Hyperledger FOUNDATION

ABOUT HYPERLEDGER

Hyperledger Foundation was founded in 2015 to bring transparency and efficiency to the enterprise market by fostering a thriving ecosystem around open source blockchain software technologies. As a project of the Linux Foundation, Hyperledger Foundation coordinates a community of member and non-member organizations, individual contributors and software developers building enterprise-grade platforms, libraries, tools and solutions for multi-party systems using blockchain, distributed ledger, and related technologies. To learn more, visit www.hyperledger.org.

TDIDN: A Paradigm Shift in Telecom

PURPOSE OF THIS SOLUTION BRIEF

This solution brief introduces the groundbreaking concept of a Telecom Decentralized Identity Network (TDIDN), a new way to improve identity management using decentralized identifiers (DID) and blockchain technology. This brief explores how TDIDN's innovative approach can improve security, efficiency, and privacy in telecom operations.

INTENDED AUDIENCE

The main audience for this solution brief is telecom operators interested in improving security, reducing overhead, enhancing privacy, and reducing disputes with their partners and customers.

A COLLABORATION

This solution brief was driven by the **Hyperledger Telecom Special Interest Group**, a collaboration with LF Networking and its associated projects that explore use cases for blockchain technology in the Telecom industry.

V1.0 published April 2024.

ABSTRACT

Introducing TDIDN, the Telecom Decentralized Identity Network, a groundbreaking solution that leverages decentralized identifiers (DID) and blockchain technology to revolutionize identity management in the telecom industry. This solution brief explores TDIDN's potential and its innovative approach to improving security, efficiency, and privacy in telecom operations.

1. INTRODUCTION

The telecom industry plays a pivotal role in connecting the modern world and powering the digital revolution. However, this role comes with a host of challenges, including security, overhead, and privacy.

In this era of digital transformation, the industry is in dire need of innovative solutions that can meet these challenges.

This solution brief introduces a game-changing concept that promises to revolutionize the telecom sector by reimagining identity management: Telecom Decentralized Identity Network (TDIDN).

TDIDN is built on the foundation of decentralized identifiers (DID) and blockchain technology. This offers a secure, transparent, and efficient way to manage identities in the telecom space while empowering users and streamlining operations.

This brief provides an overview of the telecom industry's current identity management landscape and describes TDIDN use cases, components, and user interactions. All this shows the potential for TDIDN to bring about a paradigm shift in telecom identity management.

2. THE TELECOM INDUSTRY FACES MANY CHALLENGES

The telecom industry faces many pressing challenges that demand innovative solutions. These include the following critical issues.

2.1 Security concerns

Telecom networks handle vast amounts of sensitive data, making them attractive targets for cyberattacks and data breaches. Traditional authentication methods, such as user names and passwords, are vulnerable to identity theft and credential-based attacks.

In fact, Verizon recently reported that the two main ways cybercriminals attack organizations are through stolen credentials and phishing.[1]

2.2 Administrative overhead

When each individual telecom maintains its own separate registries of allowed and blocked devices, this creates a significant administrative burden for each company. These siloed efforts create inefficiencies, hinder operational agility, and impose unnecessary costs.

2.3 Privacy issues

In an era of heightened privacy concerns, every telecom operator must strive to safeguard user data and ensure only selective disclosure of personal information. For their part, telecom users need greater control over their data and who can access it.

2.4 Billing transparency

Transparent billing processes and accurate bill calculations are essential to build trust among telecom service providers and customers. Today's somewhat opaque billing systems often lead to disputes that undermine customer satisfaction.

2.5 Weak authentication through OTPs

One-Time Password (OTP) authentication that relies on temporary codes sent via SMS or email can be cumbersome. And OTPs can be attacked with spam and phishing. The telecom industry must create simpler and more robust ways to authenticate users.

2.6 Difficulties with Service Level Agreements (SLAs)

Service Level Agreements (SLAs) are the lifeblood of telecom service providers, but managing them can be cumbersome and prone to disputes.

