POCKETNET:

A Truly Decentralized Open Sourced Content Discovery & Social Platform Based on Blockchain

by Daniel Satchkov, CFA

Summary: Internet platforms have unlocked incredible amount of value by efficiently bringing together creators and consumers of goods, services and virtually any kind of content. However, those platforms are losing users due to variety of privacy issues and scandals inherent in extreme centralization. It is now abundantly clear that virtually all of the power and wealth in the current internet landscape is concentrated in the hands of the very few and they lack the motivation to spread that wealth. That power is wielded to protect moots, monopolize, exploit profitable creators (which now have little choice due to monopolization) and arbitrarily censor.

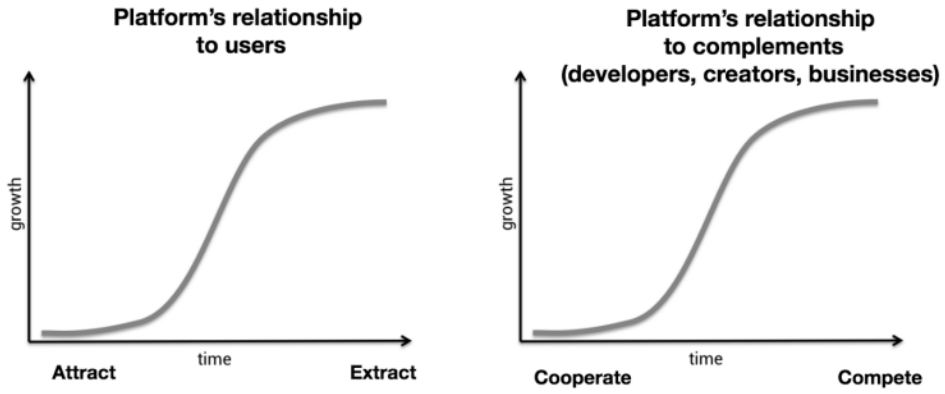
Pocketnet brings the foundations of Bitcoin to the world of internet platforms. All of the enormous value created by the platform is shared among players in the Pocketnet ecosystem in a transparent predictable way. No centralized entity exists that can disenfranchise creators by reducing their share of pay after they achieve success. Each creator earns an amount of Pocketcoin emission proportional to the success of their contributions to the platform. In addition, Pocketnet Direct Marketplace for self-serve advertising allows ad buyers to buy advertising from specific creators using trustless multisignature transactions. Ads can be predesigned or custom placement, where creator has freedom in presenting the ad. This is different from traditional platforms where vast majority of wealth is now clawed back by the shareholders of platforms.

Pocketnet is built to have elements comparable to current successful platforms such as Google, Twitter, Facebook, Reddit, Snapchat, Patreon and Wikipedia along with completely new features. Illegal content policing is done by platform creators who are verifiably invested in the success of the platform. This whole package of publishing, peer-to-peer communication, money transfers, internet search is based on equal nodes running the Pocketnet blockchain and the possibility of building multiple interfaces to suit

needs of different users. As exodus from traditional corporate publishing and social platforms accelerates, users will look for platforms where they own content, subscribers and monetization channels.

I. Current State of Internet

Enormous profitability of current internet platforms is based on efficiency inherent in the platform design, but efficiency rewards are increasingly gated and passed to owners of the platform leaving participants with only scraps and no voice in running the platform. Creators' earnings are not growing nearly as fast as the value created (and value of the platforms), algorithms are changed arbitrarily to create new sources of revenue for the platform and disenfranchise users. Platforms collect ever increasing amounts of personal information which results in regular breaches and abuse. At the same time, quasi-monopolistic power of platforms allows them to police speech in arbitrary ways, referring simply to fine print in Terms of Use[1] without so much as an explanation. A picture is worth a thousand words and there is no better illustration of the essence of centralized platforms than in this graphic, courtesy of Chris Dixon.



Source: https://medium.com/s/story/why-decentralization-matters-5e3f79f7638e

II. Pocketnet Blockchain

So, how can we solve this problem? By opening up the platform. Pocketnet blockchain is run by equal nodes, similar to any decentralized cryptocurrency. However, in addition to typical cryptocurrency token transfers, there are transactions that allows users to post content, vote for its quality, promote it and subscribe to creators (including private subscriptions that are encrypted and seen only by the subscriber).

