Restcomm Blockchain: Simplified Business Communications

Enabling decentralized and disintermediated telecommunication services

Author: Ivelin A. Ivanov

Contributors: Ameed Jamous, Lyle Pratt, Alexandr Chevtaev, Andrew Moe and others

This paper is a contribution to the Restcomm Open Source Community. It aims to further innovation in telecommunications technology and markets.

Abstract

This paper proposes a solution to a $30B telecom market problem. Telecommunications services is a global $1T annual business and growing. However nearly $30B is lost to telecom fraud. With the increased demand for consumer engagement via real time calls and SMS, the appetite for business communications fraud will likely continue to increase.

With the decisive shift of telecommunications traffic towards Internet based protocols and the advent of blockchain technology, there is an unprecedented opportunity to implement a decentralized telecoms exchange that significantly improves security, scalability and reliability of global business communications while reducing fraud and paving a path to innovation.

Keywords: telecom, calls, SMS, CPaaS, blockchain

Table of Contents

Restcomm Blockchain: Simplified Business Communications

This paper will propose an approach to solving several major challenges in the wholesale telecommunication industry and will suggest direction for future work. In particular we will focus on addressing call and SMS usage fraud as well as payment fraud issues. We will lean on the secure micropayment properties of the Bitcoin Lightning Network and minimize required upgrades to existing telecommunications infrastructure and practices. We believe this will address a substantial business problem and provide a foundation for further innovation in this space.

1. Introduction

Telecommunications services is a global $1T business[1] and growing[2]. CPaaS, IoT, UCaaS, and CCaaS are some of the leading drivers of increased real time communications traffic in person to person as well as application to person (A2P) calls and SMS.

However today the global wholesale telecom market is inefficient and resembles the Market for “Lemons”[3] due to information

---

[1] Global telecom services spending forecast from 2018 to 2022, https://www.statista.com/statistics/322995/worldwide-telecom-services-spending-forecast/

[2] Worldwide Telecommunications Industry Revenue to hit $2.4 Trillion in 2020, says Insight Research, https://www.prnewswire.com/news-releases/worldwide-telecommunications-industry-revenue-to-hit-24-trillion-in-2020-says-insight-research-300047963.html

[3] Axelrod, R., & Hamilton, W.D. (1981). The Market for " Lemons " : Quality Uncertainty and the Market Mechanism.

asymmetry as compared to other commodities markets. These inefficiencies lead to nearly $30B[4] in loses due to telecom fraud. Other frictions in the system include regulatory hurdles, incompatible legal frameworks, payment processing delays and technical interoperability challenges between telecom carriers.

Currently there are no widely adopted exchanges that enable telecom services to be traded transparently as commodities. The idea has been explored and commercially attempted since the late1990s[5] without sustained success; mainly due to the constantly decreasing telecom wholesale prices and the lack of sufficient volatility to enable commodity trading fees and other incentives for exchange operators.

Enterprises are in a fierce race for consumer wallets. Acquiring users in today's mobile first world is extremely hard using more traditional brand advertising means. Respectively retaining users and securing their loyalty is of critical importance to brands. Missing a time slice of user attention to a competitor can be the decisive element to churn. Hence proactive contextual engagement is becoming highly important competitive differentiating factor. Businesses are moving quickly from passive advertisement to real time user engagement models. They are willing to pay premium rates for calls and SMS in order to maintain constant contact with users in real time

More Tier 1 carriers are testing premium price rates to route business calls and SMS to their subscribers. From Rogers Telecom Canada, AT&T and Verizon in North America to Singtel in Singapore,

---

[4] Telecom Fraud: $29 Billion And Counting, https://www.telecomengine.com/article/telecom-fraud-29-billion-and-counting-why-it-matters-more-than-ever-in-the-digital-era/

[5] Is bandwidth a tradable commodity?, https://www.capacitymedia.com/articles/3142799/Is-bandwidth-a-tradable-commodity

MNOs have announced increased rates in 2018 for A2P SMS traffic ranging between USD 2 cents and 6 cents per message. These rates are a magnitude higher than the wholesale levels of just over a year ago.

While person to person call and SMS rates are steadily going towards zero, business to person (also commonly referred to as application to person or A2P) rates are increasing. Associations such as CTIA are issuing industry guidelines helping telecoms differentiate A2P from P2P (person to person) traffic and charge accordingly based on open market supply and demand dynamics. A recent guideline suggests that A2P traffic is roughly defined by the ratio of messages originated from a phone number. If the ratio is bigger than 3:1, i.e. the messages sent out from that number are three times more than the messages received, the traffic from the number should be billed as A2P.

Presumably consumers will respond to at least one of three messages they receive from another consumer (or bot). Although these guidelines are not perfect and continue to develop, they do indicate a new trend and opportunity for telecoms and businesses to capitalize on the high perceived value of calls and SMS as opposed to email and other more passive means of user engagement.

In the mobile and web advertisement markets brands are bidding and paying top dollar to secure consumer attention for specific key phrases related to their products and services. With A2P (application to person) traffic increasing 80 times from 2016 to 2018[6] and signals for accelerating adoption of CPaaS (communication platform as a service) horizontally into all vertical applications, we are starting to see the

---

[6] THE BICS REPORT, 2018 Outlook: Trends and drivers in wholesale telecoms, https://www.sata-sec.net/downloads/reports/BICS/BICS_Report_2018_web.pdf

beginning of the saturation of consumer's ability to respond to all incoming A2P calls and SMS. Some typical examples include: job related process & system alerts, doctor office reminders, dentist office notifications, airline flight updates, hotel guest service bots, taxi hailing, school alerts, bank transaction notifications, e-commerce delivery updates and many others.

