# Blockchain and Peer to Peer VOIP communication over WebRTC

- Altanai ( tara181989@gmail.com )



POST COVID HACK 2020

August - November 2020

https://devpost.com/software/blockchain-and-peer-to-peer-voip-communication-over-webrtc

# Introduction



## Hi, I am Altanai.

https://www.linkedin.com/in/altanai/

Specialised in voice over IP and telecom integrations.

Open Source enthusiast and tech evangelist - Telecom R & D – WebRTC , SIP , IMS, VoLTE , SaaS , SBC , REST , Cloud , IOT , media Streams

Author of WebRTC Integrator's Guide, https://www.packtpub.com/in/web-development/webrtc-integrators-guide.

Patent on "Multimedia Conferencing" US patent - US20180284957A1

https://devpost.com/software/blockchain-and-peer-to-peer-voip-communication-over-webrtc



## Hi, I am Hridyesh.

https://www.linkedin.com/in/hridyesh-bisht-22340613

Google Cloud Facilitator| Core Member of Developer Student Club at SIT | AWS Community Builder
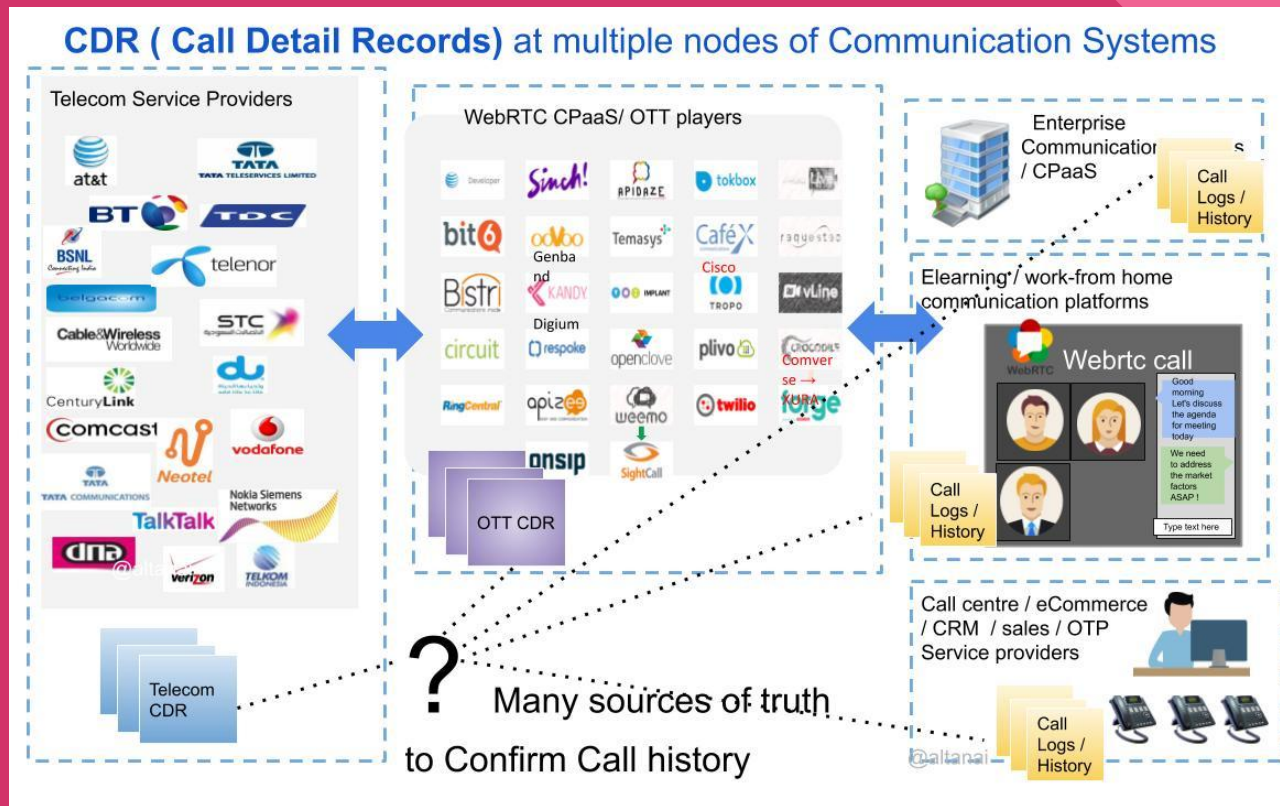
# CDR ( Call Detail Records )

