PKT NETWORK

Caleb James DeLisle (cjd@cjdns.fr), Jesse Berger (jesse@radicalstudios.com)

February 1, 2021
Version 1.0
https://pkt.cash

Abstract

The Internet is one of the most influential inventions of the 20th century. However, in many parts of the world, internet access is controlled by monopoly actors who have the power to gate access, influence public opinion and limit freedoms. In this paper we propose a new network model that provides a framework for decoupling infrastructure operation from internet service provision. This model builds on the proven concepts of autonomous systems and peering relationships, but moves them to a virtualized domain on top of a global mesh network. To finance this network, we introduce the PKT blockchain, based on a bandwidth-hard proof of work. We then propose a decentralized bandwidth marketplace where internet service providers (ISPs) lease resources from infrastructure operators, which facilitates competition in both domains.

1. INTRODUCTION

The Internet fundamentally consists of a number of independent organizations that lease bandwidth over shared physical infrastructure. Through voluntary association, these organizations together facilitate raw, un-opinionated data transit between any two users of the network [1]. This system has proven highly effective, particularly at the Internet core where competition is high and point-to-point bandwidth is widely available. However, in many places worldwide, internet access is still controlled by monopolies that own and operate the infrastructure. To mitigate monopolistic practices, many states enact *local loop unbundling* laws, requiring monopoly telecoms to share access to their last-mile infrastructure with competitors [2, 3]. While local loop unbundling laws improve quality of service, they have been criticized [4] for discouraging infrastructure investment, which in turn limits access.

Civic freedoms erode when internet access monopolies limit what information people are allowed to access [5]. Even more insidious is the effect of mass surveillance to seek full spectrum dominance over an ill-defined "enemy," which may grow to encompass society itself [6, 7]. While nationalized internet may provide high quality low cost service in times of political stability, it creates a centralization of power over free speech and the press that in a time of political upheaval, could prove catastrophic.

What is needed is a system that lowers the barrier for people to become both an *infrastructure provider* and *service provider* [8,9]. We propose a new network model where people are incentivized to provide internet access with minimal technical knowledge. This effort collectively decentralizes internet infrastructure, drives down the cost of bandwidth, and incentivizes people to improve connectivity in rural and urban areas worldwide.

1.1. Structure of this paper

In this whitepaper, we introduce the PKT network architecture (Section 2). We then describe cjdns and the integration of the route server and free tier (Section 3-5). We then outline the PKT blockchain design and discuss the novel bandwidth-hard proof of work that incentivizes the deployment of new internet infrastructure (Section 6). We offer a high level technical description of the envisioned routing device hardware (Section 7) and the decentralized

bandwidth marketplace (Section 8). Finally, we conclude with an explanation of a decentralized bandwidth marketplace and the technologies that will facilitate its emergence (Section 9).

2. PKT NETWORK ARCHITECTURE

PKT Network is designed to decentralize internet access around the world by enabling anyone to become an ISP. To virtualize the technical aspects of an ISP, while decentralizing the location-specific role of infrastructure operator, we introduce the concepts of the *Edge Point* and the *Cloud ISP*. An Edge Point is a device that is operated by an individual, business, or community group, is open to the public and provides access to the PKT Network. A Cloud ISP is a hybrid between a traditional ISP and a VPN provider. Cloud ISPs aggregate and broker Edge Point bandwidth leases and handle the administrative roles of providing internet service for their customers. PKT Network's Cloud ISP system is designed around two types of virtual assets, which are: the *virtual router lease* and the *bandwidth lease*. A virtual router lease is a temporary right to resources within the routing device for a time period. The bandwidth lease consists of a minimum bandwidth guarantee for a time period over a link between two physical routing devices. Similar to the traditional TCP/IP and Border Gateway Protocol (*BGP*) networking models [1], PKT Network facilitates the *provider*, *customer* and *peer* relationships between Cloud ISPs. These relationships are enabled via two key components: 1) *packet priority* and, 2) *the customer bit*.

