October, 2019

Decentral Park Capital

The Current State of Telegram Open Network

A sleeping giant awakens

Author: Elias Simos

Privacy is not for sale, and human rights should not be compromised out of fear or greed.
- Pavel Durov (April, 2018)

Table of contents

Key Takeaways

- If delivered as intended, with 250M (and growing) active users on its front-end, TON can be the gateway for cryptoassets and the related applications to "bank the unbanked", and become the first ubiquitous discovery platform for Web 3.0 applications, akin to the App Store for Web 2.0.

- However, at this stage, interoperability appears a long way out, as (i) it is common for blockchain networks to spend at least one or two years post Mainnet launch to achieve a stable state and (ii) other networks need to achieve maturity, in order for interoperability to make sense.

- Over a 5-year horizon, once key pieces of the platform are in place and the token economy stabilizes, we expect the network's value to surpass $20B, making *Grams* a top-10 protocol asset.

- TON introduces a collection of highly promising technologies, but the unknowns in the feasibility of some of the parts, as well as the sum of the parts, are still many.

- In the initial stages of the launch, TON appears to be less open to developers than its competitors. In a world where talent is scarce, we view that as a competitive disadvantage.

- The instability in the current macro- and meso- environments, makes the launch phase of the *Gram* token economy, all the more challenging.

- The unfriendly attitude of local governments in the countries where Telegram's users are predominantly based, may dampen the adoption of *Grams* by users, by slowing the value flow from fiat to Grams.

- With weak demand among crypto-native investors, few avenues for current Telegram users to acquire Grams, delays in delivery, the Foundations intent to not proceed with buybacks, and ~60% of the total supply of Grams coming to market in Year 1, we expect selling pressure to outweigh demand for the asset in the short-to-medium term.

About Decentral Park

Decentral Park is a family of funds that offers a diversified approach to digital asset and blockchain investing. We research, identify, evaluate and support teams, products and market opportunities within the blockchain world.

Decentral Park's founder-led team brings multi-dimensional experience, expertise, capital and network and industry relationships to blockchain technology projects. We believe blockchain technology and cryptoassets have the potential to make a hugely positive impact in many areas of the global economy.

Decentral Park Capital's Principals have a long track record of founding, funding, developing, managing, advising, scaling and exiting successful businesses in blockchain, consumer technology, consumer brands, real estate, brick and mortar businesses, venture capital, investment banking and private equity - with a specialty in emerging markets and emergent industries.

Decentral Park Capital II LP is a private investment fund (the "*Fund*") organized for the purpose of investing in cryptocurrencies, decentralized application tokens, protocol tokens and non-fungible tokens (together, referred to as "*Digital Assets*").

The Fund aims to capitalize on the opportunity presented by the current distressed valuations in the cryptoasset space. We believe there is significant alpha to be captured in backing projects with listed tokens, world-class teams, strong track record of shipping code and experience of a full market cycle behind them. We have developed a suite of tools and methodologies that both enable us to select the winners and empower us to maximize upside potential.

The Fund will be investing for the medium term (2 years) using asymmetric expertise and information advantage, fundamental analysis and proprietary fundamental asset scoring and relative valuation tool ("DPC Heatmap") developed by the General Partner to aid in the selection of undervalued tokens to maximize alpha return of its Digital Assets portfolio.

Cryptocurrencies as Digital Assets are an emerging, investable asset class that currently have very low penetration into both retail and institutional investors' holdings. The General Partner expects high volatility in the short term, but medium- and long-term positive trends with considerable asset price appreciation as technological development and user engagement increases, and as investors increasingly view cryptocurrencies as an attractive asset class.

To qualify this report, the Decentral Park family of funds is not a holder of the TON SAFT.

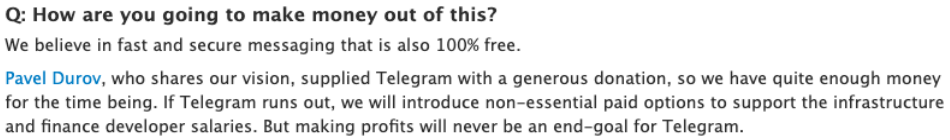
Introduction

The Telegram Open Network (TON) is a new blockchain that will soon come online as a natural response to the growing pains the blockchain ecosystem is currently subject to; namely (i) low capacity and transaction speed levels that pale in comparison to status quo financial back-ends (e.g. the Visa network) and (ii) complex user interfaces (UI) and experiences (UX) of crypto products (exchanges, wallets, digital identity management, etc)[1].

"TON is solving for (i) low capacity and transaction speed levels and (ii) complex user interfaces in production level blockchains."

The project is the brainchild of Pavel and Nikolai Durov, Russia's best known tech entrepreneurs, founders of social network VKontakte[2] and the Telegram messaging app. Over a decade, the founders of TON have created and scaled globally two era-defining internet ventures and are on the way to their third. What is particularly noteworthy is that they did so in the face of adversity, coming in direct conflict with the Russian government when it came to protecting the privacy of their users.

The ethos on which their businesses have been built and the personal brand they have developed along the way could not be a better match for the blockchain space. Telegram was born out of the founders' need to communicate privately while under the magnifying glass of the Russian security services. While growing Telegram's user base to the first 100M, the Durovs deployed a strategy of geographical arbitrage, frequently changing their base of operations between various cities in the world and building the messenger on a robust network of distributed servers. By merit of his track record, Pavel Durov - Telegram's CEO, has become an icon among privacy activists in Russia and beyond. Telegram always looked more like a stateless cypherpunk messaging service than a glossy Silicon Valley type start-up. And TON appears to be here to carry that legacy forward.



Q: How are you going to make money out of this?

We believe in fast and secure messaging that is also 100% free.

Pavel Durov, who shares our vision, supplied Telegram with a generous donation, so we have quite enough money for the time being. If Telegram runs out, we will introduce non-essential paid options to support the infrastructure and finance developer salaries. But making profits will never be an end-goal for Telegram.

Figure 1: From Telegram's FAQ, on how they plan to monetize the application.

Among their many achievements, Pavel and Nikolai Durov have also spearheaded the second largest fundraise in the history of blockchains[3], raising an estimated $1.7B over two private sales between February and March 2018; an impressive feat and inarguably

[1] With Bitcoin ad Ethereum providing 7 and 15 transactions per second respectively, the capacity of TON blockchain is expected to be millions of transactions per second - this is performance comparable with Visa and Mastercard.
[2] ВКонтáкте (vk.com) is the 15th most visited website in the world according to Alexa rankings (2019).
[3] Second only to EOS - who raised $4B over the course of a year long ICO. The team was initially aiming for $1.2B in a part-private and part-public a'la ICO sale, but due to high institutional demand, decided to hold an only-private sale, and raise ~1.5x what they initially aimed for.

far more deserving than the majority of its neighbours at the top of the list of largest fundraises in the ICO era[4]. Now, a year and a half after TON closed its final $850M funding round and with the public launch expected in Q4 2019, the world looks like a fundamentally different place, both within crypto as well as more generally.

Crypto winter and a tale of valuations

"Since Feb 2018, the total market capitalization of cryptoassets lost 85% of its value, top to bottom."

February and March 2018 marked the onset of the second longest crypto winter, through which, the total market capitalization of cryptoassets lost 85% of its value, top to bottom. Since a bottom was found at the end of 2018, the market has picked up, mostly fueled by Bitcoin's continuous ascent towards being adopted as a legitimate macro asset. At Decentral Park, we view the adoption dynamic in the blockchain world as bi-directional; namely top-down and bottom-up. The top-down dynamic is driven by traditional institutions adopting cryptoassets as part of their standard rotation, while the bottom-up dynamic involves grassroots innovation that leverages cryptoassets in order to massively improve on existing business and organization models (e.g. more markets via tokens, 24/7 liquidity, etc) and thrusting new ones into the limelight (e.g. programmatic markets powered by game theoretic primitives). Thus far, it appears that the top-down dynamic will play out faster than the bottom-up, in part because of the limited ability[5] of Layer 1 blockchains to host large scale, high throughput applications.

Figure 2: Total crypto market cap has contracted by 1/3 since Feb/Mar 2018.

"Over 2017/2018 valuations in crypto were heavily skewed towards the 'comparables' approach."

Further, the fact that cryptoassets are so new, comes in tandem with a lack of generally agreed upon valuation methodology. Due to that, over the course of 2017 and 2018 private market valuations in crypto were heavily skewed towards the "comparables" approach. However, unlike the public markets, once locked into said valuation, there is no formal way for private market valuations to adjust as the value of their comparables changes.

As a result, while publicly-traded cryptoassets lost a large proportion of their ascribed value over 2018, investments in the private markets were marked to book. At the same time, the 2018 bear market drove retail investors away, and the ones that are still around have sharpened their decision-making functions through their survivorship. The effect of

this change in landscape is that as these new assets break into the public markets, there are fewer investors to pick them up from early investors' hands and shepherd them for the remainder of their public life.

"...as these new assets break into the public markets, there are fewer investors to pick them up from early investors' hands."

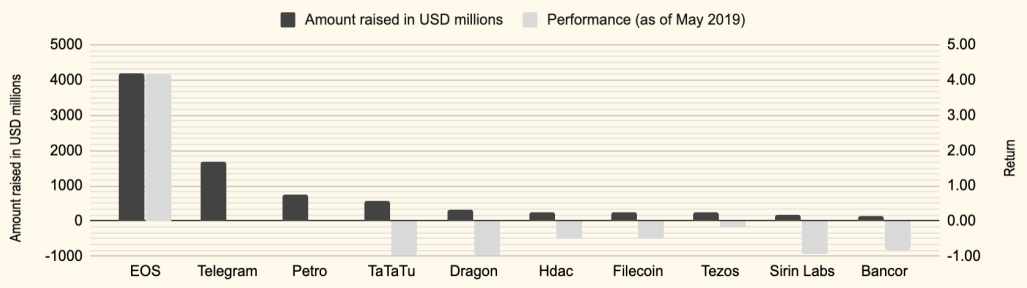


Figure 3: Top-10 ICOs by fundraise and subsequent returns until May 2019.

To highlight the effect of the "crypto winter" on valuations, over the past year and a half, the total crypto market cap lost ~25% of its value, while in the same period smart contracts platforms with liquid tokens have lost ~75% of their value. From the Top-10 ICOs of the 2017/2018 era, the ones that are liquid have lost 10% of their value on average, while the only one that remains profitable for its early investors is EOS. Removing EOS from the calculations paints a much more dire picture, with returns landing in the neighbourhood of a negative 70%. The intra-industry clusters that TON somewhat affiliates with have also performed poorly. On aggregate, equally weighted portfolios of smart contract platforms, Proof of Stake (PoS), Infrastructure and Interoperability related assets, have lost approximately 85% to 95% of their value since March 2018, signaling a lack of demand for the native tokens of these platforms.

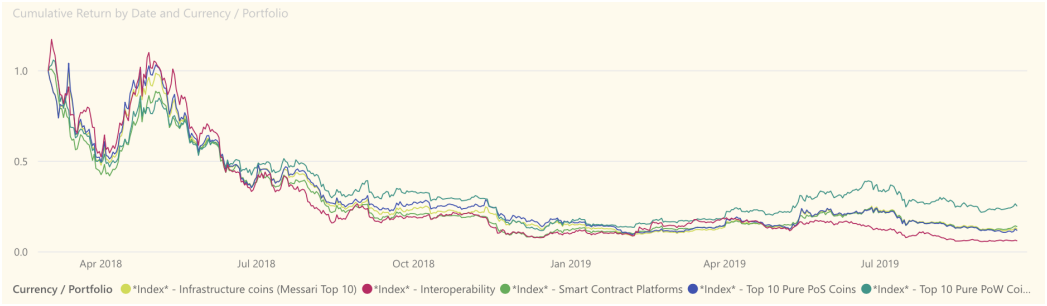


Figure 4: Aggregate performance of liquid tokens within the smart contracts, infrastructure and PoS verticals.

"PoS, Infrastructure and Interoperability related assets, have lost approximately 85% to 95% of their value since March 2018."

The recent launches of Algorand's and Hashgraph's native protocol assets[6] are indicative of the effect that comparables-based valuations had in early stage blockchain investing over 2018/2019. Both projects are made up by teams of the highest caliber, backed by

[4] Indicatively 3 out of the Top-10 raises have already gone to 0.
[5] Albeit continuously improving.
[6] ALGO and HBAR respectively.

some of the most recognizable names in venture capital, bringing to market technologies that - at least on paper - could revolutionize how blockchain technology is deployed at scale.

"It is a challenging time for assets in tech transitioning from private to public markets."

What the two projects also share, is the poor performance of their native tokens upon listing (ALGO is down 90%, while HBAR is down 80%). Indicatively, Algorand raised a total of $125M at a $7B supply-derived and a $24B implied valuation, while Hashgraph raised ~$100M at a $6B implied valuation. Both projects distributed less than 30% of their total treasury of tokens to their investors - introducing implicit overhang risk to the prospective token holder's decision model. Indicatively, the demand for these tokens is so low, that the daily OTC lending rate for HBAR tokens has been reported to be as high as 5% daily; a hint to the fact that, at the moment, current holders are not interested in being long.

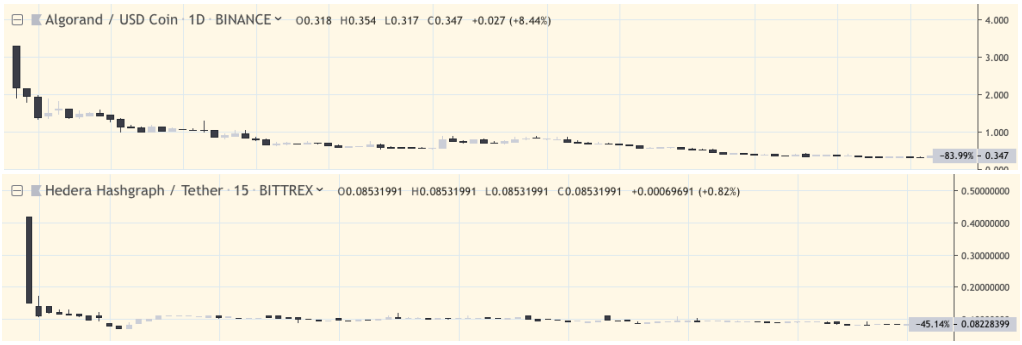


Figure 5: Performance of ALGO and HBAR after listing in Q3 2019.

"Investors are asking hard questions about the relationship between value creation and value capture."

The disparity between private and public valuations is not a phenomenon exclusive to cryptocurrencies at this moment in time. It is no secret that a decade of quantitative easing and record low interest rates have been catalysts in driving capital towards venture capital, as institutional allocators seek to take on more risk to meet their returns targets - which in turn has allowed thriving tech companies to stay private for longer. However, while venture investors are benchmarking growth over cash-flows, public market investors are not buying it. The result has been the lacklustre public market performance of highly anticipated tech-IPO stocks.

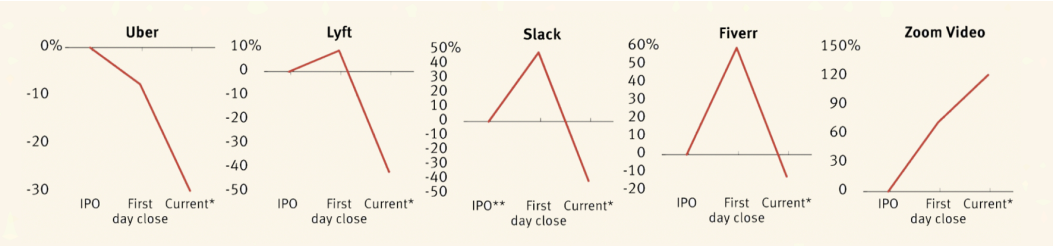


Figure 6: Popular tech IPO stock performance post listing in 2019[7].

[7] Borrowed from *The Information* [Access here: http://bit.ly/2nvFVH7]

All of the above illustrate that it is a challenging time for assets in the technology sector transitioning from private to public markets. Investors and observers alike are asking hard questions about the *relationship between value creation* and *value capture* in technology. Of course there is plenty of nuance in each of the examples here, and plenty to consider with regards to the potential upside that cryptoassets in particular still have. However, the evidence is fairly compelling that this is a landscape that requires investors to expect highly volatile listings and react and position appropriately.

TON: Special case or one of many?

Zooming back in to the main theme of this paper, TON's case is hard to pigeon-hole. While it broadly falls into the category of assets described above, it really looks like none of the assets specifically discussed. Where blockchain platforms are struggling to attract developers and users, TON is coming online piggybacking on a messenger app with approximately 250 million[8] monthly active users (2x more than Uber, 4x more than Zoom, 20x more than Slack, 500x more than Ethereum) and with the potential to become crypto's definitive distribution and user acquisition platform[9]. This is the kind of potential that conjures up $1.7B in investment from some of the world's premier patient capital, reportedly including Benchmark, Sequoia Capital, Lightspeed Ventures and Kleiner Perkins[10].

"TON is coming online piggybacking on a messenger app with approximately 250M."

Prior to the TON fundraise, the lights at Telegram were kept on by donations from the Durov brothers. Reports estimate the monthly burn rate to be approximately $1M, while the application is not generating any revenue yet. Claiming that TON is a broader effort to make Telegram a self-sustaining entity would not be a far reach - though it has the potential to become a lot more.

Overall, the Durovs' pedigree, secretive mode of operations, and this market backdrop, make the upcoming release of TON's Mainnet one of the most eagerly anticipated and attention grabbing Mainnet launches in recent years; one worth discussing, documenting and dissecting. In the following sections of the paper we will attempt to unveil much of the mystery around TON by diving deep into the recently released documentation and code, aiming to (i) shed light into the utility of the Gram (GRM) tokens, by understanding how the Messenger and the Network will interface with one another and (ii) thoroughly understand the architecture technical composition of the network.

"Reports estimate the Messenger's monthly burn rate at approx. $1M."

[8] Statista estimates Telegram's MAU at 200M as of June 2019 [Access here: http://bit.ly/2ocHcUg]. Given that Telegram passed the 200M MAU milestone in March 2018, and its total user base stands at over 500M, we believe that 250M is a more accurate representation.
[9] Provided that TON will be compatible and interoperable with all other major blockchains, something that this report is aiming to explore.
[10] As reported by Coindesk [Access: http://bit.ly/2l6Lr2h].

Part 1: All things Grams

"Grams will be used both as a consensus token and as a money token."