---

[1] To be sure, we are not here arguing that platforms should not fight illegal content. Pocketnet has a built-in structure of policing content by those that are most invested in the success of the platform, namely the creators of content.

The login to the Pocketnet platform is simply the private key converted to 12 key words. User can interact with the blockhain using that private key. There are several advantages to such a blockchain approach. As mentioned above, the first is economic decentralization that allows for maximal sharing of value with creators who are the ultimate producers of value. Secondly and surprisingly, it is usability. Using a blockchain enables the user to log in from any front end interface on any device with their private key and immediately pull in all of the personalized settings from the blockchain (whether they are encrypted or public). Typically, the weakness of decentralized platforms and strength of centralized ones was this ability to log in from any device/browser without losing the benefits of personalization.

Pocketnet blockchain is based on randomized Proof-of-Stake algorithms. However, nodes are required to perform a number of services in order for their stakes to be valid. Nodes maintain the blockchain, they also respond to RPC socket calls from the front end.

III. Economic Incentives

Since Pocketnet lacks any corporate entity that needs to earn a profit, all of the value created is shared with two broad sets of ecosystem participants. They are creators of content, operators of nodes as well as developers working on the project.

A. Creators of content are pseudonymous users identified by their public keys and information they choose to reveal about themselves.
B. Nodes are responsible for a wide variety of services in the ecosystem (blockchain, supporting front end applications to share data, defense against Sybil attacks). These services go beyond a typical cryptocurrency node. Nodes are required to perform those services to be rewarded.

Pocketnet blockchain contains a native token called Pocketcoin. Just as in any decentralized crypto system, there are two ways that tokens are naturally obtained by ecosystem participants. One is emission and another is transaction fees.

Fees. Many transactions such as share content, upvote, and subscriptions are free (but are limited in number or require a balance to prevent Sybil attacks, see below). Some transactions such as promoting content come with a mandatory fee. All transaction fees are split between node operators and content creators.

Emission. Pocketcoin emission is highly dependent on the usage of the platform. The key value proposition for Pocketcoin is not based purely on scarcity and lack of arbitrary emission, it is also based on

its use as payment mechanism for advertising to Pocketnet users. We need to make sure that Pocketcoin value is relatively stable and it is not hoarded, because that would slow down payments for advertising. Therefore long-term emission will be based on the number of active users as measured by unique users posting and interacting with content on the blockchain. This will ensure that users and advertisers are not priced out of using the system as it grows. Emission of coins will be split in the following way:

A. 47.5% goes to node operators through coinbase transactions when generating a new block in the blockchain. In addition, nodes will collect all transaction fees for Pocketcoin token transactions. These will include any transfers of Pocketcoin such as advertising or purchases in the Crypto Store.
B. 47.5[2]% goes to content creators. This occurs through additional coinbase transactions in the block where likelihood of winning such a reward is proportional to the number of upvotes received by the content creator over a certain period. Note, that this is not all of the creator compensation. In fact, over time it is expected that advertising will take over as the main driver of creator funding through the self-serve Direct Marketplace for ads.
C. 5% goes to developers working on the projects into Developer Fund transactions. Projects will be listed publically and nodes will vote for them on the blockchain, in the transaction that funds a particular project. More than 50% of nodes will have to agree to fund a certain project. Initially, all or most of those funds will go the Pocketnet Core team, who developed the whole project on a volunteer basis. Eventually, it is expected that many more developers will join and Developer Fund will enable Pocketnet to stay on top in the competitive platform game. Developer fund can also be used for marketing projects.

IV. Pocketnet.app Interface

Since Pocketnet is decentralized, anyone can build an interface to it, just like anyone can build a Bitcoin wallet. However, there is a Pocketnet interface authored by the team of Pocketnet Core developers as a first segway into the Pocketnet content discovery and interaction blockchain. There are two ways to use the interface:

a. Using Pocketnet.app mobile optimized web app

[2] During the beta test and initial months the rewards to content creators will gradually be increased from 10% to 47.5% at the 6 month mark. This is done to increase the amount of Pocketcoin for staking by nodes (it directly affects the security of the network) and ensure that content creators can accumulate large stakes of Pocketcoin only by repeatedly posting on the platform and not just with a few posts in its infance.

b. Using Pocketnet desktop app. It is built using Electron framework. It is identical to Pocketnet.app web app, except it communicates to nodes through a proxy server without having to log on to the website.