Telecoms will likely move to a dynamic pricing model akin to pay-per-click web search ad models. For example a bidding model could be "pay X for guaranteed SMS delivery to subscriber Y within 10 minutes", "pay 2X to guarantee delivery in 5 minutes", "pay 3X to get a signal when subscriber Y's line is not busy and an unsolicited call can go through"; of course "provided subscriber Y has not blacklisted the calling business". An extended version could reward businesses for good quality of customer service by not charging them a fee if they respond to consumer messages within 30 seconds. This dynamic pricing will be continuously improved with modern AI based predictive pricing engines.

When telecoms adopt dynamic pricing, their enterprise revenues will increase dramatically, which will attract more sophisticated and coordinated fraud attacks.

With the shift of telecommunications traffic towards IP based protocols such as SIP and SMPP, and the advent of blockchain technology, there is an unprecedented opportunity to implement a decentralized exchange (DEX) that significantly reduces incentives for fraud and removes certain inefficiencies in the global telecom infrastructure.

2. Telecom wholesale market challenges

The following chronic problems of the business communications industry are subject to the solution proposed in this paper:

- Fraudulent Call and SMS traffic

There are a number of widespread attacks on the telecom networks that continue to bleed material revenue away from honest operators, which hampers innovation and fuels environment of mutual mistrust between trading partners. From illegal SIM farms stacked with consumer-grade SIM cards to misused P2P binds for A2P traffic, there are many schemes that creative attackers devise and improve continuously to benefit themselves against regulatory policies and legal commercial agreements.

- Fraudulent Payments

Payment fraud is not unique to the telecom industry, but is nevertheless a notable factor. From stolen credit cards to stolen business identity, there is a range of ongoing pains endured by honest operators. Even 1% in a $1T industry is a big material number of $10B. Estimates are that payment fraud may be as high as 0.3-0.9%[7].

- Disputes for poor service delivery

Fraud is closely correlated with poor quality of service and unhappy customer experience. Affected operators end up in disputes between each other to determine who will take the responsibility for the damages. Disputes incur additional legal fees and result in no-win settlements or sometime in very expensive litigation. Yet disputes rarely resolve the root of the problem, which is caused by attackers of the network who continue their business undisturbed.

---

[7] Online Fraud Benchmark Report, https://www.cybersource.com/content/dam/cybersource/2017_Fraud_Benchmark_Report.pdf

- Disputes for billing errors

Telecom billing systems are among the most critical yet most despised elements of an operator infrastructure. Consolidating call records from many servers and interconnections, applying current and correct rates per route, applying a fiat currency value at the correct time and generating end of period invoice are all opportunities for errors and disputes.

- Delays in payment processing

While technologically it is possible to execute payment transactions in milliseconds, today's payment intermediaries often implement policies of 1-3 days delay due to incentives to capture interest for funds in their custody and to justify processing fees. Delays also allow a certain window of time for transaction reversal in case of human errors on the sending side.

- High intermediary fees for payment processing

Payment settlement between transacting operators usually occurs on a weekly or monthly basis. Each time there is a payment processing fee paid to financial intermediaries, which can be in the $40-70 range per wire transfer or 2-3% of the transaction amount. In addition there may be currency conversion fees. A small wholesale operator with tens of millions of monthly calls or messages pays annually tens of thousands of US dollars for payment processing fees. Larger operators pay in the millions. Because each operator is typically interconnected with tens or even hundreds of other operators, there are hundreds of payment events on a weekly and monthly basis. If we look at a common scenario where a hundred payment events occur in a given month with average cost of

$50 per event, its easy to see how processing fees add up to $5,000 in a month or $60,000 per year.

If payment settlements occur on a daily or hourly basis, payment fees will be an order of magnitude higher than they are today. However because of the days or weeks of time lapse between payment settlements, network attackers have a significant window of time to their benefit when their deeds can go unnoticed. Although firewalls and preventive intrusion software helps, in many cases the severity of damages aren't noticed until a payment report is produced and settlement requested.

- Business credit fraud

Organizations such as Duns & Bradstreet provide a method for operators to verify the credit worthiness of their partners before they establish an interconnection and extend payment credit terms. However D&B is known to be subjective and limited to North American companies with little access to reliable credit history information for companies in other countries.

Due to the lack of reliable global third party credit verification agency, often companies rely on partially informed score cards from D&B which are based on self reported company data and as such are subject to manipulation.

3. Telecommunication protocols

Real world telecommunication protocols today are an amalgam of modern and legacy technology, which can date back to the 1940s in some regions of the world. From rotary phones using analog switching equipment to a range of proprietary SS7 equipment and more recent IP based protocols such as H.323, SIP, SMPP, RTP, WebRTC, ICE, STUN, TURN and others.

In this paper we will focus on the most widely used IP protocols for PSTN wholesale traffic: SIP and SMPP. We consciously make this choice because of the critical mass that these protocols have reached on the global wholesale market and increasingly penetrating residential and retail business lines.

4. Carrier interconnection

Interconnection between service providers is a complex multi-step process which encompasses several key aspects:

- Master Service Agreement: legal framework for service delivery, quality guarantees, uptime guarantees, dispute resolution, payment terms and other legal clauses.
- Technical interconnection: Setting up authentication methods, whitelisting of IP addresses, service access authorization, routing codes and other technical steps.
- Transaction rate sheets: prices for terminating traffic, leasing numbers and related services vary by country, area code and quality criteria such as ASR and ACD. Rate sheets are updated frequently by trading partners. Applying rate updates is usually a semi-manual process. Carrier relationship managers regularly review rate updates from their upstream partners, then enter data one record at a time or via bulk upload from a spreadsheet. Then they prepare and push rate update of their own towards downstream partners.