This section explores the properties of the *Gram*[11] token, both as the native utility token of TON and as an investment instrument. Telegram will be introducing *Grams* both as a *consensus token* that facilitates the process validators participate in order to reach consensus with respect to the state of the blockchain via Proof of Stake[12], and as a *money token* to be used for anything between storing value, making payments on services available via the messenger and on TON (e.g. Dapps), and transferring value between Telegram users (e.g. remittances).

In that respect, *Grams* can be assimilated to what Facebook is planning to launch through project Libra. The key difference is that while in the case of Libra the token will be pegged to a basket of currencies, the value of Grams will be - partly - decided by the market. We highlight *partly* here, as TON has a Central-Bank-like entity in place (the TON Reserve and the TON Foundation) that can intervene to provide price support both in programmatic ways, as well as with open market operations.

"The official launch of the TON Mainnet is scheduled to occur some time before the 31st of October 2019."

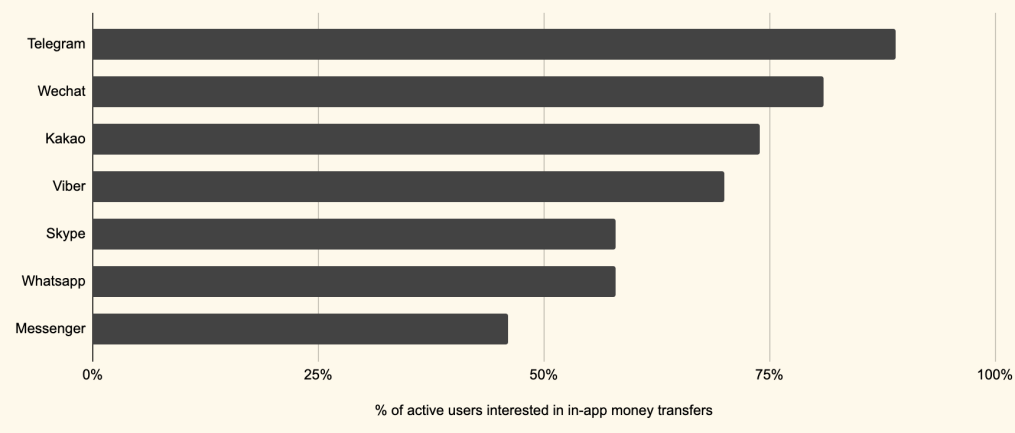


Figure 7: Telegram users are the most interested in in-app money transfer features.

The official launch of the TON Mainnet and the official start of public sale of *Grams* are scheduled to occur some time before the 31st of October 2019. According to the Telegram Final Purchase Agreement the TON Foundation will have to return capital to investors should said deadline be missed. Provided that the network launches

[11] Gram tokens are also notated as GRM tokens, the expected ticker the token will assume.
[12] The PoS mechanism that TON is proposing on its whitepaper bears a lot of similarities to that of its interoperability competitor, Polkadot.

successfully by the 31st of October, Telegram will make *Gram* wallets available to approximately ⅔ of their user base[13], gradually expanding to the whole.

1.1. Token Economics

The total supply of *Gram* tokens is initially set at 5 billion, with an inflation rate that will be approximately 2% annualized according to estimates shared in the TON whitepaper. If that holds, the total supply of GRM will effectively double within 35 years from launch. As in most PoS chains, tokens generated via inflation will be earmarked as validator rewards.

"The total supply of *Gram* tokens is initially set at 5 billion, with an inflation rate that will approximately stand at 2% annualized."

We estimate that from the total supply, ~54% was sold to investors[14] in at least 2-rounds of fundraising. Of those, ~12% will be made immediately available for investors to trade. The remaining ~42% will be gradually made available, as it is subject to a varying lock-up schedule that spans between 6 and 18 months post Mainnet launch. We further estimate that ~4% is earmarked as developer and community incentives, while the remainder[15] will be controlled by the TON Foundation and TON Reserve.

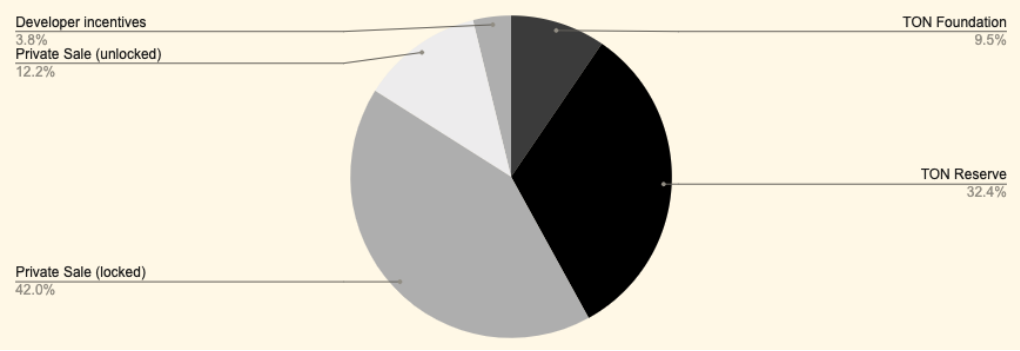


Figure 8: Expected GRM token distribution as of Mainnet launch.

While its final form is still unclear, the TON Reserve appears to be a minting facility[16] that will be issuing and selling tokens according to a set pricing function. The prices will initially start at a low level, but will increase in an exponential fashion for every marginal Gram issued. The first 2.7B Grams to be issued are earmarked for SAFT holders.

$$p(n) \approx 0.1 \cdot (1 + 10^{-9})^n \quad \text{USD}$$

Figure 9: The price function that TON has designated for the TON Reserve's operation.

[13] Estimated to stand at 300 million signed-up users - this information surfaced on the NYT and is attributed to unnamed TON investors.
[14] Lock-up schedules (find)
[15] Close to 50% of the total supply.
[16] It is unclear whether the TON Reserve will be fully programmatic or a hybrid that involves human intervention.

"The TON Reserve withholds the right to sell up to 2.5B *Grams*."

The fact that there will effectively be two markets for TON - a primary and a secondary - provides the issuer with one more lever to control the price of *Grams* by creating arbitrage opportunities, the parameters which are under their control. If the price of *Grams* is higher in the open market, more buying will take place via the Reserve and vice versa, eventually bringing the primary and secondary markets at par with one another. According to the whitepaper, the TON Reserve withholds the right to sell up to 2.5B *Grams* (½ of total supply) via the mechanism described above. Given that the estimated amount held by the TON Reserve at the moment stands at a little less than 35%, we can expect the remaining 15% to come from a mix of open market operations and validator rewards collected in the initial stages of the network's launch[17].

Figure 10: Jason Choi's comment on the recent launches of ALGO and HBAR.

"TON is likely better prepared than other networks that have come to market in 2019 in supporting the network token's price."

Arguably, the aforementioned parameters along with the patient capital that participated in the private sales and the massive war chest that TON raised in USD, mean that at the very least, TON is likely better prepared than other networks that have come to market in 2019 with regards to supporting the network token's price in the initial stages of price discovery. The above information also might imply that TON has the potential to become one of the networks with more evenly distributed token economies in the years to follow. Given that (i) TON is planning to ultimately distribute 90% of the total token supply to stakeholders, and (ii) the supply side mechanisms in place to increase the probability of healthy price discovery in the long term, TON is poised to potentially be one of the networks with the lowest Gini coefficients[18] in the blockchain space.

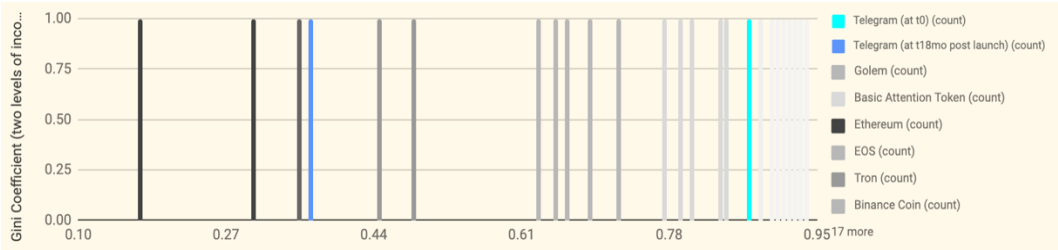


Figure 11: High level estimate of TON Gini coefficient at two levels of income (Top 100 addresses vs the rest) at launch and 18 months post-launch[19].

[17] It is still unclear whether TON will put the Reserve provision to work, as recent reports have it that were they to sell tokens directly to retail buyers, would risk the Gram being classified a security.
[18] In economics, the Gini coefficient, sometimes called Gini index, or Gini ratio, is a measure of statistical dispersion that represents the wealth distribution of a population, and is the most commonly used measurement of inequality.
[19] The Gini coefficients presented here, are a snapshot from February 2019. TON's estimated Gini scores represent more illustrative assumptions, and less formally derived figures.

1.2. What is a Gram worth?

While the purpose of this paper is not to provide explicit price targets, the subject of price is inescapable. In fact, price is not and should not be a forbidden word or concept when thinking about nascent networks enabled and moderated by protocol tokens. Price is the one variable to rule them all; the metric that contains the most information about an asset and the most singular and unifying indicator for all stakeholders in a token economy. In the following section, we provide an overview of significant events that we consider as milestones in TON's valuation and for the pricing of *Grams* with a view to arriving at a sober evaluation of the price action to ensue in the initial stages of the network's launch, and beyond.

"Price is the one variable to rule them all; the most singular and unifying indicator for all stakeholders in a token economy.

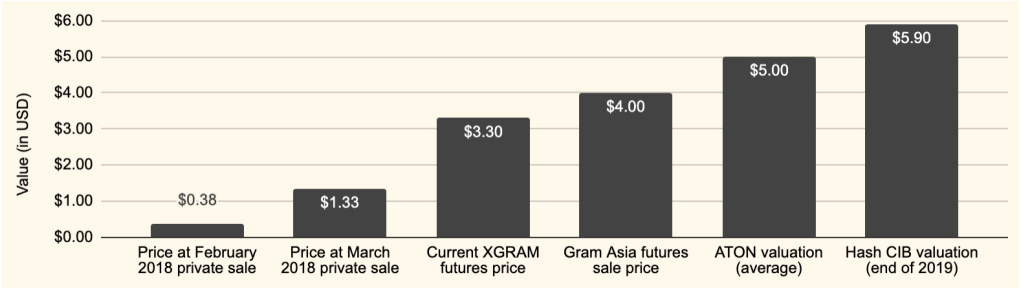


Figure 12: Summary of significant price milestones for *Grams*.

The right to claim *Gram* tokens upon the launch of the network was sold to investors in two private sales that took place in February and March 2018. The first SAFT round opened in January 2018, at an estimated price of $0.38 per *Gram*. Investors participating at this stage are subjected to an 18-month vesting period. 81 investors took part, 3 of them publicly disclosed their identities. During the second SAFT round in March 2018, *Grams* were sold for $1.10-1.45, without a vesting period. 94 investors took part, whose identities were not publicly disclosed.

"SAFT 1 opened in January 2018, at an estimated price of $0.38 per *Gram*; SAFT 2 closed in March 2018, at an average price of $1.33 per *Gram*."

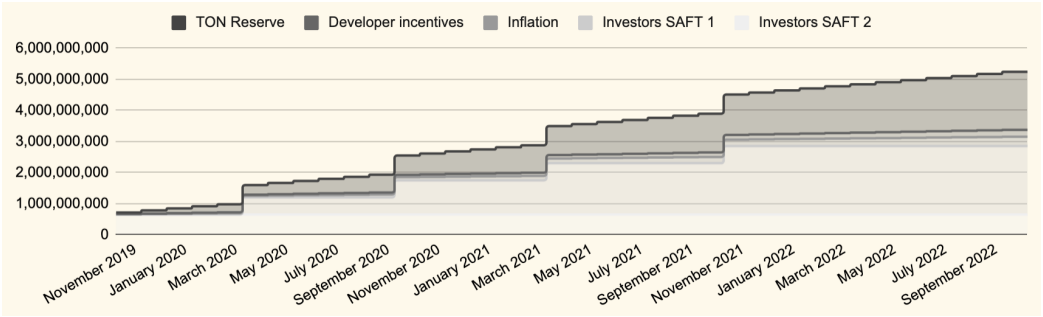


Figure 13: Estimation of *Gram* circulating supply over the first 36 months after the network's launch[20].

[20] This represents the extreme case, where all investors make their holdings available to the market, as soon as their lock-up expires. It further assumes linear distribution of the Dev and Reserve funds over 36 months, 2% annual inflation, and the 10% TON Foundation allocations remaining unavailable.

"Investors participating in the SAFT rounds were given allocations that ranged between $300k and $20M."

Each round was capped at $850M. Investors participating in these rounds were given allocations that ranged between $300k and $20M. According to TON, not more than 20% of investments originated from Russian funds or individuals. For both rounds Telegram filed a Form D 506c with the Securities and Exchange Commission (SEC); these offerings were made under a claim of federal exemption under Rule 506(c) and/or Regulation S under the Securities Act of 1933.

In March 2019, the little known Xena exchange[21] listed a leveraged, cryptocurrency-settled derivative contract for the GRM token (XGRAM), which in the first month of trading reached up to $8 per XGRAM, though in a highly illiquid environment. At the moment, the price per XGRAM stands at $3.30, however, there is barely any activity in this particular market, with the last trade being recorded on the 4th of September 2019 and the first bid in the book standing at $2.22 - marking an effective bid/ask spread of ~50%. The Chinese exchange Lbank[22] has also listed a Gram/ETH futures pair, which at the time of writing trades at the equivalent of $1.00.

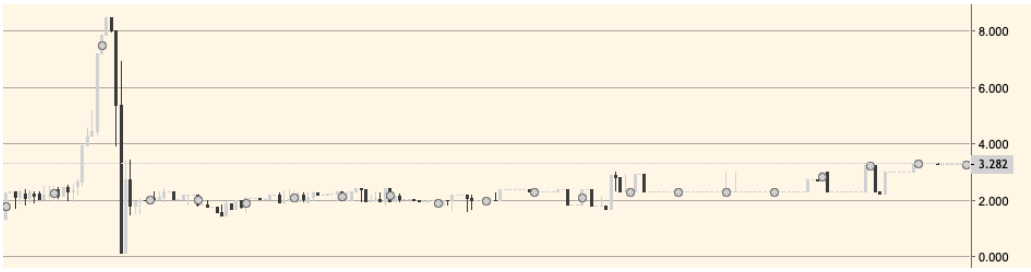


Figure 14: Gram futures (XGRAM/USD) at Xena exchange (as of 16/09/2019).

"Gram futures trade in highly illiquid markets."

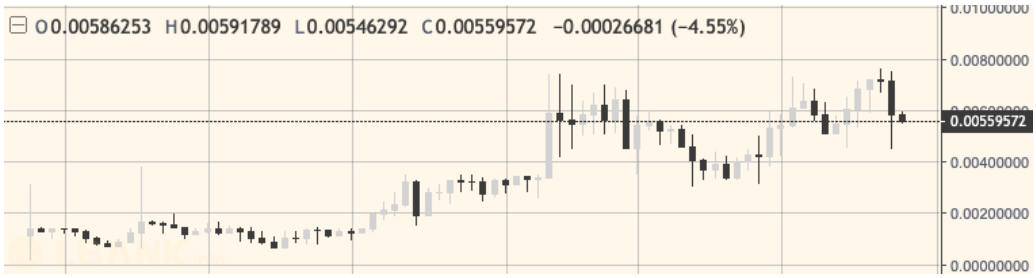


Figure 15: Gram futures (GRAMS/ETH) at Lbank exchange (as of 16/09/2019).

The latest more formal attempt towards public price discovery was made in July 2019, when Korean company Gram Asia, allegedly the largest holder of *Grams* in Asia, held a

[21] This is a Russian exchange that launched in the summer of 2017. The only listed assets on the exchange are BTC, ETH and GRM futures (XGRAM). According to Forbes, they have raised approx. $3.5M in funding thus far. Xena Exchange was one of the early Telegram Passport adopters.
[22] Lbank has been found to misreport traded volumes according to TIE. [Access: http://bit.ly/2lgwY3S]

physically settled futures sale for $4 per *Gram*. The sale took place on Liquid[23], an exchange entity affiliated with Gram Asia. Approximately 3.125M *Grams* were made available, raising $12.5M. The supply of future tokens in this case came from the notional allocation of Gram Asia, without though explicitly being given permission from TON. According to the TON private sale investment contract, the issuer does not allow the transfer of rights to future tokens before its Mainnet launches - however, depending on jurisdiction, there appear to be ways to override the clause. Finally, on the 19th of September 2019, the little-known exchange ATAIX, launched a sale for allegedly "unlocked" *Grams* - which in reality appear as unsecured futures agreements, for $3.99 per *Gram*.

In addition, multiple reports have surfaced hinting at a busy OTC market for *Grams* - though it appears skewed to the sellers side. According to a Coindesk interview with OTC trader Vladimir Cohen[24], *"OTC sellers have been striking confidential deals for Grams based on trust. Often, sellers are trying to resell their tokens for a profit, having paid either $0.38 during per gram in the first round or $1.33 in the second."* In practical terms, what is being traded in the OTC markets are IOUs - effectively gentlemen's agreements that the agreed upon amount of *Grams* will change hands, at the agreed upon price, once the Mainnet launches and the tokens are minted. More recently, we have come across anecdotal reports that early investors are looking for liquidity OTC, around the $1.50 mark, while some OTC brokers are reporting seeing offers at $0.85, with few bids.

"Initial trading in *Grams* can be expected to be volatile and initial price discovery looks likely to depend on how aggressive sellers are, and whether - and at what price - a stabilizing buyer steps in to the market."

Considering the highly volatile nature of the cryptocurrency market right now, and the poor early performance of other recent token issuances, initial trading of *Grams* can be expected to be volatile and initial price discovery looks likely to depend on how aggressive sellers are, and whether - and at what price - a stabilizing buyer steps in to the market. A repeated pattern is that once listed, token prices trend down towards the level of the earliest fundraising due to supply pressure from early investors .

At the same time, the equity research house ATON and cryptoasset investment bank Hash CIB have published two pricing models[25] that follow a modified DCF approach. ATON's price target lands at an average of $5 per *Gram*, while Hash CIB's model sets a target at $5.90 for the end of 2019.

Once again, while not the explicit purpose of this paper, we cannot help but put the aforementioned targets to the test, based on our own set of assumptions. The methodology followed here is purposefully not following on the aforementioned models' tracks, in order to add to the dimensionality of public knowledge. Our model

[23] Liquid is the largest Japenese crypto exchange platform. More details on the sale can be found on the Techcrunch article that first broke the news. [Access: tcrn.ch/2l8ODKD]
[24] [Access: bit.ly/2mauO5W]
[25] ATON's report benchmarks two prices, that represent their proposed fair value range - between $2.1 and $8. You can access ATON's report on TON here [Access: http://bit.ly/2mcs7kj]

seeks to simply match an expectation of demand with the supply of *Grams* at any given point in time, assuming that all unlocked *Gram* tokens will be available for sale. While a simplistic approach, it establishes a supply/demand based support level for a *Gram's* price.

