CRYPTO LEADERS SINCE 2014

New Frontiers™

A DEEP-DIVE ANALYSIS OF THE COSMOS, POLKADOT, AND NEAR PROTOCOLS

Kent Barton

Head of Research and Development, ShapeShift

ShapeShift

Introduction

The year is 1982. Hollywood, Calif. is about to become the epicenter of the music world.

Each night, throngs of rabid fans crowd the Sunset Strip where dozens of music clubs cater to their auditory needs. Some clubs are larger and host more popular groups, while some are small underground affairs. Each venue provides customers access to something they can't get anywhere else: bands playing a new type of rock-and-roll that would soon take the world by storm.

In spandex.

Ideally, smart contract platforms will have more longevity than hair metal bands. But if you squint a bit, the world of smart contract blockchains is a lot like the Sunset Strip back in the day.

As you stroll down this thoroughfare, you can't help but get taken up in the excitement of it all. True paradigm shifts are a rare thing in life, but here you are, surrounded by legions of other blockchain enthusiasts, early adopters, starry-eyed newcomers, and developers. The sensation of critical mass is pervasive. On the neon horizon lies the tantalizing prospect of mainstream adoption.

Continuing your stroll, you see that the lion's share of the excitement is over at the well-established Club Ethereum. Inside, it's absolutely packed to the gills! The line to get in extends way around the block. Even with Club ETH's expensive ticket prices, everyone's clamoring to get in. And why not? Uniswap is headlining tonight, along with their friends Aave, Compound, and many others.

While it's tempting to get a ticket, you're not in the mood to deal with the crowds tonight. It would be nice if Club Ethereum actually expanded so more people could join the fun. In fact, out front is a sign touting some exciting plans: in a few years, they will be building a massive arena outside of town. It'll be state of the art, and they'll charge fans just a fraction of the current ticket price.

It sounds exciting, but man, a few years feels like a lifetime in a scene as vibrant as this. Over to the side you see that Club ETH is also gradually opening up a much bigger space next door called "layer 2." It's supposed to help relieve the crowd congestion, but it's not finished and not quite the same as the club you've come to know and love.

So—what else might the Crypto Strip offer?

A few blocks down you see that many enterprising club owners are eager to serve large crowds. Club Polkadot is downright cavernous. The problem is, the crowd's pretty thin; it's brand new and the place is just not very happening yet. Over at a joint called Cosmos, there are lots of massive rooms. Sounds great on paper, but they still haven't added doors between those rooms! You've also heard some cool things about the fancy new Club NEAR too, but is it worth your time?

Might as well go back to Club ETH where at least there's some action...

The State of Smart Contract Platforms: 2021

Giant aquanet hair and blistering guitar solos notwithstanding, this analogy is an apt description of where things stand now.

Ethereum is clearly where most of the action is. However, its current challenges with scaling have opened the doors to other smart contract blockchains, all aiming to do something similar: serve the needs of the masses while maintaining the magical properties of being trustless, immutable, permissionless, transparent, and censorship-resistant, which we've all come to love with decentralized networks like Bitcoin and Ethereum.

The problem is that many of these platforms don't have the critical mass of developers, users, and projects that Ethereum enjoys. For all their promise, they're also much newer. As such, they're struggling to gain the all-important mindshare of blockchain participants. In other cases, promising ecosystem growth has been hamstrung by a lack of crucial interoperability technology.

Yet, these issues are not intractable. In this report, we'll take a look at three smart contract platforms that are in a good position to overcome their respective challenges and have a significant impact on our industry in the coming year: the Cosmos, Polkadot, and NEAR Protocols.

Why just these three platforms? In addition to preventing this report from turning into a 100-page behemoth, our focus enables readers to compare and contrast these platforms, since each differs in important ways. But have no fear, Cardano fans—we'll take a closer look at that project and other emerging blockchains in a future report.

A note on semantics: I wish there were a sexier way of saying "smart contract platform," but what this term broadly refers to are blockchains that can run a wide variety of decentralized applications (DApps)—or, to borrow an analogy from Ethereum's earliest days, trustless, global, unstoppable computers. You might hear these more colloquially referred to as "ETH Killers," which is a ridiculous concept as it assumes a zero-sum environment. But I digress...

In this report we'll focus on several important attributes of these platforms—high-level architecture, consensus, governance, community/ecosystem, token distribution, and more—and see how they stack up against one another. We'll conclude with some takeaways and conclusions about how things might shape up in the coming year. We'll be comprehensive without getting lost in the technical weeds. If you'd like to go even deeper down the rabbit hole when you're done, the Further Reading section at the end is a good jumping-off point.

Also bear in mind: this technology is evolving quickly. While we've done our best to make this analysis evergreen, that's simply impossible in crypto; as we like to say in the space, three months in crypto is like three years in real-world time. While their high-level architecture is less likely to rapidly change, the supporting DApps, communities, and routes of implementation for blockchains can grow and shift in a heartbeat. Keep this in mind as you embark on your own learning journey.

Without further ado, let's crank those amps up to 11 and dig right in.

Table of Contents

01 Cosmos: Roll Your Own Blockchains

Cosmos: Roll Your Own Blockchains

Cosmos is a good starting point for our analysis. In addition to being the most established of the three platforms, ShapeShift also has extensive experience and institutional knowledge around this technology, thanks to our contributions to a decentralized Cosmos SDK blockchain (Microtick). It provides a nice baseline of sorts by which we can gauge its two newer counterparts.

If you're already familiar with Cosmos, the following section might serve more as a refresher. But take a quick look anyway; we'll provide additional context for our focal areas, discuss important recent developments, and create a good point of comparison for the other two projects.

Cosmos ICO'd back in the 2017 bubble and thus far has partially delivered on its vision. But as we'll see, there's more work to be done.

High-level Architecture

The fundamental idea behind Cosmos is that intractable scaling problems arise when you use a "one-blockchain-to-rule-them-all" approach. This is best exemplified by Ethereum, which employs a "shared security" model. Each DApp that runs on Ethereum is able to tap into the network's robust proof-of-work security. As a DApp creator, you've got plenty to worry about, but the security of the network isn't a big area of concern; you can launch a smart contract and immediately enjoy the peace of mind that comes with thousands of nodes and ample hashpower.

However, there's a major downside to shared security; it doesn't scale very well. This is because every single node in the network must process every transaction.

Cosmos's powerful insight was to eschew shared security in favor of an entirely different paradigm: give crypto projects the tools and environment to create their *own* blockchains, then connect them all using a specialized communication protocol. This approach ought to be far more scalable, the thinking goes, because nodes don't have to process transactions for an entire universe of DApps and transactions. Better yet, certain features of these blockchains (or "Zones," in Cosmos-speak), can be tweaked to meet the exact needs of the application that's running on it.

When dealing with Cosmos, one has to be careful with definitions. “Cosmos,” broadly speaking, refers to the various blockchains that use Tendermint consensus and the Cosmos SDK. This common design space should make it easier for them to talk to one another. But while we often refer to “Cosmos” as the myriad Zones that use this technology, this is separate from “Cosmos” the token (ATOM) and “Cosmos” the blockchain (Cosmos Hub), which we’ll cover shortly.

Hypothetically, anyone can spin up a Cosmos Zone. These run on delegated proof-of-stake (DPOS), where token holders can “bond” their tokens to validators running node software for the Zone. That’s where the security comes from.

This sounds awesome. But can you spot the big tradeoff behind this approach?