Pocketnet interface is built by award winning developers and designers. It currently supports the following functionality:

1. Creating a personal profile with nick/avatar on the blockchain
2. Posting content on your channel
3. Rating content on a one to five star scale
4. Private and public subscriptions
5. Requesting donations in Pocketcoin and other cryptocurrencies
6. Integrated wallet that shows balance and any winnings of Pocketcoin based on content that was highly rated by other people
7. Flagging of illegal content
8. Peer-to-peer one-on-one and group chat (released in Feb 2019) based on WebRTC technology

User can log into Pocketnet.org from any device by entering his or her private key mnemonic of 12 words. Pocketnet.org then pulls in all of the personalized settings from the user such as subscriptions, previous content shares and upvotes in addition to Pocketcoin earnings information (as a content creator). Thus, the system is highly portable.

Any user logging on to Pocketnet.org will see content based on his subscriptions and overall algorithm for ranking content on the system (see Appendix A).

V. Self-Serve Pocketnet Advertising, Direct Marketplace, Custom Placement Ads

Pocketnet features an innovative advertising Direct Marketplace for content creators. Any creator can accept ads from ad buyers. To do that content creator can opt-in to the Marketplace and name pricing ranges he or she is willing to accept to post content to his or her subscribers (sponsored content will always be labeled). Ad buyers can see all offers from content creators on the Marketplace along with blog subscribers count, rating activity, most commonly used tags and other information to help ad buyer decide if this particular creator owns a suitable channel. Ad buyer creates an ad and selects a list of creators in the Marketplace (after considering metrics above and cost). A transaction is created and sent to nodes which includes information about the advertisement, the input of Pocketcoin from ad buyer to the creator's address, signed by the ad buyer. The transaction also includes the actual advertisement

made on behalf of creator. However, the transaction is incomplete until creator actually signs the transaction, thus approving its contents. Marketplace reputation of ad sellers will include timeliness of response, as well as review transactions on the blockchain (decentralized reputation management, for more see Pocketrep whitepaper). This way the transaction is trustless and safe for both parties, if it was verified and added to the blockchain, that means that both agreed and Pocketcoin was paid. This self-serve Direct Marketplace offers incredible targeting opportunities, because ad buyer can fine tune the actual creators/blogs used to carry the message. There is no middlemen, so the service is extremely efficient, basically matching ad buyers to channel owners directly. Direct Marketplace is a mechanism that allows for efficient extraction of the immense value created by the platform without wasting time on intermediaries. When emission as an incentive mechanism ends, this advertising will incentivize creators on Pocketnet and nodes will be incentivized by transaction fees of Pocketcoin being sent to pay for advertising in this multisignature transaction.

An additional important feature of Direct Marketplace is ability to create multisignature advertising transactions with custom product placement. This would be a special transaction that requires additional step. In this case the initial transaction from the ad buyer contains only suggested advertising language. Content creator can create a product placement, sign the transaction and send it to the node. Ad buyer can approve the transaction by signing, but this time the signature has to sign the signature of the content creator over the custom placement text, thus approving the placement text.

VI. Sell-4-Crypto Marketplace & Pocketrep

Pocketnet also contains a marketplace that enables sales of goods and services for various cryptocurrencies. In itself, a marketpace to buy and sell for cryptoFX is trivial, but what makes it a highly sophisticated engine in Pocketnet is a decentralized reputation system called Pocketrep. Pocketrep enables cryptographically verified reviews based on crypto FX transactions in Pocketcoin, Bitcoin, Ether and other cryptocurrencies. Reputation in crypto marketplaces are key, since there are no chargebacks. Pocketrep will serve that need ensuring that a review can only be left after actual transactions take place. In this sense Pocketrep is more advanced than traditional review platforms such as Yelp and Amazon, since not all purchases on them are verified, while Pocketrep uses cryptographic commitments to verify signatures. For more on Pocketrep read the Pockterep whitepaper (it does contain a bit more math than this paper).