"Our model seeks to simply match an expectation of demand with the supply of *Grams* at any given point in time."

The core assumption is that spending on Telegram functionality (via *Grams*) will start at ~35% of the current average user spend on the Apple App Store - an estimated $79 in 2018[26]. Using that as the starting point and adding a few more assumptions[27], we arrive at the following price targets.

	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
Active users	250,000,000.00	280,000,000.00	310,000,000.00	340,000,000.00	370,000,000.00	400,000,000.00
Active users spending	212,500,000.00	238,000,000.00	263,500,000.00	289,000,000.00	314,500,000.00	340,000,000.00
Amount spent per user	$30.00	$40.00	$48.00	$57.60	$69.12	$82.94
Percentage spent in Grams	30%	40%	50%	60%	70%	80%
Demand for Grams	$1,912,500,000	$3,808,000,000	$6,324,000,000	$9,987,840,000	$15,216,768,000	$22,560,768,000
Supply of Grams	716,000,000	2,319,999,999	3,552,499,997	4,784,999,996	5,000,000,000	5,000,000,000
Equilibrium	$2.67	$1.64	$1.78	$2.09	$3.04	$4.51

Figure 16: DPC's high level model parameters.

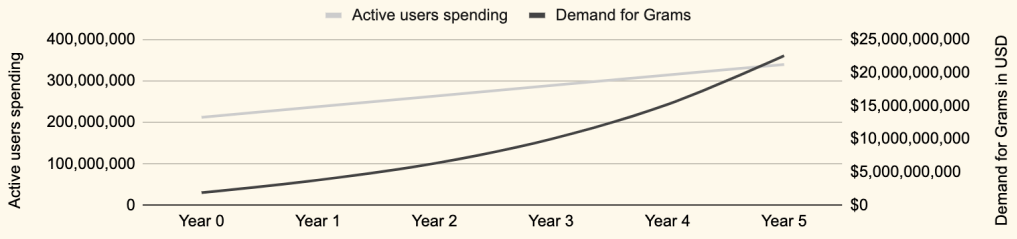


Figure 17: DPC's demand projections for Grams.

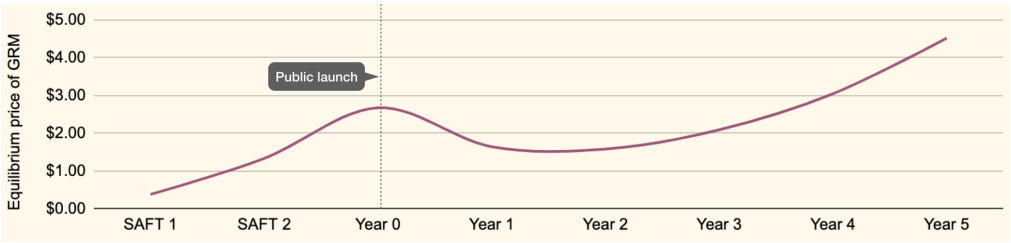


Figure 18: DPC's value bottom projections for TON.

One more underlying assumption to the model is that demand will hit the TON blockchain on day one. While somewhat unrealistic, given the early stage of the network's development, we believe this assumption to be a useful proxy for estimating speculative

[26] [Access: http://bit.ly/2kD5AwJ]
[27] We assume that (i) TONs current MAU stands at 250M and (ii) will keep growing on the same (reported) linear trajectory since 2015 - discussed earlier in the report, (iii) the percentage of that spend funneled through Grams will follow said pattern, while (iv) the supply of Grams will follow the schedule outlined in the beginning of Section 1.2.

appetite in Grams. It further both benchmarks well on the most recent *Gram* futures recorded prices and illustrates well the J-curve dynamic frequently observed in a cryptoasset's life cycle[28]. Interestingly, our estimate of an approximate fair value bottom is not dissimilar to the output of modelling work that preceded this paper, and is also in line with the implied provision for possible buybacks from the TON Reserve that are estimated to kick-in at the $1.80 price level[29]. More recently though, reports surfaced that in a letter to investors, the TON Foundation expressed their intent to not proceed with buybacks, in order to comply with SEC regulations and protect Grams from being classified as unregistered securities. Regardless, this approach can only work as long as the TON Reserve has enough capital to support it.

"More recently, in a letter to investors, the TON Foundation expressed their intent to not proceed with buybacks, in order to comply with SEC regulations."

1.3. Finding liquidity

Token liquidity and price discovery depends on multiple and high quality exchange listings. Given Telegram's clout and TON's considerable financial resources, this is not likely to be a problem. Coinbase recently published a list of tokens they are considering listing and the Gram is one of them. Further reports have surfaced naming the Binance exchange and the eToro platform as prime candidates, while also hinting to a possible listing on Huobi. However, thus far the only official announcement for a Gram listing has come from the Blackmoon Financial Group, an entity indirectly connected to TON's executive team.

Blackmoon - a Caymans-registered exchange, with an estimated 3,800 user base - was founded in 2014 as a blockchain-based fintech company, while the Blackmoon exchange itself was launched in 2017 (product of a $30 million ICO) by Ilya Perekopsky (former vice-president of VKontakte), Oleg Seydak (co-founder of Flint capital)[30]. Among the advisors, board members and investors of Blackmoon are Vasyl Latsanych (Vice President of Major Markets at Veon), Oskar Hartmann (KupiVip.ru, Carprice.ru, board member of Alfa-Bank), and Sasha Ivanov (founder of Waves). The supply of *Grams* for the Blackmoon listing will allegedly come from the Gram Vault, one of the few custody providers for Grams - thus likely becoming an intermediary in facilitating early investors' path to liquidity.

---

[28] Chris Burniske's thesis on the crypto J-curve, foresees a boom and bust cycle early in a cryptoasset's life cycle, as Discounted Expected Utility Value is substituted for Current Utility Value. [Access: http://bit.ly/2l9h0s6]

[29] According to the whitepaper, after the allocations to the TON Foundation and the founders, the minimum price for Gram should be effectively set at $1.81. TON Reserveis poised to engage in buybacks if the price drops below 50% of that calculated by Reserve's *Gram* pricing formula.

[30] According to Techcrunch [Access here: https://tcrn.ch/2mkVst3]

1.4. A TON of use cases

As we briefly touched upon in previous sections, *Grams* will have 2 primary streams of functionality; as a (i) demand side payment token and (ii) as a supply side consensus token[31]. In this section we will unbundle the two streams of use cases and examine exactly how they will find utility within the current and projected future Telegram ecosystem.

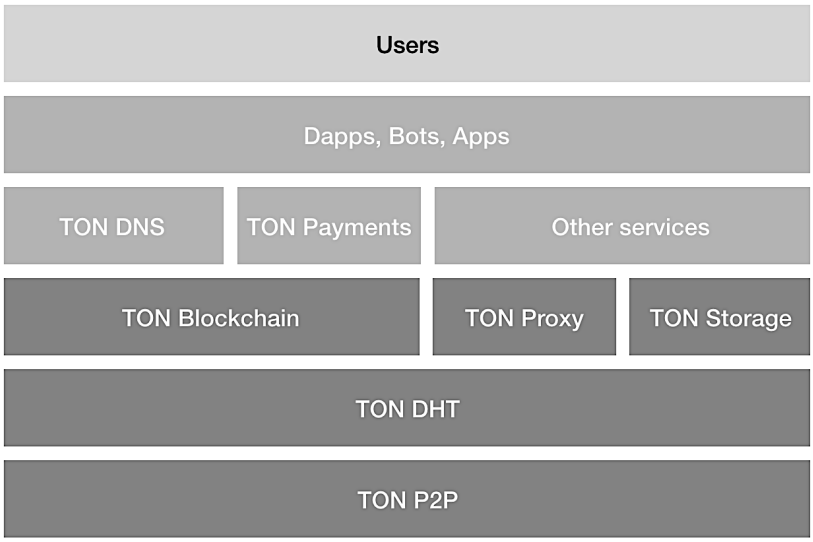


Figure 19: The Telegram Open Network stack as proposed by the whitepaper.

1.4.1. Demand-side use cases; payments, bots, content and Dapps

1.4.1.1. Monetizing bots and enabling payments between users, developers and advertisers

At the moment, we estimate that there are more than 800,000 Telegram-Bots, which are used actively by approximately ¼ of the whole Telegram user base. Telegram Bots are effectively accounts operated by AI software, that enable a series of actions on the platform, such as semi-automated payment processing, group management, game notifications, donations and more, by reading and sending messages, commands and requests to and from users. These messages and interactions are funneled from the Telegram API to the software running on the servers of each particular bot developer via a HTTPS-interface.

One of the few applications that have already integrated with the TON Testnet is the ButtonWallet - a multi-currency wallet and P2P transactions service hosted wholly within the Telegram Messenger and functioning as a bot, rather than an app.

[31] Demand-side use cases for the Gram tokens modules higher up the technology stack that makes up TON, while supply-side use cases are found further down the stack.

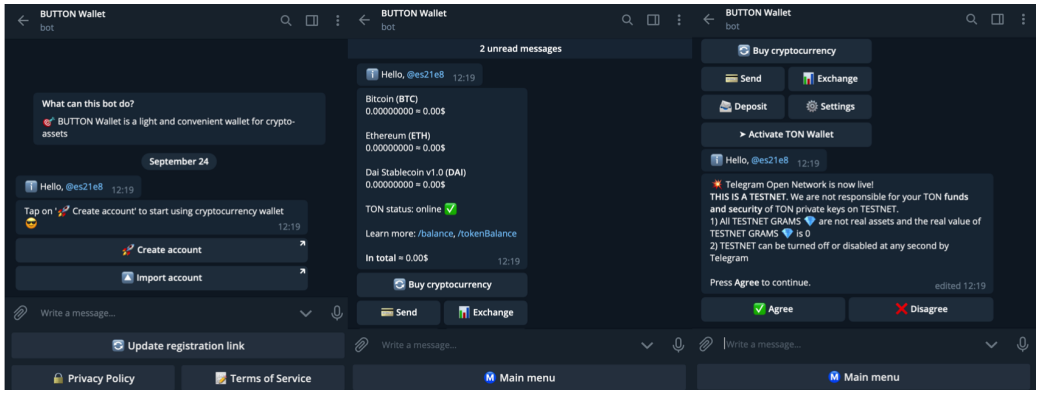


Figure 20: Button Wallet user interface and functionality.

"We expect the TON Payments platform to not be ready for prime-time, by Mainnet launch."

The Telegram payment platform is currently integrated with 8 payment processors[32] that allow bots to accept credit card payments from users in over 200 countries. By introducing Grams into the ecosystem, Telegram will provide the users, developers and advertisers on the platform with an alternative avenue to fulfilling payments on the platform; one that will presumably be a lot more competitive than the 2.9% and $0.30 that Stripe - for example - currently charges per transaction.

The launch version of TON will come with a Wallet integration in the Messenger. At this stage, however, we expect the TON Payments platform to not be ready for prime-time[33] and as such, transactions will take place exclusively on-chain, implying higher transaction fees and less throughput.

Further, there is a point to be made about volatility and its taxing overhead - both for consumers, as well as developers and businesses running on Telegram. Thus far in the development of cryptoassets, we have no tangible demonstration of a volatile cryptoasset being used widely as means of payment. Perhaps the most successful asset in that regard is ETH (Ethereum's native token) and its utility as payment token for executing work for the network[34] - but it is still far from ubiquitous.

"There is a point to be made about volatility and its taxing overhead."

At the same time, stablecoins are quickly getting traction, currently standing at over $5B in market capitalization and trading at volumes in the multiple of at least 4x their market capitalization. Nothing stops TON from launching their own stablecoin, although at the time of writing, there are no confirmed plans for such a feature.

[32] These are: Stripe, Paymentwall, Yandex.Money, Sberbank, Payme, CLICK, Rave by Flutterwave and Tranzzo [Access here: http://bit.ly/2mtnS3R]
[33] TON Payments" is a micropayment channel network - similart to the Lightning network for Bitcoin, aiming to offer instant off-chain value transfers between users, bots and other services, at a level of security equivalent to that of on-chain transactions.
[34] via Gitcoin, in and around ETH Global events etc

"While not directly related to the first-order utility of *Grams,* the Telegram Passport is an important building block in enabling payments on TON."

In the above context, an interesting layer in the stack that is at present likely missing from the available information space, is a link between users that want to pay in Grams, and merchants that want to be paid in fiat currencies. This is an interesting space for market markers to operate in, although to the best of our knowledge, Telegram has not (yet) provisioned for this type of liquidity pool.

1.4.1.2. Telegram Passport

While not directly related to the first-order utility of *Grams,* the Telegram Passport is an important building block in enabling payments on TON. With critical user data stored in the Telegram cloud, encrypted end-to-end, one can imagine massive improvements in user experience from something simple such as buying airplane tickets through a Telegram bot, to signing up to a lending facility and instantly going through the otherwise laborious KYC/AML process in order to apply for a loan. While signing up for the Telegram Passport will not be required in order to send or receive *Grams*, it will be obligatory for users interested in interfacing with an exchange venue in order to purchase *Grams,* via the Messenger.

The Telegram Passport is currently available in a test version via the Messenger with step-by-step instructions available for users to navigate its set-up[35]. The functionality of the Passport can be summarized in 3 steps:

- The user locally encrypts his/her personal data (name, email, passport scan, other documents) with a password.
- The encrypted data + meta-information are uploaded to the Telegram cloud.
- When the user needs to log in to the service, the client downloads data from the cloud, decrypts it with a password, re-encrypts it to the public key of the service that requested the information packet.

"In the initial stages of the launch, user information will be stored in Telegram servers."

In the initial stages of the launch, user information will be stored in Telegram servers, until TON releases a decentralized storage component, as foreseen by the whitepaper. It is worth noting that this decision - especially given that third-party, pluggable, decentralized storage solutions are available in the market - leaves a potentially critical window for exploits to take place, that could be detrimental to Telegram's reputation and the trust it has built with its user base, as it is readying TON for prime time. While Telegram's reputation has been built on being an ultra secure way to communicate with peers, there have been occasions where these attributes have been put to test. The latest one is an incident where the identities of, at least, 85 protesters in Hong Kong were leaked to the Chinese government due to a security vulnerability.

[35] Telegram Passport Manual - https://core.telegram.org/passport

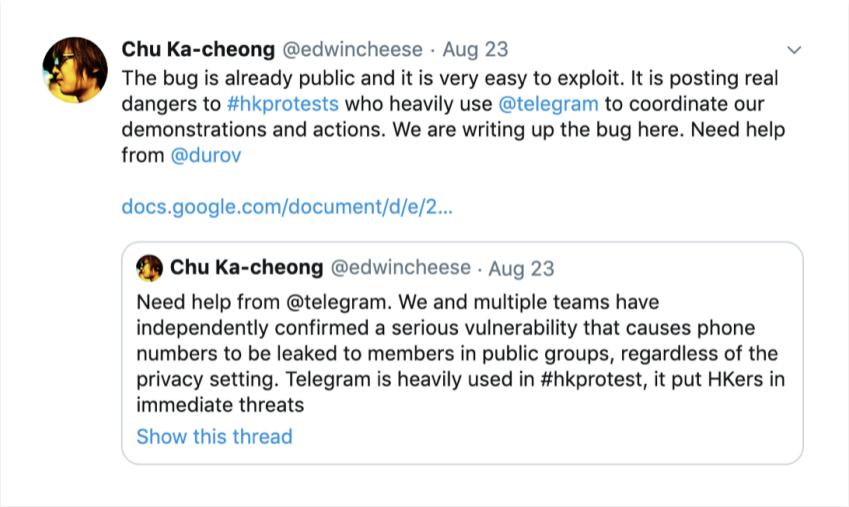


Figure 21: The Chinese government reportedly uncovered a vulnerability in Telegram's security and was able to extract the identities of 85 protesters during the recent upheaval in Hong Kong[36].

"Telegram's Passport employs a SHA-512 hash generator for the encryption - one known to be fairly simple for a sophisticated attacker to break."

Further adding to the concerns about its security profile, the Passport references Telegram's security protocol MTProto 2.0 directly via API, which employs a SHA-512 hash generator for the encryption - one known to be fairly simple for a sophisticated attacker to break[37]. Despite the fact that there are several password hashing functions that make brute forcing too complex for attackers (e.g bcrypt, Argon2, scrypt, PBKDF2), TON developers chose to not use these in the latest iteration of the security protocol. Simply put, the encryption user data stored in the Passport is critically dependent on the complexity of the password chosen by the end-user - and thus introduces a weak point in the system. Telegram has always opted for using their own proprietary encryption algorithm, breaking a common rule among cryptographers to never use one's own cryptography[38]. While the more recent update that they pushed in 2018 (MTProto 2.0) was received as a massive improvement over the previous iteration[39], the community is still puzzled as to why the developers would not simply choose a suite of far more extensively peer reviewed algorithms like "SPHINX" or "Pythia".

1.4.1.3. Dapps

One wholly new stream of functionality that will be gradually introduced as TON matures, is a universe of Dapps available to Telegram users[40]. Users will be able to access that

[36] Telegram has since explicitly addressed the issue [Access here: https://zd.net/2mtBw76]
[37] 10 GPU will test all combinations of 8-digit passwords from a 94x symbol dictionary (english letters, numbers, special symbols) in less than 5 days.
[38] Also known as "don't roll your own crypto".
[39] Some of the flaws of MT Proto 1.0 are explored in depth by Jakobsen and Orlandi (2015). [Access here: http://bit.ly/2n6MgsA]
[40] Shorthand for decentralized application.

"Backwards compatibility with Ethereum, will be enabled by a Solidity compiler built by TON Labs."

through an App Store-like search utility. Applications will be sorted by popularity ands user will receive recommendations based on their search history and downloaded Dapps. In-app premium features are expected to be paid for with *Grams*.

Further, the TON blockchain will be - in theory - interoperable with Dapps built on Ethereum. As such, Ethereum Dapps that demonstrate product/market and product/platform fit with TON and the Telegram Messenger ecosystem, could be integrated with TON. Backwards compatibility will be enabled by a Solidity compiler built by TON Labs, a startup helmed by lead investors in Telegram's token sale. The compiler has been in development since July 2019 and will be available for testing after the Mainnet launch.