- **Originating - Caller UUID**
- **Destination - Callee UUID**
- **Start/End time of Call**
- **UID of Telecom system writing the CDR**
- **Unique Sequence Number of the Call Record**

Optional fields
- Results of the Phone Call
- MOS ( Call Quality)
- Fault Condition of the Call
- Status (Failed calls with Cause of Termination)
  -
    a. Un-allocated (unassigned) Number
    b. User Busy
    c. Temporary Failure
    d. Service operation violated
    e. National Use
    f. Call Split
    g. Redirect reason
    h. Not Found
    i. Temporary Unavailable

CDR(Call Data Records) are the proof of any call transaction on a telecommunication platform.

Besides auditing , CDRs  are primarily used for billing and invoicing.

# "Call Detail Record Woes / Conflict / Mistrust" - Reasons

Existing methods of CDR ( Call Detail Records )  management are subjected to mismanagement , ransomware attacks , data breaches and provide no transparency or authentication .



CDR ( Call Detail Records) at multiple nodes of Communication Systems

# Pitfalls of centralised CDR storage

"**Once the attackers had control of the company's servers, they went after call detail records (CDRs)."** - <u>DarkReading.com</u>

6/25/2019
06:00 PM

## Global Cyberattack Campaign Hit Mobile Carrier Networks

**A nation-state group possibly out of China has attacked cell carrier networks in search of data on high-value individuals.**

Curtis Franklin Jr.
News

A global cyberattack campaign believed to be the work of a nation-state group has hit telcos and mobile carriers around the world in an effort to gather intelligence on specific individuals.

CPO MAGAZINE

CYBER SECURITY  INSIGHTS  · 4 MIN READ

**Telecom Corporate Accounts at Highest Risk for Cyber Attacks**

BOB LYLE · OCTOBER 8, 2020

ET Telecom.com
From The Economic Times
Telecom News / Latest Telecom News / Policy

**CDR use for Covid contact tracing on for months in Uttar Pradesh**

Home » Security Bloggers Network » Japanese Telecoms Giant NTT Suffers Data Breach, Takes Four Days to Learn of Intrusion

Japanese Telecoms Giant NTT Suffers Data Breach, Takes Four Days to Learn of Intrusion

by Filip Truta on May 29, 2020

Current communication systems use CDR is used for billing and invoicing .

Storage tools include - noSQL mongodb, redis cache , kafka . LTE based telecom carriers use SQL RDBMS in OSS/BSS*.

However yet , often the CDR's find their way
into excel-sheets,  FTP servers and are prone to ransomware  hacks and data losses.

OSS/BSS* - operations support system and business support system in telecommunications

# Socio-Economic Inclusion Track
## Decentralised VoIP CDR for post-COVID telco Infrastructure

### CDR storage dilema !

Fast growing VoIP industry and impetus to Work-from-home CPaaS (Communication as a Service) solutions, ad-hoc peer-to-peer , OTT( Over-The-Top)  WebRTC platforms have brought one challenge to light i.e.

maintaining call history, without sacrificing  privacy and authenticity .

### Proposed solution ✅

De-centralize call records using Blockchain and Smart contracts.