VI. Sybil Attacks

The biggest danger that a decentralized platform has to deal with is Sybil attacks. This problem is not unique to Pocketnet or even to decentralized platforms in general, but it is more acute than with centralized networks that rely on personal identification to fight it. Put simply, since a Pocketnet account is just a pseudonymous public key which can be created at will in arbitrary quantities, we need to ensure that such bot accounts cannot overwhelm honest content creators and consumers. There are two mechanisms in Pocketnet to defend against such attacks.

Account Balance. Typically, cryptocurrencies mitigate risk of Sybil attacks by requiring transaction fees and thus making it expensive to create mass dishonest acts. However, Pocketnet is a content discovery platform and requiring even miniscule transaction fees will hinder any kind of adoption. Thus, content sharing, upvoting and subscribing is free, but all transactions requires a balance of Pocketcoin. This limits ability to create bot armies, because doing so would require obtaining and holding Pocketcoin. Initially, every user will be able to create a number of posts and interactions on Pocketnet without any balance. Posting quality content on the platform will result in likes from other users and coin winnings that will enable the user to continue. The balance needed to move from a limited status to full member is relatively low and can be achieved with only a few high quality posts that attract reviews.

Antibot. We have developed a unique Antibot system on the blockchain. Since our blockchain is pseudonymous, it is easy to identify previous actions of public keys with a balance (balance is required to participate in the Pocketnet). Typically blockchain analysis systems are used to attempt to deanonimize users. We are using it in a completely different way. In Pocketnet the Antibot platform will block transactions that exceed specified limits on activity that resembles bot activity; this is pretty much the same thing all centralized social networks now do. The types of limits that Antibot can enforce in the order of increasing complexity:

1. Violating limits on posting from a given public key. Each limited membership public key is limited to 5 posts and 15 ratings per day. Each full member can create up to 15 posts per day and create up to 45 ratings. Full member cannot transfer coins and start the 15 posts/45 ratings daily counter anew; new address also has to wait to reset the limit.
2. Repeatedly upvoting content posted by the same user. We do not want to allow inflation of content creator reputation by fake accounts, because reputation drives earnings.

All limits are simply time based. There is no blocking of public IDs. It is not possible to remove all bot activity from a platform; even centralized platforms that rely on official identification can rarely do that.

However, the goal is to make bot activity expensive enough to the point where it makes more sense to just use legal ways of promoting content on Pocketnet through Promoted Posts.

VII. Privacy

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society.

The Cypherpunk Manifesto

Privacy is crucial to Pocketnet and to many other decentralized networks. However, any kind of social network requires checks and balances to ensure that dishonest actors do not turn the system into a cesspool by abusing the rules. We don't believe this to be unsolvable contradiction, but rather creative tension.

Privacy Mechanisms in Pocketnet

1. Pseudonymity. As in most blockchains, public identities are pseudonomous. However, identities for posting content and interacting with Pocketnet blockchain are fixed if a user wants to keep the reputation of the identity (public key). At the same time user can discard a public key and start a new one with blank reputation any time they want to.
2. Subscriptions. Standard subscription to a specific content creator is visible on the blockchain as belonging to a certain public key. However, private subscription is available, where the same subscription in the blockchain is encrypted using 256-bit AES key derived from the private Pocketnet key via a cryptographic hash. This way, when user logs on to Pocketnet.org, client side code can fetch and decrypt the subscriptions to show appropriate content without ever disclosing it to the world.
3. Chat. Pocketnet chat is peer-to-peer encrypted using a key derived from the Pocketnet public key. Therefore, it is private between individuals chatting in a group chat or personal messages.
4. Content share and upvoting of public key are visible in the blockchain and tied to a pseudonym.

5. Any interaction with content on Pocketnet.app (other than posting and upvoting) is private. In other words, there is no way to track what you search for, what you click on etc. etc.

Therefore, we see that Pocketnet is not anonymous. However, it offers strong privacy protections along with mechanisms (such as Antibot) to make abuse of such privacy expensive.

