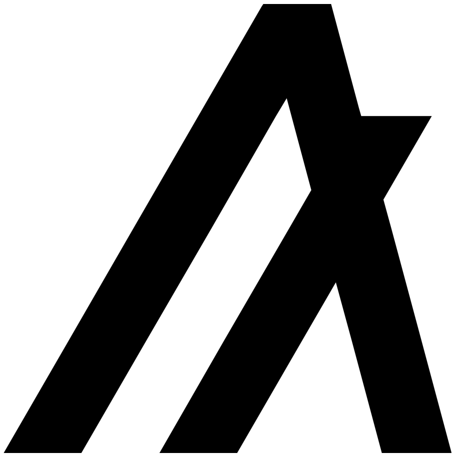
arrington
CAPITAL

Illuminating The Dark Age Of Blockchain: Algorand



July 19, 2021

John Trumbull's Declaration of Independence (1819). The Birth of the Republic of the United States.

The Enlightenment culminated in the birth of the American Republic, a revolutionary system for coordinating society – for reaching consensus.

It redefined the relationship between rules and rulers, introducing the novel idea of self-government – where the users and securers of the network are the same.

Disclosure

Arrington Capital and/or its affiliates (collectively "Arrington Capital") has a financial interest in the success of the Algorand Ecosystem, including affiliated ecosystems, initiatives and projects (collectively "Algorand Ecosystem"). Arrington Capital currently owns ALGO tokens.

As of the publication date of this report, Arrington Capital, others that contributed to this report, and those that we have directly shared our research with, are supporters of the Algorand Ecosystem and stand to realize the gains through various manners of participation. All content in this report represent the opinions of Arrington Capital. Arrington Capital has obtained all information herein from third-party sources they believe to be accurate and reliable, including Algorand Ecosystem. Third-party sources may not have been independently verified and its accuracy or completeness cannot be guaranteed and not be relied upon as such. Information is presented "as is", without warranty of any kind – whether express or implied.

This document is for informational purposes only and is not intended as an official recommendation or confirmation of any transaction. The information contained herein does not take into account the particular investment objectives, regulatory status or financial circumstances of any specific person who may receive it. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, and reflect prevailing conditions and Arrington Capital's views as of this date, all of which are accordingly subject to change without notice. Arrington Capital has no obligation to continue offering reports regarding the project. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances.

Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. This report's estimated fundamental value only represents a best efforts estimate of the potential fundamental valuation of a specific token, and is not expressed as, or implied as, assessments of the quality of a token, a summary of past performance, or an actionable investment strategy for an investor.

This document does not in any way constitute an offer or solicitation of an offer to buy or sell any investment or token discussed herein.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond Arrington Capital's control. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on all tokens discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

By accepting this information the recipient agrees and acknowledges that no duty is owed to the recipient by Arrington Capital. The recipient expressly waives any claims arising out of the delivery of the information or the recipients use thereof or reliance thereon.

Executive Summary

In this paper, we argue that blockchains are trapped in a dark age of technology centralization. The wars of multi-chain DeFi push the market to abandon decentralization, its oldest and most foundational principle. Crypto's citizens search for "fast" technologies that optimize for DeFi yield generation, even if this hands power to a new class of kingmakers – from centralized exchange operators to political figureheads who guide the destiny of these networks.

This dark age presents users with a choice: performance or decentralization, but not both. Following on from our 2019 report[1] at the launch of MainNet, we argue that Algorand represents an opportunity to transcend this paradigm. It is the first "fast L1" which can coordinate between billions of people without trending toward plutocracy. Consensus is fast yet open to anyone: Algorand currently performs 1,000 TPS with $<$ 5 second finality without sacrificing decentralization.

Solving the "blockchain trilemma" compromising other networks, Algorand has been live for two years with no downtime. A series of novel cryptographic and political breakthroughs create a new system of self-government and evolvability unlike any other L1 blockchain. The end result: a way forward for DeFi without forsaking decentralization and a ground-up network for risk-averse TradFi applications like Central Bank Digital Currencies (CBDCs) and asset securitization.

If the Enlightenment – an 18th century intellectual movement focused on the ideals of reason, liberty and constitutional government – was humanity's new base layer protocol, then the scientific method and industrial revolution were simply the apps that followed.

What apps could emerge in an Algorand age of reason? One simple application is "fast DeFi" without centralization and inefficiencies like miner extractable value (MEV). Another application – arguably the ultimate goal – is the eventual merger of DeFi and TradFi. We could see a wave of hybrid experiments where DeFi plugs into TradFi, bridging old and new capital pools.

This, perhaps, is crypto's industrial revolution – a productivity boom that will come long after the end of the DeFi wars. In our view, Algorand could be the immutable home of high-value assets, where hybrid experiments emerge and grow to global scale.

[1] URL: https://arringtonxrpcapital.com/2019/06/17/the-monetary-experiment-algorand/.

Contents

Introduction

The DeFi wars have forced new values into crypto. In the same way pre-Enlightenment masses blindly accepted the “benevolent monarch”, crypto embraces a new centralized royalty. Citizens choose mysticism over reason, assured not by ground-up constitutions, but by blessings of the elite and their carrots of temporary yield.

One core thesis underlies this report: today’s market is *underweighting decentralization.* The race for Total Value Locked (TVL) is forcing tradeoffs unacceptable just a year ago. Hardline decentralists surrender to a new, highly pragmatic ideology. With this new philosophy, the market quietly abandons L1 scaling ambitions and concedes to two new forces: multi-chain centralization and L2 as the new panacea for DeFi scalability.

Algorand represents an opportunity to transcend this rise of blockchain pragmatism. It is the first L1 to break tradeoffs between performance, decentralization and security, offering a path forward for “fast DeFi” without giving up on crypto’s oldest and most utopian ideal.

This is rooted in several scientific and political breakthroughs. Algorand leverages randomness to solve one of the hardest problems in distributed systems: *how to not only build a fast system, but one that is secured by an open and boundless set of validators.* Algorand consensus is as much a political breakthrough as it is a technical one, transcending contemporary paradigms for Proof-of-Stake (PoS).

We recast the idea of the “blockchain trilemma” as a political trilemma. Blockchains face the same set of tradeoffs as any nation or government. The Algorand network breaks these confines and builds a system of government where our rulers are not the chosen few, but the entire network. *Consensus is for the network, by the network*, akin to the American ideal of self-government. Anyone can become a validator, governed by the same cryptographic lottery.

Resulting from these breakthroughs, we believe Algorand’s positioning is twofold. It will benefit from the increased fragility of centralized blockchains. Every blowup that stems from network centralization – every coup, revolution and invasion – will make Algorand decentralization more attractive. At the same time, the network’s assurances will attract TradFi capital unable to deploy on riskier networks. The end game could be a series of *hybrid experiments* merging these parallel worlds – a new playground for DeFi to incorporate a real-world asset base and TradFi to take advantage of crypto’s global liquidity.

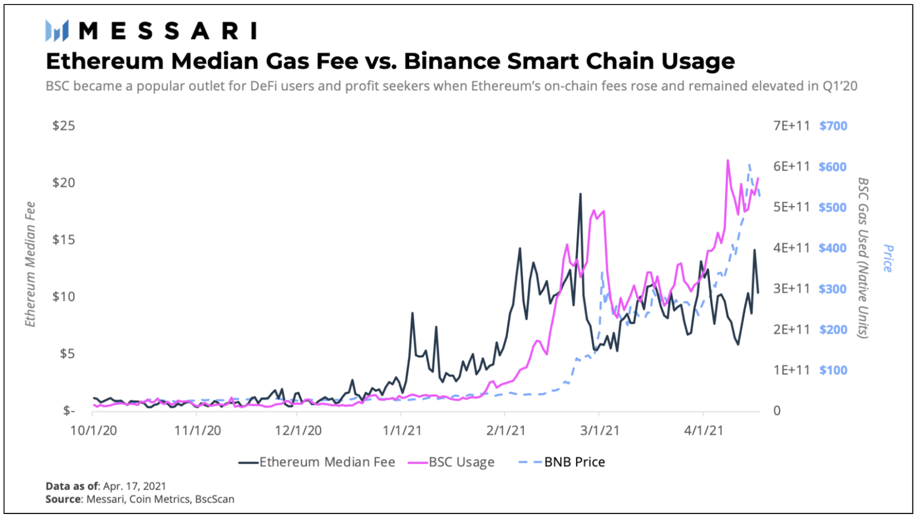
1 The Algorand Thesis

1.1 The Barbarians Of DeFi

The DeFi wars gave birth to a new regime of blockchain pragmatism. Wounded by the eternal promise of L1 scaling[2], the market waved a white flag to new invaders, the multi-chain maximalists. This was a new force that past utopians would decry as barbarian and unprincipled. It is also, we argue, the force that now holds power. The barbarians did not just breach the gates of DeFi yield – they reshaped the philosophical destiny of most blockchains.

With each battle, the nuances of L1 and L2 scaling[3] mattered less, overshadowed by the market's hunt for yield. Capital flocked to "fast L1s" and a cornered Ethereum community mounted its counterattack, L2. The market became increasingly blind to tradeoffs, migrating anywhere so long as it was free from base layer congestion.

How did decentralization lose so much ground? It starts with Binance Smart Chain (BSC). The rise of BSC was 2021's unexpected catalyst, yet it was arguably brewing for years. The failure of L1 scaling efforts which preserved decentralization left the decentralists vulnerable to attack. BSC taught us two things: (1) Most users do not care about utopianism and (2) If under enough pressure, even the old guard – the hardline decentralists – would slowly cave to blockchain pragmatism.



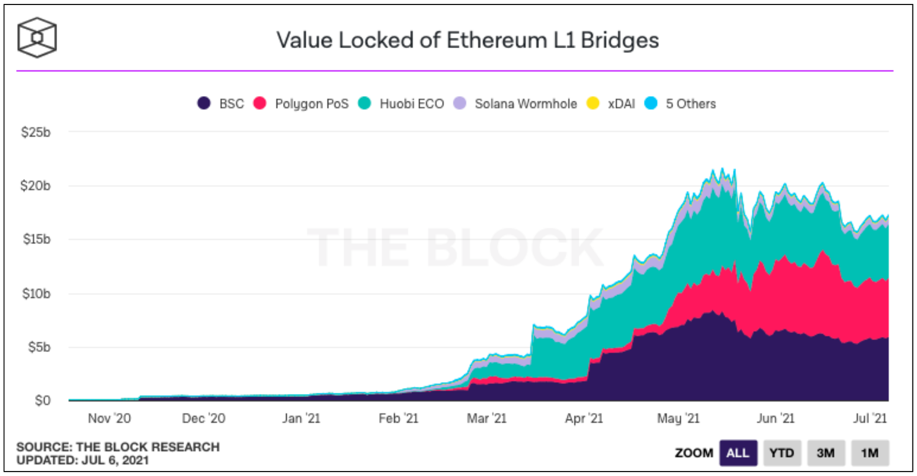
Data as of: Apr. 17, 2021
Source: Messari, Coin Metrics, BscScan

Figure 1: High gas fees on Ethereum and the commensurate growing activity on BSC. Users seeking a similar but cheaper experience were forced to compromise between scalability and decentralization. Data from *Messari*[4].

To gauge the state of blockchains, consider how much L2 debates have morphed over the last year. There was once a time when L2 was a cautious debate centered on decentralization tradeoffs. Today, it is Ethereum DeFi's panacea. A "build now, fix later" mentality supersedes the caution of early communities. ***This shift is logical: absent L1 scaling, how can Ethereum defend its cities from the barbarian takeover?***

[2] We define L1 scaling as attempts to increase throughput on a blockchain's protocol layer.
[3] In L2, transactions happen off-chain, but are usually settled on-chain.
[4] URL: www.messari.com.

Stepping back from the DeFi wars, we pose a different question: is most of the world's capital going to live on technology shaped by 2021's mercenary DeFi? Can these reactionary systems become the rails of global finance beyond the insular needs of 2021 crypto?



SOURCE: THE BLOCK RESEARCH
UPDATED: JUL 6, 2021

Figure 2: The rise of L1 bridges and L2 scaling solutions in response to high gas fees on Ethereum. Data from *The Block*[5].

1.2 Can We Escape The War Of Pragmatism?

Our core thesis is that today's market is overestimating the value of blockchain pragmatism and underpricing the long term necessity of decentralization. Systems forged by multi-chain DeFi accept tradeoffs that eventually limit their growth. Most of finance is not mercenary. Most of the world's capital does not live inside a self-referential fight for yield.

It lives in the land of risk-aversion. The old world will view decentralization like insurance: the market will ignore and underprice insurance until it *really* needs it.

We think the decentralists are correct, but early. It is tempting to be drawn into the initial permutations of a new technology and today's market is no exception. The war of centralized blockchains could be like the early Darwinism of the Internet.

Every blockchain that must choose between decentralization and performance faces a fundamental paradox. Fast but centralized chains support global-scale applications, but their growth becomes a bounty for network attacks, the mother of all rug pulls. ***Can institutions bring capital to a blockchain whose success incentivizes its own demise?*** Conversely, if a system is decentralized but slow, it cannot support scalable applications to begin with.