The required levels of service and the associated penalties for any lapses are not always clearly defined. Monitoring the actual level of service is complex. Gaps in service can be missed or identified long after they occur.

In many cases, SLA-based disputes take months to resolve, soak up vast amounts of staff time, and create bad feelings for all.

The many challenges facing the telecom industry call for an innovative and comprehensive solution that reimagines the way identity management is conducted.

3. HOW TDIDN MEETS THESE CHALLENGES

A TDIDN can meet all these challenges by providing a modern and secure decentralized network. This transformative approach uses decentralized identifiers (DID) and blockchain technology to revolutionize identity management for the telecom sector.

Here are six use cases where the TDIDN approach can solve the challenges for the telecom industry outlined above.

3.1 Enhancing security with decentralized ID

As security threats grow, old-fashioned authentication methods like user names, passwords, and phone numbers are no longer enough. TDIDN introduces DIDs as a secure and decentralized identity solution.

A user can authenticate themselves by presenting their unique decentralized identity, eliminating the need to remember a list of login credentials. This is more convenient

and more secure. And using DIDs will significantly reduce the risk of identity theft and credential-based attacks.

3.2 Reducing overhead with smart contracts

Traditional telecom systems rely on many separate registries, which take tremendous time and effort to maintain. TDIDN introduces a distributed ledger or blockchain that can store the International Mobile Equipment Identity (IMEI) number for a device, along with the owner and the status of that device (either allowed or blocked).

This eliminates the need for each telecom to maintain its own unique registry, reducing overhead and boosting efficiency.

With TDIDN, any user such as a buyer, law enforcement agency, or insurance company can quickly confirm the ownership and verify the status of any device.

3.3 Protecting privacy

In the era of growing demands for data privacy, users want control over their personal information. TDIDN empowers users with selective disclosure. This means a user can share their phone number or identity with third parties for specific purposes, such as verifying their identity or signing up for new services.

But users no longer have to disclose their entire identity for every mundane transaction. This selective disclosure promotes privacy and minimizes the risk of unauthorized access to personal data.

3.4 Making billing more transparent

Telecom billing can be a frequent source of contention and customer dissatisfaction. TDIDN enables telecom operators to securely store Call Detail Records (CDRs) on a blockchain network using decentralized identifiers (DID).

Smart contracts automatically validate each CDR against the terms of the related Service Level Agreement (SLA). This ensures accurate and transparent billing, automated in a secure and cost-effective way. This reduces disputes and guarantees fair billing based on actual usage, building trust among service providers and customers.

3.5 Strengthening authentication

OTP authentication can be inconvenient and vulnerable to spam and phishing. TDIDN replaces OTP with DID, offering a more secure and user-friendly alternative.

Users can simply authenticate themselves by proving ownership of their DID. This streamlines the authentication process, enhances the user experience, and reduces the prevalence of spam phone calls and SMSs.

3.6 Managing SLAs with smart contracts

Using a Service Level Agreement (SLA) is a common practice in the telecom industry. But managing these agreements without reliable automation is anything but standardized.

A more contemporary approach is to use smart contracts, self-executing contracts with all terms and conditions expressed in code. TDIDN uses smart contracts to manage SLAs between providers and customers.

These SLAs are stored and executed on a decentralized network where both providers and customers can access them at any time. This ensures transparency, immutability, and automated enforcement.

Real-time monitoring of SLA compliance, automatic notifications of any breaches, and streamlined dispute resolution all become possible thanks to the cost-effective automation provided by TDIDN.

Together, all these use cases show the many ways in which the proposed TDIDN architecture can solve the pressing needs of the telecom industry.

4. TWO NEW COMPONENTS OF A TDIDN

The TDIDN architecture includes two components not everyone in the telecom industry may be familiar with: decentralized identifiers (DIDs) and smart contracts. This section provides more background on each component.

4.1 Decentralized Identifiers Specifications (DIDs)

The proposed approach for a decentralized identity management system is based on the concept of Decentralized Identifiers (DIDs).