Trading Security for Scalability

Recall that with Ethereum DApps, it’s as easy as publishing your smart contract and tapping into the existing security of the entire network. Cosmos Zones, which are discrete blockchains, don’t have this advantage. Instead, they must create their own security by recruiting validators. This leads to two potential challenges:

1. *Creating a validator set out of thin air is no small task!*

It was interesting to see this evolve with Microtick in summer 2020. Overall it went pretty well, since the project had already generated a good amount of buzz in the Cosmos space and was also able to leverage ShapeShift’s contributions to the blockchain. But many new Zones won’t have this advantage; getting validators onboard could be an uphill and time-consuming battle. It’s a far cry from the “plug-and-play” consensus offered by shared security models.

2. *Per-Zone security is potentially far weaker than shared security.*

There’s no magic number for how many validators a Zone should have; that’s left up to the project. Microtick started with over 20, and now has more than 40 validators. The Cosmos Hub started with 100, and now has 150. Generally speaking, more validators means more decentralization and better security guarantees.

But how secure, exactly?

Even in proof-of-work land, we’ve seen how attackers can purchase enough hashpower to 51% attack networks such as Ethereum Classic and force block reorganizations in order to profit from double-spend transactions. Similar profit motives can lead to weaknesses in proof-of-stake networks, as we’ve seen with an apparent validator collusion cartel formed in EOS. As more money flows into the Cosmos world, the security of individual Zones will be tested.

The good news is that building your Zone's security isn't as hard as it sounds. Every Cosmos Zone uses a variant of a (somewhat) battle-tested blockchain consensus called Tendermint BFT, which provides block finality of three to six seconds and takes away the hassle of deciding which consensus mechanism to implement. Better yet, Zones also have the ability to recruit existing Cosmos Hub validators.

Bootstrapping Consensus

But what if this process could be even more frictionless? For DApps that don't want to bother with the hassle of recruiting their own validator sets, help may be on the way thanks to a project called LazyLedger.

LazyLedger is a simplified Tendermint blockchain that focuses solely on transaction ordering and data availability, not computation. In this paradigm, Zones could plug into LazyLedger's consensus and focus instead on their DApp-level functionality. This offers a tantalizing best-of-both-worlds approach where Zones take advantage of pre-existing security (facilitated by LazyLedger's own validator set), but also enjoy the advantages that come with building a bespoke blockchain that's customized for the DApp's functionality.

Both new Zones without validator sets and existing Zones will be able to build or improve their consensus thanks to the platform's data availability guarantees. LazyLedger's own security will come from a native token incentivizing its own validators.

Currently there is no LazyLedger Zone to speak of, and the validator set is not yet built out. However, given the sizable impact on Cosmos and LazyLedger's compelling value proposition, it's not hard to imagine the project building out robust security sometime in mid-2021. A successful launch of LazyLedger and its removal of validator-recruiting friction could be precisely what Cosmos needs to bring more DApps into the ecosystem.

Interoperability

The siren song of trust-minimized, cross-blockchain interoperability has been around for years, dating back to the idea of atomic swaps between Bitcoin and other chains. It's also been an elusive quarry for blockchain developers—something that's perpetually "on the roadmap."

Interoperability is especially important for Cosmos, as it's what allows there to be an "internet of blockchains" between Zones and bridging to other blockchain environments such as Ethereum. The protocol that aims to power Cosmos interoperability is called Inter-Blockchain Communication, or IBC. IBC has been in development for at least two years and is finally approaching production. Its core functionality is enabled by allowing each Zone to run light clients of other Zones.

IBC functionality is being rolled into something called "Stargate," which is a broader upgrade that also includes faster state syncing, full-featured light clients, and other behind-the-scenes improvements. The Stargate testnet went live in late-November 2020, and despite some hiccups with Zone integration, it appears highly likely that it will fully launch in January or February 2021. Following a successful IBC launch, transfers to and from external chains like Ethereum and Bitcoin will be facilitated by specialized chains called "Peg Zones."

When you zoom out and look at the current state of the ecosystem, it's remarkable that projects like Terra and Thorchain (both covered below) have enjoyed so much early success even without IBC! Once cross-chain liquidity, data-sharing, and "money lego" interoperability are unlocked, Cosmos will be well-positioned to realize its grand vision.

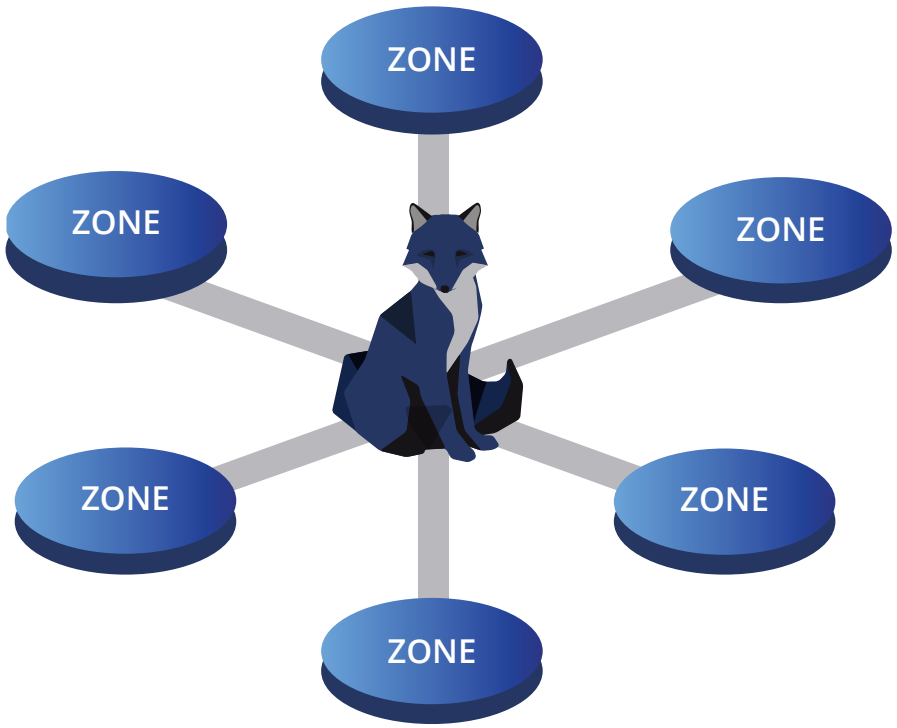
It's difficult to overstate this potential impact. As we'll explore later in the "Strategic Implications" section, the advent of IBC will likely be one of the most important developments in our industry in 2021.

Hub-and-Spoke

IBC sounds cool and elegant, but when you drill down and think about the implementation, there's a logistical problem: it's not feasible for each Zone to run light clients of dozens or other Zones. Data overhead, syncing problems, and other obstacles make this a non-starter given current technology.

The designers of Cosmos architected a clever way to deal with this limitation: a Hub-and-Spoke model where Zones (i.e., regular blockchains) connect to Hubs (blockchains that are designed to connect Zones to one another). The Cosmos website provides a succinct explanation of how this works:

> *When a Zone creates an IBC connection with a Hub, it can automatically send to and receive from every other Zone that is connected to it. As a result, each Zone only needs to establish a limited number of connections with a restricted set of Hubs. Hubs also prevent double spending among Zones. This means that when a Zone receives a token from a Hub, it only needs to trust the origin Zone of this token and the Hub.*



Source: Cosmos.network, https://cosmos.network/intro

Now we've arrived at the aforementioned Cosmos Hub. While there can be many hubs in the overall ecosystem, this Hub is special: it's the blockchain that's supported by the use of ATOM. It launched in March 2019 but thus far has been limited in its use; currently users can only send funds to and from other z Hub accounts. This will change once IBC is released and the Cosmos Hub can serve its designed purpose of facilitating the transfer of data across Zones. Given its central position in the ecosystem, many (if not most) DApps will initially connect through the Cosmos Hub. Over time, however, it's likely that many other Hubs will be created as well.