In the end, we need a system to break free from these limitations. That system, we argue, is Algorand.

1.3 Marrying Old & New Pools Of Capital

What would transcending these tradeoffs make possible? We argue that it dramatically widens the size of crypto's available capital base. Escaping the confines of pragmatism is how we ultimately marry old

[5] URL: https://www.theblockcrypto.com/.

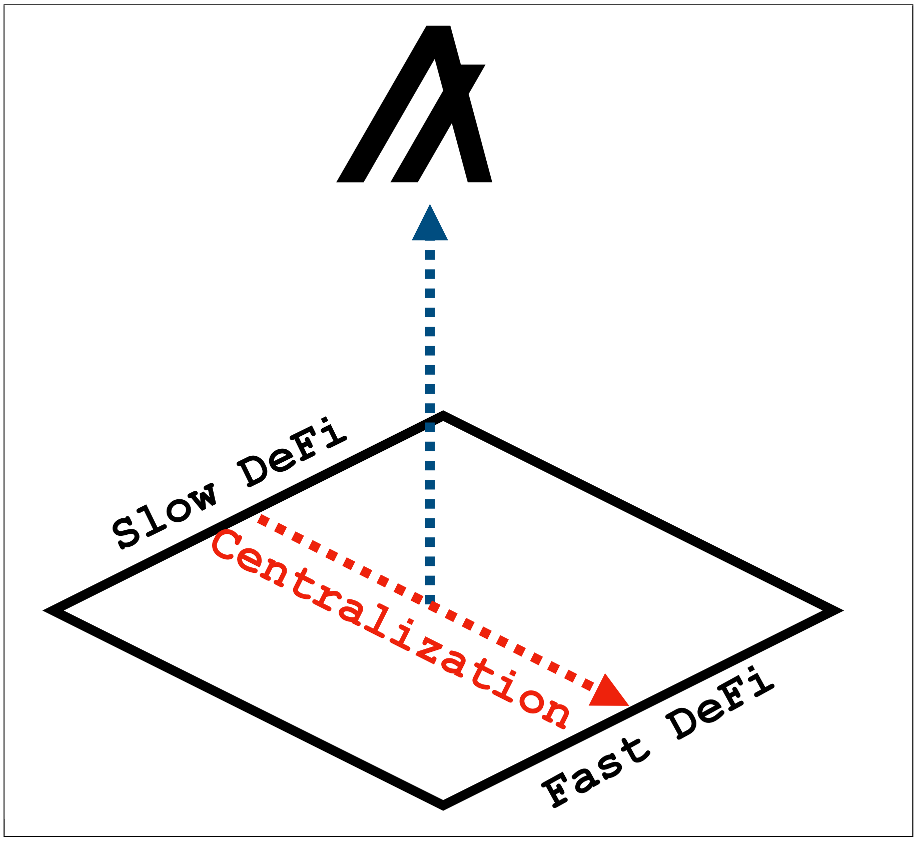


Figure 3: Algorand's design is orthogonal to the design of current blockchains; it enables scalability without sacrificing decentralization.

and new pools of capital and introduce DeFi to TradFi.

This is Algorand. The network is positioned differently to other L1s. It takes a roundabout approach to growing TVL. The Algorand path is multi-stage, focused on growing all of crypto TVL rather than feuding over today's relatively limited and mercenary capital. The first and foundational move is technological: note that not only does Algorand escape tradeoffs, it has demonstrated this capability for two years in the wild with no downtime. ***Can any L1 claim to solve base layer scalability (without collateral damage), let alone prove a solution for two uninterrupted years?***

Quantifying a DeFi protocol's TVL is straightforward. How can we price the value of network-level assurances and their eventual ability to attract and maintain long term capital?

This foundation positions Algorand to marry old and new pools of liquidity. We think of the Algorand network as a call option on three main ideas: (1) Rebuilding DeFi without giving up L1 maximalism, (2) TradFi searching for a ground-up blockchain of assurances and (3) The interaction of legacy capital with crypto-native liquidity.

We sketch out some ideas for these hybrid experiments in the final section. These experiments are akin to the industrial and scientific boom (the apps) that followed the Enlightenment (humanity's new base layer). They move beyond the insular age: *TradFi assets and yield plug into DeFi and become crypto collateral*, giving the old world access to globalized liquidity and the mercenary world an opportunity to diversify its farms into the real economy.

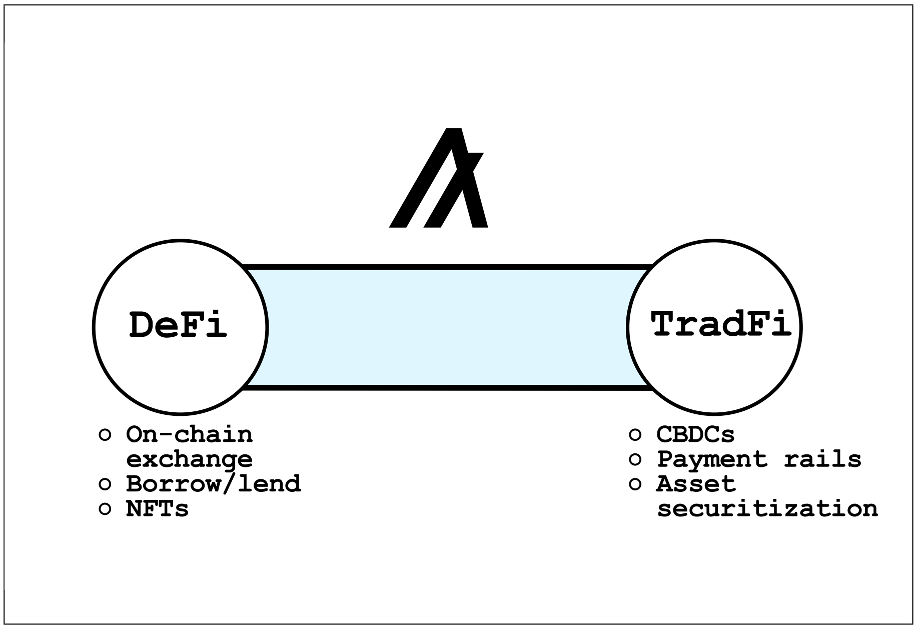


Figure 4: Algorand bridges DeFi and TradFi, spawning new hybrid experiments in capital markets.

1.4 The Promise Of ETH 2.0, Today

Before the DeFi wars, the market focused on ETH 2.0 and the aspirations of L1 scaling[6]. We remain strong believers in the need for a strong L1 and think Algorand breathes fresh life into a forgotten cohort, *the base layer maximalist.*

Stepping back, what was the promise of ETH 2.0? A base layer that is scalable, secure and decentralized. In its purest form, that's Algorand, without ETH 2.0's forward-looking risks. One does not need to wait for ETH 2.0 to realize L1 ambitions – and for reasons we explore in the next section, Algorand's unique approach to PoS could actually be *significantly more decentralized* than ETH 2.0's bonded PoS.

Think of how this first-mover advantage could play out in the next few years. Even if ETH 2.0 goes live by earliest projections, some capital will "wait and see" to assess the new network in the wild. ***The clock restarts***. Being the first to escape tradeoffs before ETH 2.0 carries significant advantages that can grow *even after ETH 2.0.*

The credibility of public networks will scale like a nation's rule of law. Capital will migrate to chains that demonstrate the longevity of their political system. ***Immigrants do not just want the promise of the rule of law, they want a history to prove it.***

Let's assume that institutions deploy structured products or that nations deploy CBDCs within the next five years. *Realistically, where can they do it outside of Algorand?* If we've established that they *cannot* do it on systems constrained by blockchain pragmatism – and that they need systems with some degree of Lindy – *what are their options*?

It is hard to find a solution as "de-risked" as Algorand.

[6] URL: https://vitalik.ca/general/2021/04/07/sharding.html.

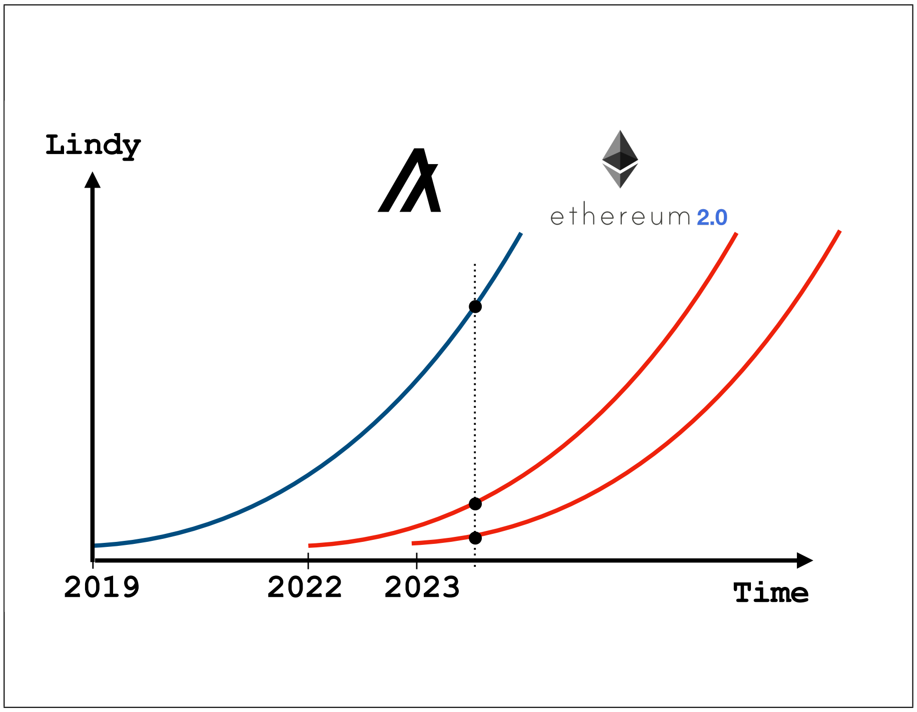


Figure 5: Algorand's Lindy effect: As the first to solve the trilemma, the Algorand network could gain credibility exponentially over coming years, while ETH 2.0 (contingent on launch date) must inevitably "restart the clock", particularly for risk-averse capital.

1.5 Moving Past The Dark Age

Algorand rises above the war of tradeoffs and shatters the dichotomy between blockchain pragmatism and decentralization. It leaves behind the dark age of technology centralization, offering both a fortress for "fast DeFi" and a bridge to risk-averse TradFi. Algorand ultimately moves past the DeFi wars, stepping back from the invasions and coups of multi-chain pragmatism to instead focus on the next decade of financial deployments – on the next age of reason.

2 The Science Of Algorand

Algorand makes a bold claim. If true, then it is L1 utopianism under the market's nose. In this section, we explore the scientific foundation of Algorand, unpacking the breakthroughs that allow the protocol to scale while staying decentralized.

2.1 Context: The Long Chain Of Cryptographers

Scientists face a paradox: they rarely live long enough to see their ideas gain recognition, let alone adoption. With its speed of adoption, cryptography breaks this paradox. In less than a lifetime, a tiny band of scientific explorers watch as their ideas upend the financial system.

There is luck in any breakthrough and Algorand is no different. The story begins with *the naive era of cryptographers*[7], theorists who boarded a pirate ship with no destination in mind, long before venture capitalists backed computer scientists. *They chased discovery for discovery's sake.*

Algorand's founder Silvio Micali was one of these early explorers, co-inventing primitives like Verifiable Random Functions (VRFs) and Zero Knowledge Proofs (ZKPs)[8]. These inventions do not just underpin Algorand; they fit into a long chain of cryptographers trying to solve one of the hardest problems in distributed systems.

2.1.1 The Byzantine Generals Problem (BGP)

One problem foreshadows all of crypto – and is at the heart of today's dark age. This is the Byzantine Generals Problem (BGP).

Picture several armies from the Byzantine empire waiting by enemy gates. They prepare to attack or retreat together. Each division's general needs a way to communicate with other generals and agree on a unified plan of attack (or retreat). *If some attack but others retreat, the enemy claims victory.*

Here is the problem: traitors may lurk within. Formulating the BGP, cryptographers in the 1970s asked a simple question: *how can a distributed system reach agreement in the face of unknown adversaries?*[9]

2.1.2 Two Answers & The Blockchain Trilemma

Originally, BGP solutions fell under the umbrella of Byzantine Fault Tolerance (BFT). Nodes relay information inside a closed network of validators. In BFT-based systems, validators know each other's identity. If at least two thirds of the chosen few are honest, the system reaches consensus. 1970s implementations supported tens of validators at most[10]. This grew closer to fifty in the 1990s with the advent of "pBFT" and continues to climb with the rise of modern blockchains[11].

Decades later, Satoshi introduced a revolutionary alternative: Nakamoto Consensus (NC). Unlike BFT-based systems, NC has an open validator set. Anyone can join. Node count scales infinitely. Validators

[7] URL: https://doi.org/10.1007/s11276-019-02195-0.

