

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

By Daniel Satchkov



support@pocketnet.app

 POCKETNET



support@pocketnet.app

Summary:

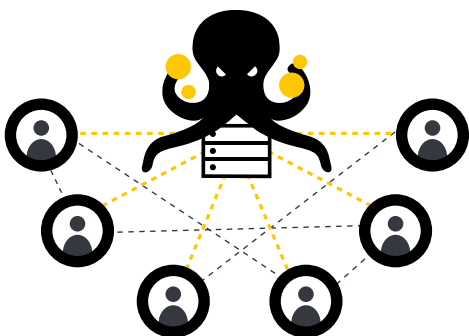
Internet platforms have unlocked incredible amount of value by efficiently bringing together creators and consumers of goods, services and virtually any kind of content. However, those platforms are losing users due to variety of privacy issues and scandals inherent in extreme centralization. It is now 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 moats, 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 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 participants 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.

The Old Way



The Pocketnet Way

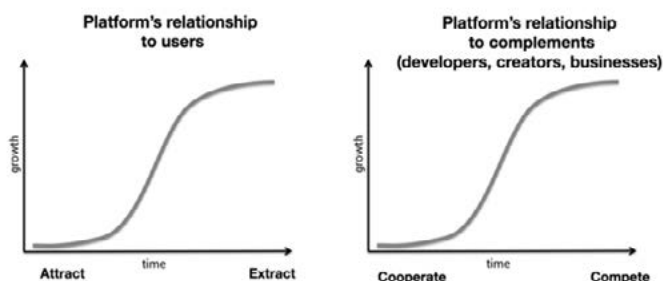




Current State of Internet

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 Use¹ 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>

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.



Pocketnet Blockchain

So, how can we solve this problem? By opening the platform. Pocketnet blockchain is run by equal nodes, like 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). The login to the Pocketnet platform is simply the private key converted to 12 key words. User can interact with the blockchain 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 node holders and 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 device with their private key and immediately pull in all 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 several services for their stakes to be valid. Nodes maintain the blockchain, they also respond to RPC socket calls from the front end.

Economic Incentives

Since Pocketnet lacks any corporate entity that needs to earn a profit, all 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.

- Creators of content are pseudonymous users identified by their public keys and information they choose to reveal about themselves.
- 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 capped at 24,375,000 Pocketcoin. No Pocketcoin will be created beyond that limit.

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
- 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
9. Ability to load and watch video through the integrated PeerTube functionality.
10. NFT 3.0

A user can log into Pocketnet.app from any device by entering his or her private key mnemonic of 12 words. Pocketnet.app then pulls in all 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.app will see content based on his subscriptions and overall algorithm for ranking content on the system (see Appendix A).

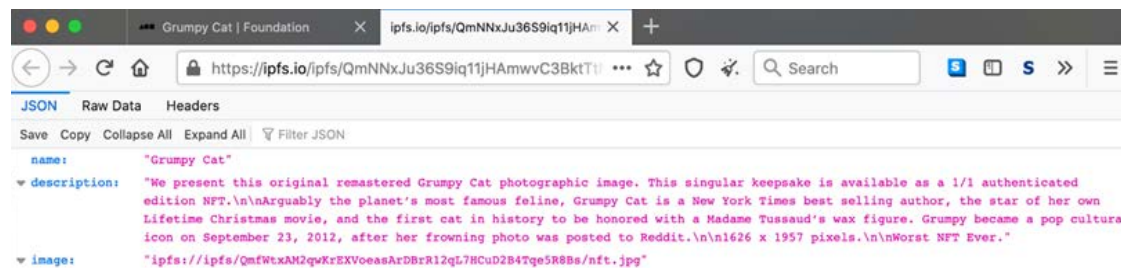


NFT 3.0 on Pocketnet

Non-fungible token transactions are developing rapidly on Ethereum and other blockchains. The main idea driving prices and adoption of NFTs is ownership of digital 'real estate'. However, in its present shape, NFTs suffer from three major problems:

Problem 1: Million Dollar 404 Errors

NFT are simply some metadata attached to a blockchain transaction. In this metadata is the link to the actual work of art being sold. This link is a URL or some other identified on the web. Recently, quite a few NFTs are using IPFS (Interplanetary File System) to store files. Here is an example of what an NFT looks like ([Source](#)):