1. Batch together call transactional CDRs

2. Deploy VoIP transaction on smart contract

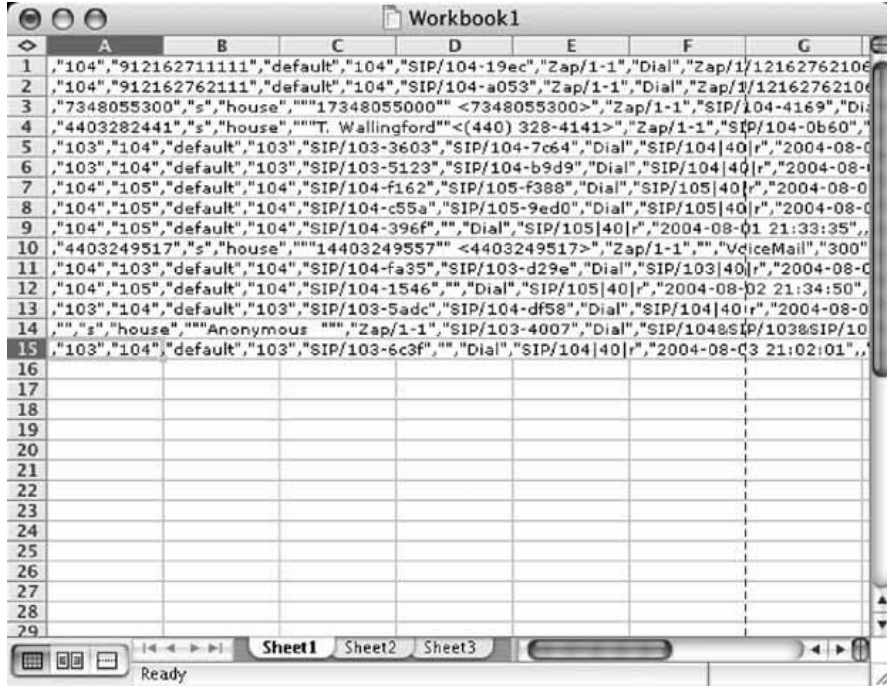3. Update Call state in smart contract .



Blockchain dApp integrated VoIP landscape
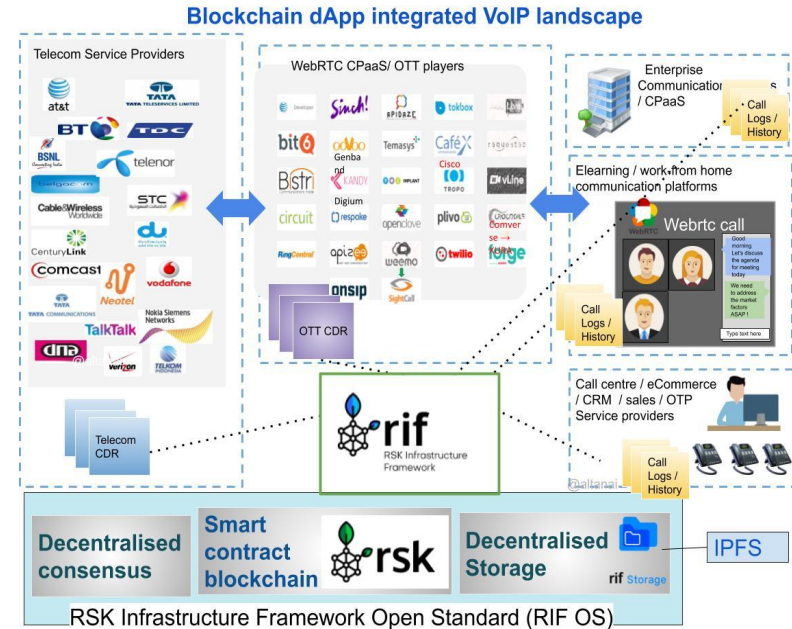
# CDR storage