DIDs are unique identifiers generated for each user in accordance with the W3C DID specification.[2] The W3C Credentials Community Group maintains and oversees these specifications, which define industry standards for the data model and syntax for decentralized identifiers.

DIDs are designed to be compatible with a wide range of distributed ledgers and networks. This ensures flexibility and interoperability within the decentralized identity ecosystem.

TDIDN delivers a comprehensive architecture for implementing DIDs on a blockchain, through two related projects from the Hyperledger Foundation:

- **Hyperledger Aries** provides a complete toolkit for building decentralized identity solutions. Aries can issue, store, and present verifiable credentials with maximum privacy, and establish confidential, ongoing communication channels for rich interactions. Aries is intended to be blockchain-agnostic, so that it can plug into any underlying blockchain infrastructure.[3]
- **Hyperledger Indy** supports digital identities rooted in blockchains that are interoperable across administrative domains, applications, and any other silo.[4]

TDIDN uses both of these open source frameworks. In simplified terms, you can think of Aries as the tools to build the client side of the system and Indy as the server side that supports the database.

In other words, Aries provides the agent side of the decentralized identity application that reads and writes to the underlying DID blockchain provided by Indy.

DIDs are characterized by a generic URL format, which serves to address DID documents and enable resolution through a DID resolver. This generic format adheres to the accepted principles of URI schemes as defined in the specification RFC3986.[5]

Every valid DID includes three required fields:

1. The urn scheme, which in this instance is *"did"*
2. The namespace or method name such as *"ethr," "sov,"* and others, depending on the chosen DID method
3. The method-specific identifier, which can be a combination of letters and numbers that uniquely identify the DID

The fields are separated by a colon (:). For example, a complete DID for the TDIDN system could be *"did:example:12345AbCDEfgh".*

4.2 Smart Contracts

Smart contracts have all with the terms of the agreement between buyer and seller directly written into code so they can run without human intervention.

Public ledgers, like Ethereum and other popular blockchain networks, provide a secure and transparent environment for deploying smart contracts. These blockchains ensure that the contract's code and execution history can be seen by all participants. This enhances trust and accountability between buyers and sellers.

And public ledgers offer a decentralized consensus mechanism to ensure that the execution of smart contracts is tamper-resistant and highly reliable.

The TDIDN architecture uses public ledgers for transparency and accessibility, while maintaining privacy through access restrictions via DIDs or Ethereum addresses.

5. TDIDN SYSTEM OVERVIEW

This section provides a high-level overview of the main parts of the TDIDN architecture. Figure 1 shows a simplified block diagram of the TDIDN system. Figure 2 shows a block diagram of a mobile customer and their smartphone.

5.1 TDIDN Network

As shown in Figure 1, the foundation of the network rests on three blockchains (also known as distributed ledgers). Each blockchain has a different purpose:

- Managing mobile device IMEI numbers
- Recording Call Detail Records (CDRs) for billing
- Tracking DIDs with Hyperledger Indy