Governance

At its worst, on-chain governance feels a lot like decentralization theater. Sure, you're going through the motions, but is it really living up to the spirit of community-led decision making? One can also make a good argument that the off-chain approach is just fine; Bitcoin and Ethereum are thriving, after all, and on-chain governance raises the risk of oligarchies if it's poorly implemented.

On the other hand, in the absence of on-chain mechanisms, you run a greater risk of disruptive schisms like the BTC scaling wars or the ETC fork. Plus, decentralized governance is a good fit with the crypto ethos.

For Cosmos, governance is baked right into the protocol; it doesn't get much more on-chain than that! Each Zone can have its own governance mechanism. In practice, it's common to simply copy/paste the process that's used on Cosmos Hub. The process is elegant in its simplicity. Each validator can vote on community proposals, proportional to their total delegated stake. So, a Cosmos Hub validator holding 5% of the total delegated ATOMs would have a 5% influence over any given vote. Individual ATOM holders can vote on proposals directly from their wallets, or cede that decision to validators they've bonded to.

One potential downside of Cosmos's approach is that validators with more stake have more weight in any given vote. This raises potential centralization concerns, as larger validators have more influence at both the consensus and governance level. In practice, the community has actively encouraged holders to switch their delegations when there's a perception that validators are getting too large.

Potential challenges also loom in the overhead that's required to track and vote on proposals. Currently the overhead for validators isn't too onerous. However, it does take some time to fully grok each proposal, and then additional time for the team to come to a consensus on how to vote. If proposals start to become more frequent, validators might find it difficult to stay on top of the proceedings—particularly for those providing security on multiple Zones.

The real test of Cosmos governance will take place in the coming years, when there will presumably be a lot more at stake in the ecosystem. Thus far, however, it seems to be working well; on-chain modifications such as inflation rate can be implemented immediately at the code level, and proposals tend to trigger healthy communication debates and discussions.

Ecosystem

Cosmos has evolved into a thriving global community over the past two to three years. Attending a late-2019 Cosmos event in San Francisco, I was struck by how similar the vibe was to the earlier days of Ethereum; an underlying feeling of energy and excitement about what might arise out of this new take on blockchain technology. Developers representing dozens of projects were in attendance, all eager to connect and learn from speakers providing advice on how to create Cosmos DApps.

Meanwhile, meetup communities have formed in important crypto hubs like San Francisco, Seoul, and Berlin. Cosmos has also made serious inroads in Asia; several of the larger validators are based in South Korea, Taiwan, and Singapore. These things are difficult to quantify, but one gets the sense that there's a sufficient "critical mass" for Cosmos to thrive in the near-future.

In terms of more quantifiable metrics, a nuanced and well-researched recent report from the Crypto VC firm Electric Capital noted that the average number of Cosmos developers in Q3 2020 was around 260—roughly the same figure as the prior year. (By way of comparison, in Q3 Ethereum had around 2,300 average monthly developers.)

Those Cosmos developers are working on the protocol itself, infrastructural upgrades such as new wallets, and of course the actual DApps living on discrete Zones.

Additionally, there are a wide range of developer tools, open-source libraries, and a helpful community to answer questions related to building on Cosmos/Tendermint.

Notable Projects

Second to Ethereum, Cosmos arguably has the most vibrant ecosystem of DApps, providing it with an impressive first-mover advantage over other emerging smart contract platforms.

What's particularly impressive is the wide variety of DeFi-oriented projects. Notable examples include:

TERRA

Fast and cheap settlement for merchants, facilitated by native stablecoins. Terra has already achieved impressive traction in South Korea, leading to an annual transaction volume of more than $1 billion.

Thorchain

Trust-minimized automated market making (AMM), implemented in a cross-chain fashion. Once it's more decentralized, it could help realize the dream of trustless swaps between Bitcoin, Cosmos, Ethereum, and other blockchains.

Kava

Cross-chain DeFi lending facilitated by a native

Binance Chain

The exchange's eponymous DEX chain is built using a fork of Tendermint and Cosmos SDK, and it will presumably see more liquidity once IBC is released.

Agoric

A blockchain focused on robust smart contract security, with an eye toward financial use cases.

Brand Protocol & Microtick

Trust-minimized oracles on Cosmos. Band Protocol has a nice first-mover advantage, while Microtick is increasingly decentralized and poised to make serious inroads in 2021 following the launch of IBC.

It appears that nearly all of the necessary financial primitives to have a thriving DeFi ecosystem are present in Cosmos. Once IBC comes along, things could get very interesting since these projects will finally be able to interact with one another. There are many non-DeFi use cases as well, and shown by this exhaustive list of Cosmos/Tendermint projects.

Token Distribution

There's been a decent amount of hand-wringing on Crypto Twitter about the Gini Coefficient of various blockchains. The Gini Coefficient refers to how equally wealth is spread across a given environment. If the ghost of Karl Marx were to build a blockchain, its tokens would be evenly distributed to each account, and its Gini Coefficient would be zero. Alternatively, if I create my own Cosmos zone and give myself all the $KENT tokens, the Gini Coefficient would be one and I'd earn the wrath of Marx's ghost. You get the idea.

These discussions inevitably tend to devolve into conversations about the usefulness of the Gini Coefficient, and whether you can even measure wealth distribution in a pseudonymous environment. It's also important to note that for proof-of-work chains, disproportionate token holdings don't directly translate to extra influence over the network's security mechanism.

However, this all changes dramatically when you enter proof-of-stake (POS) land! In POS, larger holdings can directly translate to more influence over voting on blocks, leading to more centralization and a heightened risk that a single actor or group of actors can attack the chain's consensus. With this in mind, we'll be examining token distribution for each of the three projects in this analysis.

With respect to smart contract platforms, the most important factor determining token distribution is the manner in which the initial funding was conducted. If founders, venture capital firms, and other insiders received too large of a share of the tokens, there's a greater probability that these centralized chickens will come home to roost some day, threatening the security of the blockchain.

What constitutes "too large"? Clearly, anything over 50% for insiders would be undesirable; one entity holding a simple majority is not conducive to centralization. In the context of Tenermint-based chains, the "danger" level lies closer to 30-35%.

In the case of Cosmos, its public ICO led to a relatively favorable split between insiders and other holders. As of Q4 2020, insiders held only 20% of the overall supply of ATOMs. This augurs well for the overall decentralization of the Cosmos Hub.

As we've seen, Cosmos Zones can also have their own native staking token(s). Users of these Zones will need to consider how those tokens are distributed, and Zone creators should carefully consider the implications of their distribution plans. For instance, the genesis distribution of Microtick's native staking token (TICK) was such that the two largest holders only received 10% each, with the majority given to new validators or designated for community use.

Of course, Cosmos isn't alone in finding new ways to leverage tokenized value at the protocol level. Now that we've gotten our foxy heads around how scalability can be achieved by allowing each DApp to have its own blockchain, let's consider an entirely different approach...