[8] URL: https://www.forbes.com/sites/stevenehrlich/2021/07/12/algorand-founder-silvio-micali-breaks-down-how-to-construct-a-fast-and-secure-blockchain-in-a-world-full-of-adversaries/?sh=74294f313fa3.

[9] URL: https://doi.org/10.1007/s11276-019-02195-0.

[10] URL: https://doi.org/10.1007/s11276-019-02195-0.

[11] URL: https://doi.org/10.1007/s11276-019-02195-0.

do not need to know each other. NC's defining quality is decentralization – but this open validator set comes at the cost of performance.

We end up caught between two systems, each with its own sacrifice. BFT has high throughput and deterministic finality, but is centralized. NC is decentralized with probabilistic finality, but it is slow. Vitalik Buterin eventually called this divide the "blockchain trilemma"[12]. Blockchains cannot be scalable, decentralized and secure. They must choose between two of these three properties.

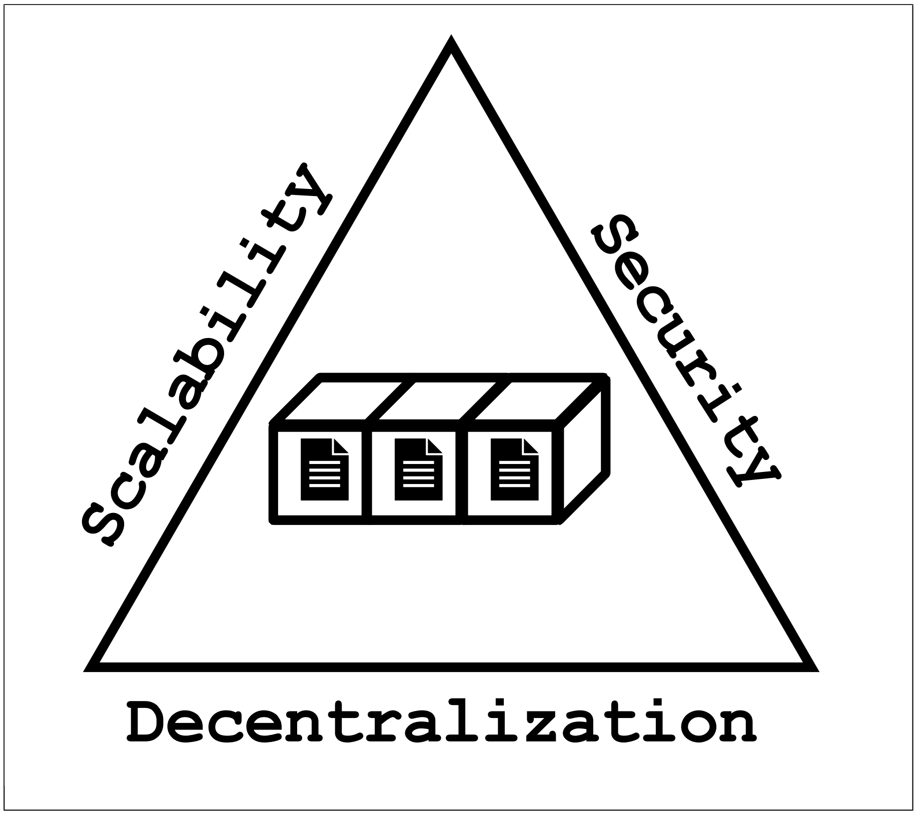


Figure 6: The blockchain trilemma. So far, current blockchains must decide between two of these three properties. Since a blockchain that is not secure would be useless as a monetary system, we are left with the tradeoff between scalability and security.

The dark age is one where L1 chains are bound by the trilemma. Even the most advanced chains claiming to scale validator count often hide behind a static validator set or *barriers to entry so high that validators are effectively static.* The same (typically small) group of people validates transactions.

Many L1s *improve* on classic BFT, but they do not create open systems with boundless participation. The question is, is there a way blockchains can leverage the speed and finality of BFT *and* the openness of NC?

We believe Algorand is the only protocol which claims a definitive yes. Defined with this context in mind, ***the Algorand protocol is an attempt to solve the BGP without accepting tradeoffs between performance, decentralization and security.***

[12] URL: https://vitalik.ca/general/2021/04/07/sharding.html.

2.2 Algorand Design Philosophy

2.2.1 Do Not Do As The Romans: A Forkless Empire

The end of every great empire is a hard fork, either by a people's own doing or at the mercy of outsiders. Ancient Rome was the longest chain until it was no more. Algorand's philosophy is fundamentally forkless, accommodating consensus-based changes without soft or hard forks.

Protocol changes are like block proposals. Community votes pass at an agreed-upon block without the possibility of a new chain. Nodes upgrade to the next regime, enforcing linearity and protecting against asset replication and transaction reversals.

This design philosophy lives between two apparently contradictory worlds, the dynamism of community evolution and the static rule of law. The constitution is a living document, but evolution is captured by one chain that can never be hijacked. There is a single empire of Algorand, free from the Byzantine incursions that destroyed Roman linearity.

Figure 7: The fall of Rome was due to the failures of consensus and endless political forks. Image from *ThoughtCo*[13].

2.2.2 Consensus: Easy To Reach, Difficult To Subvert

In most systems, consensus is hard to reach but easy to subvert. *It is hard to find the truth, but trivial to disrupt it.* Algorand is the opposite: consensus is easy to reach but difficult to subvert.

This is a cornerstone of Algorand design which will become clearer after the following sections. Anyone can take part in consensus, but cryptography hardens the system against this self-governance backfiring. Being a validator is as simple as owning a single token and running software from any local PC, but subverting consensus would take *longer than the age of the universe.*

2.3 Until The End Of Time: Secured By Randomness

We can now dive into Algorand's core cryptography, centered on mathematical randomness.

One of the hardest questions for any blockchain is deciding on *how to select validators.* Who are the arbiters of truth? How can we design validator selection to maximize the probability of honest nodes

[13] URL: https://www.thoughtco.com/what-happened-to-the-ancient-romans-4058701.

and, ultimately, an honest system?

Algorand introduces a process called **cryptographic sortition**[14] that randomly selects groups of validators called committees. By a fair lottery, the protocol chooses a 1,000 validators for block proposal and validation. Consensus is ruled by a random distribution weighted by an address' token holdings: as long as $\frac{2}{3}$ of token holders are honest, the system is honest.

Sortition is local – at the level of any user's PC. Lottery players "self-select". They do not need to rely on anyone to know if they have won or lost the lottery. There are no kings or aristocrats. Sortition is how Algorand finds truth easily but protects against its destruction: anyone pulls the lever, but attackers will fail unless they have two thirds of tokens or somehow predict and corrupt the committee (which, as we will see, is mathematically improbable).

2.3.1 The Alchemy Of Algorand: Verifiable Random Functions

No algorithmic number generation is *truly* random: creating randomness from order is a logical paradox. We can observe randomness, but cannot manufacture it from scratch. The problem, then, is that our observations in the lab do not scale. We can observe a *truly* random sequence of 300 bits, but cannot *practically* observe a truly random sequence of 1,000,000 bits on demand.

This is where one of Micali's inventions comes into play – Verifiable Random Functions (VRFs)[15]. VRFs are a major triumph in modern complexity theory. They are like the alchemy of Algorand and are ultimately why it escapes the trilemma.

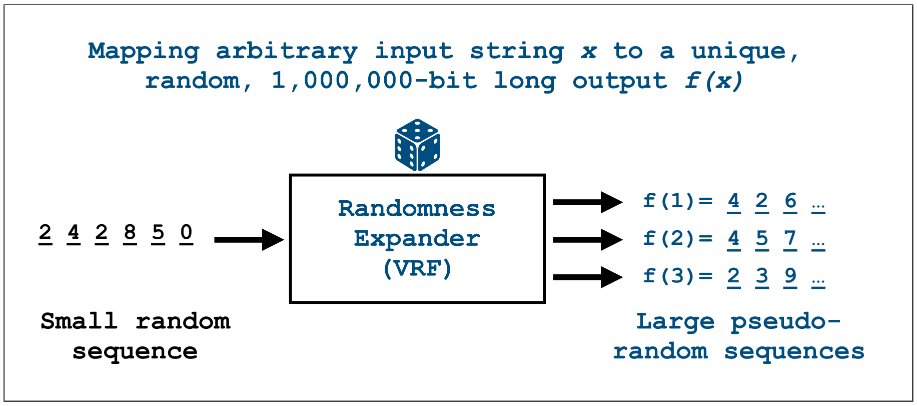

Mapping arbitrary input string x to a unique, random, 1,000,000-bit long output f(x)
2 4 2 8 5 0
Small random sequence
Randomness Expander (VRF)
f(1)= 4 2 6 …
f(2)= 4 5 7 …
f(3)= 2 3 9 …
Large pseudo-random sequences

Figure 8: Conceptual random output generation using VRFs. On-demand randomness is easy to generate, but extremely difficult to predict, which is what ultimately secures Algorand.

VRFs generate outputs indistinguishable from true randomness[16]. Here is how it works. Each wallet w_i (where $0 \leq i \leq N$, N being the total number of wallets) has an associated function (unique and random) W_i satisfying the following four properties:

1. The function W_i maps any vector input $\mathbf{x}$ to a unique, random, 256-bit string output, $W_i(\mathbf{x})$
2. Wallet w_i can, thanks to a secret key, on input $\mathbf{x}$, immediately compute both the corresponding output $W_i(\mathbf{x})$ and a short proof that $W_i(\mathbf{x})$ is the unique output corresponding to $\mathbf{x}$. This proof allows everyone to verify the correctness of $W_i(\mathbf{x})$

[14] URL: https://developer.algorand.org/.
[15] URL: https://ieeexplore.ieee.org/document/814584.
[16] URL: https://ieeexplore.ieee.org/document/814584.

3. No wallet, not even wallet w_i with its secret key, can prove that function W maps any value $\mathbf{x}$ to an output other than $W_i(\mathbf{x})$
4. Without the proper secret key, no one can predict $W_i(\mathbf{x})$ better than a random guess, even if they have seen the outputs of W_i at arbitrarily many inputs other than $\mathbf{x}$. This is how randomness secures Algorand.

2.3.2 Selecting Random Committees: Sortition At Work

In Algorand, every wallet can register to participate in block generation by posting a simple message on-chain. When it is time to select a committee to validate a newly proposed block, Algorand's lottery randomly chooses roughly 1,000 tokens based on: q, a special quantity that is part of the previous block, and t, a target number equal to 1,000 divided by the total number of tokens owned by all registered wallets.

The lottery process is completely localized: each registered wallet pulls the lever without interacting with other wallets or anyone in the protocol. Assume candidate wallet w_i currently owns 100 tokens. Then, conceptually, w_i computes 100 outputs of the function W_i at a given value of q: namely, $W_i(q, 1)$, $W_i(q, 2)$,. . . , $W_i(q, 100)$.

Recall that each such output, $W(q, ...)$ is a random number. If one of these 100 outputs is less than or equal to t, then wallet w_i has a winning ticket proving it belongs to the committee. For instance, assume that $W_i(q, 23) < t$. Then, wallet w_i sends two messages through the network: the output $W_i(q, 23)$ together with a proof of correctness allowing anyone to verify that w_i is a member and its opinion (approval or disapproval) of the new block.

If a wallet has multiple winning tickets in a lottery, it has as many votes in the corresponding committee. The key: every token has the same shot at winning the lottery.

2.3.3 One Microsecond & The Age Of The Universe

How can sortition be both fast and secure?

It is fast because it takes ***1 microsecond*** for a wallet to figure out how many winning tickets it has and prove it to the network. This is true whether a wallet has 1 token or billions of tokens[17].

Sortition is secure because nobody can cheat the lottery. For instance, if $W_i(q, 17) > t$, then wallet w_i cannot fraudulently testify that its 17^{th} token has a winning ticket: it cannot prove that the output of W_i on input $\mathbf{x} = q, 17$ produces a value other than the correct $W_i(q, 17)$.

This is how cryptography hardens Algorand consensus. Notice that wallet w_i can eventually find an integer $n > 100$ such that $W_i(q, n) < t$, but this does not give w_i a winning ticket because everyone knows that w_i only has 100 tokens.

If more than $\frac{2}{3}$ of tokens belong to honest hands, it would take ***the age of the universe*** to anticipate a committee where the majority of votes belong to malicious wallets, with a vanishingly small probability

[17] Given the number of tokens a wallet has and the probability of a token becoming a winning ticket, one can compute a wallet's Binomial distribution for the total number of winning tickets ($\sum_{i=1}^{N} T_{r,i}$) in round r when it has n tokens. Thus, with a single evaluation of W_i (conceptually with the random string $W_i(q, \sum_{i=1}^{N} T_{r,i}, n)$) wi computes its total number of winning tickets, $T_{r,i}$, for the current round r.