- Choice of payment intermediary

Before traffic trading begins, partners have to agree on settlement currency and intermediary banks or payment gateways such as PayPal.

- Business credit check

Because of the high dollar value of wholesale traffic trade, its a common practice to request business credit record from organizations such as D&B.

- Government license

Operating telecom infrastructure and selling telecom services to other businesses normally requires government issued licenses from organizations such as FCC in the US and Ofcom in the UK. Each country has its own regulatory procedure which is typically time consuming and requires a number of steps to ensure legal compliance as well as technical compliance for lawful intercept.

5. Decentralizing telecom payments

Public telecommunications is a complex web of legal, technical and business threads. In this paper we focus on addressing a small subset of well known pain points related to fraud and payment inefficiencies.

We will make an argument that if there is a way to instantly apply micro payments in a quick, irrevocable and secure fashion for every confirmed telecom transaction between cooperating partners, that will significantly reduce the incentives for fraudulent traffic schemes.

Further if we can automate these micro-payments in a way that scales at cost close to the Internet bandwidth required for the underlying telecom transactions then we can eliminate the latency and fees for traditional intermediaries. This could also solve existing problems with reconciliation of call data from disparate sources, mediation, rating and billing.

Last but not least, if we succeed with such automation, it will be possible to implement in the future dynamic real-time pricing that seeks the optimal equilibrium between trading partners based on streaming transaction events that occur in the network itself[8]. This would alleviate problems with today's pricing guesswork, manual rate sheet updates and billing challenges.

To meet all of these goals we will also have to find a way to incentivize today's telecom operators to participate in the decentralized exchange. In the following section we will look at a possible solution leveraging the Bitcoin open source cryptocurrency and the Lightning Network (LN).

6. Lightning Network for Bitcoin

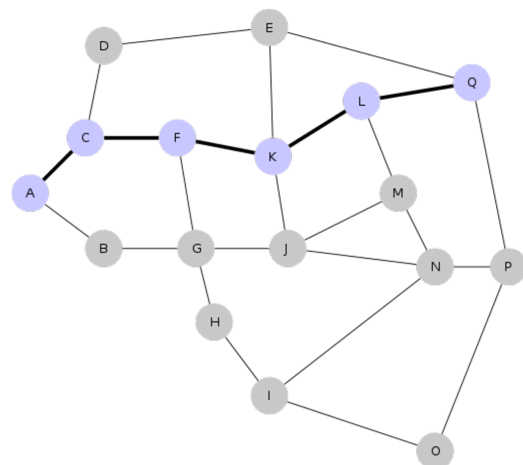
The Bitcoin Lightning Network[9] is a "second layer" payment protocol that operates on top of a blockchain(most commonly Bitcoin[10]). It theoretically enables fast transactions between participating nodes and has been touted as a solution to the bitcoin scalability problem. It features a peer-to-peer system for making micropayments of digital

[8] Salamon, David L., Gustav Simonsson, Jay Freeman, and Brian J. Fox. (2018). "Orchid: Enabling Decentralized Network Formation and Probabilistic Micro-Payments." January. https://www.orchid.com/whitepaper.pdf .

[9] Payments, Scalable Off-Chain Instant. n.d. "The Bitcoin Lightning Network:" https://lightning.network/lightning-network-paper.pdf .

[10] Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." http://www.academia.edu/download/32413652/BitCoin_P2P_electronic_cash_system.pdf.

cryptocurrency through a network of bidirectional payment channels without delegating custody of funds. Lightning Network implementation simplifies atomic swaps.



Normal use of the Lightning Network consists of opening a payment channel by committing a funding transaction to the relevant blockchain[11], followed by making any number of Lightning transactions that update the tentative distribution of the channel's funds without broadcasting to the blockchain, optionally followed by closing the payment channel by broadcasting the final version of the transaction to distribute the channel's funds.

7. Putting it all together

Let’s explore how Lightning Network (LN) can be applied to a telecom DEX.

---

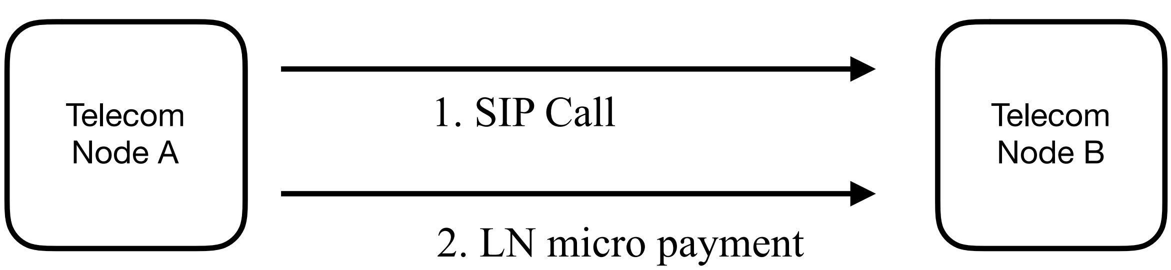
[11] By Kjerish - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=71522233

Each trading partner will host an edge LN node or a relay hub with a hot wallet that has open channels to one or more other partners in the network.