While it is too early to make assumptions about which Dapps (if any) might be ported over to TON - or at least made interoperable - it is worth noting that the architecture of the TON blockchain is robust enough to enable even the Dapps with the highest throughput requirements. Whether or not Ethereum Dapps will choose to migrate over to TON will depend on various factors, including the security, integrity and robustness of the TON blockchain, the performance it enables and the fee structure it exposes developers and their users to. And besides, interoperability on TON, is a feature that we are not expecting to see until after 2021.

"Interoperability on TON is a feature we are not expecting to see until after 2021."

There are many elements in the equation that are still unknowns. However, in an interoperable world, with TON introducing hundreds of millions of users to cryptoassets and Ethereum's state growing increasingly more valuable, one can imagine the two working together as complements; TON referencing Ethereum's state (e.g. to give access to a decentralized lending facility to link Maker DAO to their users, via the Telegram messenger) and Ethereum leveraging the Telegram messenger as the discovery platform and superior user interface that it so desperately needs.

1.4.2. Supply-side use cases

The past 10 years in the blockchain world have produced a series of replicable supply-side models (e.g. consensus algorithms) that more-or-less work, depending on the use case. As such, it takes less logical jumps to arrive to use cases for *Grams* when searching for utility further down the technology stack. The TON whitepaper makes the distinction between TON Services and Applications, with the former relating to the network layer of TON and the latter referring to the user facing end. The Services end will be seeded with functionality[41] from the TON Foundation, starting with Storage, Proxy and DNS[42], however, the expectation is for an ecosystem of validators, protocol developers and other parties to participate in the network-side economy. Below we provide a list of the use cases we see *Grams* being deployed in, in the supply side of TON.

[41] This is a provision seen in the whitepaper, the state of development of which, is still unknown.
[42] We explore these in depth in Part 2.

a. Staking from validators and nominators in order to participate in TON's variant of PoS consensus.
b. Payments to nodes/validators for verifying transactions and smart contracts[43].
c. Payments to the masterchain in order to publish a new workchain.
d. Vote on governance decisions (e.g. regarding the adoption of changes on the TON protocol).
e. Payments for storing files in TON Storage - distributed file storage system with access to Torrent technology and the use of smart contracts to maintain stability.
f. Payments for TON DNS and WWW (World Wide Web) - similar to a DNS system that provides synchronization of IP addresses and domains. The TON DNS will provide the ability to have "human" names for accounts, smart contracts, services, and nodes.

"It appears that TON is learning from the successes and failures of those that came before them, by bridging the supply and demand sides of the network, through the use of *Grams*."

Overall, what TON proposes is a fully-fledged ecosystem in which Grams find ample use cases. The architecture of TON, which we will explore in Part 2, is an amalgamation of various propositions that have been put into production from TON's proponents in the blockchain space. The type of utility that *Grams* are poised to find, follow suit; it appears that TON is learning from the successes and failures of those that came before them, by bridging the supply and demand sides of the network, through the use of *Grams*.

We often see blockchain based networks - especially those jumpstarted by incumbents with established fiat revenue streams - concentrate the token flow within the supply side of the network[44]. We think that design decision impairs the long term viability of a token economy, as effectively it leaves only one value absorption gateway open - from Dapp developers to validators[45], and splits the ecosystem into two, limiting the potential network effect the token economy can achieve. TON introduces enough value sinks in the token flow, that - in theory - should provide a good foundation for the *Gram* economy to grow on. However, given some of the demand-side risks utility tokens face, it also appears that ensuring that end-users are not wiped out by volatility is table stakes.

[43] TON will have around 100 validator nodes confirming each block on the chain. Each workchain will have 1024 smaller validators who are selected pseudo-randomly every 1024 blocks.
[44] Refer to the Appendix (Figure 1) for a schematic of the differennt types of value flow in modern day blockchains.
[45] e.g. developers collect fiat from users and with some of that, they buy and stake tokens in order to secure "real estate" on the network and pay validators for network resources.

Part 2: The current state of the Telegram Open Network

"TON positions itself as an entire ecosystem, presented as an amalgamation of some of the most dominant ideas that have surfaced in the blockchain space over the past 10 years."

This part of the report is dedicated to abstracting away the complexity in the architecture of TON, by examining its components, as proposed by the documents TON has made public, and adding to the context around those with an evaluation of recent developments in the ecosystem.

Part 2 was primarily based on a review of the:

- TON Whitepaper [46]
- TON Blockchain description[47]
- Telegram Open Network Virtual Machine description [48]
- TON Labs Toolchain and related documentation[49]
- TON SDK Client Library and related documentation[50]

Project	Year	G.	Cons.	Sm.	Ch.	R.	Sh.	Int.
Bitcoin	2009	1	PoW	no	1			
Ethereum	2013, 2015	2	PoW	yes	1			
NXT	2014	2+	PoS	no	1			
Tezos	2017, ?	2+	PoS	yes	1			
Casper	2015, (2017)	3	PoW/PoS	yes	1			
BitShares	2013, 2014	3′	DPoS	no	m	ht.	no	L
EOS	2016, (2018)	4	DPoS	yes	m	ht.	no	L
PolkaDot	2016, (2019)	4	PoS BFT	yes	m	ht.	no	L
Cosmos	2017, ?	4	PoS BFT	yes	m	ht.	no	L
TON	2017, (2018)	5	PoS BFT	yes	m	mix	dyn.	T

Figure 22: An overview of the defining characteristics of preceding and competing protocols as proposed in the TON whitepaper.

2.1. Taking TON apart; a review of TON's architecture

TON positions itself as an entire ecosystem, and is presented as an amalgamation of some of the most dominant ideas that have surfaced in the distributed web and cryptoasset space over the past 10 years. While there appears to be less innovation in each piece that makes up the whole, there is a lot in the assemblage of it all. The main aim of TON is to solve for the scalability problem in distributed networks of computation and value transfer,

[46] [Access here: https://test.ton.org/ton.pdf]
[47] [Access here: https://test.ton.org/tblkch.pdf]
[48] [Access here: https://test.ton.org/tvm.pdf]
[49] [Access here: https://github.com/tonlabs/ton-client-rs]
[50] [Access here: https://docs.ton.dev/86757ecb2/p/09bb3d]

with the ultimate goal of facilitating millions of transactions per second. TON aims to achieve that by sharding and Proof of Stake[51]. So far, there are several PoS blockchains functioning but there are no production ready, shard-based blockchains - though there are several in development that are tightly or loosely endorsing the approach, including Ethereum 2.0, Polkadot and Cosmos.

TON is, in effect, a net of blockchains, separated into 3 distinct layers:

- The *masterchain*; a settlement layer that binds the system together - similarly to the Beacon chain in Ethereum 2.0's or the Cosmos Hub in Cosmos' designs[52].
- The *workchains*; blockchains with their own set of rules that reference back to the *masterchain* to sync on global state of the TON ecosystem.
- The *shardchains*; use-case specific blockchains that reference back to the *workchains* for their specific strand of functionality. This is where user level interactions take place in the TON ecosystem.

"TON solves for scalability and interoperability by designing according to the *Infinite Sharding Paradigm*."

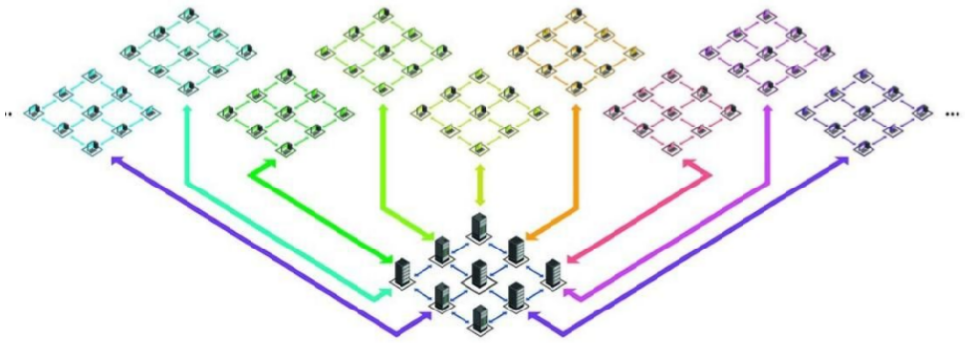


Figure 23: High-level schematic of TON's architecture.

TON's architecture is dynamic in character. TON solves for scalability and interoperability by designing according to the *Infinite Sharding Paradigm*[53], with a bottom-up approach, where each shardchain is perceived as its own account. These accounts are then grouped together based on their proximity in the network space[54], allowing for messages

[51] While sharding is a common concept in (centralized) database engineering, since it is unproven in a blockchain paradigm, it often attracts a lot of criticism. For those interested, we have prepared a set of notes to help a deeper dive into sharding. [Access here: http://bit.ly/2lzhisQ]
[52] We encourage interested readers to review our synopsis of the Ethereum 2.0 roadmap for context. [Access herre: http://bit.ly/2mFxnx6]
[53] The premise here is that data is represented in such a way that divisibility of data structures in TON is possible at a granular level. The whitepaper presents this idea, as "everything is a bag of cells", where data is represented as cells with up to four pointers to other cells, which makes cells interconnected at the lowest level.
[54] Benchmarked by the numerical proximity of their 256-bit addresses.

"In order to be resource efficient, shards that undergo activity overload can be split and merged back again."

to travel across the network at high speeds. In order to be resource-efficient, shards that undergo activity overload can be split, while the opposite is true for shards with low activity allowing for messages[55] to travel across the network at high speeds. In order to be resource-efficient, shards that undergo activity overload can be split, while the opposite is true for shards with low activity - all while maintaining continuity of state[56]. Block time is set to approximately 5 seconds, which will expectedly lead to short transaction confirmation times[57]. TON insulates the system against hostile forks by slashing the apostate validators' stakes. While as in all PoS systems it is still theoretically possible to mount a Sybil attack, presumably by the time the state on TON becomes so valuable so as to entice the *majority* of validators to collude, their stakes will be worth more than the expected value of the fork[58].

2.1.1 The TON Blockchain

This is the beating heart of TON. The blockchain is responsible for all value operations, storing and executing smart contracts, as well as interoperating with other blockchain ecosystems.

2.1.1.1. The masterchain

"The masterchain is responsible for governance and base-layer consensus in TON's PoS."

The masterchain is a specific chain (with workchain_id = -1), and acts as the base layer for the network and the connection dock between all other shardchains. The masterchain is responsible for governance (validator list) and for base layer consensus in TON's PoS. It is the layer that guarantees security for the rest of the network and contains information about the status of all workchains and shards. This is the layer also responsible for hosting smart-contract state. The smart contracts in this layer might manage anything from the validator list to the inflation for the *Gram* token economy. The set of validators that secure the masterchain will start at 100 and might increase to 1000[59]. The hash of the last masterchain block determines the overall state of the system, such that monitoring the state of all shardchains separately is not necessary. TON is currently using SHA-256 as the hashing function. If this turns out to be weaker than expected, it can be replaced by another hash function in the future. The choice of the hash function is a configurable parameter of the protocol, and can be changed without a hard fork, through voting.

[55] Messages are the primary vehicle for information exchange on the TON Blockchain. That includes any type of value transfer or state change update. Messages incur fees, as every other operation on the chain.
[56] The whitepaper provides an example of overload and underutilization conditions; for the former it benchmarks 90% of the block being full for 5 or more consecutive minutes, while for the latter it benchmarks 60% of a block's computation limit (size) for the two "sibling" shardchains combined.
[57] The chosen interval appears unrealistically fast - considering the time at which the first iteration of the whitepaper was published (December 2017), in a social context, claiming ultra-fast transaction capability was table stakes.
[58] In Proof of Stake the risk of forking or malicious attacks is never perfectly 0 - i.e. a highly motivated, cost agnostic actor, could - in theory - break the system. In practice this is highly unlikely.
[59] There are still many looming questions about (i) how validators will be selected and (ii) how consensus and governance will be streamlined as the list of validators grows towards 1000.

2.1.1.2. The workchains

The workchains are separate, domain specific blockchains that run on limited functionality virtual machines, and are bound by their own rules, programming language and cryptoeconomic primitives. Workchains are similar to *parachains* in Polkadot's, or *zones* in Comos's design. At launch, TON will come only with workchain zero (workchain_id = 0) enabled - the chain that contains the initial state and logic for *Grams* and TON Smart Contracts. It is expected that most applications will only require workchain zero.

"To become active a new workchain must have ⅔ consensus from validators."

Anyone that is part of the network can create a new workchain if they pay a masterchain transaction fee, required to publish the formal spec for a new workchain. To become active, a new workchain must have ⅔ consensus from active validators. Validators will have to upgrade their software to handle blocks/transactions on this new chain, so the parties behind the new workchain may need to offer some sort of incentive. Workchains produce blocks with 1-second delay to other shardchains and store the root hashes of the states of other chains. TON provisions for 2^{32} workchains, where each workchain can host its own native cryptoasset (*currency_id = n*), effectively raising the number of of cryptocurrencies that can be spawned on TON, to 2^{32}. As with workchain zero, *Grams* are annotated as *currency_id = 0,* while other cryptoassets that will live on TON, will sequentially assume *currency_id's* that span from 1 to 2^{32}*.*

"Workchains allow for multiple programming languages to be deployed on top of them."

Workchains play an integral role in enabling interoperability between different chains as their design allows for multiple programming languages to be deployed on top of them. To illustrate, a developer could implement the light client node logic of Bitcoin (with code written in C), with a custom coin (such as wrapped BTC) and references to the Bitcoin blockchain, in order to link TON with the Bitcoin blockchain. In other words, the developer can write a smart contract that will read data from a Bitcoin node, check that the balance is updated on a specific address, and then mint wrapped BTC tokens in the TON workchain[60].

2.1.1.3. The shardchains

Each workchain is in turn subdivided into up to 2^{60} shardchains that are bound to the same rules and block format as the workchain they are attached to, but are responsible only for a subset of accounts. Each shardchain is allocated a random set of validators

[60] This is potentially one more interesting space for market makers to operate in, arbitraging on the latency between message propagation between blockchains.

"...this particular feature safeguards TON from chain rollbacks, that can cause a lot of damage in the process of restoring state to a previous timestamp."

responsible for creating and validating new blocks[61]. Each block within a shardchain[62] is conceptualized as its own blockchain[63], so that if invalid blocks need to be changed, a new block is committed that contains the residual information necessary to correct whatever imbalance the invalid block caused[64]. This particular feature safeguards TON from chain rollbacks that can cause a lot more damage in the process of restoring state to a previous timestamp, by recalling all valid transactions that took place between the event and the initiation of the rollback[65].

2.1.1.4. Instant Hypercube Message Routing

Interoperability between shardchains is facilitated by Instant Hypercube Message Routing (IHMR) - a protocol for propagating messages across shards. Each shard is connected to other shards differing in exactly one hexadecimal digit of their shard identifiers. All shardchains constitute a "hypercube" graph[66], and messages travel along the edges of this hypercube. In IHMR, messages travel along a slow path or a fast path. On the slow path, messages hop from one neighboring shard to the other - a process that guarantees delivery albeit being slow and expensive, while on the fast path, messages can travel directly between shards that lie further from one another in the network space[67]. The two approaches run in parallel. If a proof of the success of the fast method is committed to an intermediate shardchain, the slow method can be aborted. Either way the message gets delivered. The array of sent messages between shards is a complex multidimensional DAG. IHMR effectively enables the delivery of a message created in a block of one shardchain into the very next block of the destination shardchain, regardless of the total number of shardchains in the system.

2.1.1.5. TVM (TON Virtual Machine)

Virtual Machines are the computation layer for smart contracts in the blockchain world. The TVM is used to execute smart contract logic in the masterchain and the base workchain, can run several processes simultaneously and packs data tight[68], making it

[61] The exact process with which validators are selected is unclear.
[62] Shards have two parts; a split and a non-split. The split part consists of account, smart-contract, balance and transaction history information. The non-split part consists of the information about all the accounts, with which this shard is connected. At the moment, it is unclear in which cases of cross-shard communication only the header of a block or the full body of a block will be transmitted. Without clear definition this could become a point of a double-spend attack on cross-shard transactions.
[63] Referencing the Infinite Sharding Paradigm.
[64] In effect, the best visual proxy for TON's architecture is that of a snowflake. [Access here: http://bit.ly/2n5M50v]
[65] It is as of yet unclear what the resource prioritization will be in shards that need repair (i.e. smaller first, larger first or global repair?)
[66] Refer to Figure 3 in the Appendix for an illustration of a hypercube graph.
[67] Both mechanisms are deployed in parallel, and the slow routing is aborted only when a proof that the fast path was successful in delivering the message. The slow path guarantees delivery and is therefore used to ensure that crucial information about state updates is never missed (on the fast path, it is more likely that the validators of the destination shardchain, might "miss" the broadcasted message).
[68] Data is represented as a collection of cells. Each cell contains up to 128 data bytes and 4 references to other cells.

efficient and fast. This also implies that its design supports interchain compatibility, such that validators from any chain can verify transactions on any other chain. The architecture of the TVM makes it more suitable to execute code written in higher level languages like Java - however, these will not be supported out of the box. The benefit here is that high level languages are easier to code, debug and maintain. The flipside is that programs written in high level languages are comparatively slower, less memory efficient and cannot communicate directly with the hardware (such as servers etc). The memory efficiency aspect can become a thorny issue down the line, as deployment on TON appears to be expensive. Whether it will prove to be a feature - by forcing developers to prioritize-efficiency with the programs they deploy, or a bug - by deterring experimentation and thus to some extent iterative development, remains to be seen as adoption ensues.

"The architecture of the TVM can host higher level languages like Java - however, these will not be supported out of the box."

2.1.1.6. Smart contracts

TON makes a distinction between local and global smart contracts; the former need not be aware of the global state (reference the masterchain), while the latter do. The way smart contract logic works in TON is almost like a hybrid between Bitcoin and Ethereum; the message system is similar to the one that Bitcoin employs for state updates, while the functionality of smart-contract code, addresses, etc. are similar to Ethereum. The disadvantage here is the price of operation. To illustrate, when a smart contract is deployed on the TON blockchain, there is a requirement for paying rent (in *Grams*), even if the contract is not in use - which introduces an overhead for developers, in that they have to use their allocated storage wisely.

This idea is contrary to Ethereum's architecture, where the user pays (in Gas) just for the amount of data they consume, but not for the time[69]. On the flipside though, the advantage of such a system is that it forces developers to be careful with what they deploy on-chain (removing clutter) and introduces an additional layer of security. TON also promises to deploy parallel sending and writing of smart-contracts. This feature, known as *multithreading*, allows working simultaneously with high load project with multiple computations on different smart contracts. At the time of writing, it seems that this is a feature to be deployed down the line.

"...the advantage of such a system is that it forces developers to be careful with what they deploy on-chain."