If $T_{r,i} = 0$, then w_i does nothing. If $T_{r,i} \geq 1$, then w_i propagates throughout the network both the value $W_i(q, \sum_{i=1}^{N} T_{r,i}, n)$ and the proof of its correctness, thus participating in the committee with $T_{r,i}$ votes.

that a committee member holds a majority of tokens.

Sortition captures Algorand's core design philosophy: it takes a microsecond to participate and the age of the universe to destroy; ***consensus is easy to reach and difficult to subvert.***

2.3.4 The Separation Of Powers

If one self-selected committee of 1,000 validators wasn't powerful enough, *what if there was a way to do it over and over again?* Consider that Algorand is recursive: it can run the same piece of information through several rounds of committees. The lottery selects one committee which generates a block, but doesn't stop there: at the same time, *another independent committee* of 1,000 self-selected validators does the same.

These separate committees split up the process from validation to eventual agreement.

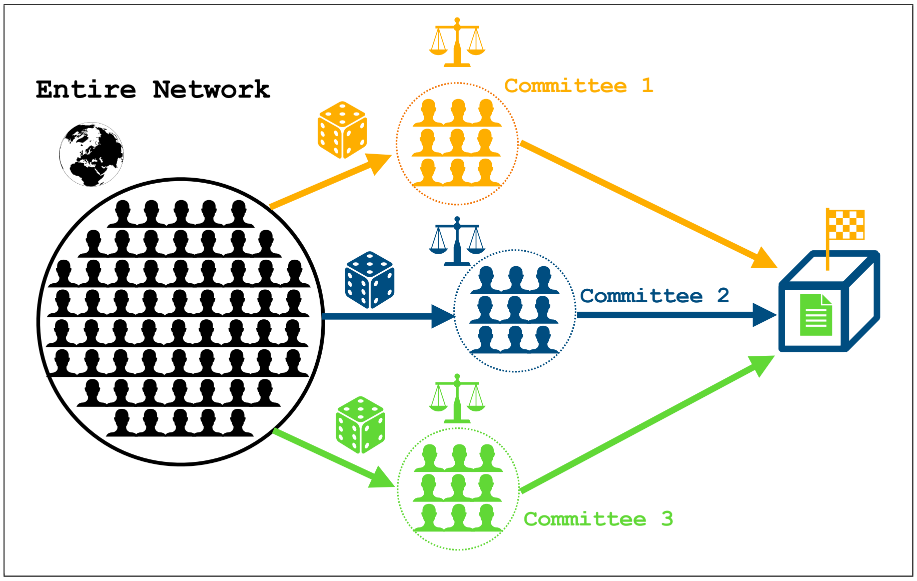


Figure 9: Simplified logic of Algorand consensus. Using many rounds of cryptographic sortition in which multiple different committees participate, the network reaches final consensus on every single block.

It is like the separation of powers in the Western legal system. Not only is the judiciary chosen by self-selecting randomness, it is then double checked by an *independent court*, divorced from the other committees. Here's where it gets interesting: *the probability of overlapping committees is negligible.*

What is the end result? If attacking one round of randomness was hard enough – how hard is it to breach the gates of (say) *nine committees* within a single round?

We return to the idea of consensus being easy to create and hard to destroy. Anyone joins the lottery, but attacking sortition is like undermining a web of *mathematically independent courts.*

2.3.5 Fast, Final & Yet Also Secure: Fortifying Algorand

The end game for sortition: a base layer that is fast, final and secure. Today, Algorand performs 1,000 TPS with 5 second finality and an open validator set. Randomness fortifies Algorand from attack. Adversaries cannot target the majority of a small group; they must target the majority of the entire network ruled by the same random lottery.

The difference between attacking a centralized blockchain and a decentralized blockchain is akin to the difference between conventional and guerilla warfare. In the table below, we summarize how Algorand's breakthrough makes conventional network attacks obsolete[18], strengthening Algorand's appeal as a home for high-value finance.

Table 1: The Fortress of Algorand: How Algorand protects against conventional attacks.

Attack Type	Description	How Algorand Prevents Them
Double spend	Attackers overturn finalized transactions by forking the chain	Forklessness
Nothing-at-stake	Attackers perpetuate multiple forks at no cost	Forklessness
Multi-period attack	Attackers validate fraudulent chain in parallel merging with true chain when selected as validator	Disposable keys, cryptographic sortition
Validator bribing	Identifying and corrupting validators beforehand	Cryptographic sortition
Sybil attack	Creating multiple addresses associated with the same entity to influence validation power	Voting power tied to token possession, not address

2.4 The Politics Of Algorand

2.4.1 Blockchains Are Political Animals

If blockchains are empires that can wage war and fight for resources and citizenry, then they are clearly far more than technologies. L1s are political animals. They replace national constitutions with cryptographic primitives and take inherent views on governance, ownership and power.

What are the politics of Algorand and how do they fit into the evolving landscape of PoS? In our view, Algorand's political contributions are as novel and important as its breakthroughs in cryptography.

2.4.2 Political Systems Face The Trilemma

Imagine the blockchain trilemma as a political trilemma. Systems of government face similar tradeoffs. Democracies invite a broad group of participants into consensus, but are slow and plagued by forks and fractures. Dictatorships push fast reform, but are centralized and fragile.

Does high-value capital want to live in a plutocracy? There is a strong counterargument to this analogy: *Singapore*. It is a highly successful centralized state, begging the question – will blockchains *need* an open validator set?

Perhaps – like Singapore, a refuge of financial stability – L1s will capture a large asset base without solving the trilemma.

[18] URL: https://ieeexplore.ieee.org/document/8972381.

We agree that in rare cases, benevolent dictatorship can win, but we are in search of a more ambitious solution. We argue that Algorand is more like the American experiment than the Singaporean one: Singapore works as a niche economy, but cannot scale to hundreds of millions of people. ***Algorand, like the Founding Fathers, dreams of a grander idea: to merge the openness of a Republic with the constitutional protections of a secure and forkless public network.***

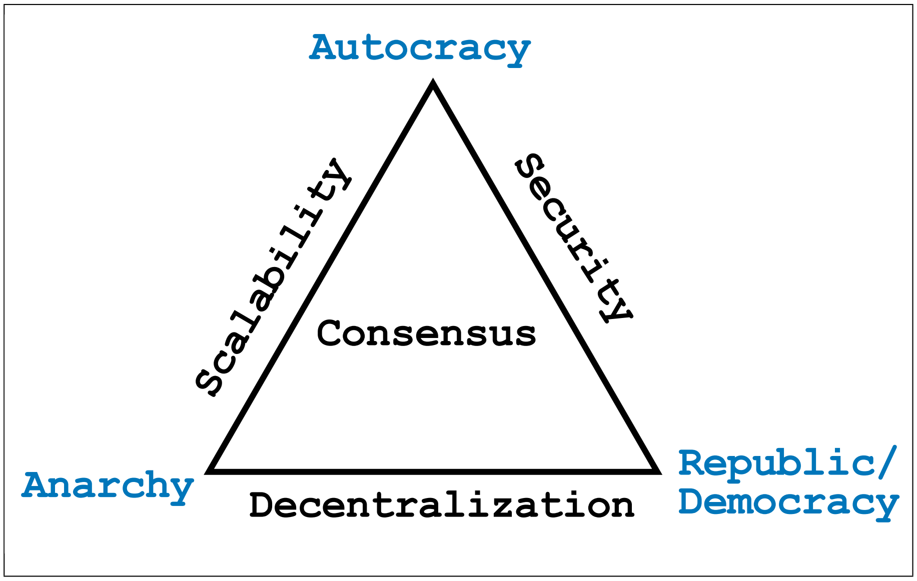


Figure 10: The political trilemma.

2.4.3 The Market Is Underweighting Decentralization

Solving the trilemma is beyond technology, requiring us to recast political debates that date back to the Ancient world. If blockchains are countries, then they will all someday face the same problems plaguing the birth and development of any nation.

The multi-chain wars overshadow the value of ground-up philosophical design. In the public square of DeFi, pragmatists shout louder than idealists, leading the market to underweight decentralization. Capital accepts plutocracy in exchange for political expediency.

If our thesis is correct and decentralization is the most important factor for long term capital inflows, *then the blockchain philosophers are undervalued.*

2.4.4 The Inevitable Aristocracy: Four Critiques Of Modern PoS

Before we describe Algorand's unique take on PoS, we survey the most common critiques of PoS systems.

2.4.4.1 Wealth Concentration

Critics argue that PoS inherently leads to the concentration of wealth[19]. Rewards are proportional to one's wealth (stake) and staking rewards grow exponentially with a growing network. Whale ownership thus

[19] URL: https://ieeexplore.ieee.org/abstract/document/8746079.

grows disproportionately, but without any compelling rationale. *Is there any difference in the complexity or value of validating transactions whether one has 1,000 ETH staked, or 32 ETH staked?*

A good measure for decentralization is ***the ratio of economic value securing the network to the economic value stored on the network.*** As the rich get richer, this ratio declines: network security depends on an increasingly smaller fraction of entities. Some systems cap each node's validation power, but this ends up inviting Sybil attacks and attracting mercenary validators who lose interest in securing the network over time.

$$DR = \frac{\alpha_S}{\alpha_{NW}},$$

$$\begin{aligned} \text{where } DR &= \text{decentralization ratio,} \\ \text{where } \alpha_S &= \text{economic value securing the network,} \\ \text{where } \alpha_{NW} &= \text{economic value stored on the network.} \end{aligned}$$

The defining property of a truly decentralized system is that its decentralization ratio tends towards unity as the number of users (N) grows large, i.e. $\lim_{N\to\infty} DR = 1$.

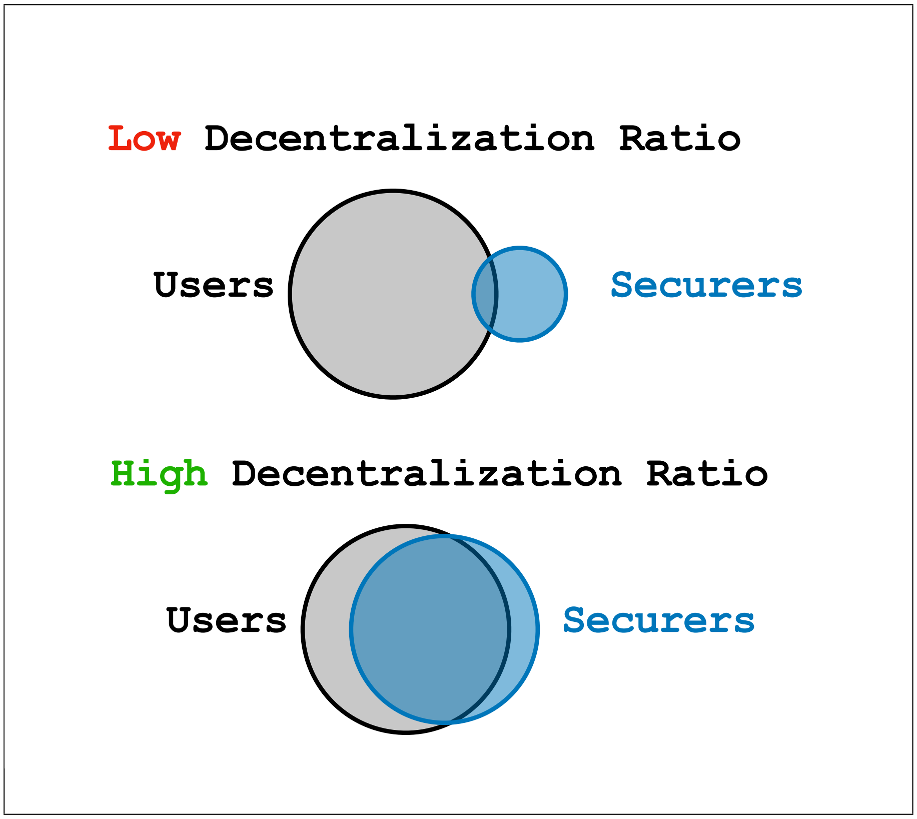


Figure 11: Visual representation of the decentralization ratio. Decentralized systems are ones where the users and securers of the network are the same, and the security of the network is the responsibility of everyone. On the other hand, centralized systems are where the security of the network (and capital of the majority of the users) is the responsibility of a small minority of the network.

2.4.4.2 A Bounty For Bribes

A second critique relates to the economics of staking in bonded PoS[20]. Bonded PoS (like ETH 2.0's Casper) requires validators to lock up a pool of money as a "bond" which can be "slashed" if they are malicious or incompetent.

This raises several questions. How big does the bond need to be to keep validators honest? Couldn't well-capitalized attackers simply bribe nodes off-chain? If the bounty for misbehaviour is larger than the cost of slashing, the disincentive breaks down. *Will these incentives hold up when bounties are worth trillions?*

2.4.4.3 A Sinkhole For Capital

The next problem is opportunity cost[21]. Most "wasteful" arguments are directed at Proof-of-Work (PoW), yet arguably, this argument is more compelling when applied to bonded PoS. *What is the societal opportunity cost of locking up all this non-productive capital*?