The edge nodes will include a Restcomm Blockchain (RCB) SDK with the following main features:

- LN wallet. Each node in the network will be able to participate in at least one LN channel. Most nodes will be bi-directional. They will send and receive traffic from/to interconnected nodes and respectively make/receive micro-payments for each confirmed telecom transaction (i.e. SMS or call minute).
- API for CDR integration. The purpose of this API will be to integrate with the underlying telecom components running on the node and allow to confirm in real time the completion of an SMS or call transaction. Once a transaction completion is confirmed the servicing node will issue a micro payment request with a hash derived from the transaction metadata. The client node in the transaction will immediately issue a micro payment on the private LN channel upon receipt of a payment request. If the client node does not issue micro payment promptly, the serving node may refuse further service and may even terminate an ongoing call until micro payments have caught up with all unpaid telecom transactions served to the client.

The following diagram illustrates how two nodes interact in a simple call use case:

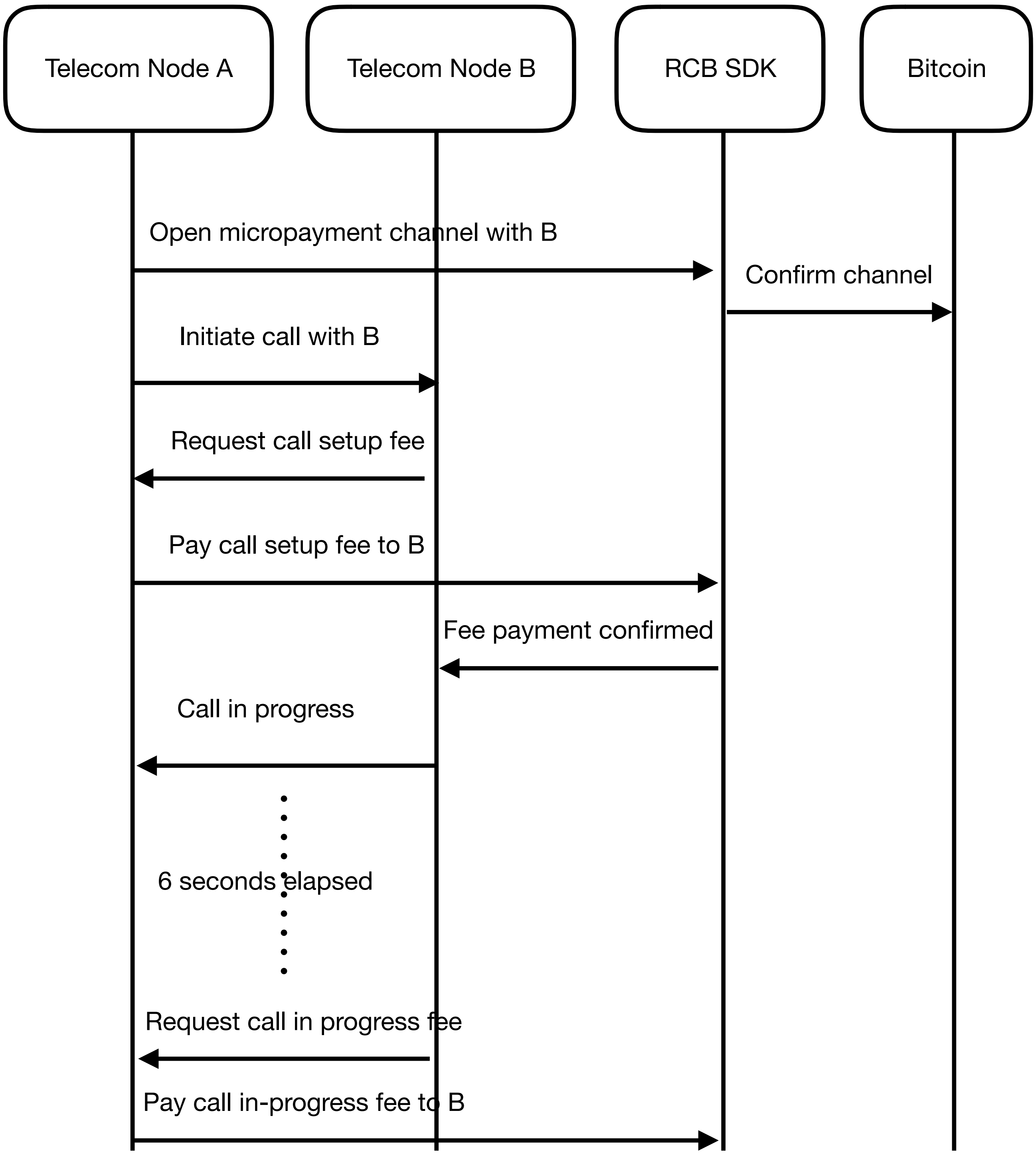


For each completed call minute initiated by A to B, A will send an immediate micro payment to B. B can choose to suspend service to A if A has an outstanding balance $\beta \geq C_{AB,}$ where $C_{AB} \geq 0$ is the maximum extended credit line from B to A. A and B agree to credit line terms as part of their MSA prior to opening an LN micropayment channel. In the future we will explore automating credit terms via smart contracts on the blockchain.

It is worth noting that each time a participating telecom node opens a new LN side chain channel, there is a transaction associated with it confirmed on the public Bitcoin main chain, which is accompanied with a transaction fee paid as an incentive to the mining node which includes the transaction in its block. The irrevocable bitcoin transaction fee paid by each node to open a new channel should deter malicious actors who join the network with the intention to run telecom some free traffic and then disconnect before paying owed fees.

Further in this paper when we refer to RCB channels micropayment, we will imply the LN channel micropayments embedded in the RCB SDK.