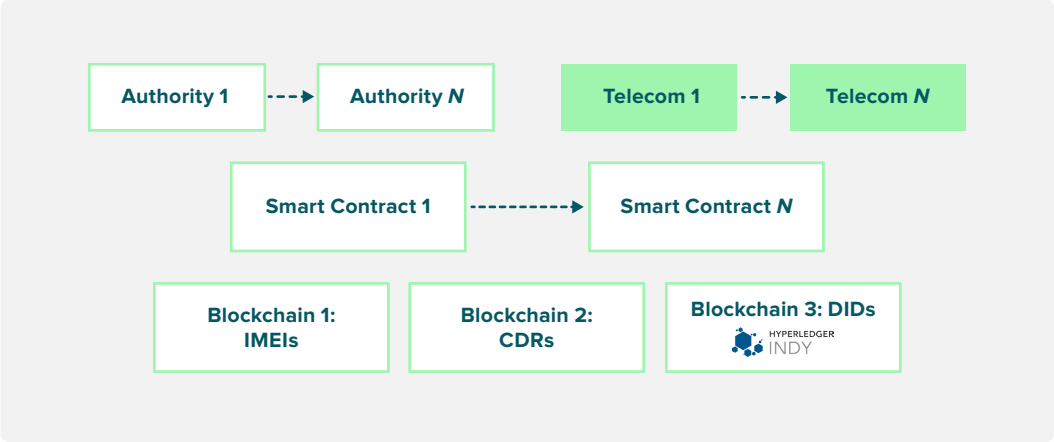


FIGURE 1: TDIDN BLOCK DIAGRAM

In the reference instance of TDIDN, both the blockchains for IMEIs and CDRs use the sepolia testnet. Sepolia is an Ethereum testnet that provides a stable infrastructure for developers to deploy and test smart contracts, without spending any ether.

The DID blockchain uses Hyperledger Indy, an open source project from the Linux Foundation that provides a public and permissioned blockchain ideally suited for identity management.

All three blockchains in this instance of TDIDN are available free of charge.

These blockchains provide a decentralized way to update these three ledgers. That means each telecom operator can save the time and effort they once spent maintaining their own siloed databases.

When required, any valid authority can write data to a blockchain. The network can support an unlimited number (N) of authorities, as long as each one is validated. An authority can be any telecom operator or third party trusted by all the other members of the network.

5.2 Telecom Operators

As shown in purple in Figure 1, telecom operators are key users of the network. The network can support an unlimited number (N) of telecom companies.

The business arrangements between one telecom and another are governed by smart contracts, which spell out details such as SLAs and inter-carrier billings. Each smart contract can access and update blockchain data as required. And the network can support an unlimited number (N) of smart contracts.

As described earlier, the blockchains spare telecom operators the major expense of maintaining their own databases for IMEIs and CDRs. And the smart contracts usher in a new era of intelligent automation.

Together, these two innovations enable telecoms to manage devices in a more secure and cost-effective way than ever before.

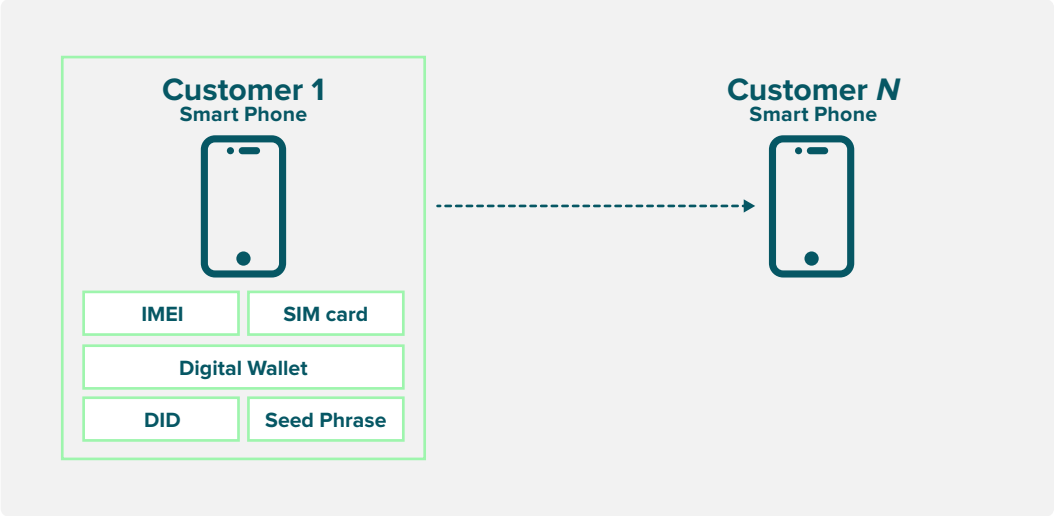


FIGURE 2: MOBILE CUSTOMER BLOCK DIAGRAM

5.3 Mobile Customers

As shown in Figure 2, each customer with a mobile device receives a unique IMEI number and SIM card for that device from their telecom service provider.