VIII. Illegal Content & SPAM

We have already seen the Antibot system that will make spamming the network very difficult, potentially as difficult as any centralized social network.

What about illegal content? Pocketnet adopts an approach that is successfully used by Wikipedia and other crowdsource knowledge platforms. Any user can mark content as "Illegal" and this will mark it as such on the blockchain. There will be clear guidelines on what "Illegal" means. It cannot mean something I disagree with or something I personally find offensive. If a user finds some content merely offensive, they can choose to never see anything from that user, but not prevent others from seeing it. Of course, a single or even numerous "Illegal" marks will not remove the content from the platform, there has to be enough consensus on illegality. "Illegal" marks from users with higher reputation will have higher weight. At a certain number of flags, there will be an "Illegal" warning, and at a higher threshold content will simply be hidden. As the above quote from Cypherpunk manifesto eloquently stated, privacy only works with cooperation. The key to Pocketnet's policing mechanism is an agreement of participants of the platform based on clear guidelines of illegality and transparent algorithms. Illegality flags will be based on the ratio of Illegality Complaints to the number of ratings of 3 stars or above.

At "5% Illegality Complaints"/"Ratings Greater Than 3 Stars" the material has a warning "Review For Illegality". At 10% the post is hidden from the Pocketnet interface (subject to a minimum total of 7 complaints). However, there are two important caveats.

1. Votes will be proportional to the reputation of the platform.
2. Same or largely the same group of people (even with high reputation) cannot repeatedly vote something off the platform in a group. Thus, when a post reaches critical complaint level, an additional check is run. The check involves checking for overlap between groups of complainers. If the overlap is greater than 95% for any two posts, then the material stays visible until there is

enough difference in the group of objectors. This prevents groups of people silencing dissenting voices in an organized way.

IX. Emission & Pocketcoin Token Value

Many cryptocurrencies are created with a fixed supply. The motivation is to counteract arbitrary whims of sovereign monetary policy, which is a noble and valid goal. Pocketcoin, the Pocketnet platform token for advertising and Sybil attack defense, so it should be scarce enough to have value for ecosystem incentives, but that value should be realtively stable. In other words, it should have elements of what is now called stablecoin. With that in mind, the emission curve will follow Bitcoin but with additional supply formula based on the number of users of the platform. Every user requires a balance of at least 1 Pocketcoin in order to interact on the platform. Initially, these coins will be given away to users to bootstrap the platform. They will also be available to purchase. Pocketcoin is never spent to participate on the platform; it is only spent on advertising transactions to boost a post. Every month, the emission algorithm will check how many Pocketnet users shared a post and will increase upcoming month emission upward if number of active users is greater than one half of the money supply.

In short the formula for total supply to be created in the next month is:

MAX(Bitcoin Algorithm Projected Money Supply,Active Users - Current Circulation)

Where:

Current Supply – Current Pocketcoin in circulation

Next Month Projected Supply – supply of Pocketcoin that matches Bitcoin emission projected for the corresponding period in the lifecycle of Pocketnet[3]

Active Users – number of users that posted at least 6 times or upvoted at least 20 times during the past six months

In other words, total circulation above a certain emission amount dictated by the Bitcoin Core algorithm will be kept roughly equal to the number of users if the number of users grows above the number of tokens. This is done, so that Pocketcoin, while valuable, is not hoarded in expectations of 'going to the moon', but rather is spent on advertising and other uses within the Pocketnet ecosystem.

---

[3] The reason we used Bitcoin emission as a default is that it is widely known and easier to understand than some completely new formula.

What can we expect Pocketcoin token value to be? First observation is that it is not a security, there is not any kind of share ownership implied. Pocketcoin has a number of uses, primary ones being advertising payments and transaction fees for advertising payments on Pocketnet and Pocketrep reputation reviews (for more on the decentralized reputation system within Pocketnet, see Pocketrep whitepaper).

It is hard to estimate the value due to reputation transactions in Pocketrep, but advertising token value can be estimated reasonably well. Annual Revenue Per User (ARPU) of similar platfroms ranges from the low Snapchat at $5 per year, Twitter's $7.2 per year per user to Facebook's whopping $24[4].