2.1.1.7. The role of validators, nominators, fishermen and collators

As in all PoS blockchains, validators[70] are nodes that are tasked with confirming and reporting the state of the blockchain truthfully to the rest of the network. A validator operation is a non-trivial activity that requires considerable disk space, computing

[69] This approach is not efficient, as it introduces additional clutter on the Ethereum chain and will be replaced in future versions of the Ethereum platform.
[70] Validators in PoS, equate to miners in Proof of Work (e.g. in Bitcoin)

"In order to become a validator candidate, interested parties will have to stake a minimum of 100k Grams."

power, and network bandwidth. Validators on TON will use an efficient variant of the BFT (Byzantine Fault Tolerant) consensus protocol, similar to PBFT or Honey Badger BFT. Each validator may be in multiple validator subsets and be expected to run validation/consensus algorithms in parallel. In order to become a validator candidate, interested parties will have to stake a minimum of 100k Grams. In order to become an active validator[71], however, it is likely that the minimum requirement of Grams will be much higher[72]. Active validators perform useful work for the network and in return, receive inflationary rewards (in Grams), proportional to their stake.

Validators need to run 2 smart contracts; the controller & the elector. The former interacts with other contracts to run the validator, while the latter enables one to participate in validator elections or collect unfrozen stakes and bonuses. Validators must ensure that they keep uptime, perform computations requested by smart contracts, receive updates about other shardchains etc, or risk getting slashed[73] partly or fully, and even getting permanently excluded from the validator candidate pool. The estimated token denominated annualized return for TON validators stands at approx. 20% of the validators stake - according to the whitepaper[74]. If this is indeed true, it would place *Grams* among the highest yielding PoS cryptoassets in the Top-100.

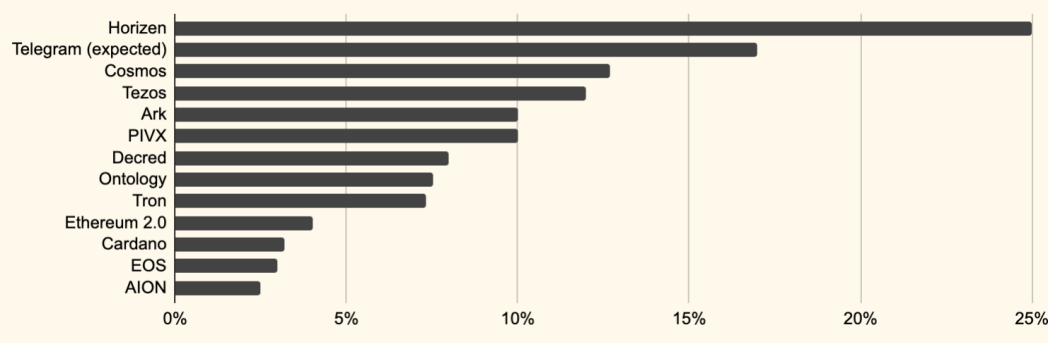


Figure 24: Annualized (token denominated expected) returns in popular PoS networks.

"The estimated annualized return stands at approx. 20% of the validators stake."

The global set of validators is known about one month in advance[75], while the local set is established about one hour in advance[76]. The validators' stakes are frozen for two months in order to make sure that validators are slashed if they are proven to misreport on the blockchain's state by fishermen or other network participants. The algorithm that selects task group validators each hour, is pseudo-random. All of the parameters for choosing validators could be later changed though voting. After the proposal is put forward, 2/3 of the total number of network validators need to agree to it, in order for it to take effect. There are also provisions in place, in order to limit the power of validators with large *Gram* holdings – they are however, still unclear.

[71] i.e. actually performing work and receiving rewards for it. Not all validator candidates will be active validators.
[72] Which could be as high as 10M Grams, according to reports from the early validator community.
[73] Slashing refers to the validators stake being burned.
[74] This could translate to 2% newly minted and 18% for tx/proc fees.
[75] Or 219 masterchain blocks.
[76] Or 210 masterchain blocks.

In rounding out the entities that help the system reach consensus, TON appears to have borrowed a page from Polkadot[77], introducing nominators, fishermen and collators, as consensus making parties. Below, we give a brief description of the role each of these parties fill in TON.

"Nominators piggyback on validators' infrastructure and large initial stake in exchange for a % off the validator rewards."

- **Nominators** are "delegators" that lend their holdings to validators, with a view to profit sharing. Effectively Nominators piggyback on validators' infrastructure and large initial stake in exchange for a % off the proportional rewards. The return profile that nominators are exposed to depends wholly on the validator's performance. Present validators, nominators "vote" for validators by lending them Grams. Nominators can be individual holders of Grams or staking pools who will collect Grams from TON users and send them to the TON smart contract to become a validator, acting like delegates. If they succeed, the members of the staking pool receive the reward and distribute it depending on the invested assets percentage.

- **Fishermen** can be thought of as light validators that oversee other validators. If a fisherman successfully reports a misbehaving validator, then that validator's stake is slashed and the fisherman receives part of it as a reward. Fishermen will operate locally (shardchains) and although requiring less computing power than validators to operate, it will still be non-trivial.

- **Collators** act as a support function, by suggesting candidate blocks for inclusion in the blockchain to validators - one can imagine them as the validators' associates. Collators are paid by the validators for the services they provide - via sharing a % from the block rewards. Collators will only start appearing as the ecosystem grows.

Actor	Required node	Economic incentive	Participation
Validators	Full node	Validation reward	Validate blocks
Fisherman	Full node	Partial payout of slashed stake	Masterchain tx to publish invalidity proofs
Nominator	undefined	Partial payout of validation reward	Provide validator with capital
Collator	undefined	Partial payout of validation reward	Point out shardchain block candidates

Figure 25: Classification of integral consensus parties by defining characteristics.

2.1.1.8. Programming on TON; Fift

TON is proposing a new programming language to run at its core; Fift. While technically multiple types of VMs and programming languages can be deployed on different

[77] We view this design decision favourably, as Polkadot's design although not yet in production, is theoretically the most well balanced design proposed in PoS thus far.

"Fift was chosen for high usability in terms of nodes' connections - acting as the nuts and bolts that bring the 'everything is a bag of cells' design philosophy to life."

workchains, Fift is designed specifically for developing and managing TON smart contracts on *workchain_id=0* (the masterchain). Fift is an abbreviation of Forth - a 50 year old programming language, known for simplicity, extensibility, and enabling powerful programs. In this case it appears it was chosen for high usability in terms of nodes' connections - acting as the nuts and bolts that bring the "everything is a bag of cells" design philosophy to life. To illustrate, a developer can take two different nodes or even part of nodes and connect all the necessary parts in their smart contract using Fift, and extending that logic any part of the program can be divided and assembled backwards.

Perhaps an assertion one can make - besides the functional benefits of choosing Fift as the core programming language for TON - is that the core developers want to (i) increase their level of control over the core protocol and/or (ii) create a mechanism for self-selection, such that only the worthy become part of the "small council" that decides the fate of the core protocol. To illustrate, Fift employs Polish notation, which at least on the surface does not have any functional benefits. In fact, if anything it makes learning (let alone mastering) it, all the more challenging. This increases the potential risk for protocol level mishaps, as it is both easier to make mistakes - even as an experienced developer - and harder for third parties to audit the contracts deployed. Given that blockchains have value transfer in their core, both the risk and the EV of critical failures, increase.

2.2. Best of the rest; other key pieces of the TON stack

The information that TON has released at the time of writing also foresees the following on- and off-chain applications that complete the vision for the network stack. To avoid overload, this section will be limited to brief descriptions of these:

2.2.1. TON Payments

"Workchains will be able to support both free and paid state storage."

A highly secure, fast and decentralized payment system with a transaction speed comparable to that of Visa and MasterCard. Payments are generalizable to any unit of account - i.e. it will facilitate the transfer of far more than just *Grams*. Although it introduces innovations such as *smart payment channels* that enforce smart contract logic on state channels, and an optimization for the number of nodes necessary to securely support such as system, it still remains at the concept stage and will not be launched until after the network is up and running.

2.2.2. TON Storage

File-storage technology available for storing files with torrent-like access technology and smart contracts used to enforce availability. TON Storage employs 'Merkle trees' to store hashes of the data, allowing data operations at high speeds. The module is also the core data store technology for the TON Blockchain. In its simplest form, it allows users to store files off-chain, by keeping on-chain only a hash of the file to be stored,

and possibly a smart contract where some other parties agree to keep the file in question for a given period of time for a pre-negotiated fee. Workchains will be able to have both free and paid state storage. Paid (like Ethereum has) will make users to pay for every action - transferring coins, for instance. Free portions are going to be limited by the threshold set by workchain logic - i.e. one might be able to run small transactions without fee on some workchains. Validators are also expected to act as "caretakers", tending to removing any accounts or smart contracts that are not utilized, to decrease the blockchain size.

"Validators are also expected to act as 'caretakers', tending to removing any accounts or smart contracts that are not utilized, to decrease the blockchain size."

2.2.3. TON Networking

TON's networking architecture is built on the Abstract Datagram Network Layer (ADNL), a layer that regulates how all the TON nodes connect and share data. ANDL itself is an abstraction over the commonly used UDP protocol. Further up the networking stack, one finds a Reliable Large Datagram Protocol (RLDP), along with a series of Gossip and Multicast protocols. The former is a transport layer abstraction that optimizes for speed, while the latter moderate communication between use case specific clusters in the greater network (e.g. payment channel networks, storage networks, block propagation networks etc). The networking stack is completed by a Kademlia-like distributed hash table (TON DHT), that every TON supporting node across the core protocol or services and apps on top of it, will be using[78]. What the table effectively does, is to keep reference of every node in the network, so that queries are fast and effective.

2.2.4. TON DNS

A service to assign human-readable names to accounts that will allow users to access decentralized services as easily as browsing the World Wide Web. TON's DNS will allow all the TON clients to quickly find and connect to the Messenger service, increasing the security and overall privacy of the Messenger - which also potentially explains the decisions to design a DNS from the ground-up.

"TON DHT helps keep reference of every node in the network, so that queries are fast and effective."

2.2.5. TON Proxy

An anonymizer layer, similar to TOR[79]. This layer can be used to create decentralized VPN services and blockchain-based TOR alternatives to achieve anonymity and protect online privacy. In place to primarily protect large entities on the network (e.g validators) from DDoS attacks.

[78] The DHT can be used as a "torrent tracker" for TON Storage, as an "input tunnel locator" for TON Proxy, and as a service locator for TON Services.
[79] Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".

2.2.6. TON Services

"TON Services is a pluggable utilities layer, akin to AWS's or Azure's suite of cloud services."

This is a pluggable application/utilities layer (akin to AWS's or Azure's suite of cloud services) that will initially is expected to be seeded with utility by TON, with modules such as DNS, Storage, Proxy and Payments discussed above. These services will live in a spectrum between purely on-chain and purely off-chain based and will be connected with one another and the TON Blockchain, through the TON Networking layer. The purpose of this layer will be to provide valuable tools for developers, while not requiring a direct interaction with the base layer (i.e. the TON Blockchain).

2.3. Developer communities & recent updates

2.3.1. TON core, TON Labs and the early settlers

"TON has two main research groups working on its development; TON core and TON Labs. The two co-exist like Parity and Geth on Ethereum."

TON has two main research groups working on TON's development; TON core and TON Labs. The two co-exist like Parity and Geth on Ethereum, working on the client in a language of their choice - TON core opting for C++ and TON Labs opting for Rust.

TON Labs have consistently publicly claimed their arm's length relationship with Telegram and complementary (to TON) nature of their solutions.

The business model of TON Labs follows the standard open-source model, and is based on providing network infrastructure and cloud and enterprise services.

TON core, led by the Durov brothers, is using the main Github repository[80] for delivering code in stealth mode[81]. While stealth development has its advantages early on, members of the wider TON developer community we interviewed expressed frustration over the unpredictability of it all. Further, we currently have no way of knowing exactly how many people are working with TON core at the moment, but assuming that each of the released modules has a dedicated team, we can approximate that there are currently 10 to 20 core developers putting time towards protocol-level work.

What TON core has released so far:

- TON node and validator software
- a CLI based "lite-client", with limited support for the Testnet
- a Testnet explorer

[80] [Access here: https://github.com/ton-blockchain/ton]
[81] No public development is allowed in this repo.

- in depth technical documentation on the TON Virtual Machine, the TON Blockchain, and Fift.

TON Labs, on the other hand, are more open to the general public about future plans; at the moment, they are reportedly working on extending the LLVM compiler they recently released for TON, while later planning to develop two-way payment gateways for cross-blockchain interoperability.

"Developers in the community we have spoken to, view TON Labs as a high value-add entity."

What TON Labs has released so far in their SDL:

- a local node server and node wrapper
- an ArangeDB database queried via GraphQL
- compilers that take Solidity and C and partially C++ code and compiles it down to TVM bytecode[82]. In the near future, the LLVM compiler is also poised to support Rust - a C++ lookalike, modern systems-level programming language, focused on safe concurrency[83], and SWIFT

Developers in the community we have spoken to, view TON Labs as the more approachable entity in this small universe, and have found all their releases to be high value-add. Indicatively, the node wrapper they recently released, brings the sync time for nodes to less than a minute – down from ~10 hours, while the Arange DB database makes it so that Dapp developers will no need to interact with the blockchain layer of TON. TON Labs also announced a partnership with Wirecard[84], back in April 2019, through which they aim to develop a suite of financial services that link the legacy consumer finance world with TON.

Besides the two aforementioned entities, there are a few open working groups consisting of independent researchers and developers that are the early consumers of TON infrastructure. Our research points to the largest of those communities being *Copper-Bits*[85], while we also discovered an organization called *Formony*, that has published a python API client for the TON blockchain.

"At the moment, TON is live in Testnet mode, with approximately 100 nodes running."

2.3.2. Current state of development

At the moment, TON is live in Testnet mode, with approximately 100 nodes running - presumably many of which are controlled by TON core and TON Labs. Engineers in the validator community outside the two main hubs, reference the need for a lot of backward induction in order to set up a validator node in Testnet and an overall lack of streamlined

[82] The compiler is still at 20%-30% completion rate, deeming what is out there as a bare-bones PoC.
[83] In computer science, concurrency is the ability of different parts or units of a program, algorithm, or problem to be executed out-of-order or in partial order, without affecting the final outcome.
[84] Wirecard is one of the world's leading full-service providers of products and services for electronic payments, servicing some of the largest fintech companies, including Revolut and Atom Bank.
[85] [Access here: https://github.com/copperbits/TON]

communication channels, which make the process difficult. On the flipside though, we are informed that more recently TON core is proceeding with frequent update releases in the TON repo, in an organized and consistent fashion – a process well received by the early developer community.

"More recently TON core is pushing updates in the Github repo, in an organized and consistent fashion."

tdutils	updated tonlib, new fullnode queries	3 days ago
terminal	liteclient signature check support	13 days ago
test	updated block header	9 days ago
third-party	updated tonlib	5 days ago
tl-utils	initial commit	20 days ago
tl	tonlib updated	2 days ago
ton	fullnode: support for TCP master/slave replication	8 days ago
tonlib	tonlib updated	2 days ago
utils	initial commit	20 days ago
validator-engine-console	changed validate broadcast logic, added new queries to	16 days ago
validator-engine	fullnode: added getCapabilities query	3 days ago
validator-session	tonlib updated	2 days ago
validator	tonlib updated	2 days ago

Figure 26: Snapshot of TON's main Github repository and recent code releases there.

Telegram also recently announced the launch of a hackathon, with a total prize pool of ~$400k[86]. The competition is focused on (i) building smart contracts for the TON Blockchain, (ii) suggesting improvements for the TON VM, and (iii) finding and fixing issues on the Testnet. Participants are expected to implement at least one of the five suggested smart contracts, including multi-signature wallet, two types of simple TON DNS Resolver smart contracts, a synchronous two-party payment channel, and an asynchronous two-party payment channel. The response from the developer community has been overwhelmingly positive. As it stands, there are 64k members in the Telegram Contests group, while the announcement for the competition over 350k views.

"Telegram also announced the launch of a TON focused hackathon, with a total prize pool of ~$400k."

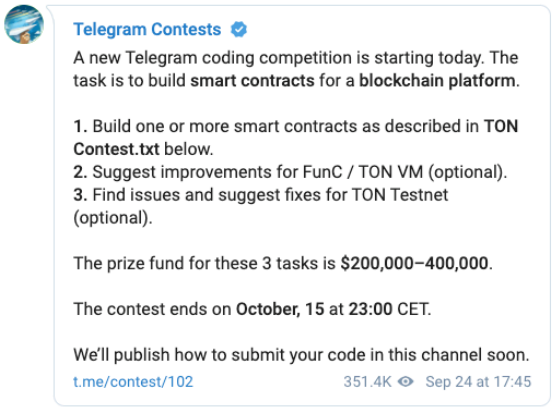


Figure 27: Snapshot of the original announcement of the TON Contest.

[86] [Access here: https://t.me/contest/102]

2.3.3. Looking ahead

At the time of its fundraise, TON had set out the grand vision of having the platform fully rolled out by 2021, at which point it would transition from “Telegram Open Network” to “The Open Network” and the open source community would take the reigns. However, given the team’s delivery history thus far, the current market conditions, the technical complexity in bringing all the pieces together and attracting developers both in-house and into the broader community on TON, we believe that delivery in 2022 (at the earliest) is a more likely outcome.

Date	Events and Milestones	Actual delivery	Delay
Q2 2017	Start of the development of TON	-	
Q1 2018	Launch of Telegram External Secure ID	-	
Q2 2018	Launch of the Minimal Viable Test Network of TON	Q3 2019	1+ years
Q3 2018	Testing and security audits of TON	Expected in Q4 2019	1+ years
Q4 2018	Deployment of the stable version of TON	Q4 2019	1 year
Q4 2018	Launch of Telegram Wallet	Q4 2019	1 year
Q1 2019	Creation of TON-based economy in Telegram	Expected in Q1 2020	1+ years
Q2 2019	Launch of TON Services, Storage and Proxy	Expected in Q2 2020	1+ years

Figure 28: Updated roadmap as initially featured in the TON Primer.

According to information that members of the TON developer community have shared with us, TON core’s immediate development plans include the development of standard techniques and algorithms such as airdrops, timelocks, escrows, oracles, smart contracts, DAOs, voting process structure, governance, etc.

Over the longer term, we expect the team to release privacy features for secure transactions - however, at this point in time it is almost impossible to predict how this feature will look like and when exactly it will be delivered.