This is similar to current practices; the only difference is these items are now managed by two decentralized blockchains that can be viewed by any member of the network.

Each customer also has a digital wallet, which contains a unique DID and a unique seed phrase. Their DID can be used to validate their phone number and device status, while the seed phrase can be used to update the status of their device if it is ever lost, given away, or stolen.

The network can support an unlimited number (N) of mobile customers.

6. KEY FUNCTIONS OF THE TDIDN ARCHITECTURE

Figure 3 shows the process flow for many functions of the network. This section describes four key functions of the TDIDN architecture:

- A user getting ready to access the system
- Managing IMEI numbers
- Managing SIM cards
- Handling CDRs

As you can see, the TDIDN approach tremendously streamlines the allocation, verification, and management of IMEIs and SIMs for telecom operators.

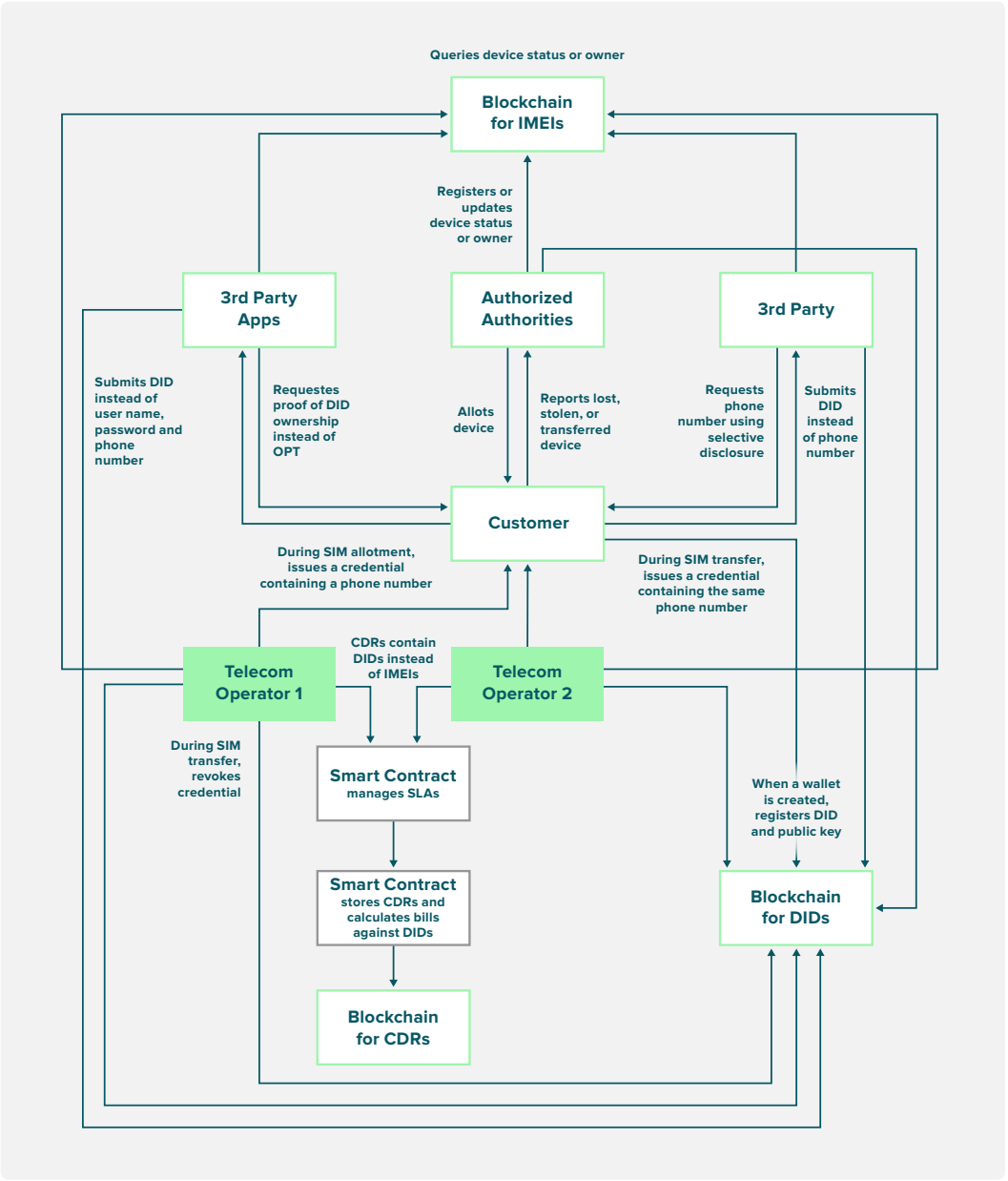


FIGURE 3: TDIDN PROCESS FLOW

6.1 Getting Ready

Before a user can access a TDIDN, they must do three basic tasks, as follows.

USER DOWNLOADS THE WALLET APP

The user must download and install the recommended digital wallet app on their device.

USER CREATES AN ACCOUNT

The user must create an account in the wallet app. This includes providing some personal information to validate the user's identity and location.

USER SECURELY STORES THE SEED PHRASE

After their new account is created, the user will be provided with a seed phrase. The user must securely store this seed phrase They will need it to generate cryptographic keys and maintain control over their DID.

6.2 Managing IMEI numbers

As you know, an IMEI is a unique 15-digit serial number assigned to every mobile phone in the world. The TDIDN can allocate a new IMEI, map it to a user's DID, and change a device's status on request, either allowed or blocked.

USER REQUESTS AN IMEI NUMBER

The user starts the process by supplying their DID and requesting an IMEI number from an authority.

AUTHORITY MAPS AN IMEI TO A DID

The authorized authority generates a random IMEI number and maps it to the user's DID. This mapping is published to an IMEI distributed ledger (blockchain), including the device status, in other words, whether the assigned IMEI is allowed or blocked.

