

Blockchain as a Measure to Curb Challenges in Telecommunication

It is without any doubt clear by now how the introduction of blockchain has caused a disrupt to almost every sector of the world's economy, from entertainment to groceries shopping, from ensuing a new method of payment to put on check the gross irregularities plaguing a few payment systems. Blockchain has moved beyond its initial usage which included a system of P2P payment initiated by bitcoin. However, more recently, research has also proven how the use of blockchain can be used to solve (if not all) most of the challenges facing the Communication Service Provider's (CSP) industry. According to a research by Monitor Deloitte, at least 53% of the leading CSP firms have started discussing (if not implemented) the usage of blockchain to solve the problems faced by the industry. The study also highlighted how these firms expect value from this new strategy. The telecom service providers sector expects blockchain to help them through the simplification of operations, cost reductions, creation of new revenue streams, enhanced teamwork, and real-time transparency. In addition to these issues, blockchain is predicted to assist in resolving issues with complex agreements, roaming fraud, worries about digital identity, GDPR rules, and data protection. Even though the telecommunications industry has undergone significant transformation over the past 20 years, roaming, exorbitant costs, the possibility of fraud, privacy concerns, and a host of other problems continue to be problems for both providers and consumers. Fortunately, a lot of the marketing hype and false information around blockchain is starting to fade away as more practical blockchain use cases and applications appear.

Leveraging Blockchain in Telecom for Fraud Prevention

Another Deloitte analysis claims that CSPs experience losses of up to \$48 billion annually as a result of fraud. Unauthorized voice and data traffic that is intended to steal money from CSPs or their clients constitute fraud in the telecom industry. It can take months to find and is frequently the result of hacking into a clumsy subscriber verification process.

Fraud in the telecommunications industry is a serious issue and can be broadly classified into two categories: Roaming fraud and Identity fraud.

Roaming Fraud

Roaming or roaming services refers to the concept of a mobile phone being used outside the range of its native network and connecting to another available cellular network. The telecom sector has been using a traditional method for billing and settlement for roaming services for many years, which entails the exchange of Transferred Account Procedures (or TAP files) between the roaming partners. Traditional roaming settlement will likely become more difficult as new technologies like 5G enter the market because of a rise in users, partners, and traffic.

Billing and Charging Evolution (BCE) enables the new generation use cases brought on by cutting-edge technologies like 5G in addition to streamlining complex multi-party settlement processes. This is made possible by distinguishing characteristics including obviating the requirement for special editors to read various TAP file formats like ASN1 and the necessity of exchanging raw files inside certain timelines. The XML-formatted reports created by BCE can be easily exchanged to facilitate settlement and reconciliation operations.

International mobile roaming has long faced difficulties with the negotiation, management, and reconciliation of inter-operator agreements, particularly when it comes to assuring correct clearing and settlement of international transactions among a vast network of roaming partners. As 5G networks spread, roaming will no longer be restricted to network operators, creating new connections between carriers and business networks. As a result, mobile carriers will need to improve the accuracy, precision, and security of all of their international roaming transactions as well as the underlying systems that underlie them, from rating and pricing through clearing and settlement.

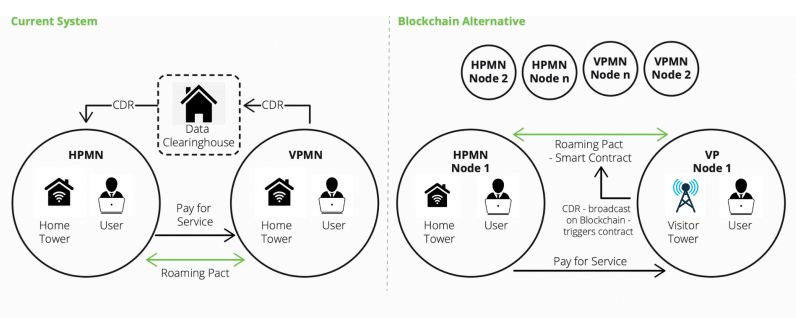
Every day, hundreds of connected networks handle billions of mobile interactions that are controlled by dozens of buyers and sellers. Currently, telecom businesses manage settlements manually while negotiating this complex web of procedures and technologies, and in many cases, they outsource the reconciliation process.