2.1. Packet Priority

In traditional networking, a provider typically connects to a customer using a slow network link in order to control the amount of bandwidth the customer can send, which mitigates network congestion. However, this often leads to under-utilization of available network resources. The intention is for the PKT Network to never deny packet transmission while network capacity sits idle, so packet priority is designed to maximize data transmission via available infrastructure.

Packet prioritization is achieved using a *priority* field in the packet header and a configurable called *max-priority-bandwidth*. With the max-priority-bandwidth configurable, a Cloud ISP is able to configure a maximum amount of priority-bandwidth (units of priority multiplied by kilobytes), which can flow through a *bandwidth lease* each second. If more priority-bandwidth flows through the bandwidth lease then the configured limit, the routing device begins dynamically reducing the priority of that traffic, thus protecting the Cloud ISPs network without unnecessarily dropping traffic. Packet priority helps Cloud ISPs choose which packets to drop if a link becomes overloaded.

The max-priority-bandwidth configurable is effectively a share of bandwidth within a given network. If a Cloud ISP's network becomes overloaded and each of their customers have the same max-priority-bandwidth then each will have an equal share of passed packets. However, if one customer has only 1/10th the max-priority-bandwidth of the others then they will only be able to pass 1/10th as much traffic. As priority is reduced multiplicatively, the relative priority of each customer's traffic is preserved even as it passes from one Cloud ISP to another.

2.2. The Customer Bit

PKT Network offers a peering capability that improves on the way TCP/IP network operators exchange traffic. Traditionally, when two network operators enter into a peering agreement, they agree to directly exchange their customer's traffic, but not to carry any other traffic for each other. This type of peering agreement is mutually beneficial and therefore it typically does not include any type of financial settlement [1]. However, if one party sends traffic with destinations that are not the other party's customers, routers will forward that traffic to their upstream provider. Sending this type of traffic to a peer uses a paid connection and amounts to stealing. Network operators in the TCP/IP internet handle these peering indiscretions on a case-by-case basis because they don't have technology that outright prevents it. PKT Network improves this function by including a one-bit "customer" field in the packet header along with two configurables: 1) *clear-customer-bit* and, 2) *deprioritize-non-customer*.

Any incoming traffic on a bandwidth lease with a clear-customer-bit configurable set will have its customer bit cleared. This is used to indicate that the bandwidth lease in question connects the network either to a peer or a provider. The deprioritize-non-customer configurable affects outgoing traffic on a bandwidth lease, so if the customer bit is not set then the packet will have its priority reduced to no more than the specified value. A bandwidth lease between two virtual routers that are controlled by the same Cloud ISP will not have either of these configurables set.

3. CJDNS

In order to understand PKT Network's architecture, we must first introduce the open-source network technology called cjdns.

Cjdns is an open source mesh routing protocol designed to create decentralized mesh networks that are easily configured, yet have robust security properties in the face of adversarial participants. Cjdns uses always-on end-to-end encryption and cryptographically generated IPv6 addressing. Since each IPv6 address is effectively a key fingerprint, all cjdns traffic can be encrypted and authenticated without the need for PKI or other similar central authorities. The IPv6 addresses are in the fc00::/8 unique local address space [10] which is large enough that risk of address collision is negligible.

Cjdns deploys a technology called *compact source routing*. Instead of every packet of data containing the IP address of its destination, cjdns instead includes the route to get there. Moreover, cjdns uses a compact representation of this route in roughly the size of an IP address. By replacing "where do you want to go" with "how do you want to get there" cjdns optimizes for the best way for data to get where it needs to go. Cjdns has been developed since 2011 and is live and active in the Hyperboria network [11].

4. ROUTE SERVER

In order to support efficient virtualization of routers, the decision-making in the routing process is coordinated by a *route server* belonging to each end user's Cloud ISP. The route server provides pre-computed paths through the PKT Network using cjdns compact source routing. As packet forwarding decisions are predetermined in cjdns, routing devices are not required to keep any significant state to execute. In order for client devices to learn paths through the PKT Network, the resolution of the source route is queried similarly to a DNS lookup. This query is made against the route server.