PoWs energy sink at least economizes otherwise idle energy. Bonded PoS is a pure sinkhole. Can a global economy live on a system incurring this much opportunity cost – where the sinkhole widens as the economy gets larger?

2.4.4.4 DPoS: The Chosen Few

Finally, it is easy to see the centralization risks of Delegated PoS (DPoS), a common flavor of PoS. DPoS whitelists a small set of "honest" validators (the preferiti). These plutarchs become not just a centralized band of rulers, but the primary attack vector of any DPoS network. They are identifiable and often public, making them ready targets for network attacks[22].

ETH 2.0 isn't explicitly DPoS, but we argue that 2.0's bonded PoS model may trend toward DPoS over time, for the following reasons:

- Validation has a high barrier to entry (capital and hardware requirements)
- The rise of staking aggregators centralizes liquidity, inviting network attacks
- MEV motivates miner collusion.

2.4.5 The Politics Of Algorand: PPoS

Algorand introduces a version of PoS called Pure PoS (PPoS) that escapes the above critiques.

PPoS is "pure" because sortition is open to anyone. Every token has the same probability of being selected for the lottery. Consensus is so trivial that we do not need to start with the assumption of other PoS networks: that we must reward good behaviour and "slash" bad behavior.

Instead, it is as simple as owning an ALGO, which is always governed by the same mathematical ballot as other ALGOs. Individuals can acquire more coins, but they can never privilege one ALGO against another.

[20] URL: https://ieeexplore.ieee.org/abstract/document/8746079.
[21] URL: https://arxiv.org/abs/2006.11156; URL: https://research.paradigm.xyz/staking.
[22] URL: https://ieeexplore.ieee.org/document/8972381.

Algo is a system of equal representation[23].
Just as 'one man, one vote', one ALGO, one vote.

PPoS doesn't divide validators and users: ***the securers and users of the network are one and the same.*** This is a profound contribution. Going back to the American analogy, Algorand consensus is for the network, by the network. *There is no dividing line between citizens and government, resulting in a far higher decentralization ratio than bonded PoS.*

Consensus is so scalable and cheap for anyone to perform that Algorand doesn't need to incentivize validators with preferential inflation. PPoS escapes the drive toward wealth inequality. Voting power is non-dilutable. *Owning an ALGO is like owning a fixed piece of voting equity in the network: an individual can acquire a certain number of ALGO without worrying about whale growth diluting the power of their individual vote.*

PPoS prevents the plutarchic rule of the minority. Majority attacks are also uneconomic. Why would a majority attack itself? Even assuming a majority of tokens could collude, this is self-defeating. Ultimately then, we put our trust in *an honest majority of the network, not a majority of a resource-accumulating minority.*

The rise of the lobbyists is a major threat to PoS security. The market identifies those with the rings of power and tries to corrupt them. These power games can undermine network confidence. *There is no way to lobby validators in Algorand.* It is like trying to lobby math. At every layer, VRFs build independent judiciaries and mathematical failsafes. Attackers only ever learn a validators' identity after they've announced themselves onto the network and, by then, it is too late to bribe them (everybody now knows their identity).

Finally, PPoS is more capital efficient than naive PoS. It can grow to a multi-trillion dollar system without a proportional rise in opportunity cost. There is no sinkhole in Algorand. This seems trivial in a time when L1s are a drop in the financial ocean. *Revisiting the idea of the roundabout strategy and thinking decades down the line, can we build an economic system on L1s where more success does not translate into more sunk capital?*

2.4.6 The American Experiment Versus The Algorand Experiment

The iterative games of sortition – one self-selected committee to the next – create an open system of self-government.

Recall our political analogy. Algorand is a fast government without a dictator, equal representation without forks and the decentralization of anarchy without giving up national security.

Breaking the trilemma is a political achievement as much as it is the culmination of decades of cryptography. *Algorand has found a way for humans to agree at scale without compromising a system's security or decentralization.*

The Algorand experiment is ultimately akin to the American experiment: a radically open political system coordinating masses of people without carving out any one group's destiny.

[23] URL: https://developer.algorand.org/.

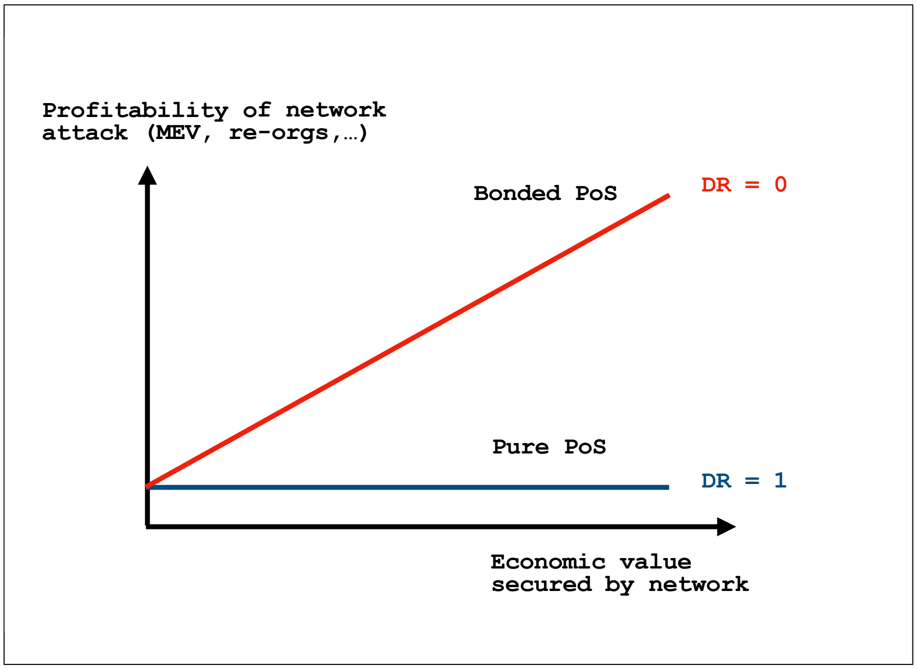


Figure 12: For centralized networks, the profitability of attacks (and thus the incentive for attacks) grows with the economic value of the network. Faced with a growing bounty, the minority securing the network has an increasingly stronger incentive to attack the network – just as outside adversaries are attracted by the growing bounty.

2.5 Algorand's Unconstrained Stack

On top of solving the base layer, Algorand's technology stack is highly expressive. It makes particular use cases more compelling, offering users customizability they cannot get on other L1s. When blockchains are bound by tradeoffs, the technology stack adapts to the base layer, caught by the barbed wire of today's limitations. Think of how DeFi primitives optimize for Ethereum congestion. Algorand is ground-up: less about patching today's limitations, instead focused on crafting a post-trilemma feature set.

2.5.1 Algorand Primitives

Algorand-native primitives are designed to be programmable. They create a highly expressive environment catering to everything from simple DeFi applications to highly specified institutional use cases.

As we will see in Section 3, Algorand-native primitives introduce novel opportunities that aren't available in more constrained environments[24]:

1. **Algorand Standard Asset (ASA):** These are natively issued assets with customizable transaction and ownership features (fungible and non-fungible). ASAs add to the customizability of standard ERC20s with a new feature called Role Based Asset Control (RBAC). They let issuers program clawbacks, asset quarantines and ownership rights. As we will see in Section 3, RBACs are a compelling way to introduce TradFi to DeFi.
2. **Atomic Transfers:** Atomic transfers are batch transactions that allow two or more parties to

[24] URL: https://developer.algorand.org/.

exchange any number and type of assets, guaranteeing transactions part of the transfer either all succeed or all fail. This allows for group payments, circular trades, multi-party payments and trustless settlement on decentralized exchanges. Atomic transfers on Algorand are purely at L1 and do not require smart contracts – thus making them more secure and truly irreducible.

3. **Rekeying:** Rekeying solves an operational problem for high security users. It allows users and institutions to maintain externally visible public addresses while either changing the authorized spending keys or keeping authorized spending keys cold at all times. Rekeying is implemented at L1 and does not require smart contracts.
4. **Algorand Smart Contracts:** Using the Algorand Virtual Machine (AVM), smart contracts developers can write smart contracts in high level, accessible, languages while maintaining the same speed (1,000+ TPS) and cost (.001 Algos) as simple pay transactions. They are also purely at L1, enjoying the same security and finality properties as consensus.

2.5.2 Upcoming Roadmap: 46k TPS & Smart Contract Composability

One objection to Algorand is that decentralization does not matter. While it may be decentralized and 1,000 TPS is fast enough for most financial applications, how will it compete with centralized L1s with much higher TPS?

For reasons we described earlier, we do not think this logic holds. High-value finance will look beyond a TPS bidding war, viewing decentralization as insurance. This capital cares about upfront assurances, rule of law and mitigating tail risk.

With that said, Algorand's upcoming roadmap is focused on three main areas, which may ultimately make these counter-arguments moot (even if one takes a different view on decentralization):

1. **Performance** – Algorand has a stated goal of improving TPS from ∼1,000 to ∼46,000[25]. Part of this implementation will be something called pipelined consensus, which will see blocks finalized at sub second speeds.
2. **Smart Contracts** – Algorand's goal is to make its smart contracts more expressive while remaining relatively simple to write. The team recently introduced the Algorand Virtual Machine (AVM), focused on increasing capabilities and composability[26].
3. **Interoperability** – Algorand is creating technology for completely trustless bridges between Algorand and other smart contract capable chains, starting with Ethereum. While bridges currently exist, Algorand's implementation will introduce novel cryptography. It will create portable cryptographic proofs that contain the current state of the Algorand blockchain, attested to by the Algorand blockchain itself. It is also worth noting that this interoperability project will include a focus on making Algorand "post quantum", led by Algorand's Head of Cryptography Chris Peikert – one of the world's leading minds on post-quantum cryptography[27].
4. **CoChains** – Algorand will launch CoChains[28], where anyone can launch a permissioned chain interoperable with the main chain. Institutions will thus be able to launch private networks that

[25] URL: https://www.algorand.com/resources/blog/algorand-2021-performance.

[26] URL: https://www.algorand.com/resources/news/june2021_protocolupgrade_avm.

[27] URL: https://www.cryptoninjas.net/2021/01/06/algorand-welcomes-chris-peikert-expert-in-lattice-based-and-post-quantum-cryptography-as-head-of-cryptography/.

[28] URL: https://www.algorand.com/resources/blog/algorand-co-chains.

leverage the security and functionality of the public network. CoChains are like "sidechains": permissioned but free to optimize the underlying parameters for different applications (e.g. can achieve higher throughput with longer finality times, or vice versa).

2.5.3 An ESG Network

Validators on Algorand do not engage in a computational race to win blocks. Each participation node performs a simple and cheap local calculation (cryptographic sortition) and 1,000 validators broadcast their results to the network. *This creates scalability without a rising energy footprint.* If the ESG narrative continues to gain traction amongst institutional investors, this will be a strong selling point for TradFi deployments on Algorand. Future upgrades that increase throughput will continue to reduce energy used per transaction.

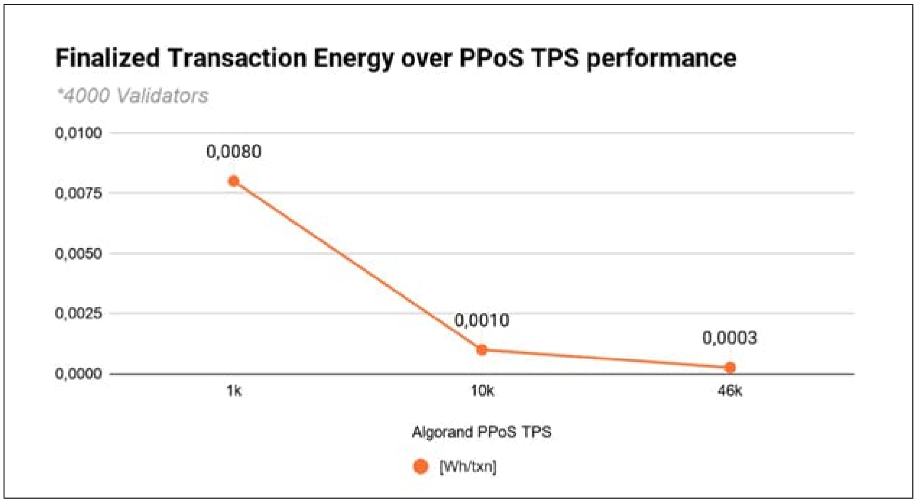


Figure 13: An already low transaction energy footprint is set to decline as Algorand continues to upgrade throughput[29].

[29] URL: https://www.algorand.com/resources/blog/how-algorand-offsets-carbon-footprint.

3 The Marriage of DeFi & TradFi

As the West adopted the *Enlightenment base layer* in the 17th and 18th centuries, otherwise impossible applications began to emerge – from the rapid rise of science to a new industrial age. We argue that Algorand's fundamental breakthroughs will make new applications possible not just in DeFi and TradFi respectively, but position the project to embed these two capital pools into one another.