Part 3: Discussion

TON has undeniable promise as a 5th generation blockchain designed to solve the key issues that those that preceded it uncovered in the blockchain space. At the same time, there are many challenging factors which will define the fate of TON and the *Gram* as an investable asset, including uncertainty in the macro environment, the project's many technical intricacies, the cryptoeconomic model that underpins the network's native asset (the *Gram*), and the contempt that many governments have for the network's front-end (the Telegram messenger) as a harbor for illicit activity. These issues are discussed in sections 3.1 to 3.3 below.

"TON has undeniable promise as a 5th generation blockchain."

3.1. All those in favour...

3.1.1. A huge market opportunity

A little over 10 years ago, the Bitcoin whitepaper proposed a proof on solving the double spending problem, planting the seed for the first digitally native monetary unit. 5 years ago, Ethereum introduced the concept of programmability in digitally native, money-like assets, opening up a blue ocean of opportunity with the idea of smart contract based applications. As the space matured, the lack of a de-facto distribution platform - like the App Store is for the Web 2.0 world - has become an obvious hurdle to conquer. TON could be that platform. If delivered as intended, with 250M (and growing) active users, the majority of whom are located in parts of the world where they cannot access the full breadth of financial services available in the West, TON can be the gateway for cryptoassets and the related applications to "bank the unbanked".

"If delivered as intended, TON can be the gateway for cryptoassets and the related applications to 'bank the unbanked'."

The use case for a financial system enclosed in a messaging app is beyond any doubt, courtesy of WeChat's spectacular growth in China since 2011. It is estimated that in 2018, WeChat processed transactions north of $20T in value[87] amongst an estimated 1B MAU[88] - a tremendous feat in creating and capturing value in the short span of 8 years. Besides payments, users of WeChat can access a series of services that span from managing credit cards to purchasing insurance[89]. However, the WeChat model is not easily generalizable at a global scale, as the tall structures that govern Chinese society, allow for privacy violations that are not tolerated in other parts of the world.

This is where the combination of a net of interoperable, value storing blockchains, and the Telegram front-end can really shine, as a permissionless system that connects

[87] [Access here: http://bit.ly/2n7o3Tj]
[88] [Access here: http://bit.ly/2nSuxW8]
[89] Other use cases include scheduling doctor appointments, paying traffic fines, bike sharing, booking transportation, checking crowd density, searching for online trends, making contributions, business communication and tracking, calling landlines or other mobile devices.

"Assuming volumes similar to those WeChat processed in 2018 and a 0.1% transaction fee, the annual value stream to validators stands at ~$20B."

multiple blockchains, protocols and the apps and services built on top of these, with millions of users, where the only blockage to value flow is in the bridge between the legacy fiat world and the cryptoasset world.

The growth of the DeFi ecosystem within Ethereum[90] is a strong testament to the traction that the application side of the platform is getting. WeChat is proof that the user need exists. All that seems to be missing is a platform to link the two. TON has the potential for market leadership in this space, and *Grams* as the native protocol token have the potential to capture some of that value creation.

To illustrate, given the above figures, if one assumes that *Grams* will only be used to secure the network and act as a vehicle for validators to capture ledger fees, at transaction volumes similar to those of WeChat in 2018 and assuming a 0.1% transaction fee[91], the potential annual value stream is ~$20B. That said, while the promise is undeniably there, there are many obstacles in the way of TON achieving this scale, which we explore in section 3.2 of this paper.

3.1.2. A collection of promising technologies

Both at the protocol and application layers, TON proposes a collection of some of the best tech that has been iterated upon over the last 10 years in the blockchain world . While there is much to be proven still in the deployment of it all, we cannot help but ascribe merit where it is due. TON, along with NEAR protocol, will be the first sharded blockchains network to go into production. By splitting activity centers in the network into shards that are responsible for most of the local resource management, TON promises transaction speed and resource efficiency never before seen in a global distributed network of value - a sorely needed addition to the space.

At the same time, contrary to DPoS blockchains that centralize consensus among a closed group of validators and create opportunities for collusion, eroding the integrity of the chain[92], TON's architecture has budgeted both for performance and sufficient decentralization. Some of the more granular highlights from the architecture include (i) the Infinite Sharding Paradigm, (ii) the dynamic messaging system for cross-shard communication, and (iii) the efficient resource management via sharding that makes DevOps more manageable at the local level.

[90] DeFi is an abbreviation of Decentralized Finance, and refers to a collection of on-chain applications that propose novel ways to translate banking and finance services, on chain. At the time of writing the total value of assets locked in DeFi, currently stands at 3M ETH (or ~500M USD), having increased by 450x in USD terms since October 2017.
[91] For reference, Visa currently charges merchants 1.51% plus $0.10 for a swiped consumer credit card, while Stripe charges 2.9% and $0.30 for online purchases.
[92] See 'Rampant Collusion in EOS Exposed by Huobi Leak' on Trustnodes [Access here: http://bit.ly/2oOEV1v]

3.1.3. A world class team on a mission

TON is brought to life by one of the most talented and resilient teams in the technology industry. Their track record speaks for itself; from releasing VKontakte and growing it to 500M accounts[93], to self-funding the development of the Telegram Messenger, to more than 250M active users with minimal marketing, and from championing the right of Internet users to privacy, to proving the hardness of their encryption technology and distributed server infrastructure during the Russian and Iranian ban campaigns in 2018, the team has proven beyond any doubt that they can build distributed systems at a global scale.

"The team has proven beyond any doubt that they can build distributed systems at a global scale."

3.2. And those that stand undecided…

3.2.1. Many unknowns in the token economy

When abstracting the protocol layer complexity away from blockchains, what remains is a predominantly 'social' technology. Blockchains are the vehicle for decades worth of insights from the fields of Game Theory and Mechanism Design to be deployed in industry, and native protocol assets (tokens) are the glue of it all. Good token economics and token economy management can help a network flourish. Conversely, bad token economics can break an otherwise fundamentally sound network by incentivizing (or not disincentivizing) adverse behaviours among the many stakeholders. In TON, while there are many commendable elements in the way the token economy is structured, there are also - still - a lot of unknowns which could sway the pendulum towards either side for the network.

"Bad token economics can break an otherwise fundamentally sound network by incentivizing adverse behaviours."

Figure 29: Zaki Manian's (Head of Research for TON's competitor - Cosmos) take on social scalability in blockchains today.

[93] VK is ranked 19th in Alexa's global Top 500 sites.

"The TON Foundation will neither be involved as validators, nor will they be buying back Grams."

The aspects of the token economy that we think TON has gotten right are (i) the multiple use cases they have instilled in *Grams* and the circular token economy that it has designed around them, and (ii) the dual token market (primary and secondary) that programmatically controls for wild price fluctuations by creating clear arbitrage opportunities between the minting facility and the open market. Given that a lot of the utility value in *Grams* is poised to come from payments, low volatility and an upwards trajectory in value are very important over the long term. While businesses and enterprise worldwide increasingly – albeit slowly - warm to the idea of transacting in tokens, extreme volatility is a not-so-silent killer.

On the other hand, there are some potential points of failure in the overall design that center around the poor initial distribution of Grams among the broader ecosystem. While we can only speculate about the propensity of early investors to also be validators, the relative concentration of Gram holdings - at network launch - is high. And to make matters worse, as Telegram informed investors in a recent letter, in order to comply with SEC guidelines, the TON Foundation and Reserve will neither be involved as validators in the initial phases of the launch, nor will they be buying back Grams, as the whitepaper initially suggested. This puts the network launch firmly between "a rock and a hard place". The risk of Grams being classified a security is nullified at the expense of a strong network launch.

"This type of centralization can deter new entrants by raising questions about the network's integrity."

With the Foundation out of the picture, and given the initial validator set is projected to be heavily concentrated among those early investors that are adequately prepared, it is not a far cry to expect a very concentrated launch phase. With the minimum stake requirement at 100k Grams, and the relative sophistication required to run a validator node, the pool of candidates becomes small. This also implies that this limited pool will be accruing the early validator rewards, until the network attracts more supply-side participants[94]. At the time of writing, there are a little more than a dozen entities setting up validator nodes in Testnet. This type of centralization can deter new entrants by raising questions about the network's governance and its overall integrity. And if not diffused quickly, can put the long term prospects of TON and the *Gram* as an investable asset in a precarious position.

3.3. And all those against…

3.3.1. A vision too grand

While an impressive proposition as a whole, the feasibility of TON is still a theoretical exercise. The team has been secretive in their endeavors since March 2018 and remains so, even as the network is less than a month away from launching.

[94] For an illustration of the problems that arise from a centralization of a staking token economy, see a report on the WAX Mainnet token economics we drew up, in May 2019. [Access here: http://bit.ly/2nnVuBb]

The lack of robust communication channels combined with the high technical complexity, leave us wondering whether the vision of TON, as it has been proposed, is actually possible in its entirety. While we have no doubts about the talent of the development team, we do have concerns about the amount of over-engineering that seems to be going into TON. Below we present some of the aspects of TON's architecture that could transform from big question marks to Achilles heels;

a) The Infinite Sharding Paradigm; as mentioned in Section 3.1.2, conceptually, the idea is nothing short of brilliant. Given, however, its novelty and the lack of a formal proof and/or exposure to the code that translates it into a system[95], we cannot help but question its feasibility. Over-promising and under-delivering is, sadly, almost the norm in the cryptoasset space. For context, Ethereum started its journey as the scalable world computer, only to find that they would have to build a new platform from the ground-up, a short 3 years after its initial launch, in order to fulfil that vision. That said, members of the validator community we interviewed, noted that early indications in TON's Testnet, are that the principles of the *Infinite Sharding Paradigm* seem to work, and expressed their excitement to see the full range of possibilities it might enable.

"While we have no doubts about the talent of the development team, we do have concerns about the amount of over-engineering that seems to be going into TON."

b) TON Networking; it is questionable whether the network can hit the throughput and latency targets it has set in the whitepaper, while a five second validation interval for block creation may not be - at all - necessary. While theoretically possible, with nodes placed thousands of miles apart, synched on a customized networking stack, such short intervals could lead to poor network performance (e.g. missed blocks)[96]. Again - theoretically, according to the *Infinite Sharding Paradigm,* these blocks would heal without the need for a rollback, so there would be no collateral damage. The feasibility of it all though, is still a question mark.

c) Governance; getting governance right is crucial in decentralized open source networks. A poorly governed system will fail to attract developers and users necessary to sustain itself over the long term. So far, little is known about how governance will be organized on TON. Given the similarities the consensus design in TON has with Polkadot, and the scale the network hopes to achieve, it is likely that coin voting will have a part to play in TON governance[97]. In that case, a TON Foundation actively diffusing the concentration of holdings and getting multiple parties involved to preserve the integrity of the network would be positive. The large initial concentration of holdings along with a feature of TON that allows users to open direct (and possibly private) payment channels with validators - deeming bribes a

[95] As of yet, we have come across no information that points to the TVM supporting the cellular structures that power the *Infinite Sharding Paradigm.*
[96] We understand that a custom networking stack is necessary to improve the hardness of the network, and given the team's experience keeping a network under attack from multiple governments (often concurrently) live, we believe that there are good reasons behind those particular design decisions
[97] We are firm in our belief that rough consensus [see here: https://en.wikipedia.org/wiki/Rough_consensus] doesn't work for large scale systems as well as formal on-chain governance.

possibility, are potentially serious confounding factors that could compromise the network's path to maturity.

"The fact that all blockchain history - except for the most recent 2 months - will be deposited in TON Storage, is a single point of failure."

d) TON Storage; the module lives further up the stack from TON Networking and through its dependency is subject to all the adverse effects that the unknowns in the networking layer could cause. Further, TON Storage is a module to be developed further down the line and given the delay in the delivery of TON, an early version of it is unlikely to go live before Q4 2020. Furthermore, it is possible that in the initial phases of the rollout, all Storage nodes would be run by the Foundation. The fact that all blockchain history - except for the most recent 2 months - will be deposited in TON Storage, is a single point of failure. While we understand that in the spirit of homogeneity, certain pieces of the TON puzzle need to be built from the ground up for the whole to work, we fail to find a good justification for this particular design decision. Provided that distributed cloud storage networks have been in iterative production in the blockchain space since at least 2014, we believe a better design decision to be an integration with one of those (e.g. the Tardigrade Cloud from Storj)[98]. This type of decision would enable TON to go live with distributed storage ready to go, and increase the overall decentralization in the network.

e) *Security & Privacy:* As an encrypted messaging service, Telegram has not escaped public criticism about the encryption techniques they have used over the years. Further, while their track record of protecting their users' data is good, it is not without stains. TON employs SHA-256 and SHA-512 as encryption hashes for the Blockchain and Passport respectively. Both are known to be susceptible to brute force attacks, and while pluggable and open to discussion, this particular design decision looks questionable. It is likely that the overall security of the system will be hardened with TON Proxy going live - a building block estimated to be released sometime in 2020/2021. Moreover, engineers in the developer community we spoke to, mentioned that deploying SNARKs and Bulletproofs on TON contracts will be a relatively simple process.

"Telegram has not escaped public criticism about the encryption techniques they have used over the years."

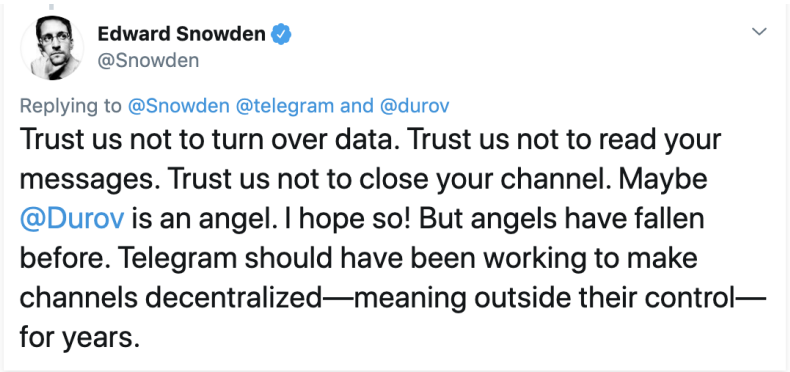


Figure 30: Edward Snowden's tweets echoing the overall public sentiment against Big Tech's mishaps, relating to sensitive consumer data.

[98] [Access here: https://storj.io/]. Without having an insight into the deep technical details of the project, we believe that modifying TON Proxy and TON DHT to be compatible with an existing distributed storage network, would both harden the network and save TON precious time and resources

f) Execution: given all of the above, along with the limited size of the core teams and the limited community outreach the TON Foundation has performed thus far, execution becomes a major risk for TON. While the team's talent and experience are stellar, this might just be their most ambitious project yet, in a space that consists of several moving targets. TON is already an estimated 1+ years behind schedule and it is hard to imagine how the window from roadmap to delivery will become narrower. Protocol level talent is hard to find in the blockchain space and the best developers are vying to start their own projects. The small pool of the next best, join those projects. Community building and good external communication are differentiators in attracting that level of talent, and thus far it appears that TON has been underperforming in that aspect. Failing to attract developers capable of executing the roadmap will thus add to the overall execution risk.

"TON is already an estimated 1+ years behind schedule and it is hard to justify how the window from roadmap to delivery will narrow."

3.3.2. An unstable environment for cryptoassets

At this stage, *Grams* are "risk assets". The Mainnet launch is coming at a time where both the macroeconomic and the intra-industry environments seem to be hanging in the balance. After a strong H1 in 2019, the cryptoasset market capitalization has retracted by 42% from Q2 highs at the time of writing, while the yield curve remains inverted for the 3rd quarter in a row. While Bitcoin may be in the early stages of becoming adopted as a safe haven asset, the same cannot be said for anything else in crypto.

Concurrently, at the time of TON's launch, it is possible that the SAFT 1, and possibly the SAFT 2 investors in Telegram will be in profit. Given the general macro uncertainty, many of these early investors are likely to at least want to retrieve their cost basis upon finding liquidity. Were that to occur, the potential supply of *Grams* (assuming an average price of $2 per Gram)[99], points to 2/3 of the unlocked coins flooding the supply side of the market surface, over the course of Year 1. At the assumed average price level, this translates to $2.3B worth of *Grams* hitting the market. For the price to appreciate beyond the assumed $2 threshold, the supply of Grams would need to be met by more than $2.3B in demand; which translates to every single Telegram MAU buying at least approximately $10 worth of Grams. If we assume that only a 10% of that MAU base will be interested in purchasing *Grams,* each would have to contribute $100, and so on.

"The cryptoasset market cap has retracted by 42% from Q2 highs, while the yield curve remains inverted for the 3rd quarter in a row."

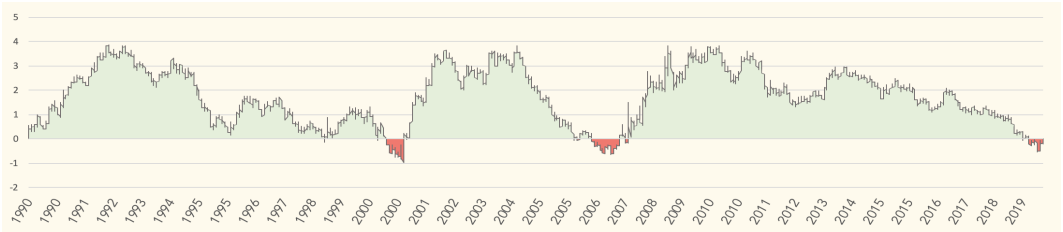


Figure 31: The 2 yield curve inversions since 1990 (excluding the current) have successfully predicted upcoming recessions.

[99] This is a purely illustrative figure.

"It is unlikely that *Grams* will find real utility in the Telegram Messenger ecosystem in Year 1."

Considering that the cryptoasset market is currently at a crossroads, with Bitcoin alone having shed over $40B of its market cap over September 2019, the retail speculative appetite for *Grams* might not materialize in the initial stages of the float. Moreover, considering the early stage of the project's development, it is unlikely that *Grams* will find real utility in the Telegram Messenger ecosystem in Year 1. And the fact that over Year 1 the circulating supply is subjected to the largest increase in the asset's life (approx. 2.5x increase from launch until the end of Y1), certainly won't do the project any favours.

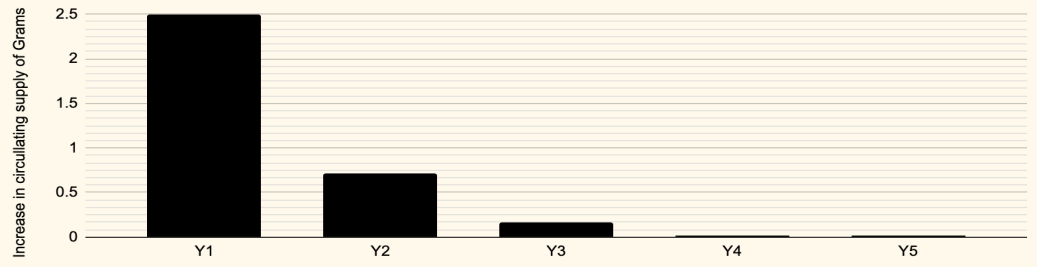


Figure 32: Projected increase in the circulating supply of Grams.