In fact, NFT resembles a Pocketnet social transaction, but with one important difference. Pocketnet not only has a blockchain node, but also contains a companion database (initial version used a database called Reindexer, but in June 2021 Pocketnet is schedule to switch to sqlite to reduce RAM usage by the node). This companion database is an equivalent of the IPFS, but the one that only works for Pocketnet. In fact, the Pocketnet Core team considered using IPFS (as many other projects have done), but we found two issues with it. Issue #1 is that links can go bad over time. Issue #2 is that it is costly in terms of time and money to maintain

the IPFS file (obviously, it stems from #1). IPFS has its own coin called Filecoin, so in addition to Ether gas fees, there are additional fees to maintain the file. And unlike the Ether gas fee, this fee needs to be projected over decades or longer (the whole life of the NFT).

An article on [theverge.com](#) explains the Issue #1 in this way: *"Still, the system has flaws. The team behind Check My NFT has been looking inside of NFTs to see if their IPFS addresses actually work, and in several cases, they've found files that just won't load. The team found artworks that were temporarily missing from major artists, including Grimes, deadmau5, and Steve Aoki. The files came back online eventually, but only after the team called attention to their absence... That is an awfully expensive 404 error for buyers of these NFTs,"* Aaron Perzanowski, a law professor at Case Western Reserve University and co-author of *The End of Ownership*, wrote

in an email to The Verge. ([Source](#))

Pocketnet solves both problems by construction. In fact, every post on Pocketnet can be considered a proto-NFT, it really has all the aspects of the NFT with absolutely no reliance on external databases. Pocketnet transaction has a blockchain component and a companion database component that is stored in a separate storage in the nodes, but it is closely tied to the blockchain with hash of every piece of content written into the transaction. And this leads to the problem and the solution for problem 2.

Problem 2: Loose Connection Between NFT & Blockchain

A transaction in the blockchain is loosely related to the actual NFT through metadata. No direct connection of proof exists, files at many URLs can change. In Pocketnet, the hash of the NFT is stored in the transaction, so it can always be proved that the NFT is the actual NFT that was sold in each transaction.

Problem 3: No Scarcity

The content of the NFT is accessible and downloadable by anyone. Someone paid \$69M for the Beeple NFT recently (see image of it below). Buying this image is simply owning the right to the specific file on a specific blockchain. There is not any scarcity of the work, it can freely be copied by anyone.



So, there is extraordinarily little uniqueness or scarcity². But because in Pocketnet both parts of the NFT reside in the same ecosystem, in fact on the same node, and because Pocketnet already includes digital identities, we can do one more thing that will create much more scarcity. In Pocketnet, seller of the NFT has an option to show only the preview (say a low res version of an image) and auction off encrypted full work. Then, the winner of an auction will get the ownership and will get a key to decrypt the work. But only the winner will be able to decrypt since the key will be encrypted to the Public Key of the winner.

So, here are the steps in a Pocketnet NFT 3.0 auction:

1. Pocketnet post with terms of action, metadata and the actual NFT is made. Pocketcoin (PKOIN) fees will be assessed by the nodes proportional to the size of the transaction. If a seller chooses to encrypt the full NFT and only show the preview, transaction will contain the preview, but the full NFT will be encrypted using AES key derived from (Seller private key times the transaction ID).
2. Bids. Bids for the work will be made with Hashed Timelock Contracts. (HTLC) Essentially buyer creates a transaction locking the amount of PKOIN equal to the bid for the work. This transaction has an expiration date for a week after the auction ends and it includes a hash deterministically derived from seller's private key, transaction ID and repeated hashing. If a buyer wins the auction, this PKOIN will be claimed by the seller who will present the preimage of the hash in the transaction. If a bid needs to be

² Author appreciates productive conversations with Sean Walsh about this topic.

increased, additional HTLC transactions will be made only for the additional amount.

3. Seller chooses winner with another transaction. It is also a Hashed Timelock Contract, but the amount of PKOIN is nominal. Seller includes the same hash that was included in the step 2. The timelock is for the auction date end plus 3 days.
4. Buyer claims the nominal amount of PKOIN, for that he must reveal the preimage of the hash in transactions #2 and #3. Buyer has 3 days after the end of the auction to claim the win and reveal the hash. If buyer backs out, he is blocked from future participation in NFTs and nodes won't accept future transactions from that public key.
5. Seller now knows the preimage of the hash for the transaction #2 and so can claim the PKOIN paid for the NFT in transaction #2 (plus additional increased bid HTLC transactions with the same hash). If a work was encrypted, then this transaction also includes in its metadata the decryption AES key encrypted to the public key of the buyer, so that nobody else can claim it.