For crypto-natives, Algorand is *the return of the L1 maximalist*, reviving base layer utopianism. At the same time, it gives legacy capital safety and expressiveness that no other L1 can provide. Since the protocol can deliver performance while boasting (1) a forkless empire, (2) radical decentralization and (3) zero downtime since inception, it can play a leading role in the transition of closed TradFi asset bases into supercharged, DeFi-native infrastructure.

Our bet is that Algorand-native markets will marry old and new pools of liquidity. This is an opportunity not just for Algorand, but the rest of crypto. Onboarding traditional liquidity escapes the zero-sum war for mercenary capital. Legacy assets like bearer CBDCs or yield-generating debt or equity introduce new forms of collateral into DeFi, bringing crypto innovation to the real economy (and vice versa).

In this final section, we describe how Algorand is the natural marriage of DeFi and TradFi. We start by describing each. We conclude by imagining the hybrid experiments that could follow from Algorand.

3.1 Algorand DeFi: The Return Of The L1 Maximalist

The decline of L1 maximalism captures the triumph of a new, unspoken belief system: *We cannot rely solely on L1 scaling and must tone down the religion of decentralization, lest we are overrun.*

To fight their enemies, the old guard adopted their values. They made concessions that felt like the necessary evils of adoption. Centralized L1 amassed victory after victory and forced the Ethereum community to over-index on L2 and underplay centralization risks, ultimately diverting intellectual capital from L1. They spoke the language of decentralization, but accepted details that empowered a new type of crypto feudalism.

We wonder: is there a risk these concessions will not be temporary; that they may fundamentally reshape DeFi's longer term trajectory?

This is why we find Algorand compelling. It gives the L1 maximalist new ground. It offers the opportunity for performant DeFi without compromising on the promise of DeFi itself: decentralization. The protocol delivers on the oldest L1 aspirations. DeFi does not have to wait for ETH 2.0, surrender to semi-centralized L1 or over-index on naive L2.

3.1.1 Build Now, Fix Later: The Hidden Danger Of Silicon Valley "Iteration"

L2 will play a strong role in DeFi, but we are cautious of the narrative of L2 as a panacea. We see the current L2 landscape as a temporary patchwork, a suboptimal compromise urged by the rise of centralized L1. Short term fixes permeate today's market. The mantra is simple: build an EVM compatible chain requiring minimal modification and leverage it as a centralized side chain. Many of these L2 solutions run into the same problems at L1 – just at higher throughputs. Similarly, semi-centralized L1 could be better

[30] URL: https://ournetwork.substack.com/p/our-network-issue-74-revised.

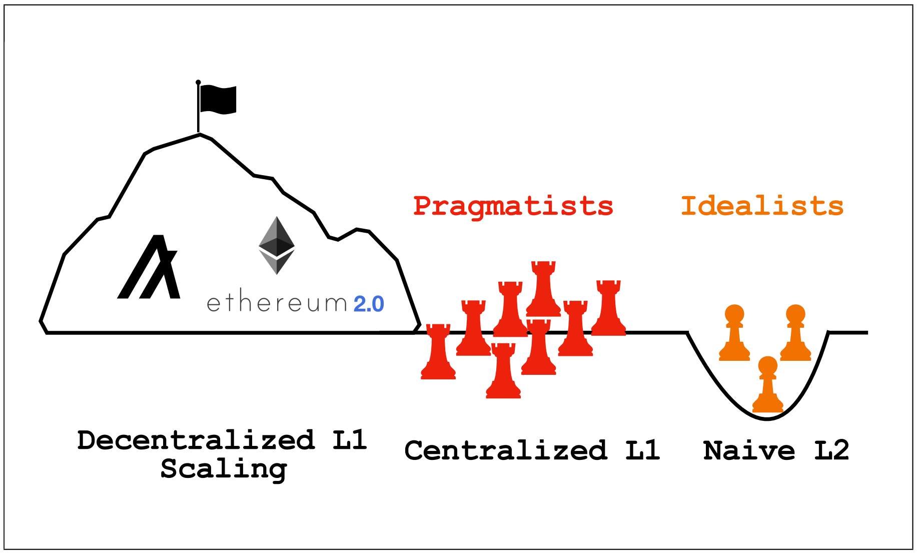


Figure 14: How multi-chain pragmatists blocked crypto's march toward L1 scalability and forced idealists to change course and over-index on L2 solutions.

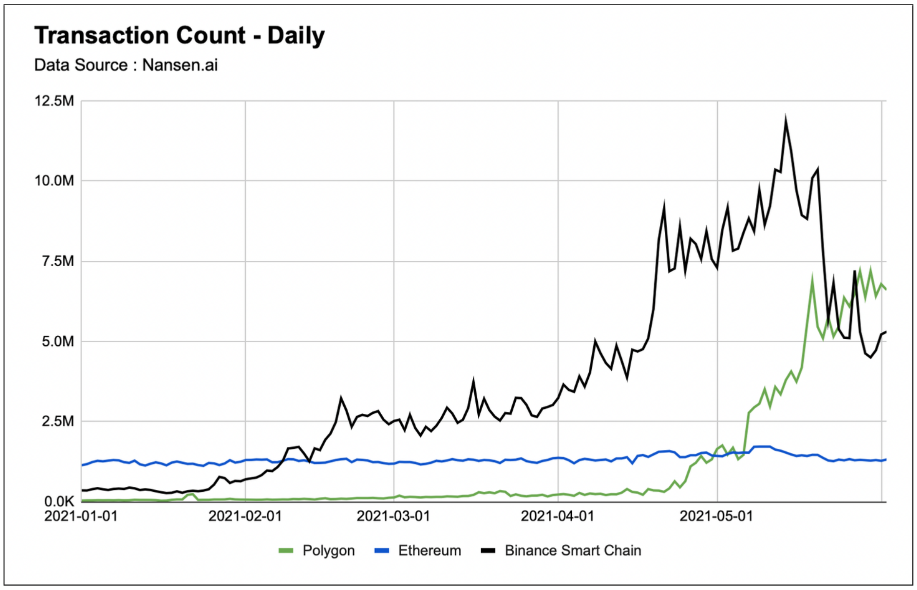


Figure 15: The rise of naive L2 in response to lack of scaling on Ethereum. Data from *Our Network*[30].

than a single-node banking system, but is this where high-value assets will live in the long term? Can these chains survive network attacks, whether economic, political or regulatory? Beyond individual rug pulls, network attacks represent systemic failures, threatening to unwind the system and expose everyone on the protocol to the risk of ruin.

A once careful conversation about tradeoffs has been replaced by the Silicon Valley imperative to "build now, fix later". This mindset has inspired incredibly creative ideas, but if these ideas trend toward plutocracy, will they survive, regardless of how brilliant? The "iteration" mindset worked for the Web,

Table 2: Game theory of L1 and L2 scaling. Even though it is Pareto optimal for users and developers to coordinate decentralized L1 scaling, the Nash equilibrium favors sidechains/centralized networks.

		Protocols	
		Algorand	Sidechains/Centralized Networks
Users	Algorand	Pareto Optimal	Least Optimal
	Sidechains/Centralized Networks	Least Optimal	Less Optimal (Nash Equilibrium)

but does it apply to open and global financial systems? Finance requires a more careful and roundabout approach. The concessions of today could haunt protocols in just a few years if they become large enough to entice attackers. "Fixing later" is comforting psychologically, but embeds tail risk into these protocols in the long run.

Table 3: Why L2 solutions are not a Panacea.

L2 Solution	Description	Example	Potential Problems
State channels	Independent off-chain settlement between specific users	Connext, Raiden Network, Celer	Liquidity fragmentation, long uptime and continuous monitoring
Plasma/childchains	Smaller copies of parent blockchain, relies on parent chain security guarantees	Gluon, OMG Network	Continuous monitoring, no smart contracts
Sidechains	Independent chain with own consensus and security guarantees, communicating with parent chain through two-way bridge	xDai, Polygon	Centralized, not trustless (custody of funds)
Rollups	Transaction bundling off-chain	Optimistic rollups (Optimism, Arbitrum), ZK rollups (zkSync)	Slow withdrawals due to challenge periods (optimistic), no/limited smart contracts (for ZK)

3.1.1.1 How Will The DeFi Wars End?

What is the eventual catalyst for DeFi fleeing these patched L1 and L2 solutions? It could, like many trends in crypto, only change after a major blow up event. In the same way that March 12 changed derivatives market structure – open interest fled Bitmex and rushed from BTC-margined contracts toward stablecoin-margined contracts – we could see something similar play out as we reach the end of the DeFi Wars.

By analogy then, Algorand is not just a call option on decentralization, but a put option on the tail risks of blockchain pragmatism. It could become DeFi's *truly decentralized* insurance policy. If compromised blockchains blow up, surviving users will be forced to temper their tolerance for centralization and find a new, safer home.

3.1.2 Algorand: DeFi Without Tradeoffs (Or MEV)

If we started from scratch, how would DeFi look free from the trilemma? Ethereum DeFi optimizes for the limitations of ETH L1 – but how would DeFi evolve if free from these constraints to begin with?

On Algorand, any of today's experiments could be recast into a playground that is faster, cheaper and less prone to centralization. Applications like Central Limit Order Book (CLOB) Exchanges – clunky and unworkable on Ethereum – are natural extensions of Algorand performance. A low-fee environment escapes the variability and expensiveness of gas on Ethereum, widening the appeal for active market makers.

With no public mempools or the ability to reorganize blocks, Algorand DeFi is significantly less threatened by MEV. We avoid the arms race developing on Ethereum today[31].

We can also imagine a world where cross-chain bridging puts Algorand at the center of other ecosystems. Any asset or ecosystem could leverage Algorand to scale. It could be a solution to Ethereum DeFi's woes, allowing protocols to compete with the pragmatists without forsaking decentralization. It could be the "real" cross-chain scaling solution.

In the end, anyone can solve the trilemma: *they simply need to plug into Algorand.*

3.2 Onboarding The Old World: TradFi Use Cases

We now explore TradFi. The base layer is a natural home for risk-averse, high-value capital. Algorand also has uniquely expressive tooling that differentiates it from other chains and makes particular TradFi use cases more compelling.

We explore three broad areas:

- Central Bank Digital Currencies (CBDCs)
- Payment rails (including asset-backed stablecoins)
- Asset securitization.

3.2.1 CBDCs: The Next Phase Of Fiat

If one believes central bankers will race to deploy CBDCs, and that some of these deployments intersect with public networks, all roads lead to Algorand. The next phase of fiat will inevitably have a set of firm requirements: (1) a system that can scale (2) a system that cannot be forked and (3) a system with inherent customizability that can express granular and programmable monetary policy objectives.

Algorand's network can power the rapid testing and deployment of CBDCs. Central banks can leverage Algorand to reduce friction in capital markets and reimagine payment rails as well as international and domestic monetary policy.

In this section, we will reserve moral judgement – whether we think CBDCs are tools for financial inclusion or accelerants of government control – and instead try to *think like a central banker, assessing the risk/reward of an on-chain deployment on top of Algorand relative to other L1s.*

[31] URL: https://arxiv.org/abs/1904.05234.

Where else can they go, if not Algorand? Bankers are not motivated by upside, but career risk. They need a system they can trust, expressive enough to program controls and clawbacks at the protocol level.

3.2.1.1 Programmable Central Banking

CBDCs empower central banks to tighten control over sovereign currencies and more effectively pull the levers of monetary policy. ***Through the use of Algorand's RBACs and CoChains, they can do this at the protocol level.***

Issuers can whitelist and blacklist addresses, institute rules for different transaction types and replace the financial system's monitoring and enforcement apparatus with on-chain instructions. This replaces regulatory bloat with elegant on-chain solutions like automatic clawbacks programmed into a smart contract.

3.2.1.2 The Monetary Scalpel: Address-Level Policy Tools

Algorand allows for address-level policy tools, another purpose-built feature for CBDCs. *Central bankers can target monetary policy at the individual address level.* It transforms coarse macroeconomic policy objectives like aggregate inflation and unemployment into precise and programmable levers. Think of a world where central bankers can identify addresses with different consumption and savings profiles and assign them different interest rates.

This is monetary policy targeted at the individual level. *This could also blend monetary and fiscal policy.* Reimagine the blunders of COVID19 stimulus in light of on-chain address specification. Governments could have targeted cheques for specified groups (like restaurant owners), lowering administrative bloat.