3.3.3. A developer unfriendly experience

"Members of the validator community describe the process of setting up a validator node in Testnet, as requiring a lot of reverse engineering."

Developer talent in the blockchain space is scarce and community building in Layer 1 protocols is often as important as protocol level work. TON seems to - thus far - put community involvement on the backburner, frontloading the platform build. There are few communication channels with the TON core developer team, and those that are available are of low quality. Members of the validator community that we have spoken to - unaffiliated with TON core or TON Labs - describe the process of setting up a validator in the TON Testnet as "requiring a lot of reverse engineering" as "the documentation is sparse and difficult to consume"[100]. Their evaluation is that without experienced developers driving the project, they would not be able to get as far as they have gotten and expressed concerns that due to the overall difficulty it is likely that the network will launch with a highly centralized validator set.

Moreover, developers interested in TON are faced with the problem of 'abnormal programming'. The complexity of writing and testing a code in Fift is already proving challenging, according to reports from members of the early developer community. Until the compilers are ready for prime time[101], Fift will be the only option to write smart contracts on TON, reducing the pool of available talent to those interested in low-level programming. To provide some colour here, TON Labs engineers we interviewed,

[100] Conversely, engineers from TON Labs, describe an easier experience of setting up validator nodes in Testnet.
[101] As we understand, the Solidity compiler exists only in a very limited version for now - i.e. it isn't fully supported, while no decorator or modifier is present. Everything is working to the extent of 20-30% of the full functionality.

referenced that equivalent processes take 10x longer in Fift, than they do when programming on Ethereum with Solidity. That said, they also highlighted that Fift is an elegant and highly efficient language, and underlined their conviction that over the long term, this is will pan out to be an excellent design choice for the network.

"Equivalent operations, currently take 10x longer in Fift, than they do when programming on Ethereum with Solidity."

Be that as it may, TON currently remains without a debugging environment, which in combination with the relative difficulty of programming in Fift, make it near-impossible to write any meaningful programs. Further, even in the presence of a fully functional Solidity compiler, porting smart contracts from Ethereum to TON, will be a non-trivial process, as a relative redesign will be necessary in order to adapt the contract's rules to TON's logic – the same will most likely be true for smart contracts transitioning to Ethereum 2.0.

In addition, as discussed earlier in the report, independent third-party audits of smart contracts will likely be very expensive, as only a few highly specialized parties will be able to carry out that type of work. Tezos illustrates the problems that a developer unfriendly programming language can introduce - the smart contact platform leverages Michelson, a low level programming language unique to Tezos. The result? A dearth of smart contract applications built on Tezos[102]. Arguably, Layer 1 chains that leverage WebAssembly at the Virtual Machine level and more widely adopted programming languages such as Golang, sacrifice specificity (and to some extent performance) for generalizability; however, at this early stage of development in the blockchain ecosystem, generalizability might be necessary in order to attract talent and create a developer friendly experience.

```
BASIC COMPILATION AND INSTALLATION INSTRUCTIONS

1) Download and unpack the newest version of this archive, available at

https://test.ton.org/download

The TON Blockchain Test Network is updated quite often, so we cannot guarantee that older versions of the Lite Client will always work. Backward compatibility is not enforced at this
development stage.

2) Install the newest versions of make, cmake (version 3.0.2 or later), OpenSSL (including C header files), and g++ or clang (or another C++14-compatible compiler as appropriate for
your operating system). We strongly recommend installing OpenSSL version 1.1.1 or later for better performance, especially if you intend to run a Full Node or a Validator as well.

3) Suppose that you have unpacked this archive to directory ~/lite-client, where ~ is your home directory, and that you have created an empty directory ~/liteclient-build. Then run
the following in a terminal on a Linux system:

cd ~/liteclient-build
cmake ~/lite-client
cmake --build . --target lite-client

You might also build some extra utilities useful for smart-contract development:

cmake --build . --target fift
cmake --build . --target func
```

Figure 33: A section from the lite client documentation.

Developers tinkering with deploying smart contracts in the TON Testnet have also reportedly been facing issues with the fee structure of the TVM. Reading and writing to the TVM is expensive, as every deployment requires a fee to be submitted to validators. This not only is a discouraging factor for less well capitalized entities or experimenters, but also makes functions that require a high volume of interactions (e.g. on-chain order-book storage on a DEX application) unviable. Compounding on that point is TON's commission-fee system, which at least at the moment makes it hard for developers on TON to calculate the cost basis for their operations. As of yet, no rules have been set on

"Reading from and writing to the TVM appears expensive."

[102] As of October 6th, 2019 Tezos had only has 108 contracts that contained code. This compares to over 11,000,000 contracts with code on Ethereum.

how the fee structure will pan out. All that is known is that the final fee will depend on the number of used nodes and the number of shards the users' message has travelled through in order to get to its final destination[103].

3.3.4. A series of competitors

"On the messaging app front, Facebook's Libra is arguably the most serious threat."

By merit of the broad spectrum TON covers across the technology stack, it faces competition in multiple different layers. TON's primary competition is concentrated in the messaging application and the blockchain layers of the stack. On the messaging app front, Facebook's Libra is arguably the most serious threat, followed by a series of smaller/regional players that are also integrating cryptoassets and blockchain wallets in their offerings (with Kakao/Klaytn in Korea and LINE in Japan being the most notable examples).

All of the aforementioned, while providing similar solutions, fail to translate the integrity and censorship resistance that truly decentralized systems bring to the table, by introducing a centralized front end. Telegram's architecture is unique in that it makes no such compromise, while introducing a much broader value proposition than just payments. Where we see Telegram somewhat lacking is in the volatility of *Grams* as a native asset. All messenger layer competitors are introducing some fiat equivalent as the rails for their payments feature to run on - arguably a more attractive proposition for the user, both in that it provides assurances for value preservation, and in that the user is required to make less effort to become familiar with the new feature[104].

"Where we see Telegram somewhat lacking is in the volatility of *Grams* as a native asset."

That said, the benefits of building a system that allows for a consensus mechanism with wide participation from different parties are starting to show. Recently, 3 key members of the Libra Association[105] (Visa, Mastercard and Paypal) are reportedly considering retracting their participation[106] following the strong backlash the project received from US and European lawmakers, due to its effective singular control by Facebook. Besides its - provisionally - decentralized architecture, Telegram achieves sufficient differentiation, both drawing from the geographies where the core of its user base is located, as well as the fabric of behavioural preferences that its user base exhibits (e.g. privacy first, crypto native, censorship resistance).

Considering the competition on the blockchain layer of the stack, TON competes more closely with Ethereum (2.0), Cosmos and Polkadot along the interoperability and scalability vectors[107]. Each of the contenders have a unique differentiator about them; Ethereum has the state and the developer community, Cosmos has Tendermint and

[103] With reference to the slow path routing of the IHMR.
[104] The complexity that underpins cryptoassets is known to cause a very sharp dropoff in user engagement, very early in the funnel.
[105] The consortium of enterprises that would run consensus on the Libra blockchain (similar to DPoS in EOS).
[106] [Access here: on.ft.com/2OkoTaD]
[107] For a feature for feature comparison between the 4 competitors, please refer to the Appendix.

multiple iterations behind it and Polkadot has the most mature and developer friendly design, and a strong effort on community outreach[108][109]. However, while in development for longer than TON, all the above are still far from maturity, with Ethereum 2.0's Beacon chain[110] expected in 2020, Cosmos's IBC is expected in late 2020[111] and Polkadot's launch expected around the same time. That said, all three projects have engaged developer communities working on different implementations of the technologies, both on the protocol and the application layers. What they currently lack, is 250M active users to spoon-feed their technology to, through a familiar interface. We believe that if all the (significant) risks mentioned in sections 3.2 and 3.3 are sufficiently mitigated, TON is in a unique position to catch-up with and potentially outpace its competition.

"Ethereum has DeFi and the developer community, Cosmos has Tendermint, Polkadot has Substrate; TON has the users."

3.3.5. A regulatory mountain to climb

Last, but certainly not least, is the regulatory minefield that most blockchain projects have to navigate. We estimate that approximately 60% of Telegrams MAU base is distributed between Iran, Russia, Brazil and China[112] - all markets where heavy government intervention in industry is commonplace. With concerns about the classification of the Gram as a security under SEC regulations recently being further diffused, we believe that most of the regulatory headwinds Grams will likely face will come from Telegram's rocky history with the local governments.

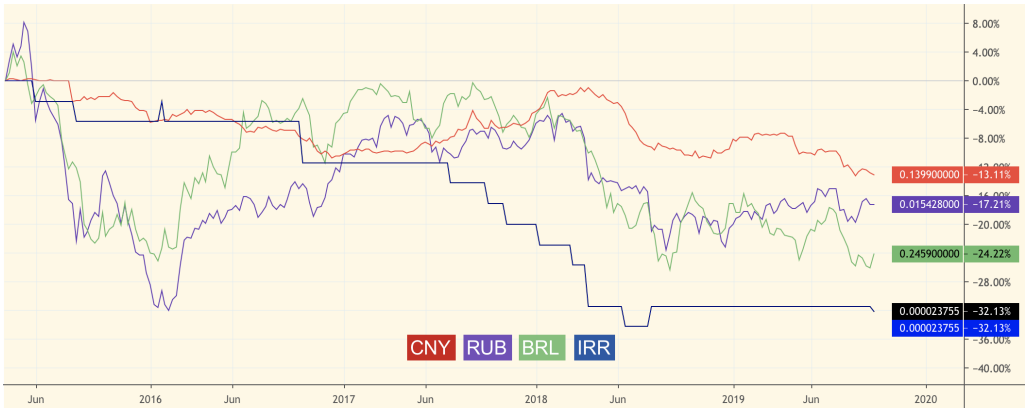


Figure 34: Local currencies have performed poorly against the USD in at least the past 5 years, increasing the appetite for capital flight from the local economies.

[108] Tendermint Core, is a high-performance, consistent, secure PBFT-like consensus engine, where strict fork-accountability guarantees hold over the behavior of malicious actors. Tendermint Core's BFT consensus algorithm is well suited for scaling public proof-of-stake blockchains, and is already in use from various projects, including the Binance Chain and DEX.

[109] Substrate is arguably the most mature SDK in the blockchain space. Developers can use Substrate's modules to spin up parachains (the equivalent of workchains in TON) on the Polkadot ecosystem in minutes.

[110] The Beacon chain is the equivalent masterchain in TON, and is the subject of the first out of four or five delivery phases that will be required to complete Ethereum 2.0.

[111] The IBC (inter-blockchain communication protocol), is a protocol that will allow application-specific blockchains that are built using the Cosmos-SDK or Tendermint BFT to connect to the Cosmos Hub and interoperate with other blockchains that are connected to it.

[112] [Access here: http://bit.ly/2ocHcUg]

"We believe that most of the regulatory headwinds TON will likely face will come from Telegram's rocky history with local governments."

To make matters worse, Telegram has been targeted several times as a harbor for illicit activity, including terrorism. A recent report by MEMRI, found that terrorist organizations like ISIS and Hamas are using the Messenger to run recruiting campaigns and raise donations from supporters in cryptocurrency. As mentioned earlier in this report, decentralizing the network as quickly as possible will help de-risk the project and separate it from Telegram, the entity, making *Grams* a harder and more censorship resistant medium of exchange.

Given Telegram's history with the authorities in Iran and Russia specifically, we can assume that it will be hard for local governments to cut off access to the platform. However, further assuming that Iran, Russia, China and Brazil will be key geographies in driving adoption for TON Payments, and by extension the *Gram*, we estimate a relatively high risk of government intervention in cutting off the fiat on-ramps to the TON economy.

As laid out by the whitepaper, there will be two gateways to the Gram economy; the primary market, where presumably users can interact with the TON Reserve and purchase *Grams* via the Telegram app, and the secondary market, namely native crypto exchanges, OTC desks and P2P exchanges. While the secondary market can prove difficult to tame, the primary is easy to censor. The local currencies have shown continued weakness compared to the USD over the past half decade, and as such we expect both the demand for *Grams* and the incentive for government intervention, to be quite high[113].

[113] Indicatively, Iran recently outlawed trading Bitcoin and other non-sovereign money-like assets, while Localbitcoins - a popular P2P exchange for Bitcoin, had to halt operations in the region.

Conclusion

The fundamentals of TON, the magnitude of its fundraise, the caliber of the team, and the shroud of mystery that surrounds the project, have made the launch of the network the most highly anticipated launch of the last two years. Its fundamentals promise the dawn of a new era in the world of blockchain facilitated networks of value. The user base of the messenger, as an endowment, hints to a probability distribution more favourably skewed towards a positive outcome for the *Gram* token economy[114].

Today, Ethereum works well for the developers that want to build high dollar value transactions and low throughput applications, but leaves much to be desired in the opposite domain. Platforms such as Cosmos, Polkadot and TON open up the possibility of low dollar value and high throughput applications, while being able to reference pre-existing, valuable state from other networks through their interoperability features. Yet, the road to the promised land appears thorny.

The benefits of the Web 3.0 movement are found in its potential for enabling open innovation. Early indications of this are found currently in Ethereum, where new smart contracts are building on the state smart contracts deployed before them have accrued, to create a sprawling ecosystem of value flows, that spins up network momentum that, in turn, further attracts more talent and capital.

Telegram appears - initially - as more of a walled garden. While introducing a crypto layer on top of the Messenger might increase the value of the present ecosystem by unlocking new features for Telegram's users, it is hard to see how TON will transcend this narrow definition without opening up to the world.

Given the competition that TON faces in the blockchain/network layer, baking a philosophy of openness early on in the development of the network, without compromising on the core tenets of privacy and security, will drastically improve TON's position in the competitive landscape - and pave a clear path for value creation and capture. Failure to do that, will likely lead to "tons" of wasted potential and will most likely mark one of the largest fundraising efforts in tech history, as little else than socializing the cost of running the Telegram Messenger.

Irrespective of outcome, TON's launch, early-life and overall development will undoubtedly be full of learnings for entrepreneurs and investors alike. We, at Decentral Park, are looking forward to supporting the initiative as it finds its way in the world.

"Baking a philosophy of openness early on in the development of the network, without compromising on the core tenets of privacy and security, will improve TON's competitive position."

[114] A similar experiment, the KIN token - courtesy of the Kik messenger, with an estimated 15M MAU, failed to get its token widely adopted by its user base. Telegram, with 15x the MAUs of Kik, has better chances of conjuring up the network effect necessary to sustain TON's token economy. To provide some colour, Kik announced that it will proceed to shut its messenger down and downsize by 80% in order to continue pursuing its legal battle with the SEC, over whether its ICO was an unregistered security sale. [Access: http://bit.ly/2lkXBob]

Appendix

Table 1: Analysis of TON's competition in the blockchain space, point by point.

	TON	Ethereum 2.0	Polkadot	Cosmos
Website	test.ton.org	https://www.ethereum.org/	https://polkadot.network/	https://cosmos.network/
Year announced and year deployed	2017, (2018)	2013, 2015	2016, (2019)	2017, ?
Community Growth			Telegram - 3923 members[115] Twitter - 31300+ followers[116]	Telegram - 11562 members[117] Twitter - 28300+ followers[118]
Type	Decentralized	Decentralized	Decentralized	Decentralized
Consensus Algorithm	PoS BFT	PoW	PoS BFT	PoS BFT
Support for Arbitrary Code	yes	yes	yes	yes
Blockchain System	multiple mix	single	multiple heterogeneous	multiple heterogeneous
Interactions Between Blockchains	tight		loose	loose
Speed Transaction	50 000 - 70 000 transactions per second (Visa and MasterCard speed level)	2000 - 4000 transactions per second	Custom User-defined protocol	100 000+ transactions per second with the help of Tendermint Protocol
Block Creation Speed	5 seconds	12,5-15 seconds	Custom User-defined protocol	
Block Delivery	Delivery based on 1-2 blocks	15 seconds	Custom User-defined protocol	
Validators	App. 100 validators will be selected monthly for a period of 30 days by the system among all participants who have sent contributions to the		New validators are selected every 24 hours. Validator can be any person, after registration and compliance with	At the early stage, the Cosmos network will have 100 validators (who has the largest stake in Atom), but every year the number of validators will

[115] Polkadot Telegram Chanel [Access here: https://t.me/PolkadotOfficial]
[116] Polkadot Official Twitter Page [Access here: https://twitter.com/polkadotnetwork]
[117] Cosmos Telegram Chanel [Access here: https://t.me/cosmosproject]
[118] Cosmos Official Twitter Page [Access here: https://twitter.com/cosmos]

	smart contract. In order to become a voting validator, the user needs at least 100K GRAMs. To participate in the validators election round, the user needs first to lock (stake) the tokens. Funds can be released only after the start of the next round. Thus, participation in each new round is, firstly, not automatic, and secondly, the user cannot participate in consecutive rounds with the same funds.[119]		conditions.[120]	grow until it increases 300. Any member of the network can offer his candidacy as a validator.
Cross-Shards Messages Routing	Two types: 1 - Long way 2 - Fast Way		Through relay chain	Cosmos -> Cosmos Hub -> Tendermint Hubs Model
Errors in Shards	Errors are managed by Patch use		Polkadot will return all chains up to the point when the invalid transaction was made.	Everything depends on the choice of validator
Developer Tools	fift + TONVM - low level language TON Labs: Solidity flavor compiling to (based on LLVM) Vanilla C language support https://github.com//TON Copper-Bits		Works: • Rust-based DSL (templated) • + special Rust Style Guide from Polkadot - https://wiki.polkadot.network/en/latest/polkadot/build/rust-style-guide/	• SDK: Tendermint team develops the number of basic modules, which are required for Cosmos Hub. • Cross zone assets transfer - not working yet

[119] TON Blockchain Test Network — files and resources - https://test.ton.org/download.html
[120] Official Polkadot Community - https://polkadot.network/ru/community/

Figure 1: ATON's methodology on arriving at a fair value for Grams

Year	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	TV
Current utility value (CUV), USDbn	9	22	61	142	276	482	759	1 040	1 280	1 510	
Incremental utility value (IUV), USDbn	9	14	39	81	133	206	277	281	240	229	168
Average number of GRAMs in circulation, bn (average)	2.99	3.30	3.69	3.81	3.91	4.01	4.11	4.21	4.31	4.42	4.42
Velocity (S-curve)	1	3	8	14	21	25	27	27	27	27	28
At 20% discount rate and 80% share of CUV paid in GRAMs											
Discounted IUV, USDbn	7	9	22	37	51	66	74	63	45	36	78
Value per GRAM, USD	1.86	0.85	0.77	0.68	0.63	0.67	0.68	0.55	0.38	0.29	0.64
Share of TV in total value	16%										
Implied value of GRAM	**8.00**										
At 50% discount rate and 40% share of CUV paid in GRAMs											
Discounted IUV, USDbn	3	4	7	10	11	11	10	7	4	2	2
Value per GRAM, USD	0.93	0.34	0.25	0.17	0.13	0.11	0.09	0.06	0.03	0.02	0.01
Share of TV in total value	3%										
Implied value of GRAM	**2.14**										
Implied Value of GRAM, USD						**2.14-8.00**					

Figure 2: Illustration of the various forms of value flow in modern day blockchains.

