a16zcrypto

Crypto & Blockchains Overview

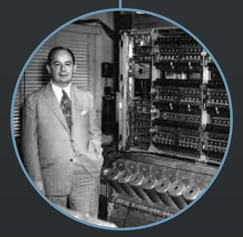
Chris Dixon, a16z crypto

The best way to think of blockchains
is as a new type of computer

History of Computing Platforms

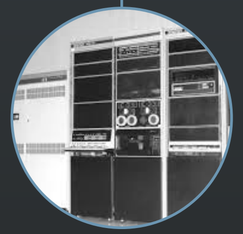
Past

1930–1940s



1950–1960s

1970–1980s

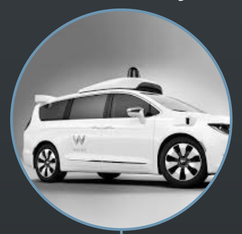


1980–1990s

1990–2000s

2000–2010s

2020s & Beyond



2020s & Beyond

2020s & Beyond

2020s & Beyond

Blockchains

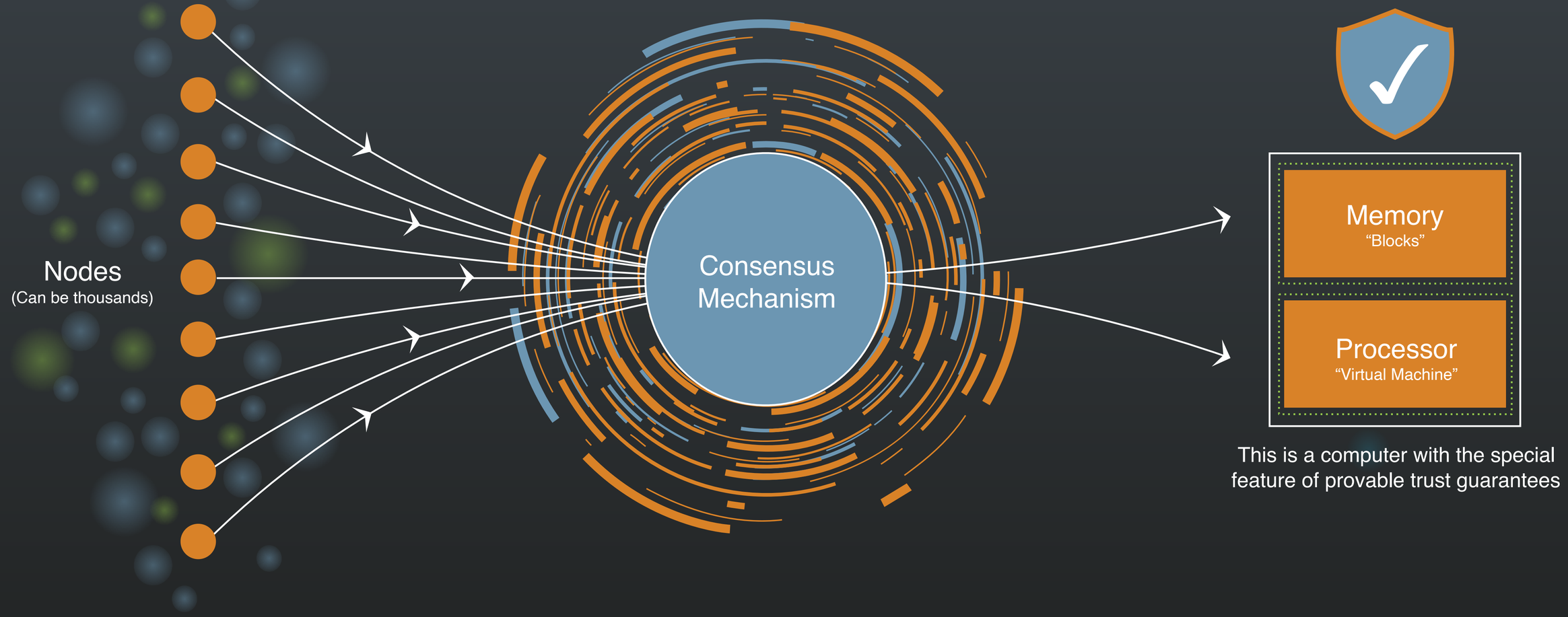
Future

a16zcrypto

Blockchain = 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.