Following is a more detailed call flow diagram for the same A to B use case. We assume that each node runs its own RCB SDK, which includes an LN wallet and APIs for integration with the telecom stack. For simplicity, in the diagram we show the RCB SDK as a single component, although it represents the RCB SDK logic running on a node.


Telecom Node A
Telecom Node B
RCB SDK
Bitcoin
Open micropayment channel with B
Confirm channel
Initiate call with B
Request call setup fee
Pay call setup fee to B
Fee payment confirmed
Call in progress
6 seconds elapsed
Request call in progress fee
Pay call in-progress fee to B

8. Channel stakes and payment strategies

Tier 1 P2P Binds

It is a common practice between Tier 1 carriers to not charge each other for person to person (p2p) traffic between their respective subscribers. It is assumed that the amount of calls and messages from subscribers of one carrier are approximately the same as calls and messages from subscribers of their Tier 1 partner.

Tier 1 carriers implement direct binds between each other dedicated for mutual traffic exchange between their subscribers. This eliminates an otherwise complex and expensive problem of high volume charing, billing and payments between Tier 1 partners.

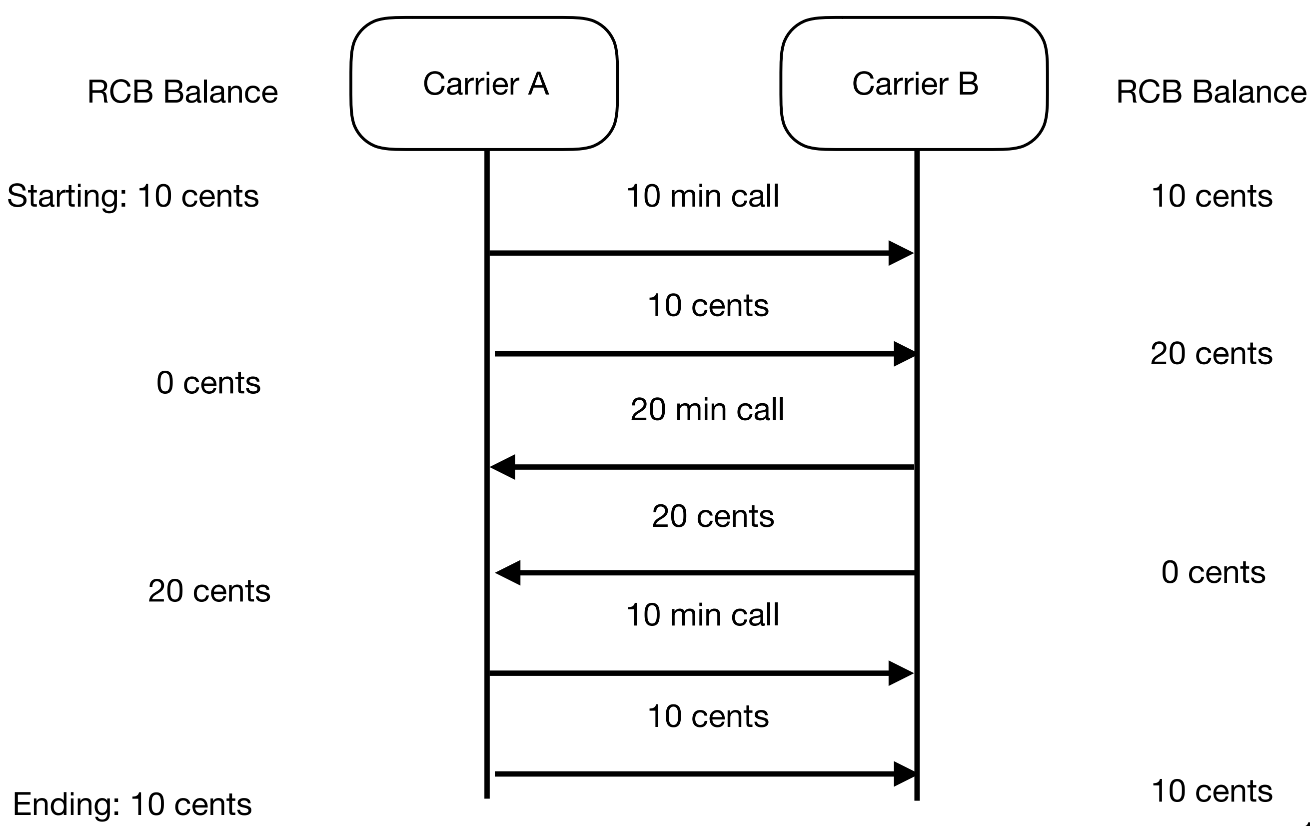
However this approach is also one of the common vectors of attack of the public telecom network. Malicious operators and aggregators either unknowingly or knowingly for profit enable attackers to exploit p2p binds in order to push their traffic at zero or very low cost compared to official wholesale and retail peering binds that are designated to non p2p traffic such as wholesale, retail, and roaming.

To prevent this type of fraud, carriers purchase and deploy firewall equipment designed to detect and block illegal traffic. However often this is a cat and mouse game with attackers staying one step ahead with new creative ways to camouflage their traffic in ways that subverts firewall algorithms.

With RCB enabled peering binds, each call and SMS transaction between two trading partners is instantly and irrevocably paid at fair market value by the benefitting party. When two carriers exchange approximately equal amount of traffic in any given day, week or month period, the bitcoin balance between their respective end of the RCB channel will remain fully funded.

In cases when one side of an RCB channel makes a disproportionate amount of calls and SMS transactions in a given time period, their end of the channel will reflect that. It will be eventually depleted and will require additional funds in order for the peering bind to remain active. This will deter some attacks that rely on unsecured zero or very low cost p2p binds.