In order to estimate value of the token we need the following assumptions:

a. User base

b. Annual advertising revenue per user (ARPU)

c. % of overall token emission that can buy ads for one year

Let's consider them in more detail.

a. User base estimates. We consider three scenarios with first year end user base of 50k, 70k and 100k users growing at 45%, 75%, 100% for 10 years. We do not believe that these are wildly optimistic, rather they are all reasonably conservative given the kind of problems that legacy platforms are having and the user base they already gathered.

Growth Rate->	45%	70%	100%
Year	Users Pessimistic	Users Base	User Optimistic
2020	100 000	200 000	300 000
2021	150 000	350 000	600 000
2022	225 000	612 500	1 200 000
2023	337 500	1 071 875	2 400 000
2024	506 250	1 875 781	4 800 000
2025	759 375	3 282 617	9 600 000
2026	1 139 063	5 744 580	19 200 000
2027	1 708 594	10 053 015	38 400 000

[4] https://www.cnbc.com/2018/01/31/facebook-earnings-q4-2017-arpu.html

http://dashboards.trefis.com/no-login-required/ctA0xPyO?fromforbesandarticle=twitter-earnings-preview-margins-to-expand-despite-slowdown-in-arpu-growth

https://www.marketingcharts.com/advertising-trends-77000

2028	2 562 891	17 592 776	76 800 000
2029	3 844 336	30 787 359	153 600 000

b. ARPU - In the Base Case we have 30.7 million users of the platform in 10 years (quite conservative for a surviving social network). If we take $7 ARPU, we get $214.9 million overall annual advertising value.

c. The hardest assumption is to estimate how much of token issuance it would take to pay for all annual advertising on the platfrorm. Since some amount of coins will be tied up in staking (needs to be around 35% at least, to make the network secure), the rest of the 65% needs to support all of the marketing activity. It is not likely that all of liquidity would be used every year. A conservative number could be 1/2 of total liquidity used to buy all of the annual advertising on the platform. In this case, annual advertising revenue of content creators would be 32.5% of the token supply. So in the base case with total number of tokens at ~30.8 million, that 32.5% of the Pocketcoin supply would be worth ~30.8 million users times the ARPU of $7. That number is ~$215M. Thus the whole Pocketcoin supply would be worth $215M*(1/.325)=$661.5M of total Pocketcoin market cap.

Per value token is not difficult to estimate, since at both Base and Optimistic scenarios, the emission would make it so that the number of tokens is ~ equal to the number of users. In such a case we can simplify the token value to (Number of Users*ARPU)/(Number of Users) or simply ARPU. If ARPU is $7 then token value is also $7. We believe that ARPU on Pocketnet will be closer to that of Twitter and possibly higher due to the fine targeting in Direct Marketplcase and especially possibilities for custom product placements, which are worth much more than cookie cutter advertising.

Year	Tokens Pessimistic	Tokens Base	Tokens Optimistic
2020	2 625 000	2 625 000	2 625 000
2021	5 250 000	5 250 000	5 250 000
2022	7 875 000	7 875 000	7 875 000
2023	10 500 000	10 500 000	10 500 000
2024	11 812 500	11 812 500	11 812 500
2025	13 125 000	13 125 000	13 125 000
2026	14 437 500	14 437 500	19 200 000
2027	15 750 000	15 750 000	38 400 000
2028	16 406 250	17 592 776	76 800 000
2029	17 062 500	30 787 359	153 600 000

Summary: Pocketnet is a new kind of publishing and social platform. It combines convenience of popular centralized platforms and targeted advertising with decentralized blockchain. The result is a platform that produces a great deal of value that is efficiently distributed to stakeholders. Efficient distribution of value occurs through rewarding of content creators, node operators and developers through emission, node operators additionally through transaction fees. Content creators are able to see advertising on their channels/blogs directly on Direct Marketplace where ad buyers sell predesigned or custom placement ads using trustless multisignature transactions between add buyers and creators.