02 Polkadot: Scalability Through Sharding

The self-sovereign-blockchain-per-DApp model employed by Cosmos is compelling. On the other hand, shared security has worked very nicely with Ethereum (scaling shortcomings notwithstanding). So why not stick with this proven model while making some fundamental changes that allow it to scale?

This is precisely what some smart contract blockchains are trying to do. Ethereum has embraced this approach with Ethereum 2.0. NEAR Protocol is using shared security as well, as we'll see in our next section. And it's also part-and-parcel of the emerging blockchain ecosystem that is Polkadot.

The path to scalable shared security lies in a concept called sharding. The basic premise of this concept is pretty straightforward. In Ethereum 1.0, scalability is limited by the fact that every single node must process every single transaction. (Sure, you could simply require that each node processes more transactions, but that would translate to fewer, more expensive nodes, thus hampering efforts to be maximally decentralized.)

Sharding splits things up and allows each node to process only a specific subset of transactions. Scalability increases proportionally with how many of these subsets (or shards) exist on the network. So, all things considered equal, 64 shards would provide a 64x increase in transaction throughput.

The devil's in the details here, and things get fiendishly complex once you start to consider how all those shards will talk to one another. But years of research have borne fruit, and Polkadot is a prime example.

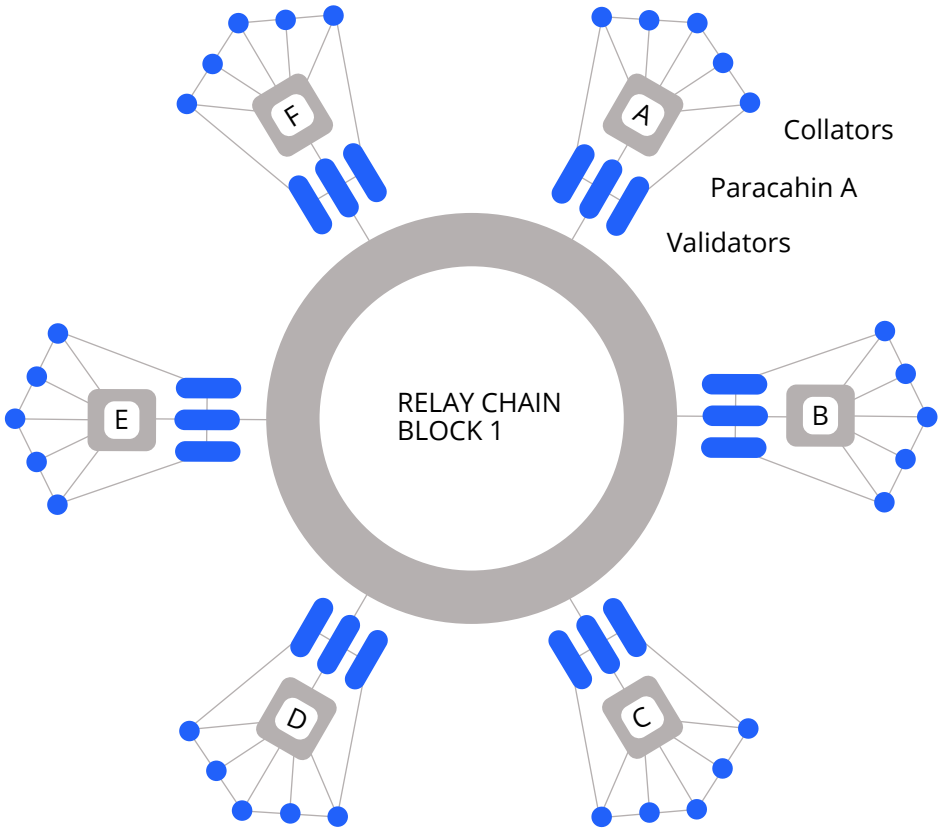
Polkadot is the brainchild of Gavin Wood and Parity Technologies. Wood knows blockchains; he was the author of Ethereum's Yellow Paper, which laid out how the Ethereum Virtual Computer (EVM) would operate. The Parity client provided invaluable redundancy and saved Ethereum from a disastrous chain halt when the more widely-used Geth client was DDOS'd in 2016.

Over time, however, Wood began to articulate a vision that marked a clear departure from both Ethereum 1.0 and the sharding plans for Ethereum 2.0. The resulting Polkadot project was funded via a 2017 ICO and two subsequent rounds of private funding, eventually leading to a mainnet launch in June 2020.

High-level Architecture

As noted above, Polkadot employs a shared-security mechanism. In this model, one primary chain (the Relay Chain) is tasked with ensuring everything runs smoothly. It provides consensus and passes messages between its constituent shards, with blocktimes of six seconds and finality guarantees of roughly 60 seconds.

Those shards, which are independent-yet-connected blockchains, are where things get interesting. In a contrast to the Cosmos approach of giving each blockchain its own consensus mechanism, they instead rely on the Relay Chain to serve that function. Hence, we have shared security, as shown here with multiple chains connecting to the Relay Chain:



Source: The Plasm Network, https://docs.plasmnet.io/ecosystem/polkadot

Enter the Parachain

Each of the blockchains running under the Polkadot Relay Chain is called a Parachain. This name comes from the fact that every Parachain is designed to run in parallel with one another. Wood likens them to cores in a CPU:

> *(Cores) do different workloads. One of them might be processing smart contract transactions, another might be processing balance transfers like kind of Bitcoin transfer transactions. Another one might be doing governance. Another one might be calculating what the optimum staking situation is. So each of these cores, each of these parachains, can do different things at any given time.*

In a nutshell, this parallel processing is how Polkadot achieves scalability. Currently, Polkadot is designed to support up to 100 Parachains, with a total scalability ceiling of up to 100,000 TPS.

Note that unlike Cosmos, where anyone can spin up a Zone, Parachains are a finite resource since there's a maximum of 100. Access to this resource is metered by Parachain auctions. Winners of these auctions (which are denominated in DOT) earn the right to use a Parachain for 6, 12, 18, or 24 months.

Interestingly, Parachains can also differ from one another in important ways. Even though they share the security of the Relay Chain, they can employ differing logic at the code level. This could be useful, for example, in implementing a Parachain with privacy-preserving properties. And in cases where it makes economic sense, Parachains can also have their own tokens. In practice, we have yet to see many DApps effectively employ this approach, but the coming year will likely see a lot of experimentation on this front. (In this sense, Parachains enjoy some of the attributes of Cosmos Zones – i.e., logic and tokens of their own—while also using the same type of shared-security approach employed by Ethereum and NEAR.)

One important question remains unanswered in these relatively early days: can Polkadot provide the seamless money-lego composability that DeFi users have come to expect in Ethereum, or does the Parachain architecture make this more difficult? 2021 should provide some answers as more Polkadot-based DeFi DApps come online.

Parathreads

Projects can purchase their own Parachain slots. But what about DApps that use the chain less frequently? For this type of use case, Polkadot has introduced the concept of Parathreads.

Parathreads allow parachains to take advantage of Polkadot's security without having to purchase a parachain lease. The upshot is that projects that would otherwise be priced out of Polkadot (because Parachain slots are too expensive) can instead pay a per-block fee and connect to the platform via a Parathread.

This is a clever and possibly necessary design decision by Polkadot; in order to make the chain extensible and scalable well into the future, there needs to be some mechanism that allows all manner of DApps, large and small, access to the blockchain. Parathreads facilitate this.