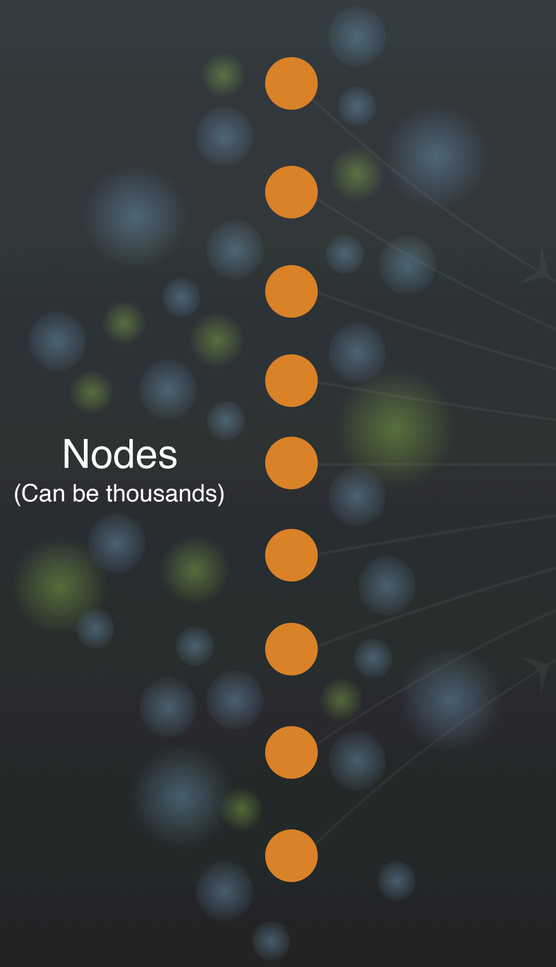
Architecture of Blockchain Computers

Computer composed of nodes which are physical computers (e.g. PCs), joined together via a consensus mechanism.



Nodes

Nodes are the method by which anyone—without needing permission—can join the network and become part of the blockchain computer.



Each node runs all or part of the code required to make the system function.

Nodes are incentivized to behave honestly, but a well-designed consensus mechanism enforces the correct operation of the blockchain computer even if a significant number of nodes misbehave.

Consensus Mechanism

Consensus mechanism aggregates the “votes” from the nodes to determine the correct operation of the blockchain computer.

The rounds of voting are broken into “blocks” which are then chained together, hence the term “blockchain.”

A well-designed consensus mechanism gives mathematically provable guarantees about trustworthiness of the computer as a whole.

The Result: Trust Guarantees

The game theory of nodes + consensus mechanism provides trust guarantees to anyone using it—users, developers, creators, businesses, other computers or services—that no previous computer architecture could provide.

These trust guarantees mean that the rules of the system can't change without due process as defined by the system's governance protocols. "Don't be evil" becomes "Can't be evil."

These trust guarantees also enable the credible creation of new computing primitives such as digital money, digital goods, smart contracts, decentralized organizations, etc.