Appendix A: Content Ranking

Content Ranking Formula

$$(P-1)*f+S*d$$

where,

P – Cumulative rating of a post

S – Content creator (public key) reputation derived from ratings received by creator over the past 30 days

$$f=(1-.7)*.7^{h}$$

h – hours since the post

$$d=(1-.9)*.9^{m}$$

m – minutes since the post

*Note that before content had a chance to be seen and receive Ratings, its rank will depend on the rank S of the content creator. However, rank of creator is decayed much quicker in minutes and then Ratings for the specific post of content take over.

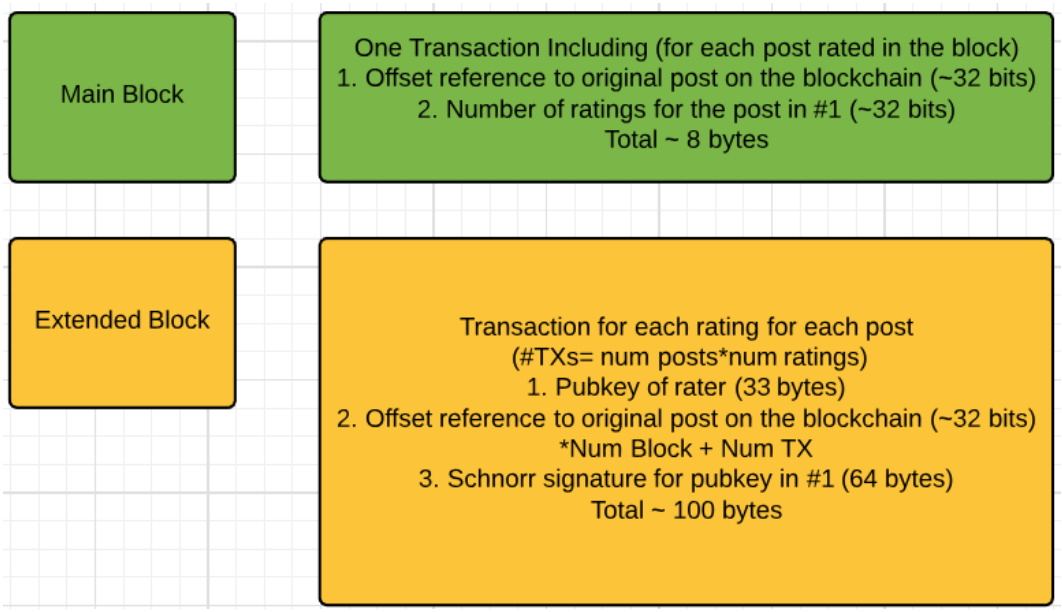
Appendix B: Scalability

A major factor in building any content discovery and social platform is scalability. Can a blockchain really handle the type of volume required by a platform with tens or hundreds of millions of users? We believe that relatively simple enhancements can easily serve tens of millions of users and more fundamental ones can scale up such a system to almost any desired level. The biggest issue with scaling decentralized crypto systems are (arguably, in order of increasing complexity):

1. Verification speeds
2. Storage for blockchain on verifying nodes
3. Networking and transaction processing

Let's use Bitcoin example, since Pocketnet code is loosely based on Bitcoin Core. With 1 megabyte blocks every 10 minutes and an assumed transaction size of 250 bytes that comes up to 24,000 transactions per hour and 600,000 transactions per 24 hours. That is woefully inadequate for a system like Pocketnet. If we assume that every Pocketnet user will make 5 on-chain actions every 24 hours, the 600K limit comes out

only to 116K users. However, not all is lost. If we carefully look at the types of non-token-transfer transactions, we will see that they are perfect for what we would call radical aggregation. For that we will need two concepts that are already well established in the cryptocurrency world: Schnorr signatures and Segregated Witness[5] plus possible improvements to block relay and transaction mempool acceptance. For example, let's consider an act of rating a post made by the user on Pocketnet. In the long run, we only care about how the post was rated, we do not really care who rated it. So, we could aggregate all ratings into one transaction as described in the diagram below. The yellow part of the block contains all of the 'rating' transactions made by the users. Each individual rating transaction can by up to 100 bytes. There can be a huge number of such transactions, potentially thousands per second when the platform scaled to levels of Twitter, Reddit. If there are 50M users of the platform and they each rate 5 posts per day on average, this would mean an average rate of 2894 transactions per second and 250 million transactions per day.