The following diagram illustrates balanced trade between two carriers.



In the example above each party stakes the bitcoin equivalent of 10 cents ($0.10) to open an RCB trading channel. After several calls and corresponding micro-payments for a total of 40 cents, the balances are back to 10 cents each. Because of a good trade balanced between the partners, the channel stakes are a fraction of the total value of trade.

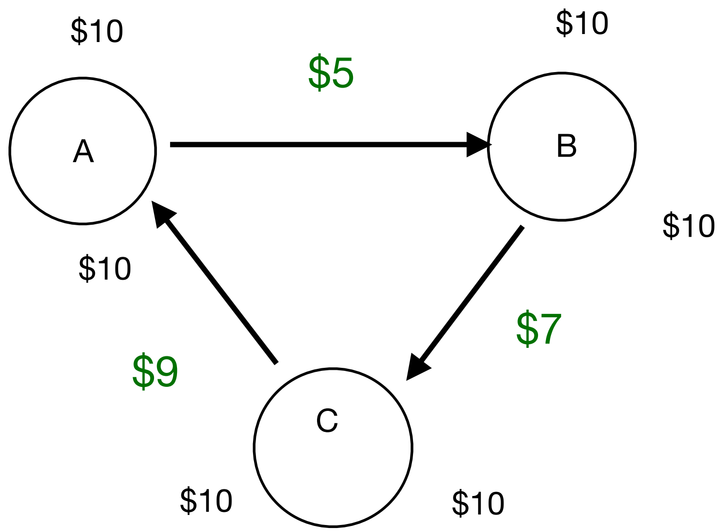
Telecom aggregators and RCB relay hubs

Today's complex international public telecom network topology resembles the global Internet switching topology. Some Tier 1s are interconnected directly, others rely on secondary aggregators or hubs to relay traffic to service providers and enterprises on the telco network which these Tier 1s are not directly connected to.

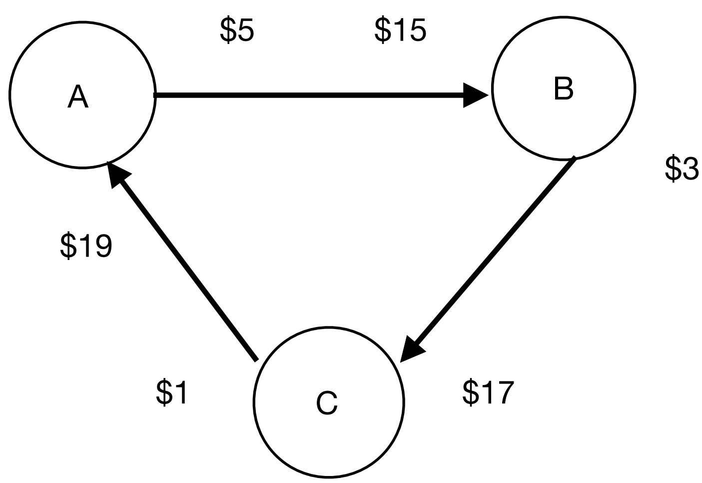
LN complements well the telecom network topology. LN is also designed to accommodate direct two party payment channels as well as indirect payment routes.

In well connected networks such as the Internet and PSTN, it is possible to achieve secure, high volume, high scale transactions with relatively small stakes at each RCB node. The following figures illustrate an example of a cyclic node arrangement which enables the same type of theoretically unlimited, blockchain secured transaction volume as we discussed in the P2P binds section.

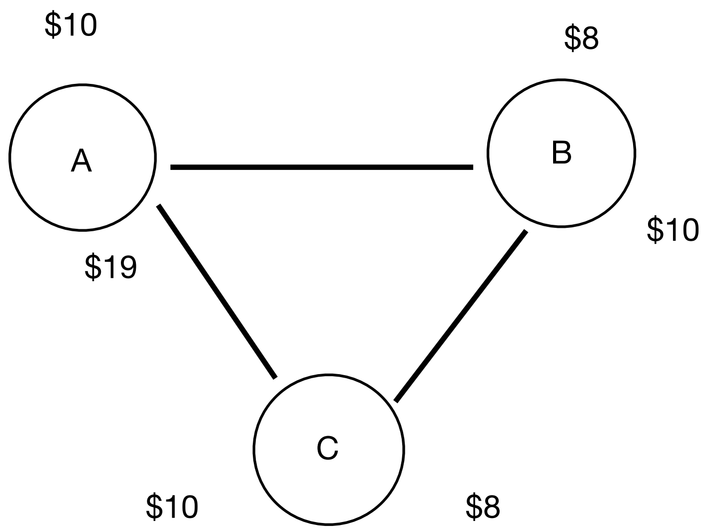
In the diagram below, nodes A, B and C are in a cyclic network arrangement such that A is directly interconnected to B, B to C and C to A. Each node has $10 (in bitcoins) staked at their ends of RCB channels.



Lets look at a scenario where A makes a sequence of calls or sends SMS to B, B to C and C to A a amounting to $5, $7 and $9 respectively. After this round of transactions, the bitcoin balances at each RCB channel end change as shown on the next diagram.