Like All Early Computers, Blockchain Computers Have Strengths and Weaknesses

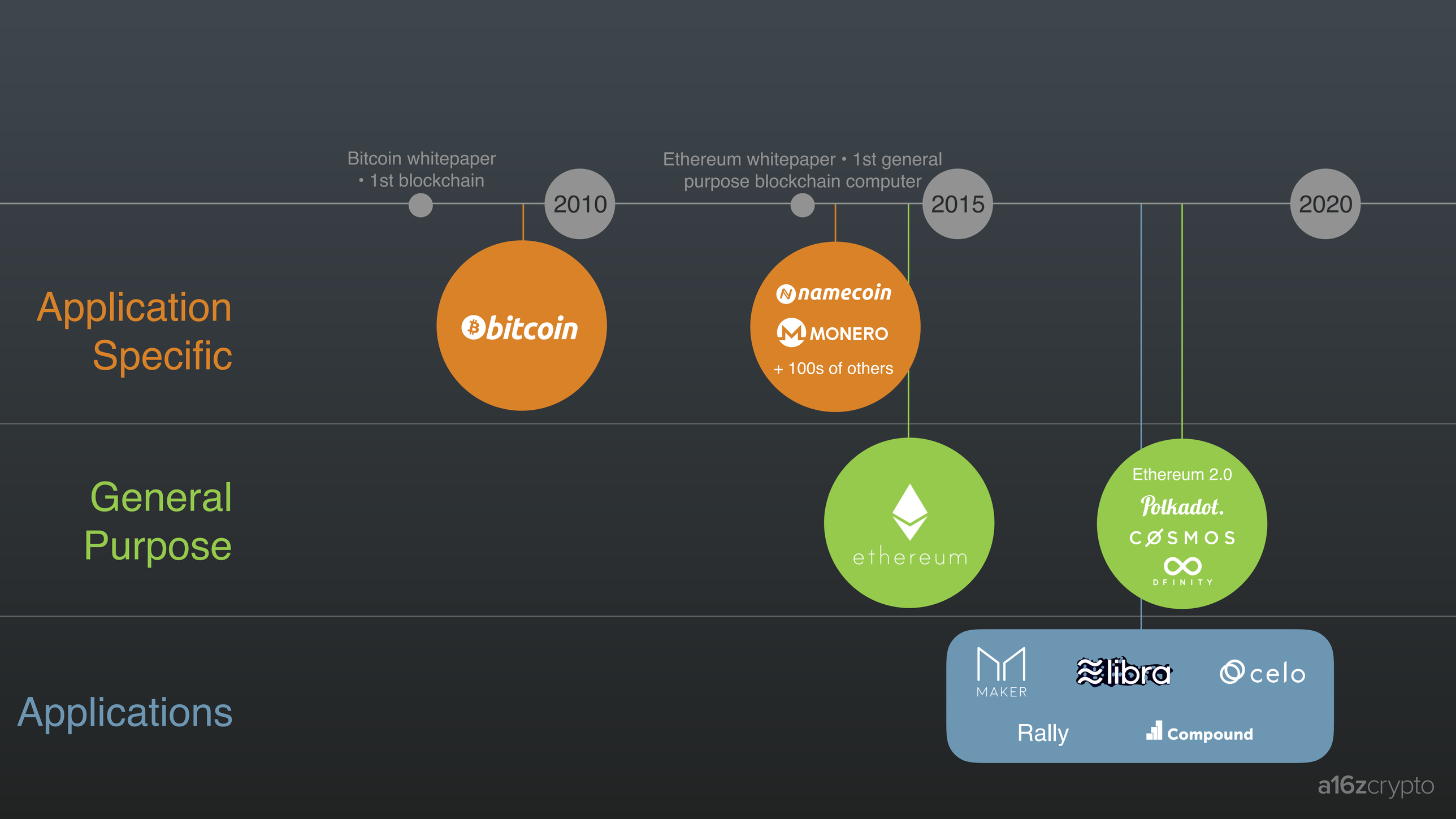
	Strengths	Weaknesses
Early PCs	Smaller, cheaper	Slow, expensive, user experience
Early Smartphones	Portable, GPS, camera, cellular connectivity	Performance, price, inputs (keyboard)
Early Blockchains	Provable trust guarantees	Scalability, user experience

Killer Apps Took Advantage of Strengths: Weaknesses Diminished Over Time

	Killer Apps
PCs	Word processing, spreadsheet, desktop publishing Took advantage of price/size to become ubiquitous
Smartphones	Ride hailing, photo sharing Took advantage of GPS, camera, connectivity, portability
Blockchains	Trust enables new digital primitives: Digital money, digital goods, smart contracts, DAOs, trusted software platforms, community owned and operated digital services, + much more as-yet-invented?

Computers Can Be General Purpose or Application Specific

General Purpose	Application Specific
DEC minicomputer	Wang word processor
WWW	AOL
iPhone	Blackberry
Apple Watch	Fitbit
Ethereum	Bitcoin
Benefit: Unlocks third-party developer creativity	Benefit: Optimize full-stack for specific application