In the PKT Network model, every device in the network interacts with some route server. The route server is implemented as software, so new technology to resolve routes can be improved over time. If a device has no known route server, it asks it's nearest neighbor, similar to how DHCP is used to find DNS servers. In addition to making route queries as needed, devices in the network also send periodic, signed, timestamped messages containing the identities (key fingerprints) of all devices directly connected to them, as well as link quality and bandwidth lease related information. Because these messages are signed, any route server who comes into possession of one of them is immediately able to validate it. The combination of cjdns compact source routing with the route server will allow Cloud ISPs to use software-defined networking (*SDN*), giving them significant flexibility to control their networks. We expect that Cloud ISPs will evolve from virtual private network (*VPN)* service providers, whereby they can also begin providing internet access via local Edge Points.

5. FREE TIER

The PKT Network enables Cloud ISPs to construct networks using bandwidth leases and virtual router leases, whereby no packet is ever dropped unless a physical link is saturated. Additionally, we propose that every physical link should have an available *free lease*, which is a hardwired, unowned bandwidth lease with a guaranteed bandwidth of zero. Furthermore, every routing device should have an unowned virtual router which is always

interconnected to the free lease on every physical link. This creates a *free tier* which allows bandwidth to be used at no cost if the infrastructure would otherwise sit idle.

We believe that it is unethical and inefficient to waste resources while denying people access because they are unable to pay. The free tier supports two key services: 1) it allows Cloud ISPs to perform bandwidth, latency and jitter tests before purchasing a bandwidth lease, and 2) it protects against accidental misconfiguration. If a routing device is misconfigured and becomes otherwise inaccessible to its lease holders, the free tier can be accessed to reach that device's onboard computer. In essence, the presence of a free tier changes the failure mode of many types of faults from fail-closed to fail-open.

6. PKT BLOCKCHAIN

PKT Network utilizes a blockchain [12] to economically incentivize nodes to become Edge Points and Cloud ISPs. Based on Bitcoin's codebase, PKT replaces Bitcoin's SHA-256 hashing algorithm with PacketCrypt, the first ever bandwidth-hard proof of work. PKT also introduces a novel mechanism called the *Network Steward* to fund development, including internet infrastructure and network technology.

6.1. PKT Cash

Nodes support the network by expending bandwidth, CPU time and performing encryption to mint new PKT coins into circulation, called *PKT Cash*. PKT Cash provides an incentive for miners to increase network throughput at the edge. PKT Cash is designed for microtransaction scalability with a 1 minute block time that makes it 10x faster than Bitcoin, and just over 1 billion atomic units per coin instead of Bitcoin's 100mn. There will be 6 billion total coins issued over a period of 63 years, all with no central issuer. Block rewards undergo a recurring *decimation*, whereby distributions reduce by 10% every 100 days. Each decimation ensures a smooth issuance decay.

6.2. PacketCrypt

The PacketCrypt proof of work allows communication between miners to be substituted in lieu of processor effort, making the optimal mining strategy bandwidth-intensive [13]. Mining is separated into two distinct stages: *announcement mining* and *block mining.* In announcement mining, CPU work is expended resulting in creation of many 1KB announcements, which have a structure that cannot be efficiently compressed. In block mining, miners pre-commit a merkle tree root of announcements they have collected and then perform a memory-hard mining algorithm on the set of collected announcements. The block mining algorithm accesses 4 random announcements per hash cycle and when a block miner finds a successful result, they provide the announcements which they accessed as well as merkle branches linking them to their pre-commitment, thus statistically proving that they had the number of announcements they claim to have had. This makes it infeasible for a block miner to pretend to have announcements they don't actually have. Announcements decay in value until they become unusable, so block miners are incentivised to pay announcement miners for a steady supply of fresh announcements[1]. The announcement mining algorithm uses random programs to favor CPU over GPU or ASIC mining, which encourages mining on otherwise-idle resources rather than in centralized farms. The block mining algorithm relies only on memory hardness, making GPU hardware a good target for block mining. Both algorithms make use of encryption operations such that high performance mining equipment will also be useful for VPN packet encryption.