Numerous types of roaming fraud might exist. The most obvious is that scammers exploit the ineffective roaming data transfers across carriers. A dishonest customer can switch from a home public mobile network (HPMN) to a visited public mobile network (VPMN) and utilize services without paying for them. The use of premium-rate numbers by fraudsters enables them to make expensive overseas calls. The

HPMN, which is now in charge of the service costs, receives the consumption statistics from the VPMN. The HPMN chooses to take the financial hit because data audits and follow-up procedures are time-consuming and expensive. Although right now, there are many obstacles in the way of a faster, smoother and more efficient wholesale roaming clearing and settlement process. Including:

- Limited opportunities for monetization and rising running expenses for legacy and new tech deployments
- Average processing periods to clear, settle, and pay partners are lengthy
- Conflicts that result in write-offs and other negative debt situations
- Delay or failure to receive money

The challenge of maintaining the legacy setup must be overcome at the same time as addressing these issues, which necessitates a redesign of wholesale roaming operations to make them future-ready. This problem doesn't deter mobile providers, who are working to further enhance their entire roaming operations.



Identity Theft Fraud

Another significant cause of fraud is identity theft. When a customer signs up for telecom services, it includes gaining legal authorization for them. The goal is to use the services without having to pay. Through clearinghouses or aggregated SIM accounts, fraudsters can access numerous carrier accounts. As a result, the attackers might effectively have access to various revenue sources.

Blockchain-based identity management lowers fraud using keys to prevent identity fraud. The foundation of blockchain identity management is a public-private key encryption technique. Mobile and fixed telecom devices with cryptographic capabilities can be connected to the corresponding subscriber identities. When accessing any telecom service, the device can use the private key to digitally sign the transaction rather than broadcasting its IMSI number to the network as is currently the case. After that, the network is informed of the public key. Prior to granting access to the telecom service, the transaction is cryptographically validated by identifying the public key to make sure it was started by the legitimate subscriber and was unaltered.

How Blockchain intends to curb the challenges facing the telecommunication industry

The introduction of BlockRoam

Mobile service providers (MSPs) are particularly susceptible to roaming frauds, especially those that take advantage of the lengthy lag time in the data exchange process of the modern roaming management systems, which results in multi-billion dollar losses every year. For this purpose, one of the technologies developed to curb incessant roaming charges is the BlockRoam. BlockRoam is a cutting-edge blockchain-based roaming management system that offers an effective platform for data sharing between MSPs and mobile users. BlockRoam can significantly reduce the information exchanging delay, thereby addressing the roaming fraud issues. It does this by utilizing the Proof-of-Stake (PoS) consensus mechanism and smart contracts.

The concept of Selective Disclosure Through Digital Identity

Digital identifiers (Digital IDs) are references to characteristics of an individual's identification (such as a passport's passport number or an ID's age) that establish an individual's identity and validate their ability to access services or information. These digital IDs are frequently under the control of large organizations, which manage and analyze this data for marketing and advertising purposes. These digital

IDs contain a variety of personal information, including an individual's age, gender, or address. A user can then request claims against it for verification from issuers (such as the government, a school, or a bank). DIDs are less susceptible to data breaches and theft since they are not stored in vendor or organization databases like normal digital IDs are. These DIDs can be utilized for a range of tasks, such as secure and confidential client KYC, e-voting, tax payments, and event check-ins, among others. By enabling users to create IDs and store credentials in their wallets with the option to control with whom those credentials are shared.

Conclusion

Blockchains core attributes to make data immutable, verifiable and traceable enables the Telecom industry to create an ecosystem where consumers are in full control, and there is trust, security, and transparency in the participating ecosystem. The result is lower costs for consumers, better networks and an overall improved experience for all stakeholders. However, Billing and Charging Evolution is a new generation solution for the settlement of 5G roaming. Implementing BCE over blockchain provides a platform where all participants can have their nodes, thereby simplifying the settling and reconciliation processes. Using blockchain for BCE will also ensure transparency of transactional data, better scalability due to improved TPS, and provide an immutable platform that brings trust among telecom partners and blockchain network members.