## Centralised system vs dAPP



Figure : Existing database CDR storage
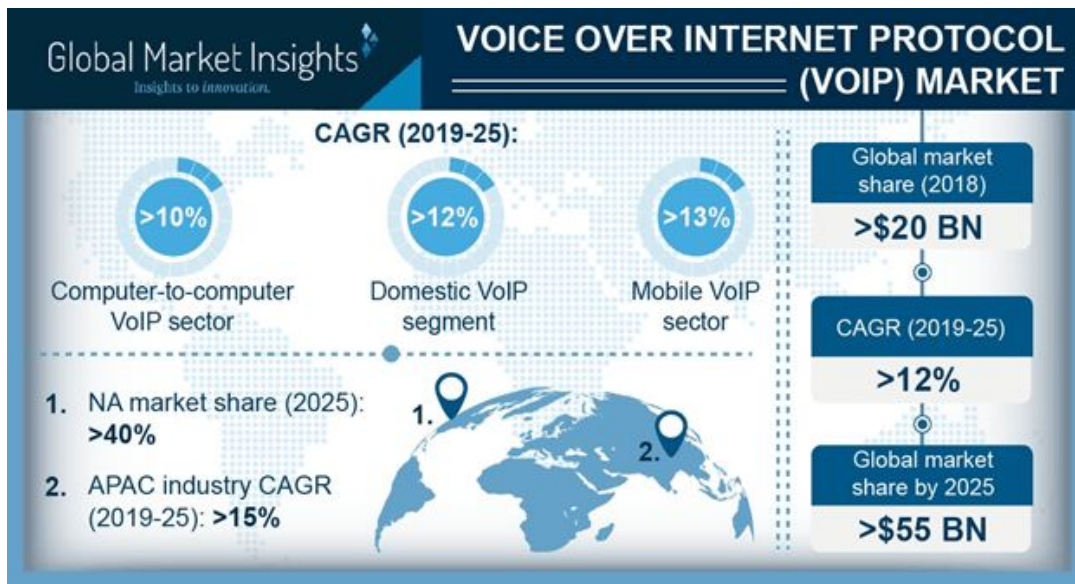 -   Can be erased , tampered..

Figure : Proposed chained CDR storage
 -   Immutable , Authentic , Transparent

# Value Add-ons for WebRTC/VoIP CDR dAPP

Immutable call records for call transactions ( calls, messages, conferences, redirections, OTP calls , spam calls .. ) on all networks and systems.

- ❏ Cloud telephony servers ( Freeswitch , asterisk , kamailio , opensips .. )
- ❏ Telecom Carriers
- ❏ Hosted call centres, elearning , telemedicine , CRM ..
- ❏ SIP / WebRTC CPaaS

**VoIP is a competitive and fast growing market , currently growing at 2x the pace due to high demand for remote calls**



Global Market Insights
Insights to innovation.

**VOICE OVER INTERNET PROTOCOL (VOIP) MARKET**

CAGR (2019-25):