USER REQUESTS A CHANGE OF STATUS

If a user's mobile phone is lost, given away, or stolen, that user usually doesn't want to pay for any further network access for that device. In this case, a user can request an authority to change the status of a certain IMEI number (either allowed or blocked). The user must prove they own the DID associated with that IMEI by opening the wallet app on another device using their seed phrase.

AUTHORITY UPDATES THE STATUS OF AN IMEI

The authority verifies the user request and their DID ownership. If the request is properly verified, the authority updates the IMEI number's status in the IMEI blockchain, marking it either blocked or allowed.

6.3 Managing SIM Cards

As you know, a SIM card is a tiny smart card that links a mobile device to a specific telecom service provider. The TDIDN can allocate a new SIM card, update or renew a SIM card, and support the verification of a user's phone number by a third party.

USER REQUESTS A SIM CARD

The user starts the process by requesting a SIM card from a telecom authority, supplying their DID and an authorized government ID credential.

AUTHORITY VALIDATES CREDENTIALS AND ISSUES A SIM

The telecom authority checks the validity of the government ID credential stored in the user's digital wallet.

If the credential is properly verified, the telecom authority issues a SIM card and generates a new digital credential for the user. This credential contains information such as the phone number, operator name, and other details.

AUTHORITY RENEWS OR UPDATES A SIM

The telecom authority can also use the TDIDN system to renew or update a SIM, ensuring that the user's identity remains verified and secure.

For example, if a user sells a phone to someone else, or trades it in, the telecom authority can revoke the original owner's credential and issue a new credential for the new owner linked to the same device IMEI.

If a user loses a phone or has it stolen, the authority can change the status of that device to mark it blocked.

USER PROVES THEIR PHONE NUMBER

From time to time, a user may need to prove that they own their phone number to a third party—such as a bank, government agency, or service provider—or to a third-party app from a service provider. In this case, the user can present their digital credential.

