains make macroeconomics an experimental science

Before, people studied virtual economies in the context of video games.

Crypto takes that to the next level. Whatever your thesis on economic governance - inflationary, deflationary, demurrage - if you can get enough people to try it, you can run the experiment.
Now that blockchain has turned macroeconomics into an experimental science, you can try out every philosophy under the sun - simultaneously, with part of your net worth.

Hayek vs Keynes vs heretofore-unseen hybrids. It’s all happening in realtime.

Tens of millions of people (and billions of dollars) are now invested in these experiments.

©2020 Andreessen Horowitz. All rights reserved worldwide.
Thus, the new laboratory of the states is a laboratory of networks.

If federalism meant the laboratory of the states, decentralization is creating the laboratory of the networks.
History
Concepts
Applications: 2020
Applications: 2025
Three apps at $1B revenue: exchanges, mining, issuance

These are the infrastructure parts of crypto.
One app at $100M revenue: hardware wallets

This is growing but is not yet as large as the other three sectors.
Mainly Tether, but USDC and DAI also worthy of note.

Stablecoins at $5B+ in stored value

<table>
<thead>
<tr>
<th>Name</th>
<th>Circulation</th>
<th>Change (24h)</th>
<th>Price</th>
<th>Tracked Volume (24h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tether USD (USDT)</td>
<td>4,491,590,765.41</td>
<td>24,500,000.00</td>
<td>$0.99991 (-0.05%)</td>
<td>2,248,922,149.09 (21.83%)</td>
</tr>
<tr>
<td>USD Coin (USDC)</td>
<td>425,911,624.60</td>
<td>-627,897.23 (-0.15%)</td>
<td>$1.0003 (0.05%)</td>
<td>60,073,283.05 (6.33%)</td>
</tr>
<tr>
<td>Paxos Standard (PAX)</td>
<td>226,048,198.19</td>
<td>6,818,059.22 (3.11%)</td>
<td>$1.0001 (0.03%)</td>
<td>19,138,640.77 (0.89%)</td>
</tr>
<tr>
<td>TrueUSD (TUSD)</td>
<td>138,867,102.96</td>
<td>2,519.28 (0.00%)</td>
<td>$1.0003 (0.04%)</td>
<td>27,293,205.00 (-22.81%)</td>
</tr>
<tr>
<td>Binance USD (BUSD)</td>
<td>30,278,034.13</td>
<td>-5,270,073.28 (-14.83%)</td>
<td>$1.0006 (0.16%)</td>
<td>33,102,373.23 (-2.47%)</td>
</tr>
<tr>
<td>Dai (DAI)</td>
<td>23,182,265.20</td>
<td>-286,645.18 (-1.22%)</td>
<td>$0.99999 (0.11%)</td>
<td>4,242,453.98 (63.98%)</td>
</tr>
<tr>
<td>Gemini Dollar (GUSD)</td>
<td>5,138,109.94</td>
<td>385,156.88 (8.10%)</td>
<td>$0.9966 (0.22%)</td>
<td>1,496.76 (-84.81%)</td>
</tr>
<tr>
<td>StableUSD (USDS)</td>
<td>664,923.59</td>
<td>-1,500.00 (-0.23%)</td>
<td>$0.9968 (-0.21%)</td>
<td>98,013.06 (10.59%)</td>
</tr>
</tbody>
</table>
DeFi now at almost $1B in stored assets

Maker, Synthetix, and Compound are leaders, but many more apps.
Decentralized Cold Storage (Casa)

Casa is gaining traction here. Paradoxical but similar to Coinbase: a centralized service facilitates custody of a decentralized asset.
Privacy Coins and Privacy Features

Also becoming more standard in more chains over time. Others also (Dash, Enigma, Beanstalk).
SaaS-for-gas (Starkware and others)

Smart contracts that are on-chain and charge for each API call. Defensibility through trust of author, network effects/switching costs, and backlinks.
Many different business models here for decentralized lending (has API, works across borders, works 24/7, no limits, etc).
Insurance (Opyn, Nexus Mutual)

Allows parties to (in theory) insure against defi contract and default risk. Though the insurer themselves has risk.
Scaling (Starkware, many others)

A number of these technologies are coming online and will likely be deployed by 2025. Many stack on top of each other.
Multiwallets with many verbs (MyCrypto)

Beyond just send/receive, we will see all the common verbs come to wallets
Security innovation (ZenGo)

Highly innovative wallet that uses FaceID and similar techniques for convenient save/restore
Novel financial instruments (Fomo3D, PoolTogether)

In the spirit of crypto: incentivize good behavior with the spirit of a lottery.
Blockchain games (egamers, Forte, EOS)