>10% — Computer-to-computer VoIP sector

>12% — Domestic VoIP segment

>13% — Mobile VoIP sector

1. NA market share (2025): >40%
2. APAC industry CAGR (2019-25): >15%

Global market share (2018) >$20 BN

CAGR (2019-25) >12%

Global market share by 2025 >$55 BN

Image Credit : gminsights.com

# Technology used in demo POC

### Web Phone

★ WebRTC browser API

★ JSSIP - SIP protocol over Websockets

★ Web3.js - Ethereum JSON-RPC API

★ Metamask - Browser Extension

### VoIP Network

➢ Kamailio SIP server

### Blockchain Network

❖ RSK smart contract



Webrtc Desktop Browser Call

WebRTC browser

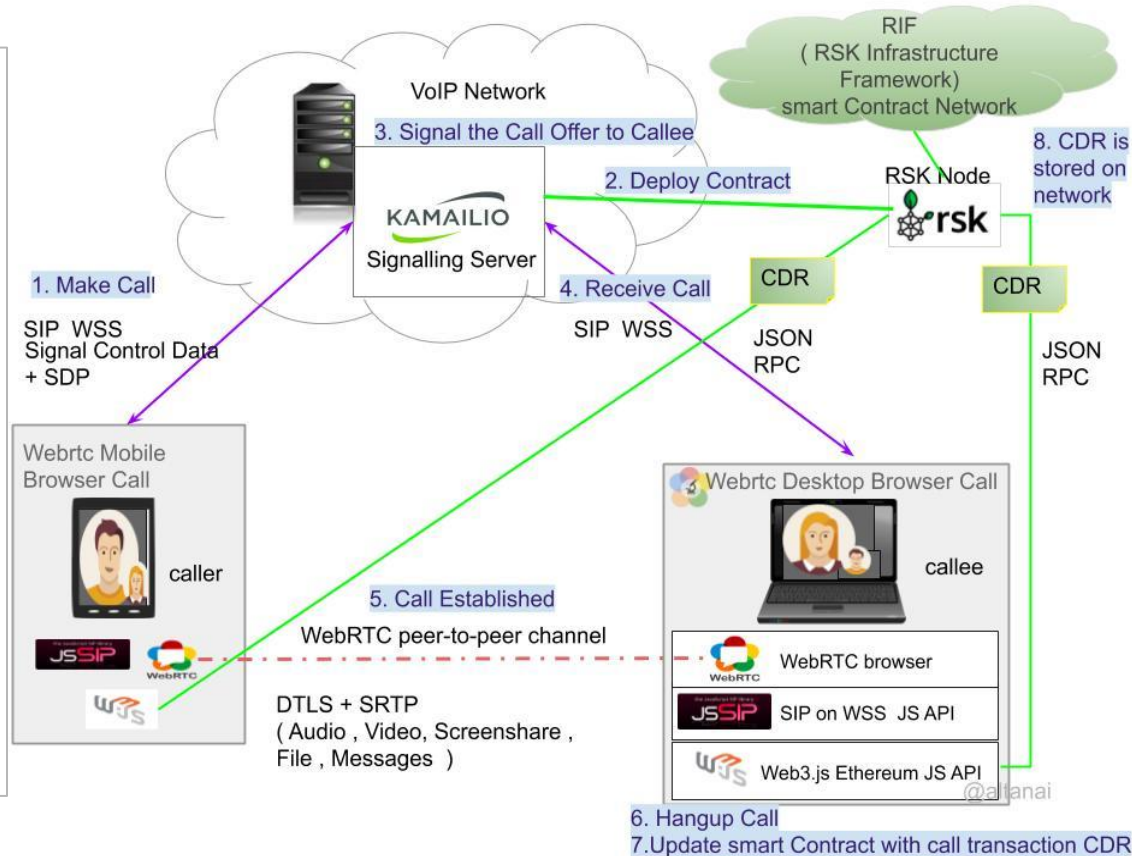SIP on WSS JS API

Web3.js Ethereum JS API

# FlowChart



POC Outline

Step 1 : Create a Smart contract for call on RSK Testnet via Remix IDE

Step 2 : Make a WebRTC Call via Kamailio SIP Server using jsSIP library

Step 3 : Call Transaction is updated on Smart Contract by WebRTC browser using web3.js and MetaMask wallet

**VoIP Network**

3. Signal the Call Offer to Callee

2. Deploy Contract

**KAMAILIO** Signalling Server

1. Make Call

SIP WSS Signal Control Data + SDP

4. Receive Call

SIP WSS

RIF ( RSK Infrastructure Framework) smart Contract Network

RSK Node

8. CDR is stored on network

CDR

JSON RPC

CDR

JSON RPC

Webrtc Mobile Browser Call

caller

Webrtc Desktop Browser Call

callee

5. Call Established
WebRTC peer-to-peer channel

DTLS + SRTP
( Audio , Video, Screenshare , File , Messages )