Any cryptocurrency which is issued by proof-of-work inherently creates artificial market demand for the relevant work. In a purely static economic analysis, proof of work wastes resources which might otherwise go to good use. However, in real economies, we see demand motivating supply, eventually causing cost declines. PacketCrypt is designed to create a background demand for bandwidth, which we foresee driving increased investment in network infrastructure and reducing bandwidth cost in the future.

[1] Announcement mining is designed to be most effective on CPU. Block miners can mine their own announcements, but they will have to compete with the otherwise-unused compute resources of casual announcement miners.

The result of bandwidth-hard mining and miner collaboration fosters a *network effect*, including the scaling of decentralized, low latency network connectivity and encryption. This network effect is useful for cjdns as well supporting commodity markets, including a decentralized bandwidth marketplace (Section 9).

6.3. Network Steward

PKT implements a Network Steward into the blockchain design, which is an address that receives 20% of the PKT Cash from each new block. The Network Steward exists for the purpose of funding development of the PKT ecosystem. The Network Steward can be changed by way of a proof-of-stake based vote. Voting is performed by "marking" a transaction output with additional metadata. Active votes are those unspent transactions containing such metadata so that spending the transaction output withdraws the vote. Each vote metadata can contain two PKT addresses, one vote *for* and one vote *against*. When the sum of votes *against* the incumbent Network Steward reaches over 50% of all PKT minted to date, the consensus rules identify the PKT address with the most votes *for* and that address becomes the new Network Steward.

The Network Steward is a system to fund development of the PKT ecosystem in a way that project proposals must not be unfairly beneficial to any one participant (including the applicant). This competitive research model generates budgeted calls for projects from time to time and evaluates project proposals against each other based on the Network Steward's criteria. The Network Steward policy encourages all accepted projects to be structured around producing open source software, public documentation, and to encourage infrastructure growth of the PKT Network. All ongoing funded projects, completed, and rejected proposals are publicly found in the Network Steward's git repository [12]. If the Network Steward does not deploy funds held in its wallet address within 90 days from the day the PKT Cash was minted, the coins are burned[2]. In this way, each project proposal must be evaluated such that the value that any given project proposal must generate should be of greater benefit to the PKT Network than burning the coins.

7. ROUTING DEVICE

The scalability of the PKT Network will require the development of a high-performance sub-dividable routing device. This hardware innovation will guide and support the scalability of the PKT Network. To determine the basic requirements of an optimized PKT Network hardware implementation we must understand the complexity of implementing such a device in silicon and explore the flow of data packets through the device.

A packet entering the routing device does so through one of its physical network links. The incoming packet is tagged indicating which bandwidth lease it belongs to as well as the packet priority. The first processing which the packet encounters is re-prioritization in accordance with max-priority-bandwidth. This requires a bandwidth/priority meter such as an IIR filter.

The device will parse the compact source route label to determine which bandwidth lease the packet should be sent to. The device then updates the compact source route label to show where the packet came from using the cjdns switch algorithm [11]. Cjdns requires accessing a small index table in order to compute the physical interface number and determine the bandwidth lease tag to be used for sending.

Once the routing path has been resolved, the packet will enter a switch circuit. Designs such as crossbar and clos are already commercially available [14, 15, 16]. Before the packet leaves the device, it will be decided whether the packet needs to be dropped. This should be achieved using a token bucket design with a 2-level hierarchy whereby

[2] As of January 23, 2021 PKT276,889,678.84 have been burned

the primary level is based on the guaranteed bandwidth of the outgoing bandwidth lease and the secondary level is based on the declared packet priority. This is common technology used in simple ethernet switches.