Video games with micropayments built-in. Merges esports and crypto. Josh of Forte will talk more about this.
Crypto social networks (Voice, Twetch)

Could list many more. These are still in their infancy. Many levels of decentralization. Some just use a decentralized currency and centralize everything else.
Decentralized DNS (ENS, Unstoppable, Blockstack, Handshake)

Fully programmable and liquid DNS without the central registry. Get a domain like setting up a virtual machine.
Automated Market Making (Uniswap, Kyber Bonding Curves)

Liquidity for the long tail. This is questionable as to whether it will work given presence of other markets, but people are trying.
Decentralized Identity (3Box)

Many efforts here too. May require bootstrapping by a centralized agency.
Personal Tokenization (CNSL, Dinwiddie)

Issue an equity-like token for your time or some function of your time (like a consult).
Mutuals and Guilds (Moloch, Gitcoin)

Attempts to incentivize collective action. Gitcoin allows people to vote with their funds for the direction of protocol development.

Moloch DAO explained: Using self-interest to Ethereum’s advantage

May 30, 2019

What is Moloch DAO?

What the heck is all this talk is about Moloch DAO? Well for starters, this is a moloch:

Okay, that’s not the Moloch you seek. Jokes aside, Moloch DAO (DAO stands for “decentralized autonomous organization”) is a new Ethereum community funding initiative. It’s part charity and part playfully terrifying meme (Moloch is an ancient god of child sacrifice).

A contribution to Moloch DAO isn’t an investment in the traditional sense. Instead of seeking a direct financial benefit, members share in the collective benefit from improvements to public goods funded by the DAO. Moloch will initially focus on funding Ethereum 2.0 development.
Mutuals and Guilds (Moloch, Gitcoin)

Attempts to incentivize collective action. Gitcoin allows people to vote with their funds for the direction of protocol development.

Moloch DAO explained: Using self-interest to Ethereum’s advantage
May 30, 2019

What is Moloch DAO?
What the heck is all this talk is about Moloch DAO? Well for starters, this is a moloch:

Okay, that’s not the Moloch you seek. Jokes aside, Moloch DAO (DAO stands for “decentralized autonomous organization”) is a new Ethereum community funding initiative. It’s part charity and part playfully terrifying meme (Moloch is an ancient god of child sacrifice).

A contribution to Moloch DAO isn’t an investment in the traditional sense. Instead of seeking a direct financial benefit, members share in the collective benefit from improvements to public goods funded by the DAO. Moloch will initially focus on funding Ethereum 2.0 development.
Founder’s Rewards (Zcash, BCH)

New business model for funding developers from rewards.
On-Chain Developer Bounties (Tezos)

On-chain governance for funding developers via bounties.

Tezos Is About to Enact Its First-Ever On-Chain Blockchain Update

May 28, 2019 at 11:44 UTC • Updated May 28, 2019 at 15:10 UTC

After nearly three months of voting by token holders, the Tezos blockchain will undertake a series of backwards-incompatible changes to the network on Wednesday.

Called Athens A, the upgrade proposal was the first to undergo the network’s “self-amendment” process in which bakers on Tezos - equivalent to miners on bitcoin or ethereum - stake tokens bound into “tails” to show their support for or against competing upgrade proposals. Tezos is a proof-of-stake (PoS) blockchain with an estimated valuation of over $1 billion.

Tying up this week’s event, a developer group known as Nomadic Labs kick-started Tezos’ first on-chain governance process back in February. At the time, the news was a notable given the turbulence that took place during the project’s early days.

In March, Nomadic Labs put forward two proposals, Athens A and Athens B. Athens A and Athens B both suggested an increase to the computation or gas limit of Tezos blocks. This would effectively make smart contract deployment easier for application developers building atop the platform.

Athens A, on the other hand, also suggested a reduction to the minimum amount of tokens - called a roll size - that’s required for a user to become a baker. This would reduce the barrier to entry for baking and encourages a higher number of bakers on the Tezos blockchain.

After three months of voting and testing, bakers have now officially passed the final voting threshold to activate Athens A on Tezos’ main network.
Clients for dApps

A Coinbase-like UX whose backend is a blockchain or smart contracts.
Developer Tools (Alchemy, Bison Trails)

Improved APIs for geth and general performance improvements.
Oracles and Prediction Markets
Put data on-chain and make bets on it.
DAOs—Decentralized Autonomous Organizations

Semi-autonomous programs—many of which make you money. Trading on dexes is pure internet arbitrage.
Community-Owned Organizations

Collectives, akin to cooperatives, owned and operated by their users.
a16z
[CRYPTO STARTUP SCHOOL]