In summary, Pocketnet NFT 3.0 framework solves major problems of the current NFT technology in one simple and intuitive package.

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

Pocketnet is set to include 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 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. 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 are 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.

Sybil Attacks

The biggest danger that a decentralized platform are 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 require 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 several 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). Blockchain analysis systems are used to attempt to deanonymize 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 15 posts and 45 ratings per day. Each full member can create up to 30 posts per day and create up to 90 ratings.
2. Prohibition on reciprocal voting
3. Prohibition in coordinate upvoting, downvoting, flagging of posts

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.

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 pseudonymous. 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.app, 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.

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 or pornography? When users first log on, they will see the following rules:

Pocketnet Community Rules:

- Upvote quality content, your vote matters
- Place proper categories and tags on your content
- No pornography of any kind
- No threats of violence
- Downvote poor quality content

Pocketnet adopts an approach that is successfully used by Wikipedia and other crowdsource knowledge platforms. Any user with high enough reputation can flag any post. Users will be encouraged to flag the content that violates the rules. It cannot be the content that I disagree with or personally find offensive. If a user finds some content merely offensive, they can simply block that user. Of course, a single or even numerous flag marks will not remove the content from the platform, there has to be enough consensus between high reputation users. Here are the rules:

1. If there are 50 flags and the ratio of 5 star votes to flags (both only from high rep users) is below 5, then transactions from that account will not be accepted into the nodes for 1 week.
2. If this happens twice in any 3-month period, the account is blocked for 3 months and its reputation zeroed out.
3. Same group of high reputation users cannot affect the same account in stages 1 (one week block) and stage 2 (three-month block)

and loss of reputation). In other words, we cannot allow a group of people to coordinate and attack certain accounts.

4. High reputation users will have special tabs visible in their apps with flagged content and with potential botnet colluders. So, our assumption is that high reputation users are invested enough in the success of the platform to perform as moderators. First two years of testing this framework has shown this to be true and Pocketnet remains remarkably free of pornography or threats.

Emission

The total emission of Pocketcoin is fixed at 24,375,000. Once that number is reached, no more Pocketcoin will be issued.

Pocketnet will not have an ICO. But we will need a way to attract initial users, before viral growth mechanisms will kick in. Pocketnet also needs to motivate initial developers because they will be paid only in Pocketcoin. Therefore, we instituted initial phase of more emission i.e. for the first 75,000 blocks, the emission will be 50 Pocketcoin per block. This is equal to the initial Bitcoin emission per block, but with blocks made 10 times more frequently. Therefore, at 75,000 block phase the emission stands at 3.75M POC. After 75,000th block, the long run emission switches to the long run Bitcoin emission i.e. 5 POC per block with 1 minute blocks (so 50 POC per 10 minutes), then 2.5 POC per block after 2.1M blocks (again, because blocks are 10X more frequent than in Bitcoin, the switch happens after 2.1M blocks as opposed to 210,000 blocks as in Bitcoin).

95% of emission goes to nodes, video servers, and chat servers and 5% goes to content creators.

Pocketnet Extensions: Video & P2P Chat

Pocketnet blockchain creates a central ledger not just for social network activity. Pocketnet blockchain enables integration of other services, such as video platform and p2p chat. In a centralized platform, everything is done through central servers that are controlled by a corporate entity. Decentralized infrastructure such as torrent was historically cumbersome, slow and unreliable. The crux of the problem with decentralized platforms is a tragedy of the commons along with the inability to maintain a standard. How Pocketnet solves these problems:

1. Tragedy of the commons ensues when there is a public free resource that is overused selfishly by the players. For example, say there is a public video server (for example, PeerTube is a decentralized video technology). Running such a server is a significant cost and it is borne by a single enthusiast. As time goes on, users demand more storage. Some may donate to the altruist, but over time there are many more freeloaders. The server is shut down, videos disappear, platform experience is ruined. In Pocketnet, Pocketcoin and ability to direct emission to nodes creates a way to pay video servers for their service (same thing with p2p chat servers). But now we have a second problem. What if the server collects their pay and disappears?
2. Inability to maintain a standard ensues when decentralized servers do not provide good uptime or reliability, and nobody can force them to. Every video or chat server registers on the blockchain and stakes some Pocketcoin. They can then get paid Pocketcoin for providing a service, but only

if their reputation for uptime and quality is high. The reputation is maintained by special votes of the users. As an example, if someone watches a video that is tied in the blockchain to a certain server public key and speed is incredibly slow (or video does not load at all), that user can give a 1 star rating to the server, thereby lowering their payout. If rating goes low enough, the server is barred from providing a service and their staked coins are lost.