8. DECENTRALIZED BANDWIDTH MARKETPLACE

When a routing device is connected to the PKT Network, it will immediately 1) begin measuring and announcing available bandwidth and other metrics on each of its network connections, 2) create a token to represent bandwidth on each network connection as well as its virtual routers, and 3) begin offering those tokens for sale in a decentralized bandwidth marketplace. Those tokens will be able to be bought and sold by different participants and anyone in possession of those tokens will be able to use the underlying bandwidth and virtual routers by sending signed configuration requests to the routing device. To make this possible, we will need to build a decentralized bandwidth marketplace with near-zero-cost token issuance and nearly frictionless exchange. The technology for near frictionless exchange of assets is already possible using HTLC atomic swaps [17] and this is currently being exploited by the OpenDEX project [18]. To enable near-zero-cost token issuance, we are pursuing multiple different solutions.

8.1. TokenStrike

Tokenized bandwidth and router resources have an interesting property of being “only as good as their issuer” because in the worst case, the issuer could simply turn the routing device off. This property means that global verification of such token transactions is no more secure than verification by the issuer, as long as the issuer is unable to violate the protocol in secret. We propose a new token standard called TokenStrike [19] where each token is represented using a private blockchain that is signed by the issuer such that almost any nefarious activity by the issuer can be detected and proven to have occurred. TokenStrike is designed to be HTLC compatible so any TokenStrike based token can be exchanged for any TokenStrike tokens or other Lightning Network assets.

8.2. Open Transactions

Another promising technology for scalable token transactions is Open Transactions, which uses a pool of notary servers to validate coin or token transactions and to sign them using multi-signature [20]. We anticipate Open Transactions and the TokenStrike project to provide parallel token issuance solutions for a decentralized bandwidth marketplace.

8.3. RGB - Colored Coins

Finally we have identified *colored coins* as a possible way to represent bandwidth and router resources. Colored coins are minute amounts of cryptocurrency which the token issuer can attach special significance by declaration [21]. Colored coins rely on the fact that in non-privacy blockchains, coins can be traced from one party to the next, however similar to Ethereum based tokens, they require global verification to transact. Currently the RGB project [22] is researching technology to allow transaction of colored coins using Lightning Network. We are not currently working on any technology using RGB, but we are monitoring it as a possible 3rd candidate.

In conclusion, we are confident that the problem of near-zero-cost token issuance is solvable and PKT Network will leverage these technologies for a decentralized bandwidth marketplace. Based on the work done on HTLCs, we are also confident that whatever our choice, tokenized bandwidth and router resources will be able to be quickly atomic-swapped for assets on any other HTLC supporting blockchain including, but not limited to Bitcoin, Litecoin and Ethereum. We intend that a fully decentralized marketplace will emerge without any need for centralized custodians or exchanges in order for participants to trade tokenized bandwidth, VPN, and router resources.

9. CONCLUSION

We have introduced the PKT Network and PKT blockchain as scaling solutions for the Internet to extend beyond core data centers. The PKT Network is a decentralized network that harnesses cjdns for end-to-end encryption and technological advances that improve internet routing and packet transmission efficiency. PKT Network architecture

incentivizes Edge Points and Cloud ISPs to operate infrastructure at the edge. PKT Network's free tier ensures internet access is always available when resources are unused. We have briefly described the PacketCrypt protocol, which creates artificial demand for bandwidth and PKT Cash, which provides an economic incentive for people to operate internet infrastructure at the edge. We described a decentralized bandwidth marketplace, which will leverage blockchain technology for settlement, bandwidth lease provision, and market propagation. Finally, we introduce the routing device to further optimize the advancement of high speed data transmission, encryption and everyday use cases, such as VPN. These innovations solidify the relevance of PKT Network to ensure that internet access, networking and data communication is inexpensive, readily accessible and decentralized.

We expect the internet infrastructure of the future to be owned and operated by *many small operators*, with individuals making up the largest group and micro-enterprises being second. Innovation in the area of satellite based internet access will likely have a major impact on internet availability around the world. However, some short distance communications links, such as a wifi connection to the house of a nearby neighbor, will always be more efficient than satellite communications. For transcontinental and intercontinental communication, we think satellites may become the most efficient solution based on the reduced cost of infrastructure, but we cannot rule out the possibility that as technology evolves, terrestrial shielded cables will reach much higher throughput than is possible with free space communication. What is clear to us is that a decentralized bandwidth marketplace will be necessary for the evolution of the Internet and there will be a growing need for the open protocols and interoperability of the PKT Network.