However, there are some big unknowns here. For starters, there are few projects currently using Parathreads, possibly because Parachains themselves don't yet have high demand. Thus, it's hard to say how well this works at scale. Additionally, in some scenarios it may be impossible to guarantee that Parachain transactions get included in every block.

So: Parathreads. Cool idea, but you may want to wait until it's proven out at scale.

Consensus Mechanism

Polkadot employs a variant of POS called Nominated Proof of Stake (NPOS). This approach has some similarities to Cosmos, where ATOM holders can delegate their DOT tokens to a finite number of validators. In Polkadot, there's also a finite number of validators – the total number is determined by governance – along with a bonding/unbonding period of 28 days (as opposed to 21 days in Cosmos).

Unlike Cosmos, each Polkadot validator has an equal say in what happens on chain; validators with more delegations don't get to vote on more blocks. Spinning up a validator requires more than 350 DOTs. As of this writing there are around 260 Polkadot validators. However, the number of discrete entities is likely a good deal smaller; one actor can increase profitability by spinning up multiple nodes.

While the specifics may vary, the Polkadot validator incentive model is similar to Cosmos. Validators are rewarded via DOT inflation (currently around 9%) that changes depending on how much total DOT is staked, along with transaction fees. Additionally, validators also have the option of charging a commission on nominated DOTs.

Interoperability

Polkadot is building out a set of cross-chain protocols it sensibly refers to as “Bridges.” (Note that this refers specifically to Polkadot interacting with separate blockchains like Ethereum, and not to interaction between Parachains.)

On the Polkadot side of things, one endpoint of these cross-chain connections is a Bridge Contract that receives messages from the external chain. On the other blockchain is a smart contract that facilitates cross-chain value transfers. This dual-contract system sounds fairly straightforward, and is similar to interoperability solutions being developed in other crypto ecosystems.

Polkadot also features Bridge Modules, which may allow an external blockchain’s functionality to be replicated or extended in a Parachain.

At least six teams are working on Bridges to various blockchains, including Ethereum, Bitcoin, Cosmos/Tendermint, and EOS. However, the timeline for when any of these might be functional is unclear. Given the importance of drawing DeFi liquidity from Ethereum, it’s crucial that Polkadot has operable Bridges in 2021. Otherwise, it may run the risk of becoming an insular, slow-growing ecosystem.

Governance

Compared to Cosmos's relatively straightforward approach, Polkadot's governance process is more complex. A few key concepts:

Referendums: Anyone depositing a fixed amount of tokens can propose a referendum. DOT holders can then vote on these proposals either directly or by temporarily locking their DOTs. Locked votes are weighted more heavily than direct votes. Cleverly, this locking mechanism discourages vote buying.

Councils: Perhaps inspired by local councils in Wood's native England, Polkadot Councils "are an on-chain entity comprising a number of actors, each represented as an on-chain account...called upon primarily for three tasks of governance: proposing sensible referenda, cancelling uncontroversially dangerous or malicious referenda, and electing the technical committee." These Councils get complicated. There are "Prime Members," "Technical Committees," proposals to blacklists, and council appeals.

The added complexity of Polkadot's governance raises some potential issues. For one, it's difficult to grok and far less intuitive than alternative approaches such as Cosmos. Many would-be governance participants may be dissuaded by a perception that Polkadot is grafting elements of real-world Kafkaesque bureaucracy onto the platform.

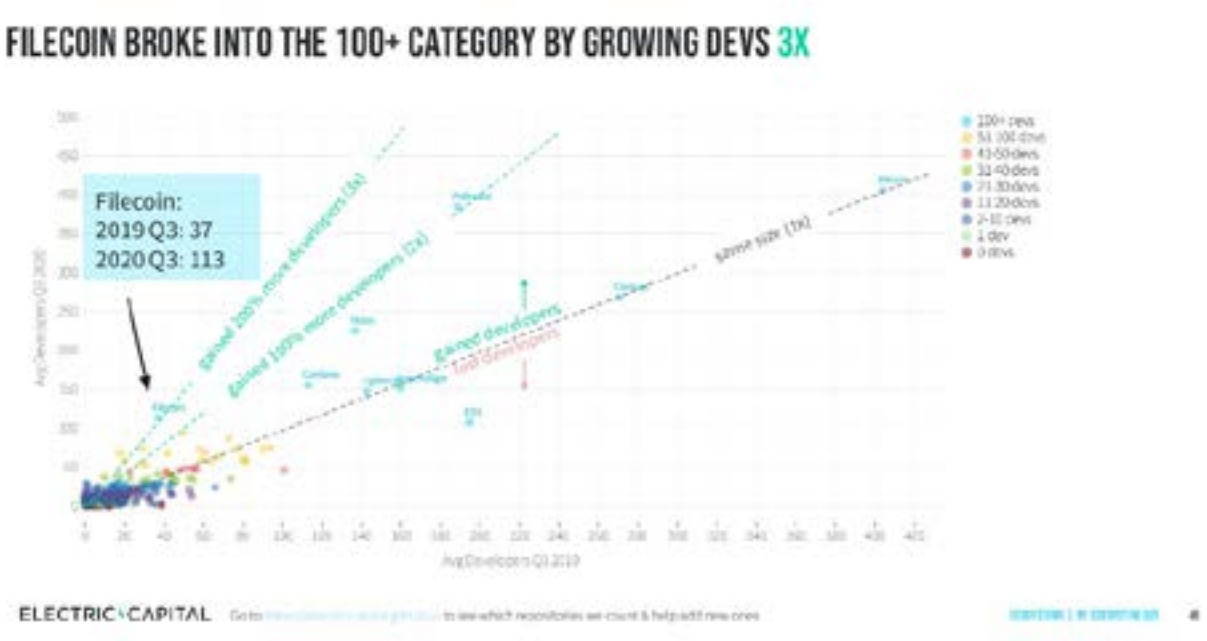
Additionally, the introduction of Councils that wield unique powers raises the specter of centralization. So while Polkadot's efforts to introduce a more nuanced form of governance are interesting, ultimately they might be counterproductive to the underlying goal of bringing decentralized decision-making to blockchains. Time will tell.

Ecosystem

Polkadot has been on the radar of blockchain developers for a few years. Now that the platform is live, its scalable architecture is paying dividends. This can partially be attributed to Substrate, an application framework that makes it easy for developers to tap into the consensus and networking functions of the Relay Chain.

Impressively, Polkadot doubled its developer count in over one year, growing to nearly 400 average monthly developers in Q3 of 2020. That's roughly equal to the number of developers contributing to Bitcoin. This growth looks particularly strong when compared to where Ethereum was just two years into its launch (although one can argue that Ethereum had to do the hard work of bootstrapping an entire new type of blockchain ecosystem).

CHART (p. 48): https://medium.com/electric-capital/electric-capital-developer-report-2020-9417165c6444



This listing site counts more than 300 projects in Polkadot, spanning across DApps, developer tooling, infrastructure, and wallets. Taken together, the rising number of developers and diverse range of projects paints a picture of a nascent-yet-healthy ecosystem.

Notable Projects

Kusama

Testnet Schmestnet. Kusama is an Polkadot fork incentivized testnet, where protocol and parachain developers can experiment in an environment where there are economic consequences via Kusama's native token.

Moonbeam

Ethereum's EVM on Polkadot. Solidity support and built-in ERC-20 compatibility could make this a compelling choice for existing Ethereum DApps; there's already a proposal to port over Sushiswap.