3. The third problem is redundancy. In many decentralized platforms one server houses content or provides a service and there is no redundancy. In Pocketnet, decentralized servers form clusters, where all servers in a cluster back one another up. Each server is assigned to a cluster using their public key and an algorithm called rendezvous hashing. This ensures minimal disruption when new servers enter or leave the platform.

Summary: Pocketnet is a decentralized social network and a communication system. It includes ability to post, comment content, upload videos and build p2p chat. Pocketcoin

is a network token that can be used to promote content, buy advertising, buy special profile features (fonts and skins). Pocketnet is governed by a decentralized model of high reputation users. With rampant censorship around us Pocketnet offers a stable and a scalable way to maintain community communication, while keeping undesired content out.

Appendix A: Merit-Based Post Feed

Anyone can join Pocketnet without identity check, so if posts are chronological, this can easily be abused. That is why developers implemented a merit-based post feed. Here are the calculation details for it:

Pocketnet originally was released with a purely chronological feed. The setting for chronological feed is available in the settings, but the default ordering of the feed is based on quality. We define quality of the post as:

$$.4*[(.75*(LAST5R+BOOST)+.25*REP)]*DREP+.6*POSTR*DPOST=POSTRF$$

LAST5R — Percentile of the number of the 5-star ratings for posts over the 24 hours

BOOST — Boost is a percentile of all active boosts within a certain number of blocks (currently that number is 500). There is a ceiling beyond which adding money to boost is not helpful and Pocketnet interface will show the range (much like the bid range for ads in traditional advertising like Google AdWords). In this framework, boosting will have a market and higher bids will get higher placement in the feed.

REP — Percentile of the reputation of the user across all users

DREP — Decay rate (equal to .7) for the reputation related parameters and boost.

POSTR — Percentile of a post rating over the past 24 hours

DPOST — Decay rate (equal to .96) of the post rating

***all ratings are only from users who are above a target level of reputation**

Discussion: For simplicity we can think of the left side of the formula (everything up to .6) as related to user reputation and the right side as related to the actual post itself. The overall goals of this formula are as follows:

- **Highly rated posts should stay longer near the top of the feed to provide users with a more quality experience. This is achieved by giving more than ½ of the weight to the right side of the formula and by making the DPOST decay rate higher. The decay formula for the left side of the formula with the reputation (rate of .7) will go to zero over about 12 blocks, but the decay for the post (.96 rate) will go to zero only after more than 100 minutes.**
- **The left side that deals with the reputation should not overweight the user reputation. Pocketnet should not be in the situation where past reputation allows one to get to the top of the feed, even if the content quality has dropped. Therefore, within the left side, the user reputation only gets .25 weight, while the reputation of the user's last 5 ratings gets the weight of .75. Therefore, the important reputation comes from the recent content created by the user.**
- **Boost is essentially equivalent to adding some juice to the LAST5R (number of 5 star ratings for the last 5 posts of the user).**

Appendix A: 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 Witness³ plus possible improvements to block relay and

³ 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.

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 be 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.

Main Block

One Transaction including
(for each post rated in the block)

1. Offset reference to original post on the blockchain (~32 bits)
2. Number of ratings for the post in #1 (~32 bits) Total ~8 bytes

Extended Block

Transaction for each post (#TXs = num posts * num ratings)

1. Pubkey of rater (33 bytes)
2. Offset reference to original on the blockchain (~32 bits) * Num Block + Num TX
3. Schnorr signature for pubkey in #1 (64 bytes) Total ~ 100 bytes

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, 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

transaction verification, but once it is deep enough in the blockchain, the whole nature of the blockchain suggests that they have already been verified.

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 access⁴) that is 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.

⁴ Pocketnet Core developers were inspired by Reindexer, an incredibly fast open source in-memory database built by Oleg Gerasimov <https://github.com/Restream/reindexer>

Appendix B: Generating public keys for Diffe-Hellman exchange in Pocketnet

Our goal is to generate public keys that can be used in a Diffie-Hellman key exchange to facilitate encryption in Pocketnet. ECDH (Elliptic Curve Diffie-Hellman) exchange will provide the key that will then be put through a Key Derivation Function to be used in an AES-SIV "nonce misuse resistant" cipher.