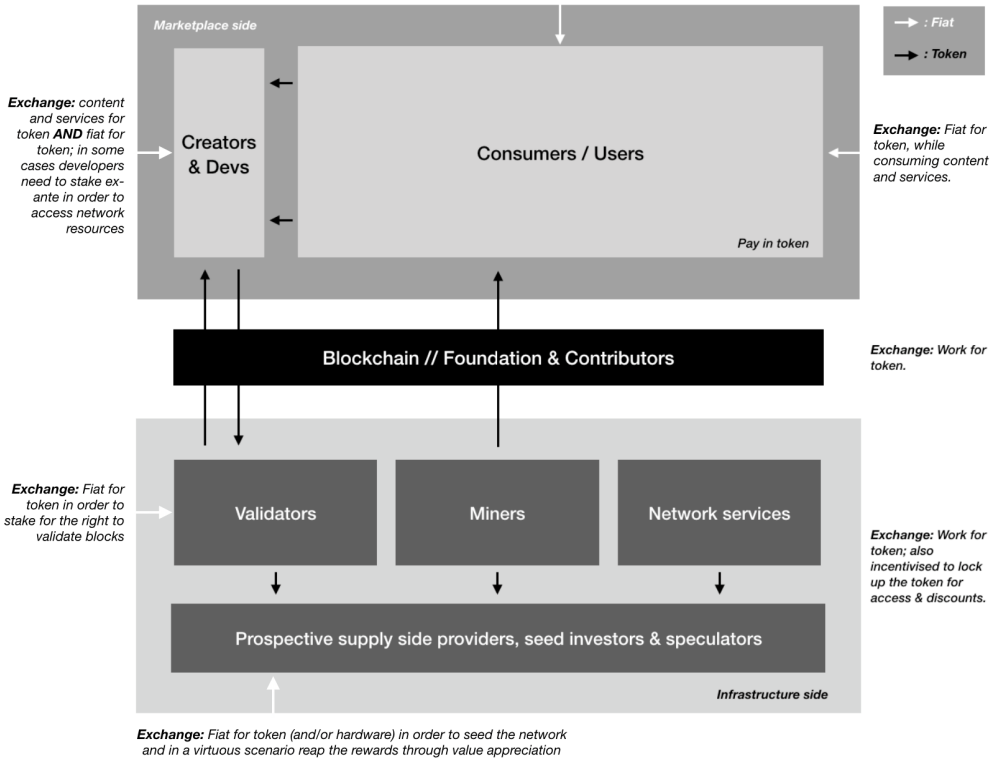


Figure 3: Graphical illustration of a hypercube structure.

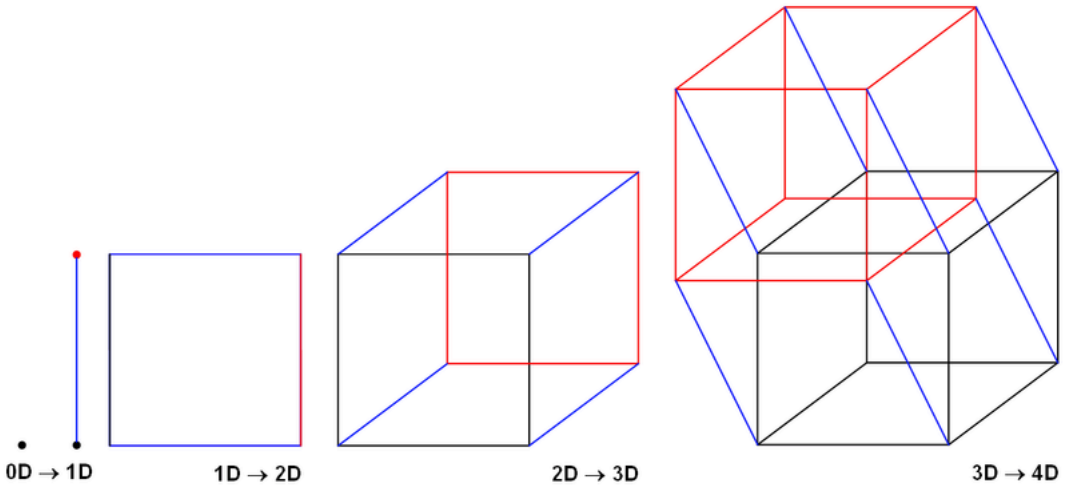


Figure 4: Graphical illustration of the Sawtooth PBFT consensus algorithm.

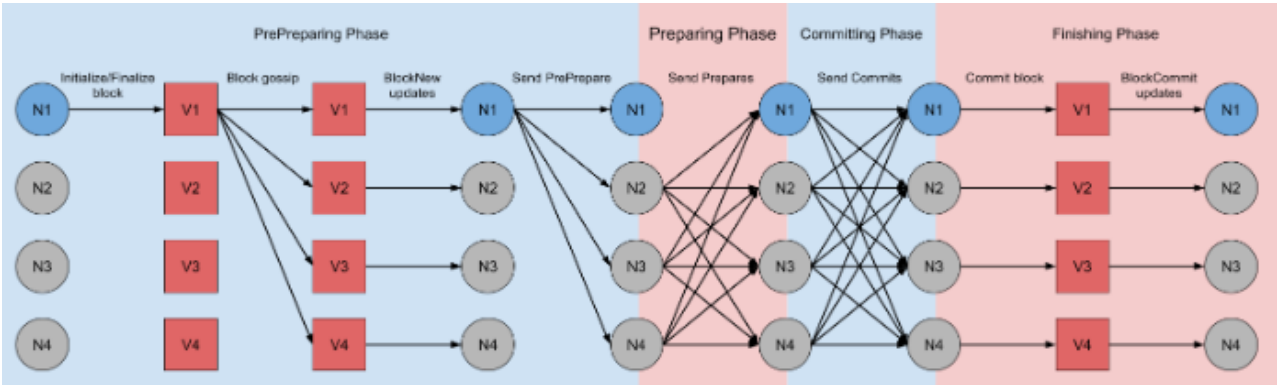


Figure 5: Comparison of message complexities of some classical BFT consensus algorithms.

Protocol	Authenticator complexity			Responsiveness
	Correct leader	*Leader failure (view-change)*	*f leader failures*	
DLS [25]	$O(n^4)$	$O(n^4)$	$O(n^4)$	
PBFT [20]	$O(n^2)$	$O(n^3)$	$O(fn^3)$	✓
SBFT [30]	$O(n)$	$O(n^2)$	$O(fn^2)$	✓
Tendermint [15] / Casper [17]	$O(n^2)$	$O(n^2)$	$O(fn^2)$	
Tendermint* / Casper*	$O(n)$	$O(n)$	$O(fn)$	
HotStuff	$\boldsymbol{O(n)}$	$\boldsymbol{O(n)}$	$\boldsymbol{O(fn)}$	✓

*Signatures can be combined using threshold signatures, though this optimization is not mentioned in their original works.

Figure 5: Estimated communication cost in megabytes (per node) for varying batch sizes in HoneyBadgerBFT.

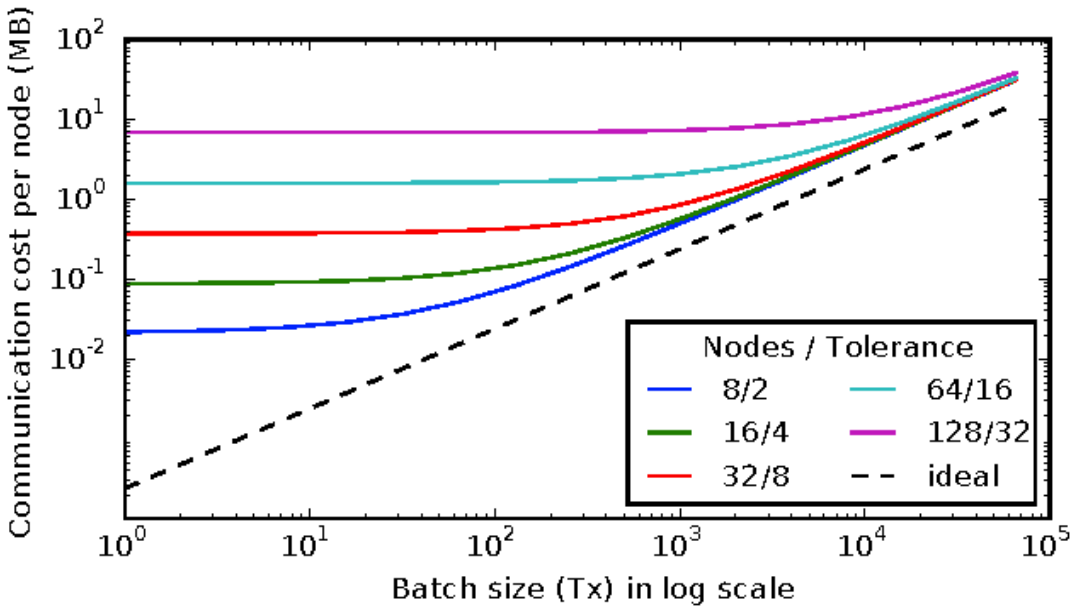


Figure 6: Throughput (transactions committed per second) vs number of transactions proposed in HoneyBadgerBFT. Error bars indicate 95% confidence intervals.

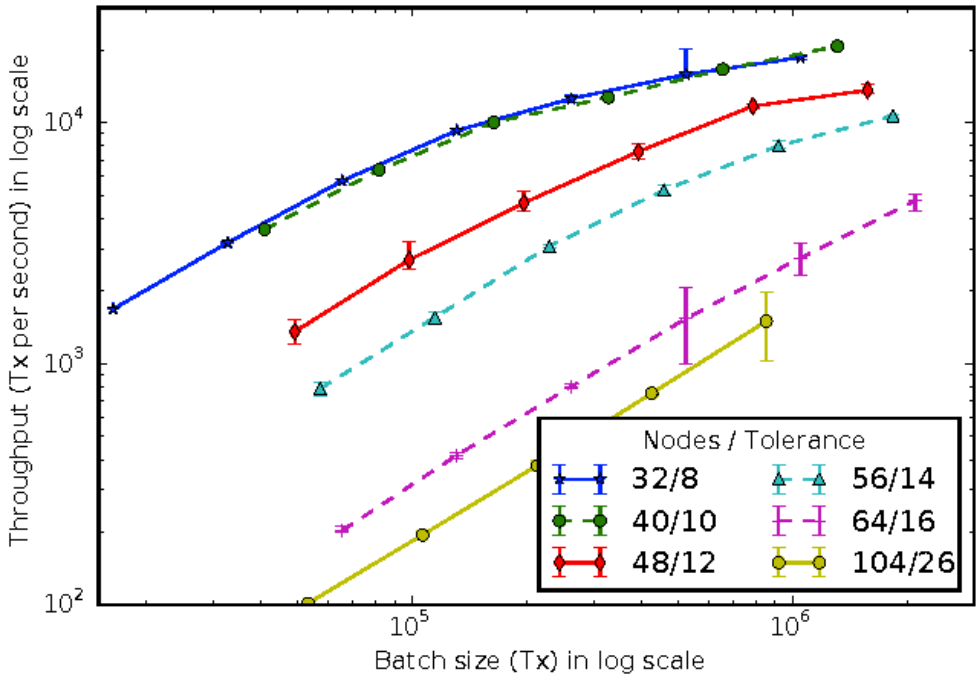


Figure 7: Latency vs throughput for experiments running HoneyBadgerBFT over Tor.

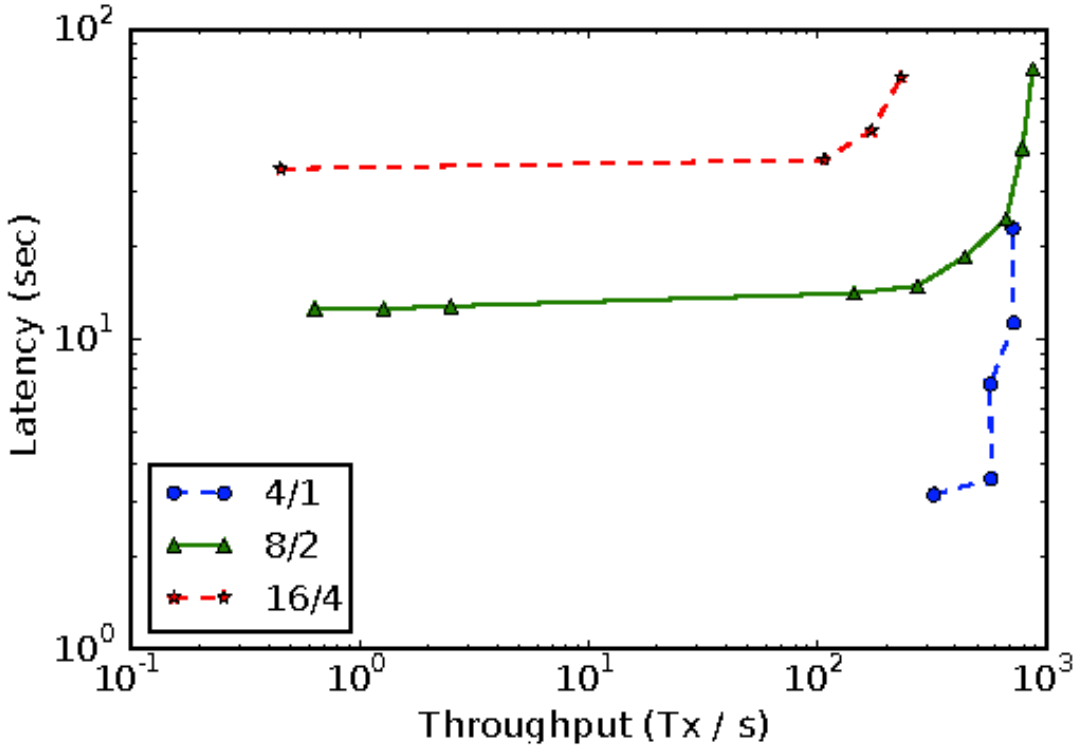
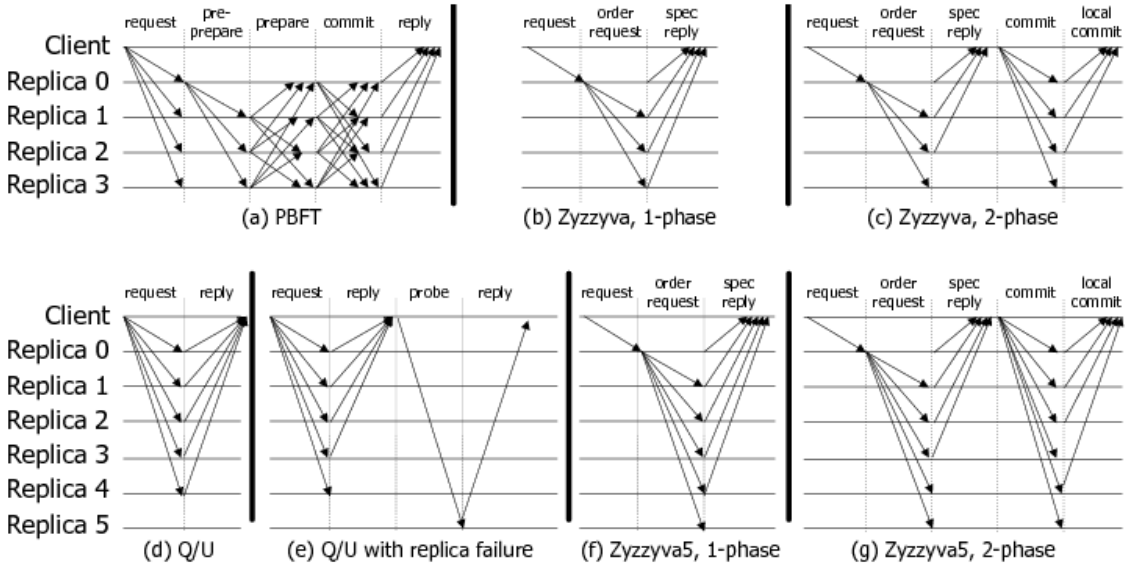


Figure 8: A high-level view of PBFT, Q/U, and Zyzzyva.



Important Disclosures

Decentral Park Advisors, LLC ("Decentral Park") has prepared this material for informational purposes only. This material does not constitute trading strategy or investment advice, or an offer to buy or sell, or a solicitation of any offer to buy or sell, any security or other financial instrument.

The information and opinions contained in this material are those of Decentral Park and are subject to change. We make no representation or warranty with respect to the accuracy, timeliness or completeness of this material and have no obligation to update it. We make no guarantee that any forecasts or forward-looking information will happen. The performance of any specific investment, sector or market included in this material does not reflect the expenses, fees and taxes generally paid with the active management of an actual portfolio.

Decentral Park, its affiliates or their employees or members of their families, may at times have a long or short position in the securities or financial instruments discussed in this material and may make purchases or sales of these securities or financial instruments while this material is in circulation.

Decentral Park does not provide legal or tax advice. Decentral Park is not acting as a fiduciary under either the Employee Retirement Income Security Act of 1974, as amended, or under Section 4975 of the Internal Revenue Code of 1986, as amended.

Investing involves risk, including the possible loss of principal. Investments discussed in this material are not be suitable for all investors. Alternative investments often are speculative and include a high degree of risk. Investors could lose all or a substantial amount of their investment. Alternative investments may be suitable only for eligible, long-term investors who are willing to forgo liquidity and put capital at risk for an indefinite period of time. Alternative investments may be highly illiquid and can engage speculative practices that may increase the volatility and risk of loss. An investor should create a customized investment plan, and any investment plan should be subject to periodic review for changes in individual investor circumstances. Past performance is no guarantee of future results.