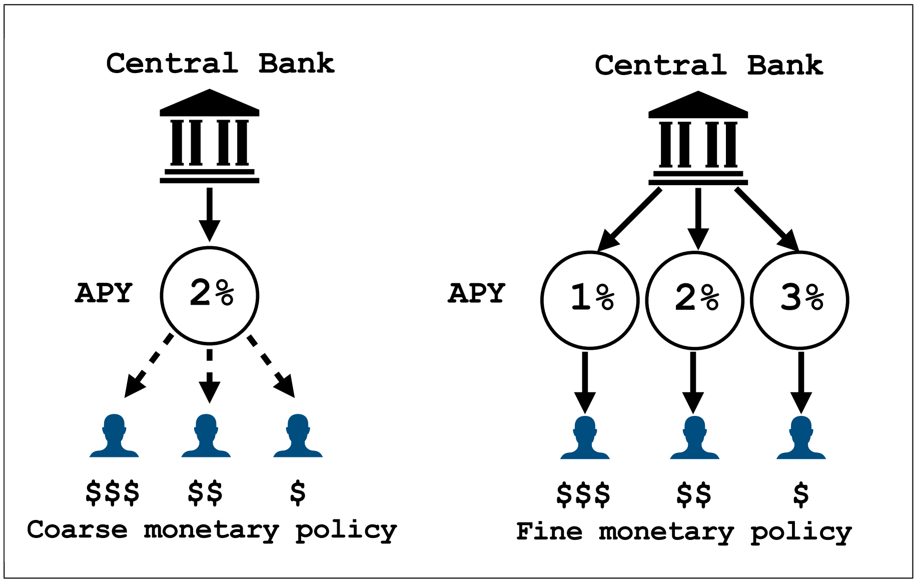


Figure 16: Central bankers' traditional tools enable, at best, coarse control and economic targeting (e.g. an aggregate interest rate). Algorand enables fine monetary policy, tailored at the address level.

Now extend this idea of a monetary scalpel to "non-fungible" currency. Not all dollars are created equal. *On Algorand, the Fed could distinguish domestic and offshore versions of the dollar, enabling different* *capabilities across each "coin"*. This theoretically transforms international debt payments. The Fed issues "*blue dollars*" to pay foreign nationals, shielding the US population from direct inflation (this could manifest in other ways, depending on trade policy). If most of the Fed's debt is domestic, it does the opposite and avoids influencing its foreign trade policy.

Granular control over monetary policy destroys the intermediating forces over any currency. CBDCs are a direct attack on the private banking system. They empower central bankers, who become the fiscal and treasury enforcement arm. *If one believes that CBDCs are an inevitability, then all roads lead to a technical architecture* ***like Algorand's.***

3.2.1.3 The Customizability Of ASAs: Controlling the Velocity Of Money

The velocity of money underpins monetary policy, yet it is highly esoteric. Can central bankers quantify the velocity of money, let alone influence it? They are usually left throwing darts in the dark.

The customizability of ASAs introduces the scalpel to the velocity of money. *Central bankers can program an ASA to require a token burn below or above a particular token velocity, directly influencing saving and consumption patterns.*

This reimagines counter-cyclical policy. Not only can central bankers deposit stimulus directly at the address-level, they can encourage programmable consumption and saving behaviour; "*spend it, or lose it*". In addition, to deal with lost private keys, they could remove tokens from circulation if velocity dropped below a particular threshold.

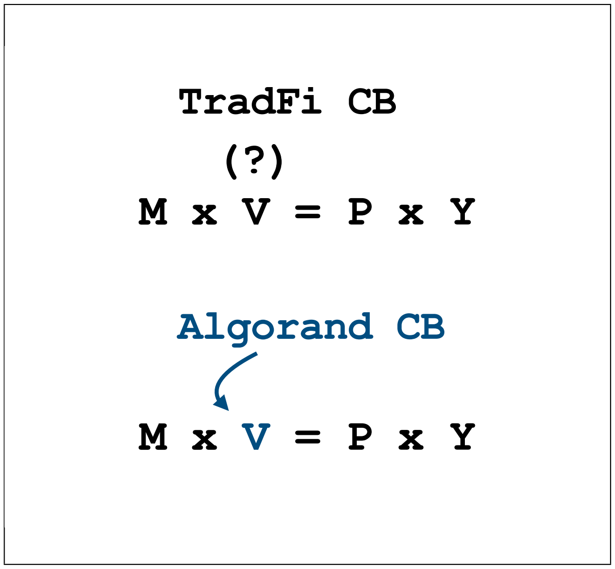


Figure 17: Fisher's equation. The customizability of ASA's enables fine control of difficult-to-control variables such as the velocity of money.

3.2.1.4 Ending Trade Wars: Algorand As The On-Chain WTO

Another paradigm shift in public policy is how CBDCs on Algorand change international trade and debt. Bespoke agreements govern world trade, brokered bilaterally or by unilateral international organizations like the WTO and IMF. Through these agreements, nations trade, borrow capital and broker disputes. Imagine bespoke partnerships could instead be programmed at the protocol level. Countries would no longer need to "trust" one another to honour trade agreements, relying on the programmability and neutrality of ASAs.

Countries could make a particular non-fungible version of their currency only redeemable for specified goods and services. *This is Algorand as the on-chain WTO:* nations enforce trade obligations by code, not political rank, reducing trade wars and increasing transparency.

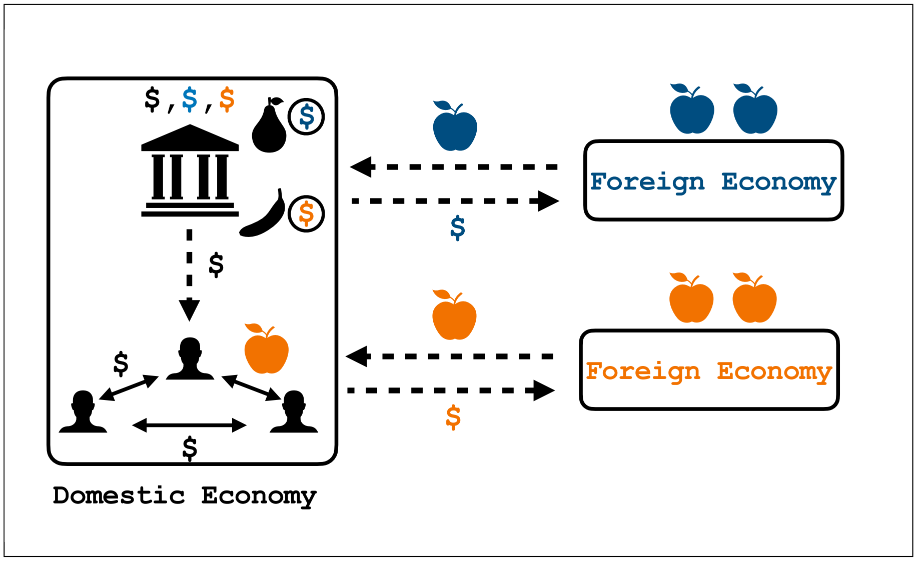


Figure 18: Algorand as the on-chain WTO. International trade agreements can be enforced programmatically, through the use of non-fungible sovereign currencies.

3.2.1.5 The Nation State's ICO: Crowdsourced Debt Offerings

In this world of CBDCs on Algorand, currency holders are active participants in national debt financing, with pro rata contributions guaranteed on-chain. Citizens can participate in foreign fiscal policy and customize their exposure to debt obligations. Instead of buying and selling standardized debt instruments, they use "governance rights" as "token holders" to fund specific debt obligations on-chain.

TradFi debt restructuring moves a web of bespoke agreements and international arbitration to simple on-chain instructions. CBDCs transform the inaccessible sovereign debt market into a borderless and capital efficient system. Governments crowdsource "debt offerings" where citizens participate directly, meaning that restructuring events happen at not just the national stage, but at an individual level – ultimately breaking the dichotomy between currency ownership and governance.

3.2.1.6 High Value Assets & The Marshallese Sovereign

The patched landscape of blockchain pragmatism fails to give decision makers the assurances they require for high-value deployments. CBDCs are a classic example. ***The economic bounty represents the sum of all transactions in an economy. We can rest assured that attackers will be motivated.***

Algorand's roundabout approach to technology makes it a prime candidate for CBDCs. In March of 2020, the Republic of the Marshall Islands became the first sovereign nation to announce its intention of deploying a CBDC on Algorand[32]. The Marshallese legislature embraced the idea of programmable monetary policy, committing to an algorithmically-fixed inflation rate of 4%. They announced an intention to crowdsource the sale of currency notes from domestic and global participants[33].

3.2.2 Global Payment Rails

It is hard to imagine a world where most payments are not digital by the end of the decade. WeChat and Alipay adoption in the East foreshadow a bigger push for global payments in parallel – and perhaps together with – the rise of CBDCs[34].

Why have crypto payments not taken off? For on-chain payments to be compelling, blockchains need to be a stepchange improvement. Why shift from PayPal or Visa (or rebuild PayPal and Visa on-chain) if we are migrating to patched systems that are slow but decentralized or fast but centralized?

This is where Algorand's new paradigm shines. It can support global payments systems that scale to billions of daily users, with < 5 second finality and future upgrades poised for sub-second finality. Algorand primitives allow payments providers to dip their feet into on-chain deployments slowly, with customizable RBACs and co-chains giving providers necessary assurances. Algorand customizability makes these on-chain migrations less "all or nothing" – and thus, we argue, more likely.

3.2.3 STOs & Asset Tokenization: The New Capital Markets

Just like payments, tokenization and securitization have been underwhelming. The pitch is simple: tokenize assets and bring the benefits of being on-chain to any asset or capital market. Why has this idea floundered?

From our perspective, the sluggish adoption of security tokens is not because of a weak value proposition, but because they came before DeFi. Without DeFi rails, what is the point? Now reimagine asset tokenization in a post-DeFi world: protocols collateralize real-world assets, generating yield and increasing the capital efficiency within any asset class.

3.2.3.1 Marrying Structured Finance With DeFi

As DeFi plumbing matures, structured finance becomes more compelling on-chain. Algorand is primed for digital securities and tokenized assets. ASAs allow issuers to wrap and exchange securities like any digital asset. Compliant issuers program customizable features into the ASA, monitoring and enforcing possession rights on-chain. This could slowly onboard legacy capital and disrupt every stage of finance from security issuance to investment banking, trading and institutional lending.

3.2.3.2 The Best Hedge: Programmable Compliance

Whenever securities are involved, regulatory needs are higher and more uncertain. The customizability of Algorand ASAs makes compliance programmable and gives issuers *regulatory optionality*. They can explore the market while adapting to its regulatory iterations.

[32] URL: https://www.algorand.com/resources/news/marshall-islands-to-power-worlds-first-national-digital.

[33] URL: https://www.algorand.com/resources/news/marshall-islands-to-power-worlds-first-national-digital.

[34] URL: https://www.theblockcrypto.com/post/111648/china-digital-yuan-whitepaper-smart-contract-programmability.

This is yet another example of how Algorand offers risk-averse capital comfort that cannot be found elsewhere. Issuers can port value on-chain, program in-built compliance tools and hedge their fundamental worries about the regulatory black box.

3.2.3.3 Open Financial Systems Prevent 2008

How big is the intersection between legacy capital markets and DeFi? It's hard to quantify a market that does not exist, but we can look back at some of the failings of TradFi and replay them on-chain. Think of 2008, where banks repackaged securities to the point that nobody knew what they were buying or selling. Credit agencies overstated the quality of tranched securities and the market completely mispriced counterparty risk[35].

On Algorand, depositors could have programmed default conditions by customizing their ASAs and allowing the system to algorithmically seize capital when interest payments were missed.

The mother of all blowups would not have happened on DeFi. Post-DeFi financial markets quantify counterparty risk and system leverage at any point in the game. If Algorand marries this post-DeFi opportunity with on-chain security issuance and asset tokenization, we could see a new golden age in structured finance without the excesses of 2008.

3.3 Algorand's Hybrid Experiments

If Algorand recasts "fast DeFi" without centralization or MEV and onboards TradFi with assurances and customizability, *then perhaps its ultimate product-market fit is the breeding ground for hybrid experiments between two otherwise separate worlds.*

This is DeFi backed by a real-world asset base and TradFi supercharged by crypto yield and composability, a win-win for both financial systems. Capital lives on a continuum: some is mercenary, some is risk-averse; most is somewhere in between. Hybrid experiments help different pools interact with one another and, while maintaining their own agenda, widen and diversify economic opportunities.

Below, we speculate on these hybrid experiments. We outline a few hypothetical examples, some very imaginative (likely years away) and others more concrete.

3.3.1 Increasing Capital Efficiency Through KYC

One of the biggest barriers to TradFi embracing DeFi is the mystery of Know Your Customer (KYC). DeFi is one massive pool of pseudonymous counterparties. Algorand's feature set could finetune KYC in DeFi. With the help of CoChains and ASA customizability, TradFi participants KYC what needs to be KYC'ed while DeFi markets extract out and freely trade everything else. Hybrid DeFi creates a granular view of the counterparty base, crucial for TradFi participation.

Let's use a concrete example: an emerging market wants to raise equity funding for rights to a future industrial project (i.e. a new building). They raise on-chain, distributing NFTs to global financiers who receive ownership rights to the project and its future cash flows.

Here is where it gets interesting: creditors could separate yield from the principal. ***Now, only KYC'd entities can redeem the principal or hold a representative token for the principal, but the yield can be set free: fractionalized, sold on a DEX and used as DeFi collateral.***

[35] URL: https://arringtonxrpcapital.com/2021/06/01/the-space-race-for-open-markets-vega/.