Acala

This project is bringing DeFi to Polkadot via a stablecoin, lending protocol, and DEX. More than $50 million was locked in a recent Acala testnet, which bodes well for adoption once it goes into production (possibly sometime in the next few months).

Polkaswap

As you might guess from its name, Polkaswap is trying to port Uniswap-like AMM functionality to the Polkadot world.

Token Distribution

Polkadot's fundraising did not exactly go smoothly. Although the initial 2017 ICO was a wild success (raising $140 million), more than half of those funds were famously locked in the Parity multi-sig wallet exploit on Ethereum. One hopes that the auditing process that was applied to Polkadot is much more robust than what Parity was using three to four years ago! While Wood insists that Polkadot's audits were extensive, the multi-sig exploit provides a persistent reminder about the dangers of coding smart contracts.

Two rounds of private funding helped recoup those losses, and the project soldiered on. Now that the dust has settled and the project is live, Parity Technologies still owns roughly 30% of all DOTs, with insiders owning another 5%. While there's no hard-and-fast rule about what constitutes too much token decentralization, it's not hard to imagine how a single actor holding roughly a third of the voting power could be problematic in a POS environment with on-chain governance—particularly in light of the fact that Polkadot's finality mechanism can fail if more than 20% of the nodes are byzantine (i.e., failing to act, or acting maliciously). Moving forward, Polkadot may struggle with perceptions of centralization unless Parity makes a concerted effort to distribute its holdings.

03 NEAR Protocol: Room to Grow

We've saved the newest platform for last. NEAR's unrestricted public mainnet launched in October 2020 and is the creation of Illia Polosukhin and Alexander Skidanov, two experienced engineers who didn't enter the crypto space until 2017-2018.

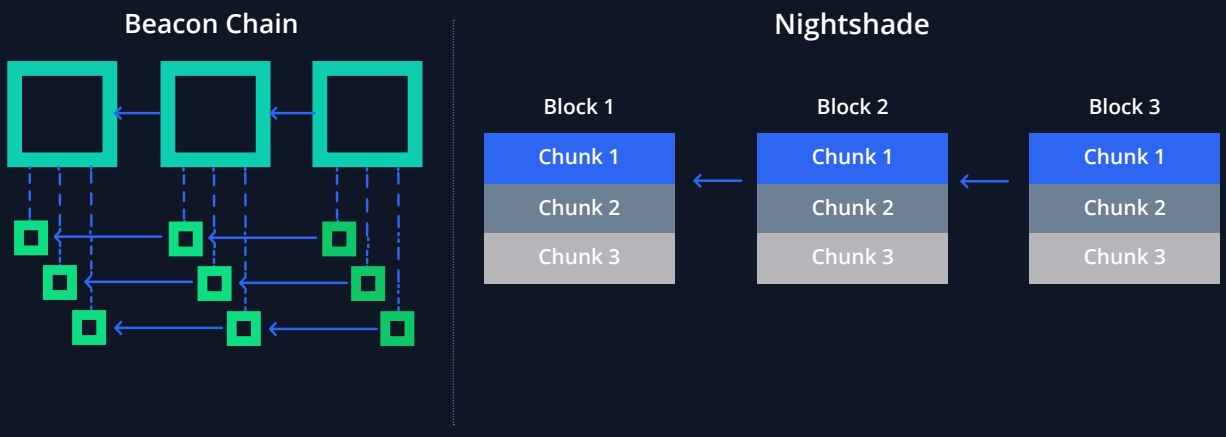
As we'll see shortly, NEAR attempts to distinguish itself from the many other smart contract alternatives by being as developer-friendly as possible. Similar to Polkadot and Ethereum 2.0, the platform aims to provide a scalable, trust-minimized blockchain through sharding in a shared-security context.

NEAR's founders previously developed non-blockchain sharded databases in roles at Google and Microsoft. This big tech street cred helped attract pre-launch funding from the likes of a16z, who led a $21 million funding round in March 2020. After pivoting into crypto, their widely shared whiteboard series evinced an exhaustive knowledge of blockchain scaling and sharding—including the pros and cons of the approaches employed by Ethereum 2.0 and Polkadot.

High-level Architecture

Although NEAR is similar to Ethereum 2.0 and Polkadot in its decision to use sharding, there are important differences in its implementation. NEAR employs a custom-built sharding mechanism called Nightshade. In tandem with a block production method called Doomslug (yes, Doomslug), the platform claims a lofty ceiling of 100,000 TPS.

The most striking difference between NEAR and Polkadot is that in the former, shards are not designed to be separate, discrete blockchains. Instead, they're implemented as "chunks" in each mainnet block.



Source: Nightshade: Near Protocol Sharding Design, July 2019, https://near.org/downloads/Nightshade.pdf

Each shard is secured by a subset of validator nodes, which in turn broadcast the state of the shard as a chunk of every new block. Each NEAR block is a combination of those chunks, as shown above. Note the contrast to the "Beacon Chain" approach on the left, where a primary chain (such as the Relay Chain in Polkadot) provides security for separate shard blockchains.

This chunked approach has a nice upside: it's not necessary for validators to download the blockchain's entire state. This reduces the hardware requirements for nodes and makes it easier to build light clients, thus benefiting the decentralization of the network. Hypothetically this could also facilitate the development of mobile-friendly clients—something that's on NEAR's roadmap.

Currently there's only one shard on NEAR. Additional shards are planned in order to deal with increased demand. This will be a big test of NEAR, since cross-shard communication is one of the most difficult parts of running a sharded blockchain.

Consensus Mechanism

NEAR uses its own unique variant of POS: a validator election mechanism called Thresholded Proof-of-Stake (TPOS) that enables blocktimes of one second and transaction finality of two to three seconds.

Unlike Cosmos, there's no in-protocol method for delegation. Instead, individual NEAR holders either need to stake directly, or contribute to third-party smart contract pools. Another notable difference is the unbonding period of 24-36 hours, which is far more frictionless than the three-week and four-week periods used by Cosmos and Polkadot, respectively. NEAR's inflationary block rewards are fixed at 5% APY.

In TPOS, because the reward is proportional to the stake, there's no benefit to pooling staked tokens. This hypothetically could improve the network's decentralization, since there's less of an incentive to pool resources. Contrast this to Cosmos, where a single validator could accrue a disproportionate amount of delegated stake.

Validator slots are limited to 100 "seats" per shard. The cost of purchasing a seat depends on the total amount of NEAR being staked, and validators and delegators can unstake (or unbond) at any time.

Interoperability

NEAR has embraced interoperability—especially with its ETH-NEAR "Rainbow Bridge." This Bridge consists of an Ethereum light client implemented in Rust as a NEAR contract, and a NEAR light client implemented in Solidity as an Ethereum contract.

The prospect of trustless transfers between the two chains is promising. However, there are some limitations with respect to finality. AS NEAR points out, "For ETH->NEAR interactions, the latency is the speed of producing X Ethereum blocks, which is about 6 minutes for 25 blocks. For NEAR->ETH interactions, the latency is 4 hours, and it will be about 14 seconds once EIP-665 is accepted."

Four hours is not great. But hey, this EIP-665 (which is an Ethereum Improvement Proposal, not a Star Wars droid) will make things much better. Sounds doable, right?!