WebRTC browser

SIP on WSS JS API

Web3.js Ethereum JS API

@altanai

6. Hangup Call
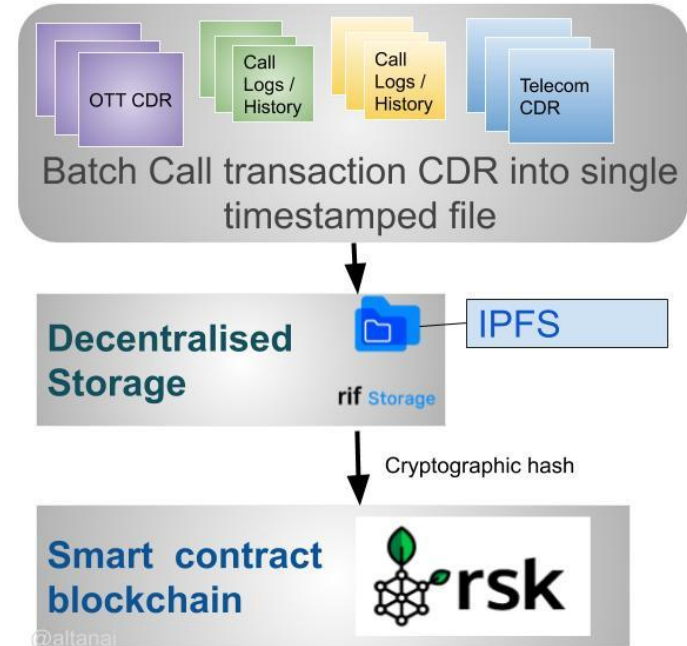7.Update smart Contract with call transaction CDR

Cost to Deploy MVP
- C5 AWS instance for RSK node and kamailio server - $438
- SSL certs - 10$
- WebRTC + JSSIP - no cost
- R-BTC tokens transaction execution fees - proportional to call traffic

# Scaling - WebRTC/ VoIP Platform CDR dAPP With RSK Network

RSK scales to up to 100 transactions per second without sacrificing decentralization. however owing to large call transactions *ranging from 500 cps to 2k cps for a VoIP network* ,

following scaling approaches are adopted -

❖ Batch Call Records into a file and upload on IPFS via RiF storage
❖ Update RSK smart contract with confirmation and address of stored file

# Conclusions



Blockchain and p2p VOIP
communication over WebRTC
- altanai

@altanai ( tara181989@gmail.com)
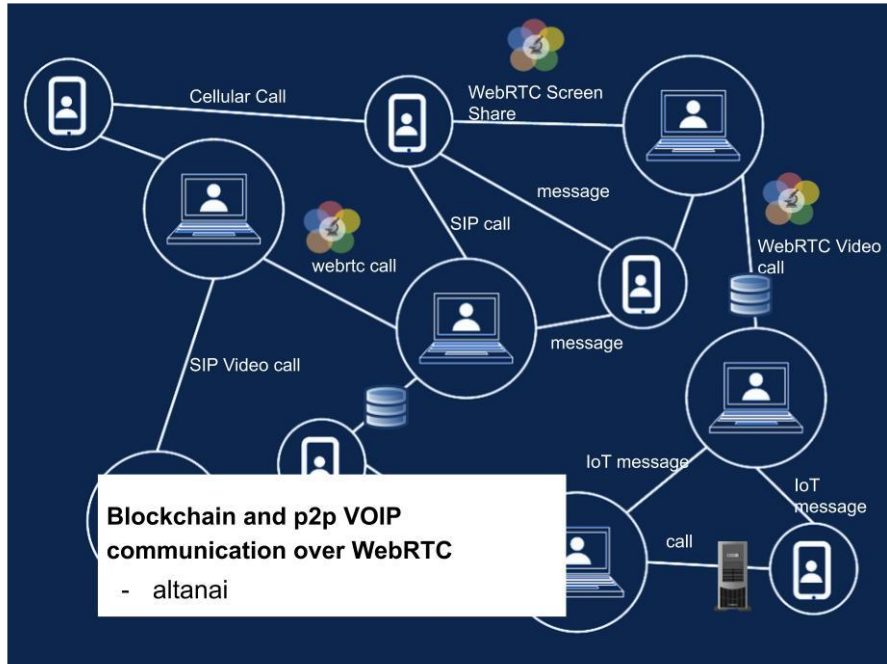
CDR dAPP is distributed across peers in SIP-WebRTC-Voice over IP such as Freeswitch , asterisk, kamailio , webrtc communication platforms ...

Call Data Records are batched together and pushed to a contract in a blockchain network.

Updated smart contract is pushed to RSK blockchain thus making them immutable for all future references.

_____

End.