Let's now analyze what we have in the three key dimensions of scalability we outlined.

1. Verification – Schnorr signatures have some incredible batch verification properties. On reasonable personal computer, Schnorr signatures can be validated at a rate close to 20,000 transactions per second. According to research done by the Bitcoin Core development team,

---

[5] Segregated Witness is a feature first implemented in Bitcoin that splits blockchain. There is the essential data referencing the essential meaning of the transaction and data that can be discarded. The permanent data in Bitcoin is the description of who paid who and transient data is signatures that are needed for transaction verification, but once it is deep enough in the blockchain, the whole nature of the blockchain suggests that they have already been verified.

batch validation can speed that up 2X at a rate of about 1,000 verifications per second. So, Schnorr signatures can allow for 40,000 transactions per second, so that is not going to be the bottleneck in Pocketnet's scaling needs.

2. Storage for blockchain on verifying nodes – note that in the main block we only keep the reference to the post being rated and total number of ratings. All of the supporting information is in the extended block. Extended block is going to be far larger than the main block, because it will contain a separate transaction for each rating of each post, but once those ratings are verified and kept in storage for 1-2 months, they are no longer needed. The reason we need to keep individual transactions for 1-2 months, is because Pocketnet Antibot system needs to observe the limits on actions such as ratings or postings. So, ultimately, each post that was liked at least once during the 2 minute time of the block will occupy 8 bytes of storage. Note, that we are referencing the original post transaction rather than adding URL or hash of it to the blockchain every time it is rated. As of 2018 facebook users generate four million likes every minute. Even that enormous amount of activity could be held in just 16 MB of data. But we are not aiming for Facebook volume, since discussions on Pocketnet are held in a decentralized peer-to-peer chat and are never stored on the blockchain. In this sense it is similar to Snapchat, because messages completely disappear after time passes. To summarize, Pocketnet is different from Facebook and is not even targeting such level of mostly meaningless liking. The activity on Pocketnet might more closely resemble Reddit where there are 58 million content votes that occur daily. On average that would mean that each block contains 80,555 rating transactions, which would require only about 160 kilobytes to store, a very manageable amount. Of course, there are other transactions on the system. For example, the post itself needs to have a 160-bit hash of the URL being shared and the comment within the post plus the 32 byte public key of poster. Reddit has 11 million monthly posts, so only about 37,000 per day and 51 per two minute span. Since all posts in a block would be aggregated in a way similar to the rating transactions, the total storage for each block would be 102*52 bytes for 5.3 kilobytes. In fact, public key also does need to be stored and could be replaced with an offset pointer to where the key first appeared in the blockchain (except the first time it posts material on the blockchain).

   Of course, actual posts do not go on the blockchain (only their hashes do). It goes to an external data store (that is also stored in an extremely fast in-memory database for access[6]) that is

[6] Pocketnet Core developers were inspired by Reindexer, an incredibly fast open source in-memory database built by Oleg Gerasimov https://github.com/Restream/reindexer

synchronized with and verified against the blockchain. All posts in that table remain for 3 months and after that only the most popular posts remain to keep the high quality material available for the Pocketnet search engine. Ultimately, when Pocketnet gets to extremely high global volumes such as Reddit, the post table can actually be distributed across the nodes, but the number of users would need to be in the hundreds of millions to make that necessary. The blockchain would still be stored on each node, so barring a hash collision it would not be possible to create fraudulent ratings for posts on Pocketnet.

3. Block Propagation – this has been a key stumbling block, however it has been resolved with enhancements such as Compact Blocks in Bitcoin Core and Xthin blocks in Bitcoin Unlimited. Bitcoin miners also successfully utilized Fast Relay Network, which uses UDP as a means of internet transport vs the slower TCIP. Note, that in practice, most nodes have already seen all or vast majority of the transactions, so that those transactions do not need to be sent twice through the network. This greatly decreases the total bandwidth required for communication between the nodes.

To summarize, specific design of Pocketnet allows for radical scaling to compete with large social networks with hundreds of millions of users.