Given:

Pocketnet public keys for Alice and Bob :
 K_A, K_B

Both Alice and Bob derive a set of private and public keys using hardened derivation.

The sets of derived public keys are:
 $Q_{A,i}, \dots, Q_{A,m}$. and $Q_{B,i}, \dots, Q_{B,m}$. These keys are published to the Pocketnet blockchain in a registration transaction with $m=12$. Let's say that Alice publishes these 12 public keys. There are corresponding private keys: $q_{A,i}, \dots, q_{A,m}$. and $q_{B,i}, \dots, q_{B,m}$.

Bob needs to perform an ECDH exchange with Alice. To do that, he generates $m=12$ random numbers $\alpha_{B,i}$ on the Elliptic Curve sec256k modulo p by taking each derived public key and putting it through
 $\alpha_{B,i} = \text{CityHash}(Q_{B,i} | Q_{A,i})$

Every block there will a new Diffie-Hellman exchange with the following modification:

$$\alpha_{B,i} = \text{CityHash}(Q_{B,i} | Q_{A,i} | \text{Block\#})$$

Every message will include block number.

Bob then takes his 12 public keys $Q_{B,i}, \dots, Q_{B,m}$ and creates a new public key
 $E_{B,A} = \sum_{i=1}^m \alpha_{B,i} * Q_{B,i}$

Corresponding private key
 $e_{B,A} = \sum_{i=1}^m \alpha_{B,i} * q_{B,i}$

This is Bob's public key for ECHD with Alice. Alice performs symmetric steps and gets a public key $E_{A,B}$

They perform ECHD with those public keys and arrive at a shared secret for Bob

$$E_{A,B} * \sum_{i=1}^m \alpha_{B,i} * q_{B,i}$$

Which is equal to Alice's shared secret:

$$E_{B,A} * \sum_{i=1}^m \alpha_{A,i} * q_{A,i}$$

Their AES cipher symmetric 256-bit key is the output of the key derivation function with the input being this shared secret.

Messages between Alice and Bob are signed with $E_{A,B}$ and $E_{B,A}$ for authentication.

The keys $Q_{A,i}, \dots, Q_{A,m}$ and $Q_{B,i}, \dots, Q_{B,m}$ can be updated frequently only subject to the blockchain transaction fees.

Security proofs for the above public/private key derivation are given in

Hierarchical deterministic Bitcoin wallets that tolerate key leakage, Gus Gutosky & Douglas Stebila

<https://eprint.iacr.org/2014/998.pdf>

<https://tools.ietf.org/id/draft-irtf-cfrg-gcmsiv-08.html>

Discussion: What does this scheme give us? There are few criteria that are crucial in our

setting:

1. We need our encryption to work on non-interactively and to be permissionless. Our schema achieves this, because all necessary components for deriving the symmetric key are observable on the blockchain.
2. We need to safeguard the main Pocketnet private key, so if chat keys are somehow compromised, the master key is not broken. This is achieved, because initial set of public keys $Q_{A,i,\dots}, Q_{A,m}$ and $Q_{B,i,\dots}, Q_{B,m}$ use hardened derivation.
3. Also, generation of public keys in step#2 is fully deterministic, thus a user logging into the Pocketnet from a completely new device can recover all the encrypted communications from their private key and the blockchain.
4. Finally, each symmetric key does not expose the derived hardened keys. There is no way to go back from the AES keys to the private keys used in ECDH.
5. If an attacker attacks digital signatures and recovers a single private key $e_{B,A}$, that does not allow to recover keys $Q_{A,i,\dots}, Q_{A,m}$ and $Q_{B,i,\dots}, Q_{B,m}$ unless there are at least m such keys compromised.

Summary: We described how to use a blockchain platform like Pocketnet with pre-existing cryptographic identities, to produce a completely non-interactive secure encryption key exchange. Now, users of the crypto platform can exchange and ratchet keys easily without having to interact and without any reference to message history.