The problem is that the EIP, which introduces precompiles for a certain type of signature curve (Ed25519), is not on the roadmap for inclusion in an upcoming hard fork. Additionally, there's been some debate in the Ethereum developer community about the impact of adding new precompiles. As such, it's not clear whether this EIP will be implemented in the next one to two years, if at all.

For some use cases, four-hour latency will be acceptable. For others, there may be an opportunity for third parties to ease the friction by facilitating faster withdrawals to the ETH chain.

The Rainbow Bridge still remains in testnet form but looks to be in good shape for release sometime in 2021. The NEAR team has given a lot of thought to the implementation details and edge cases (for instance, how do you maintain compatibility if Ethereum implements a hard fork?), and has also opened the spec up to incentivized hacking. If the Bridge is successful, it'll position NEAR as a low-cost scalable alternative to the various Layer 2 platforms emerging in the ETH space.

Governance

NEAR adds a few elements of on-chain governance without going, uh, nearly as far as Cosmos or Polkadot.

In fact, the White Paper expresses skepticism about relying too heavily on the on-chain approach as it "...suffers from the need to very clearly specify each case, has potential problems arising from a lack of "human common sense" around some decisions, and is therefore vulnerable to certain attacks that an off-chain process would not be."

In the absence of clearly stated rules, NEAR's governance process feels somewhat half-baked. Currently only validators can vote on proposals. Their assent is what led to the launch of NEAR's unrestricted mainnet.

Proposals and governance discussions take place on a community board. In this sense, NEAR seems to be replicating the social off-chain layer of Ethereum. Moving forward, it'll be interesting to see if the community can give more meat to these governance bones; currently, it all seems a bit ad-hoc and not thoroughly defined.

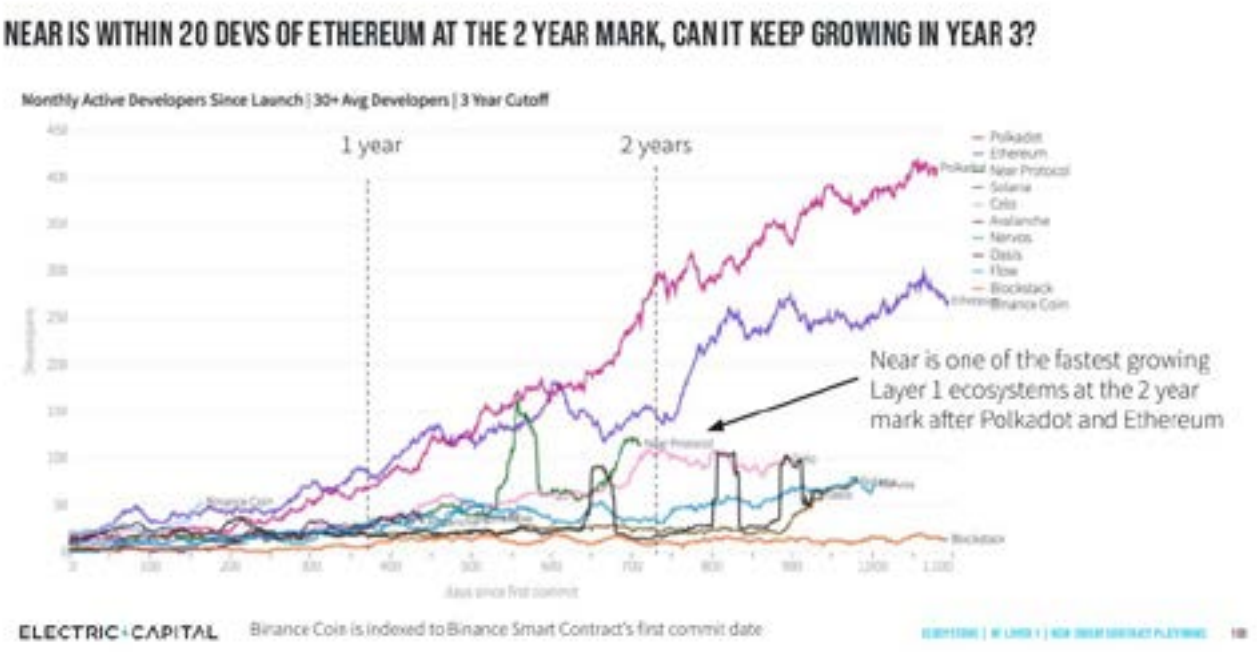
Governance centralization is a concern as well, as we'll explore shortly in the Token Distribution section.

Ecosystem

Relative to Cosmos and Polkadot, NEAR has a smaller ecosystem. Yet it's also punching above its weight, considering its "relative newcomer" status.

As Electric Capital (an investor in NEAR) notes below, the growth of platform developers is impressive considering its brief life:

CHART (p. 103): https://medium.com/electric-capital/electric-capital-developer-report-2020-9417165c6444



NEAR has gone to great lengths to position itself as developer-friendly. Its nodes run WASM, a standard that runs in most browsers. Smart contracts can be built in Rust or a variant of JavaScript. The NEAR team has created a development environment to provide one-click deploys, unit testing, deploys, and other essential tools. This could help the platform continue its developer growth, although it's worth noting that Ethereum has made massive strides in the dev-tooling area as well. NEAR has also implemented a clever way to make transaction fees more frictionless: similar to meta transactions on Ethereum, developers can subsidize users' fees from accounts maintained by the DApp.

Notable Projects

Flux

This is a NEAR DApp that's native to NEAR itself. Flux's decentralized prediction markets price the likelihood of events as derivatives. It remains to be seen what oracle technology will be used to determine the outcome of these markets.

Mintbase

A broad-based NFT market that focuses on the overall NFT space, rather than a specific niche such as gaming or art. Mintbase started on Ethereum but recently raised a $1 million round to bring its market to NEAR.

More interestingly, NEAR's website lists several well-known Ethereum DeFi DApps as projects "in development," including AAVE, Maker, Chainlink, and Balancer. Of these, the last two appear to be the furthest along; Chainlink oracles are already running on NEAR, and Balancer has offered integration grants to facilitate the integration.

Overall (and especially compared to Cosmos and Polkadot), NEAR doesn't have as many projects in its ecosystem. In order to gain traction, it'll need to recruit more DApps and developers in 2021 or run the risk of becoming a blockchain ghost town. However, the ecosystem's friendliness to both users and developers make this scenario less likely.

Token Distribution

One of the potentially problematic areas for NEAR is the fact that 35% of its token's supply is held by insiders. NEAR raised millions before conducting a public ICO in 2020. As a result, distribution is skewed toward insiders and early investors.

As noted previously, concentrated token distributions are problematic in a proof-of-stake paradigm. NEAR's partially-on-chain governance also raises the specter of centralized decision-making. Perhaps more of an issue is the fact that the NEAR Foundation (a non-profit that counts one of NEAR's co-founders as a board member) gets to decide who makes technical upgrades, and who's responsible for holding/distributing funds. The protocol also runs the risk of being overly dependent on NEAR Inc. – the private entity behind the project and the main driver behind adding new features and functions.

To be clear, there's nothing about this arrangement that would prevent NEAR from becoming more decentralized. Token distribution may become more balanced thanks to validating and trading, and it's possible that over time the community will begin to take over from NEAR's foundational entities, much like we've seen in Ethereum. The NEAR team is highly knowledgeable and seems to understand in the crypto ethos. In these early stages, however, NEAR may face a challenge in convincing developers and users that the platform is secure, scalable, and maximally decentralized.