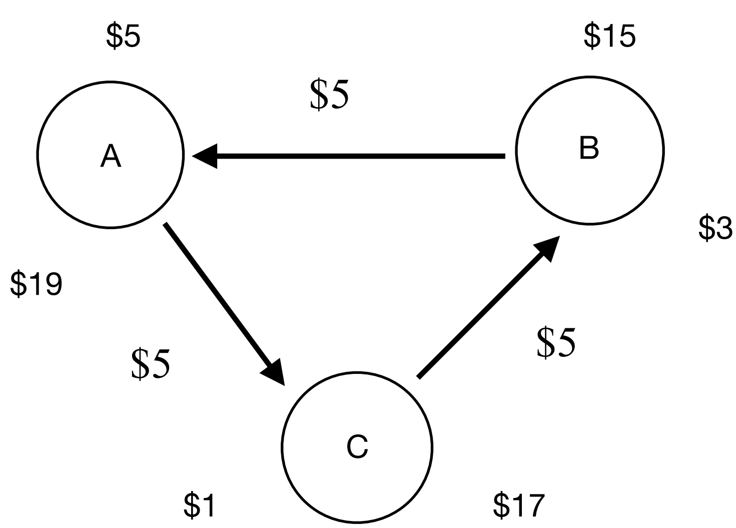


Using the relay feature of the LN protocol, we can safely rebalance automatically each of the three channels without committing to the main bitcoin blockchain and without paying blockchain fees.



Telecom aggregators and RCB relay hubs

Each of the nodes will send itself funds in the reverse direction (counter clockwise) using the same RCB channels. The diagram below shows how A rebalances its channels.



A refunds its A-B channel by sending $5 from the A-C channel in counterclockwise direction from A via C and B. In the process A pays small relay fees to B and C.

Next, B will send its B-C channel $7 in the same manner from its B-A channel via A and C. B will send small relay fees to A and C. Finally C will send its C-A channel $9 from its C-B channel via B and A. C will pay small relay fees to B and A. At the end of this rebalancing process A, B and C will end up with the balances shown below plus (or minus) any difference in the relay fees A, B and C paid each other.

After the rebalancing sequence, A, B and C end up with channel funds that are closer to their original state, which gives them additional time to continue transacting telecom traffic without delays due to payment settlement on the main bitcoin blockchain.

Notice that RCB rebalancing is only necessary when the telecom traffic between two peers is skewed towards one of them. This is usually the case for nodes closer to the edge of the network. Tier 1s and well connected telecom aggregators usually have a well balanced traffic with their telecom partners.

Retail Edge Nodes Participation

Retail edge nodes are usually enterprises who do not participate actively in wholesale traffic trade. They only consume and pay for telecom services to communications service providers (CSPs). Edge nodes do not forward and charge for inbound traffic, therefore they cannot rely on balanced traffic trade to keep their RCB channels continuously funded.

Retail nodes can periodically commit depleted RCB channels and open new ones in order to trade. They can alternatively use the rebalancing technique we discussed earlier in this paper. If they maintain one sufficiently well funded channel to the network and there are cyclic paths back to depleted channels, the funded channel can be used to rebalance the depleted channels. This way the fees and time needed to commit to the public blockchain will be reduced.

When funds run out from all channels, the edge node can commit on the main blockchain one of its channels and reopen it with sufficient funds to rebalance all others that ran out of funds, assuming the network is well connected and there are cyclic paths back to each depleted channel. This will save time and costs of committing all depleted channels on the main blockchain.

9. Optimal path for calls and SMS

In today's telecom networks, calls and SMS follow the shortest path from source to destination phone device through a network of CSP nodes. The distance between two nodes is a weighted function of cost and quality. The process of finding the next node is often referred to as Least Cost Routing.

Each interconnected node in the network shares a table (commonly referred to as a rate sheet) with the cost and quality parameters for a range of destination phone numbers. These tables can change at any time; usually once a week. Let's use the following notation for a rate table R_i that corresponds to node A_i:

$$R_i = \begin{pmatrix} \nu_1 & \alpha_1 & \gamma_1 & \cdots & \gamma_{1m} & \mu_1 \\ \nu_2 & \alpha_2 & \gamma_2 & \cdots & \gamma_{2m} & \mu_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \nu_n & \alpha_n & \gamma_{n1} & \cdots & \gamma_{nm} & \mu_n \end{pmatrix}$$

Where ν is a destination phone number, α is the per transaction rate (per minute or per SMS), γ is one of multiple quality parameters for a given phone destination and μ is the maximum concurrent transaction units (calls or SMS) per second (also commonly referred to as TPS).

The R_i matrix is a simplified representation of real world routing information. There can be multiple price parameters per destination, for example call setup rate, first minute rate, ongoing call rate, call teardown rate. For clarity in this paper, we will work with the simplified version above.

When a node A_i is considering routing options to establish a call or deliver an SMS to destination v, it is solving an optimum function over each of its interconnected neighbor nodes Ω_i and their routing tables. Node A_i is looking for a neighbor node with index j, such that its route to v is at the minimum possible cost α with the best possible quality of service γ.

Lets define as $r(\nu, R_j)$ the weighted price for node A_j to deliver a transaction (call or SMS) to destination number ν. The weighted formula takes into account the friction that each quality parameter brings into the system. For simplicity, we will assume that all nodes have the same view on the importance of each quality parameter and each node reports honestly these parameters in their routing table.

$$r(\nu, R_j) = v_k * \prod (1 \leq l \leq m, \gamma_l)$$

$$j : r(\nu, R_j) = \min r(v, R_k), k \in \Omega_i$$

In today's telecom network, quality parameters are self reported in the rate sheets. There are third party quality assurance products and services who can aid carriers in measuring more objectively these quality parameters. However the process requires significant human intervention for configuration and integration. The data produced is loosely used to reflect on rate tables.

In a more transparent and automated telecom network with ability to gather real time quality analytics from multiple sources, the values for the γ vectors can adjust dynamically and allow $r(\nu, R)$ to approximate more objectively value for money as network conditions fluctuate over time.