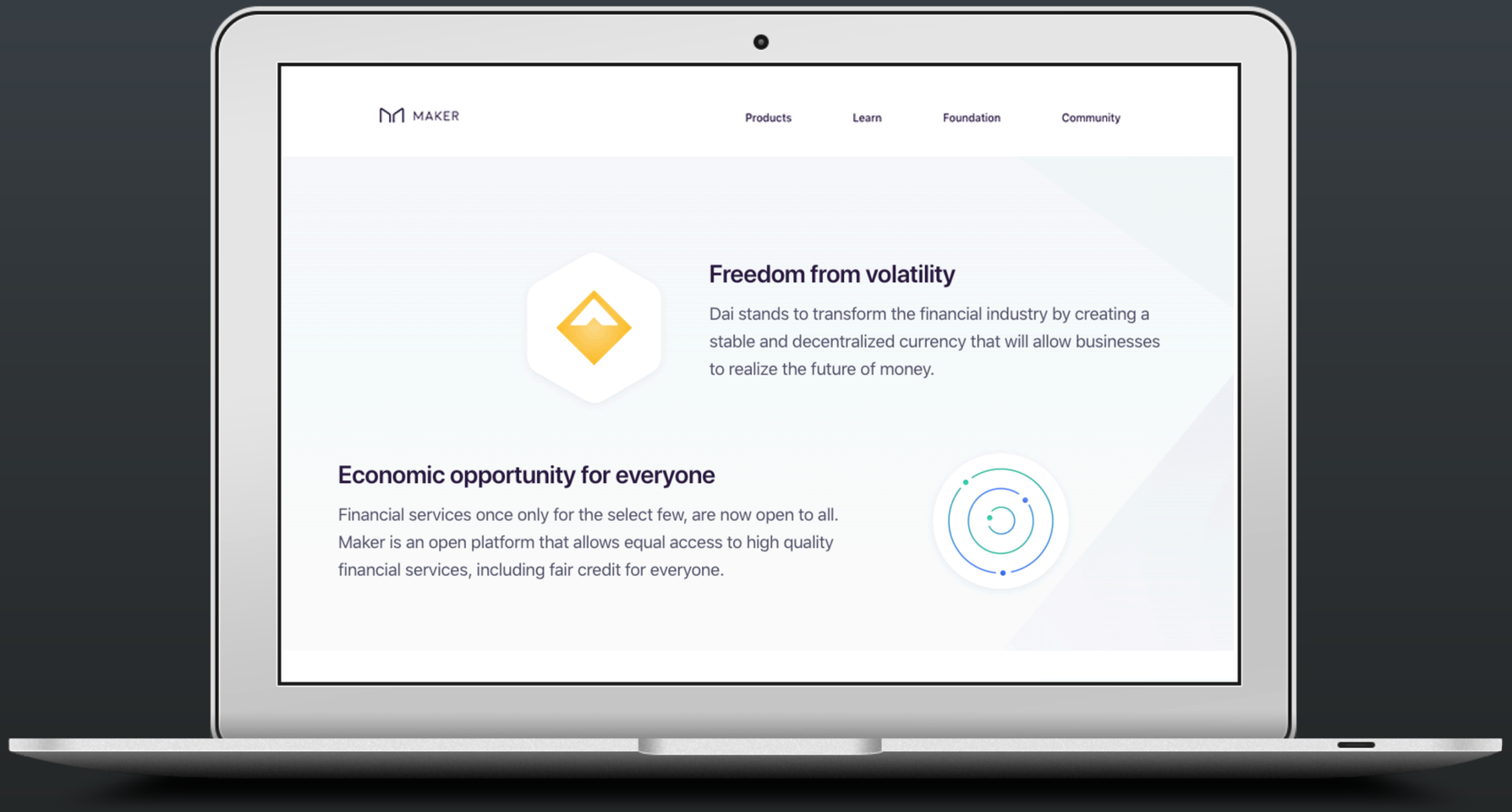

Bitcoin whitepaper
• 1st blockchain
2010
Ethereum whitepaper • 1st general purpose blockchain computer
2015
2020
Application Specific
bitcoin
namecoin
MONERO
+ 100s of others
General Purpose
ethereum
Ethereum 2.0
Polkadot.
COSMOS
DFINITY
Applications
MAKER
libra
celo
Rally
Compound
a16zcrypto

Decentralized finance

MAKER

Compound

δY/δX



celo

Mobile Peer-to-peer Payments

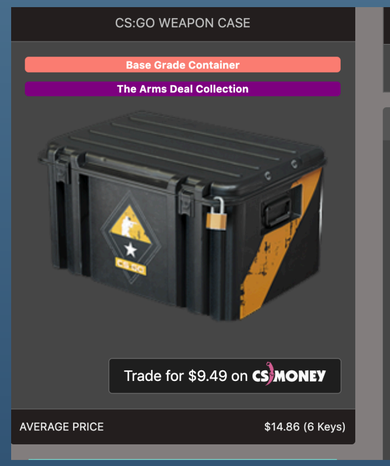
DESCRIPTION

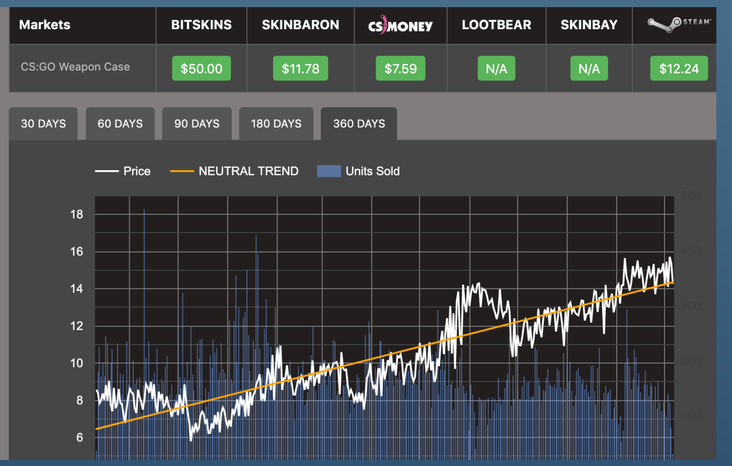
An open platform for fast, secure, stable digital payments to any mobile number at a fraction of today's cost. Helps include the roughly 1.5B people with smartphones but no bank accounts in the digital economy.

Rally, Forte, Flow: Crypto Goods

DESCRIPTION

True digital ownership of digital collectibles, gaming assets, art and more.





a16zcrypto