04 Compare & Contrast

As we've seen, while these three projects all have some broad similarities, they also differ in important ways. Here's a quick summary:

	Cosmos	Polkadot	Near
Native Token/Market Cap	Atom (Cosmos Hub) /1.3billion	DOT / $5.3 billion	NEAR/233 million
Architecture	Discrete blockchains (Zones) connected to one another via a hub-and-spoke model	Shared security. Relay Chain provides security and facilitates communication between heterogenous shards (Parachains)	Shared security. Homogenous shared are grouped into chunks and talk to one another
Permissionlessness	Anycan create a Zone, but must also recruit a validator set for secruity and consensus	Access to 100 Parachains is metered through an auction process. However, separate Parachains can be accessed by purchasing Parathreads.	Anyone can build a DApp on NEAR and tap into its shared security
Consensus Mechanism	Tendermint BFT and Delegated Proof of Stake (DPOS) facilitates up to 1000 TPS per zone. Variable ATOM inflation, currently at 7.0	Nominated Proof of Stake (NPOS), plus parachains, offer up to 100K TPS. Variable inflation, currently at 9.1%	Thresholded Proof-of-Stake (TOPS) facilitates up to 100K TPS in a sharded context. Fixed inflation at 5%
Staking Mechanics	ATOM holders can set up specialized nodes; the largest 150 nodes validate the Cosmos Hub. Non-validatros can earn rewards by delegating to these nodes.	DOT holders can "purchase" a validator for a variable cost - currently around 350 DOT. Non-validators can earn rewards by delegating or "nominating" these	NEAR holders can purchase one of a 100 validator "seats" per shard. Non-validatros can delegate tokens to these validators, and unbond at anytime.
Unbonding Period	21 days	28 days	24-36 hours
Governance	Fully on-chain governance module for voting on community proposals and enacting approved changes at the code level.	Complex on-chain voting featuring multiple layers, including Governance Councils and Technical Committees.	Limited governance where voting is currently only limited to validators. The White Paper expresses scepticism about taking too much goverance on chain.
Average Monthly Developers	260	400	125
Total Projects(DApps, wallets and other infrastructure)	125-150	300	10-20

Source: ShapeShift, 2021.

05 Key Takeaways

Whew! We've covered a lot of ground, and we've seen how these three platforms built different solutions to vexing challenges like blockchain security, scaling, and governance

1. *There is no "one-size-fits-all" smart contract blockchain.*

While all three platforms offer scalability that far exceeds what's possible on ETH 1.0, there are substantial differences as outlined above. Some projects may opt for Cosmos's blockchain self-sovereignty, complete with their own tokens and validators. Others may eschew that path in favor of shared security offered by chains like Polkadot and NEAR. With each platform offering a unique set of tradeoffs and governance options, DApps will self-select and find the solution that fits them best. Expect DEXs and AMMs to evolve quickly on these chains. On this front, Cosmos will likely see a Cambrian Explosion of DeFi DApps following the launch of IBC. Similarly, crypto users will want to keep tabs on how DEX evolution is proceeding in Polkadot and NEAR, as well as monitor how cross-chain pegs are evolving.

2. *There will be bugs and growing pains.*

Risks abound in the crypto space, and that's especially true of newer platforms. Can Cosmos Zones sufficiently scale their validator security as IBC opens the floodgates to liquidity? Does Polkadot's clever Parachain/Parathread architecture have hidden pitfalls at the code or game-theoretical levels? For all the deep thought that went into NEAR's take on sharding, could its consensus mechanism hold up to the game-theoretical rigor that comes with a market cap in the billions?

Also consider the new functionality opened up by these novel approaches to scaling—functionality that developers and users might not even be aware of yet. For instance, the rise of flash loans has led to an entirely new type of financial behavior in DeFi. This uncovered both benefits and potential risks for DApps, as shown by the myriad flash loan exploits in the second half of 2020. Emerging blockchain ecosystems will likely have their own version of flash loans—powerful new abilities that expose users to a loss of funds.

3. *Perceptions of centralization will help determine which smart contract platforms thrive, and which fail to gain traction.*

All three of these blockchains make lofty claims for scalability, and claim to do so without sacrificing decentralization. However, each has centralization risks: Cosmos with its Zone validator sets, and Polkadot and NEAR with their relatively high insider token allocations. Even if these don't cause ongoing issues, there's a sizable subset of projects and users that may opt for blockchains that are seen as more decentralized. This dynamic has already played out in EOS, where evidence of validator collusion seems to have played a role in the platform's anemic developer growth over the past year.

4. *2021 is Cosmos's time to shine.*

The Cosmos Hub is closing in on two years of liveness and security. That's an impressive track record! Meanwhile, Zones like Terra are providing useful services to users, processing hundreds of millions in transactions and delivering value to validators in the process. Now that the fundamentals have been proven out, here comes IBC with its glorious promises of cross-Zone and cross-chain liquidity. It sounds amazing on paper. How will it translate in practice?

5. *Proof of Stake – so hot right now.*

One common thread unites the three chains we've just examined: these platforms (along with Ethereum 2.0) all use proof of stake. Just a few years ago, POS appeared to be a promising-but-unproven mechanism, existing more in white papers than on production blockchains. Cosmos's two years of Tendermint, along with the more recent history of Polkadot and NEAR, suggest that POS is indeed ready for Prime Time. The increased use of staking across various chains will lead to a proliferation of staking derivatives. Smart contracts are perfectly suited to creating these derivatives, which will allow holders to leverage their staked tokens in DeFi and other use cases. The complex landscape of this new crypto sub-niche will be the focus of our next report.

6. *Bridges...bridges everywhere.*

Another commonality across the three platforms is the focus on interoperability. Cross-chain bridges are Cosmos's raison d'etre. NEAR has already built its Rainbow Bridge to Ethereum, while Polkadot has its Bridge Modules and Contracts.

Beginning in 2021, value and data will begin to flow trustlessly between crypto ecosystems. Perhaps liquidity will even flow before all three of the blockchains we've just analyzed. But how will users access these bridges, and what sorts of friction will they have to contend with? Although the answers aren't clear just yet, wider adoption will likely require that the complexities of interoperability are made nearly invisible to users.

Back to the Strip

Full circle! We finally find ourselves back on the Crypto Strip, where we started this journey. Now that we know more about those empty clubs, they suddenly seem a lot more exciting. They have lots of potential, with each offering its own unique features. And most important, there's plenty of room to expand and meet the influx of demand that's inevitably coming.

Cosmos, Polkadot, and NEAR could all thrive in the years ahead. The world will soon be beating a path to crypto's digital doors – and unlike in 2017-2018, this time the blockchain world is much more prepared for it.

The tokenization of everything will require varying solutions to meet varying use cases. While these scalable platforms face short-term challenges in adoption, avoiding centralization, and proving out new consensus mechanisms, they also offer interoperability that will allow value to move back and forth with ease.

Sitting in the middle of this buzzing thoroughfare is ShapeShift, ready to connect blockchains and DApps to the masses. It's a good place to be.

05 Further Readings

The Dirt - Mötley Crüe

Electric Capital - 2020 Developer Report

LazyLedger - A Scalable General-Purpose Data Availability Layer

LazyLedger - Epicenter Podcast

Key Polkadot Wiki

Polkadot: Limitations & Issues

ETH-NEAR Rainbow Bridge

NEAR Protocol - White Paper

NEAR Sharding Design - Nightshade

NEAR Summary - Bison Trails