10. Optimal routing for payments

Similar to calls and SMS, most micropayments in an RCB network traverse the shortest path from source to destination. However there are several differences. Payment distance between RCB nodes is a function of channel relay cost and available bandwidth in bitcoin units. It is also possible to route payments using multiple channels simultaneously.

It has been shown[12] that in Lightning Network, where multiple payment paths exist between a source and destination node, applying Atomic Multi-path Payment (AMP) can provide a better alternative to shortest path routing.

AMP is a promising area in active research. The closest problems we have been able to identify in public literature are these of Capillary Routing for real-time streaming[13] and Multi-path TCP[14].

In order to look for optimal payment routing, we need to understand the constraints imposed by the underlying telecom network properties. One such constraint is the maximum concurrent calls that a node can sustain.

If node A_i can sustain a maximum of μ_{ij} concurrent transactions towards node A_j then the maximum required bitcoin balance at the A_i end of the $A_i - A_j$ RCB channel is the most expensive sum of possible telecom transactions:

$$M_{ij} = \max \sum_{\alpha \subset R_i,} (\alpha \cdot \kappa) : \sum_{\lambda \in \kappa} (\lambda) = \mu_{ij}$$

Here α is the vector of unit rates from the A_i rate table R_i and κ is a vector of non-negative integers whose sum is μ_{ij}.

Let's also define the maximum required bitcoin for all RCB channels out of A_i as

---

[12] Specific fee routing for multi-path payments in Lightning Networks, https://medium.com/coinmonks/specific-fee-routing-for-multi-path-payments-in-lightning-networks-b0e662c79819

[13] Gabrielyan, E., & Hersch, R.D. (2006). Capillary Routing for reliable real-time streaming.

[14] Han, H., Shakkottai, S., Hollot, C.V., Srikant, R., & Towsley, D.F. (2006). Multi-Path TCP: A Joint Congestion Control and Routing Scheme to Exploit Path Diversity in the Internet. *IEEE/ACM Transactions on Networking, 14*, 1260-1271.

$$M_i = \sum_{j:A_j \in \Omega_i} M_{ij}$$

M_i signals that the required capacity of bitcoin at an RCB node is proportional to its telecom throughput. This intuitive observation will play a role in further analysis of RCB topologies.

Some nodes may choose to stake the maximum required bitcoin amount to allow them to function at maximum telecom capacity. Others may choose to use a probabilistic value that satisfies 95% of real world node loads and is a significantly lower number than the 100% capacity stake.

For example a small to mid-size wholesale carrier maintains capacity of 10,000 TPS. For simplicity lets say that the average per transaction value on the wholesale market is $0.01 (1 cent USD). This translates to M_i in the order of $100. Reasonably low requirement to run their business on RCB. Small carriers transact from several hundred thousand to tens of millions of dollars on a monthly basis at 5%-30% margins.

A large carrier with support for over 1,000,000 TPS would have to stake $10,000. Also a reasonably low number given that large carriers transact billions of dollars monthly business with 30-60% margins.

The examples above show a promising potential for the value that RCB brings to the global telecom network in terms of security and convenience. We will leave the research of staking strategies outside the scope of this paper although this may not be a top priority given that the maximum amounts required might be sufficiently low. We will need to run extensive simulation of real world network topologies to confirm this.

11. Currency volatility

A well known issue with cryptocurrency based payments is volatility relative to fiat currencies such as the USD. Cryptocurrencies have had a history of wild swings as much as 1000% in a single day.

However volatility of fiat currencies is also a well known problem in telecom commerce. There are many historical examples of local currencies fluctuating sharply or even being outright banned from international trading for periods of days, weeks and months.

The lasting socioeconomic impact that Bitcoin has had on consumers and businesses around the world since its inception in 2009 is undeniable. It has lead to an environment of broad understanding and acceptance with a critical mass of daily trading across cryptocurrency exchanges around the world.

It can be argued that the popularity and acceptance of Bitcoin as as a major currency now rivals that of most fiat currencies and is on a trajectory to reach a top world 10 currency confidence in the near future alongside USD and EUR.

While there is no certain way to guarantee stability of BTC vs USD, we believe there are sufficient fundamental factors that enable BTC to be a reliable choice for telecom payments. Some of these factors include.

- Ability to quickly and automatically convert to major fiat currency via exchanges around the world.
- Ability to quickly obtain current value against USD via public API.

- Near instant liquidity on US government licensed cryptocurrency exchanges such as Coinbase, Robinhood, Gemini and others as well as many reputable international exchanges.
- Ability to program dynamic telecom rate sheet adjustment based on fluctuation in BTC value vs USD. For example transaction rates can be updated and pushed to interconnected RCB nodes if the ratio of BTC to USD moves more than 10% in a given day, week or month.
- Full automation from transacting calls to payments allows 24x7 agility and speeds far greater than possible today. Fiat currency payments go through intermediaries such as banks and clearing houses with multiple hours to multiple days settlement periods.

As we go into implementation phase and test market sensitivity to BTC volatility, we may have to reevaluate our currency strategy and consider alternatives such as Tether and Gemini which are pegged to USD.

12. Conclusion

Public telecommunications is a global trillion dollar market that every consumer and business participates in. This paper discusses long standing known problems with fraud that amount to $30 billion each year. It also suggests a blockchain based solution which addresses these problems and lays the foundation for future innovation in business communications.

With modernized basic services in the telecom wholesale network, we can look towards the future at new business models for A2P such as dynamic pricing, higher level premium CPaaS APIs and a marketplace open for mainstream app developers.