REFERENCES

[1] Woodcock, B. and Adhikari V. (2014). *Survey of characteristics of internet carrier interconnection agreements*. Packet Clearing House. https://www.pch.net/resources/papers/peering-survey/PCH-Peering-Survey-2011.pdf

[2] de Bijl, P., & Peitz, M. (2005). Local loop unbundling in Europe: Experience, prospects and policy challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.690582

[3] Ford, G. S., & Spiwak, L. J. (2013). Lessons learned from the U.S. unbundling experience. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2378925

[4] Nardotto, M. (2016). Local loop unbundling in the UK does not affect broadband penetration - but it does lead to better service. *DIW Economic Bulletin*, 6(28), 311-317.

[5] Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? : Illusions of a borderless world*. Oxford University Press.

[6] Munkholm, J. L. (2020). The pursuit of full spectrum dominance: The archives of the NSA. *Surveillance & Society*, *18*(2), 244-256. https://doi.org/10.24908/ss.v18i2.13266

[7] Shaw, I. G. R. (2016). *Predator empire: Drone warfare and full spectrum dominance*. University of Minnesota Press. https://books.google.com/books?id=Gil0DwAAQBAJ

[8] Bourreau, M., & Doğan, P. (2004). Service-based vs. facility-based competition in local access networks. *Information Economics and Policy*, *16*(2), 287-306. https://doi.org/10.1016/j.infoecopol.2003.05.002

[9] Briglauer, W. (2014). The impact of regulation and competition on the adoption of fiber-based broadband services: Recent evidence from the European Union member states. *Journal of Regulatory Economics*, *46*(1), 51–79.

[10] Hinden, M. R., & Haberman B. (2005). Unique local IPv6 unicast addresses, RFC 4193, *RFC Editor*, https://doi.org/10.17487/RFC4193

[11] *Cjdns project page*. https://github.com/cjdelisle/cjdns. 2020.

[12] *Pktd project page*. https://github.com/pkt-cash/pktd/. 2020.

[13] DeLisle, C. J., & Seesahai V. (2020, September 4). *PacketCrypt*. https://pkt.cash/PacketCrypt-2020-09-04.pdf

[14] Ofori-Attah, E., & Agyeman, M. O. (2017, January 25). *A survey of low power NoC design techniques.* Proceedings of the 2nd International Workshop on Advanced Interconnect Solutions and Technologies for Emerging Computing Systems, Stockholm, Sweden. https://doi.org/10.1145/3073763.3073767

[15] Sewell, K., Dreslinski, R. G., Manville, T., Satpathy, S., Pinckney, N., Blake, G., Cieslak, M., Das, R., Wenisch, T. F., Sylvester, D., Blaauw, D., & Mudge, T. (2012). Swizzle-switch networks for many-core systems. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *2*(2), 278-294. https://doi.org/10.1109/jetcas.2012.2193936

[16] Xia, Y., Hamdi, M., & Chao, H. J. (2016). A practical large-capacity three-stage buffered clos-network switch architecture. *IEEE Transactions on Parallel and Distributed Systems*, *27*(2), 317-328. https://doi.org/10.1109/tpds.2015.2408614

[17] Herlihy, M. (2018, July 23-27). *Atomic cross-chain swaps*. Proceedings of the 2018 ACM symposium on Principles of distributed computing, United Kingdom. doi:10.1145/3212734.3212736

[18] *OpenDEX project page*. https://opendex.network/. 2020.

[19] *TokenStrike project page*. https://github.com/pkt-cash/ns-projects/blob/b0874ee/projects/2020_07_25_tokenstrike.md. 2020.

[20] Odom, C. (2015). *Open-transactions: Secure contracts between untrusted parties*. http://www.opentransactions.org/open-transactions.pdf

[21] Rosenfeld, M. (2012, December 4). *Overview of colored coins*. Bitcoil. https://bitcoil.co.il/BitcoinX.pdf

[22] *RGB project page*. https://rgb-org.github.io/. 2020.