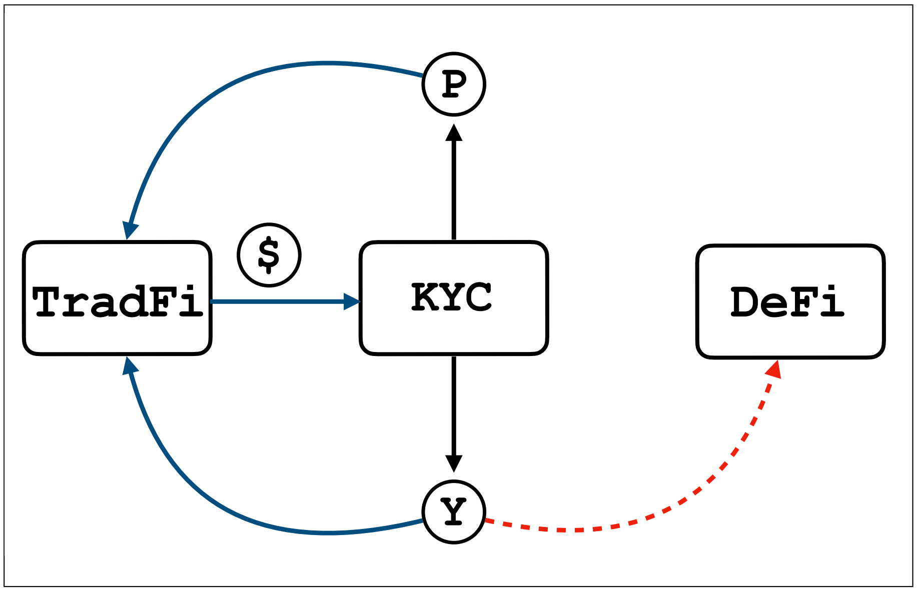


Figure 19: Increasing capital efficiency through strategic KYC. By separating the yield bearing element and principal element of a debt position, and by implementing KYC on the latter but not the former. That is, international, non KYC'd entities can indirectly participate in public debt markets.

There are three entities in our example: the government (the issuer), KYC'd entities (who can finance and redeem) and non KYC'd DeFi participants (who can neither finance nor redeem the principal, but can trade the yield).

Algorand could ultimately tokenize *future claims on equity*, separate out the principal and the yield and increase capital efficiency between KYC'd and non-KYC'ed capital.

3.3.2 Democratizing Credit Rating: Undercollateralized Lending

Algorand's RBAC feature creates unique possibilities in undercollateralized lending that (to our knowledge) cannot be executed elsewhere. RBACs allow creditors to redeem an outstanding principal upon a default, enabling undercollateralized lending without off-chain enforcement.

Speculative examples are straightforward. Non-speculative, commercial settings are more interesting. Imagine a builder takes on credit from a lender, using the loan to buy construction equipment from a vendor. *On-chain, the vendor sees that the payment is subject to an RBAC in the case of default.* Think of how this changes credit-scoring: in TradFi, creditors determine credit-worthiness based on aggregate payment history. In this case, the vendor determines credit-worthiness based on specialized and idiosyncratic metrics.

Banks run a crude process while the Algorand credit facility localizes credit scoring, making assessments more accurate, increasing capital efficiency and lowering default rates. ***Every vendor on Algorand is their own credit department.*** Vendors have local knowledge that banks who take a birds eye view would never be able to attain: if risk is high, they take the RBAC-assigned asset at a steep discount; if risk is low, they take the RBAC-assigned asset near par.

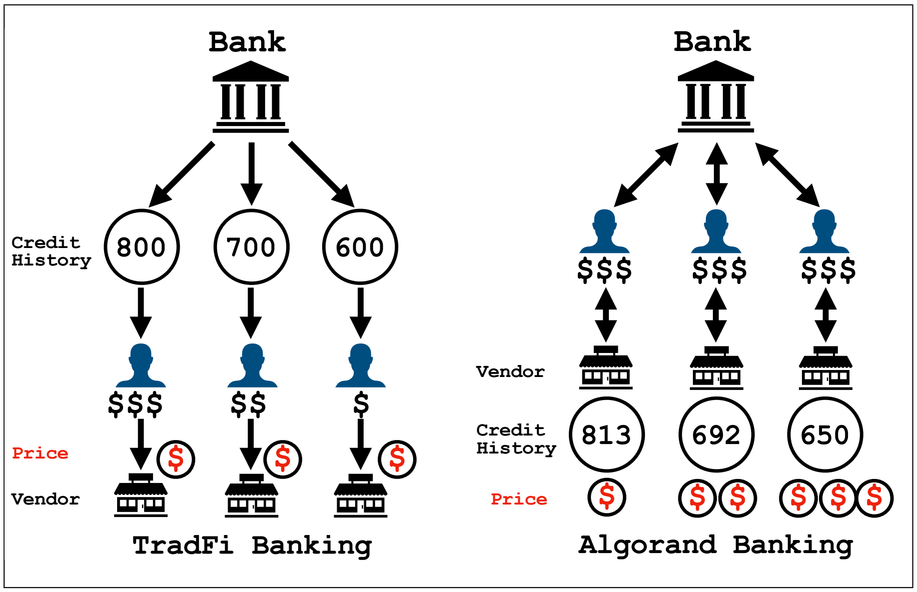


Figure 20: Algorand can enable the decentralization of credit rating, leaving the onus of due diligence to local industries. This can both increase capital efficiency and reduce delinquency rates in private markets.

3.3.3 Central Bank Yield Aggregators

We could imagine small sovereign nations (like the Marshall Islands) issuing anything from debt to CBDCs on-chain. Think of a country crowdsourcing debt offerings and running "international liquidity mining". With the help of ASA customizability, governments can issue assets while complying with international regulations.

Small countries could marry domestic opportunities with billions of dollars of worldwide DeFi liquidity, accessing pools of capital they would never otherwise touch. Conversely, DeFi farmers could diversify their yield generation into real-world, government-backed assets.

Take this a step further and imagine the concept of an Algorand-native yield aggregator bundling these unique sources of sovereign-backed fixed income into different packages. Farmers pick between structured products built on these "country coins", defined by the type of offering, geography, sector, project type and economic ranking (like debt to GDP ratios). *Just as farmers today who take more risk by LPing in newly issued, highly-speculative pools receive higher APYs in return, governments with higher debt to GDP and greater insolvency risk would offer investors higher yields.*

3.3.4 Marrying Old & New Currency Markets

Algorand could transform international FX, wedding old and new currency markets. Each country could have a CoChain where it deploys a CBDC and plugs into the super highway that is Algorand's public network. Once on Algorand, these currencies plug into DeFi protocols on Algorand and via bridges, any other ecosystem. In effect, Algorand becomes the bridge between international FX markets (built either on CBDC railing or issued as native stablecoins on top of Algorand, akin to USDC) and crypto-native markets.

3.3.5 Bringing Sovereign Debt To DeFi

Today, governments issue bonds through an auction process intermediated by qualified institutions like investment banks. These banks take these assets and sell them at a markup. What if the governments ran their auctions directly on-chain? They issue treasury bonds to any participant around the world, subject to KYC. This connects international bond markets with crypto fixed income: any government bond is now DeFi collateral. Conversely, this backs DeFi with a real-world asset base and expands crypto's total TVL.

3.3.6 The Evolution Of On-Chain Equity

Algorand could change how securities are issued as well as how shareholders interact with corporate structures[36]. Anyone around the world could KYC and buy IPOs on-chain through an Algorand wallet. Issuers leverage Algorand's customizability to tailor their shareholder base (say, by geography).

What if public companies issued ASAs and those ASAs granted on-chain dividends and governance rights? This streamlines corporate structure, wiping away the book-building rents of investment banking. These assets live on-chain natively and plug into any DeFi primitive.

Companies could take this a step further. Once they've issued equity, they can pursue other forms of financing like debt offerings. Think of Microstrategy's recent string of debt financing[37], on-chain and with a much wider capital base.

3.3.7 Connecting The Farmers & The Suits

We think this cross between DeFi and TradFi is an untapped market in its earliest innings. As DeFi matures, we will see new markets with KYC optionality and nuance amongst counterparties. By the same measure, the crypto farmer will diversify into asset pools tied to real-world economic activity, beyond self-referential yield. It's not that one is better than the other, but that each has something to offer.

Ironically – Algorand, the most "utopian" technical solution – could usher DeFi's transition from purist crypto-natives to a wider and more pragmatic capital base (without caving to blockchain pragmatism).

We conclude by referring back to the notion that Algorand escapes the war of blockchains, taking a less adversarial stance and instead extending an olive branch between the yield of the old world and the yield of the new.

[36] URL: https://www.prnewswire.com/news-releases/exodus-issues-security-token-on-algorand-expanding-access-to-the-growing-digital-security-ecosystem-301304582.html.

[37] URL: https://www.bloomberg.com/news/articles/2021-02-17/microstrategy-raises-bonds-for-bitcoin-offering-to-1-05-billion.

4 Risks

We are aggressively betting on the Algorand ecosystem. Nonetheless, it is important to understand the risks facing our thesis. What are these systemic and idiosyncratic risks?

1. Our thesis is premised on the idea that the market is underweighting decentralization. What if the market is right? ***What if decentralization does not actually matter as much as we think it does in the long run?*** Today's semi-centralized L1s are not fundamentally open systems, but what if capital markets do not need *open* systems? It's possible there is a diminishing return to decentralization. Nash equilibria can persist even against Pareto optimal conditions (or put simply, the market can remain "irrationally" decentralized longer than you can stay solvent).

2. A fast and safe delivery of ETH 2.0. In an ETH 1.0 world, Algorand has a major advantage: it is the only L1 that solves the trilemma. However, if ETH 2.0 is delivered faster than expected and Algorand's network effects are not strong enough by that point, it could lose some of this advantage.

3. Our argument relies on the idea that high-value assets and legacy financial systems will need a ground-up protocol of assurances. Capital on blockchains is like capital migrating to a new country: it wants stability and rule of law, tested over years. We also argue that the "build now, fix later" mentality of multi-chain DeFi creates tail risk and scares away risk-averse capital. However, it's possible that building ground-up assurances isn't the straightforward path to victory. *Systems that are not well-designed early on could decentralize after they secure product-market fit.*

4. If Algorand is poised to become a network for high-value assets and facilitates real-world on-chain capital flows, it needs more deployments, especially while it is accumulating a "time advantage" over other L1s.

5. While the ecosystem is growing, we think that two years in the wild with no downtime is enough evidence that Algorand's blockchain is sufficiently de-risked technically. In our view, there is now far more value in accumulating network effects across DeFi and TradFi ecosystems.

   The best technology does not always win. Think of the videotape format war, where Betamax[38] lost to VHS. The market often converges on inferior technology. We need to give credit to the serendipity of technology adoption. Sometimes market timing, marketing or luck beat the perfectly-designed – *mathematically so for Algorand* – technology.

[38] URL: https://medium.com/swlh/vhs-vs-beta-the-story-of-the-original-format-war-a5fd84668748.

Conclusion

The Enlightenment came after a series of political blowups – a long line of wars, revolutions and coups. Then came a new age of reason, symbolized by the birth of the American Republic. Similarly, blockchain may leave its dark age not by choice, but by force. The success of centralized networks invites their eventual demise – and that could be what we are seeing in today's DeFi wars. How do the wars of blockchain pragmatism end and what is the fallout of a market out of love with decentralization? What comes next, when all is said and done?

Algorand illuminates the dark age of blockchain because it both shows us what is missing in today's market but also brings together worlds that could never coexist previously. Sortition is a new kind of self-government, as novel today as the idea of America was in the 18th century. It merges BFT and Nakamoto consensus, scaling throughput and validator count. It is easy to reach consensus but difficult to subvert – it takes a microsecond for anyone to take part in but the age of the universe to subvert. It re-invents PoS without trending toward plutocracy. It allows anyone to participate in consensus without needing to know or rely on anyone else in the network. It transcends the divide between blockchain pragmatism and utopian decentralization. It is a put option on the dark age's failures but a call option on TradFi's on-chain migration. It is a home for both fast DeFi and risk-averse TradFi – for the new *hybrid experiment.*

The results of this new paradigm are compelling for both today's use cases and use cases in the future: 1,000 TPS, $<$ 5 second finality, true decentralization and two uninterrupted years in the wild – all at L1. Algorand continues to accumulate a time-advantage over its competitors bound by the trilemma, with future upgrades poised to scale throughput much higher while maintaining this core focus on decentralization.

Solving the trilemma – as much a political achievement as a technical one – unlocks new paradigms in "fast DeFi" and gives legacy capital a new, reassuring home. We are optimistic that the market will revive its old focus on decentralization and move past the current age of crypto's kings and mercenary capital, toward credibly neutral public networks that can deliver on the oldest aspirations of L1 scalability. That, in our view, is the promise of Algorand.

Lead Authors: *Ninos Mansor, Omar Yehia, Ninor Mansor*

Acknowledgements: *We are grateful to Algorand founders and employees that were interviewed and contributed to this work.*