Appendix C: Decentralized Video

Hosting Connected to the Pocketnet Blockchain

Question of creating a decentralized video hosting platform is a crucial question for several reasons:

1. Large providers inevitably abuse their quasi-monopoly positions by owning most of the value generated by the participants
2. Hosting video and playing it on the web requires large fixed cost in the infrastructure that is now mostly owned directly or indirectly by the same monopolistic players

The only solution is to somehow use users' computers i.e. a crowdsourced video hosting. However, this runs into several serious difficulties:

- A. Tragedy of the commons. In a decentralized architecture there is typically not a good way to compensate for provision of resources. If someone creates a public server, that is a real cost, both initial and ongoing. Users spoiled by Big Tech free video hosting tend to treat the services provides as worth zero, not realizing that the cost of using centralized architectures is loss of privacy, loss of freedom of choice, freedom of speech and others.
- B. Decentralized agreement. Hundreds and thousands of servers are needed to support a video hosting platform. In a decentralized world it is naturally exceedingly difficult to agree on a set of standards, who hosts which video, how the backups are done etc. etc.
- C. Quality. In a decentralized system there is no accountability for the quality of the

services provided for the same reason that there is no compensation.

How Pocketnet video solves these problems?

Pocketnet video uses an open sourced technology called PeerTube, but advances it in some important ways. Pocketnet blockchain provides a centralized coordination ledger, it controls which server hosts which video, who backs up whom, and very importantly how servers are compensated for their services. Here are the steps of providing a Pocketnet video server:

1. Pocketnet video server registers on the blockchain. The server has a public address and locks some Pocketcoin (PKOIN) to be considered a valid server. It also publishes its IP address.
2. Each Pocketnet user has a valid login and password to each of the servers (those are deterministically derived through one-way functions from the Pocketnet private key).
3. When a server registers, its public key is used to deterministically map a server into a cluster using a method called Rendezvous Hashing (see below on Rendezvous Hashing). All servers within a cluster fully back each other up. This creates stability. If several servers in a cluster is below 5, new servers are assigned to that cluster.
4. Each server confirms its participation in the network weekly, confirms its IP address and publishes its current capacity to accept video i.e. how much space is left. If the space left is not enough to remain in the cluster (it is more than 30% below the median in the cluster), then that server is excluded. It can continue earn coins on any videos already uploaded but is not considered for new video uploads into that cluster.
5. Each video post is assigned to a certain cluster based on the same Rendezvous

Hashing algorithm (video transaction ID is multiplied by the public key and the result is hashed, then the cluster with the closest hash is selected).

6. After watching a video on the Pocketnet platform users will be asked if they liked the quality of the video. High marks will increase the reputation of each server and win them Pocketcoin (PKOIN), low marks will reduce the reputation. Thus servers who provide low quality connection or do not actually store the video in a post to which they were assigned, will get penalized and eventually excluded.
7. When video first loaded, there is a minimal PKOIN payment above and beyond the blockchain transaction fee. This covers the video hosting for 6 months. This fee per MB will be voted on by all valid servers with high reputation.
8. After 6 months, videos that do not meet the minimum popularity bar (do not generate enough PKOIN for the servers) will need to be extended. The author will need to pay the same minimal amount of PKOIN to keep them from deletion.

Here is how Pocketnet solves problems A, B & C above.

- A. Tragedy of the commons. This is solved because now servers are compensated for their efforts and there is no longer a free public resource that can be abused by others. So Pocketnet blockchain and Pocketcoin (PKOIN) solve this difficult problem, while opening up vast computing resources without requiring permission from Amazon AWS or any such system.
- B. Decentralized agreement. Pocketnet blockchain serves as the consensus layer. It maps every server into a cluster, controls the number of servers in a cluster

algorithmically, while mapping every video into a specific cluster where it will be served redundantly.

- C. Quality. Servers are incentivized to provide good quality, otherwise they will destroy the reputation and lose ability to earn PKOIN and more importantly will burn the locked PKOIN.

Thus, we have a fully deterministic algorithm that maps any new server into a cluster and maps any new video into a cluster. Within a cluster all servers are synchronized, providing stability. The only known solution prior to Pocketnet only solved one problem out of three (specifically #2) and did it in a suboptimal way. We are talking about a Distributed Hash Table. DHT is used in torrent systems to locate a file within the system. Not only does that solution not solve problems #1 and #3, but DHT tables are notoriously slow and inefficient. One must bounce around the DHT table looking for the file, while in in Pocketnet combination of blockchain and Rendezvous Hashing (also called Highest Random Weight Hashing, for more read [HERE](#)), the cluster is found instantly based on the state of the blockchain at the time of the uploading of the video.