The third party or app can verify the authenticity of the credential without needing to know the actual phone number. This selective disclosure safeguards the user's privacy and enhances the security of the transaction.

6.4 Handling CDRs

As you know, a Call Detail Record is created for every phone call made by any mobile device. A CDR captures all the relevant data for each call, including time of call, length of call, source name and number, destination name and number, and further quality and diagnostic data such as completion status for the call and reason for terninating the call.

Today, each CDR is recorded in a database and managed by the telecom operator where the call originated. The CDR is then used to settle any related costs between the original operator and any other operators involved, according to the SLAs in place between those operators.

Different operators have different levels of automation and sophistication in handling CDRs and resolving any discrepancies or disputes. Yet every operator devotes significant resources to maintaining a CDR database, calculating bills, and resolving disputes with other operators.

The TDIDN can handle CDRs in a more transparent and precise way that reduces disputes. The TDIDN can record a CDR, manage SLAs between operators, and calculate bills from CDRs.

RECORDING A CDR

When a customer makes a phone call, a CDR is created by the local operator. The call is identified by DID rather than IMEI. Each CDR is recorded on an immutable blockchain where any valid authority can view that record, but no one can alter it. This makes CDRs more precise and far more transparent.

MANAGING SLAS

When an operator agrees to an SLA with another operator, all the terms and conditions are coded into a smart contract that can access the CDR ledger. To view an SLA, an operator can view the related smart contract with the related operator. To renegotiate an SLA, the related operators can renegotiate their agreement and then update the related smart contract.

CALCULATING BILLS

All the terms and conditions of the customer contract are also coded into a smart contract.

To create a bill for a customer, the smart contract uses the DID to find all the related CDRs and then calculates the bill for each call according to the related terms and conditions. Next it assembles all the information required to bill the customer, and exports that data to the operator's billing system.

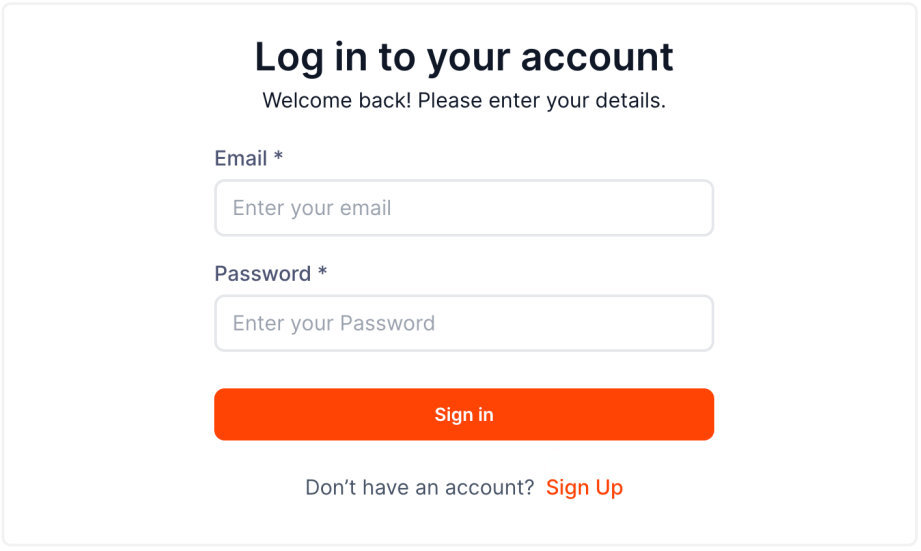
To calculate a bill for another operator, the smart contract finds all the related CDRs and then calculates the amount owing according to the related terms and conditions. The smart contracts for the related operators can be set up to automatically pay bills as required, with each transaction recorded on the blockchain.

7. PROPOSED USER INTERFACE

This section documents the user interface for a reference instance of the TDIDN that currently exists. The code is available as open source through the Hyperledger Telecom SIG. This system uses the MetaMask web wallet, but it can support any other digital wallet that can sign and send transactions over the Ethereum network.

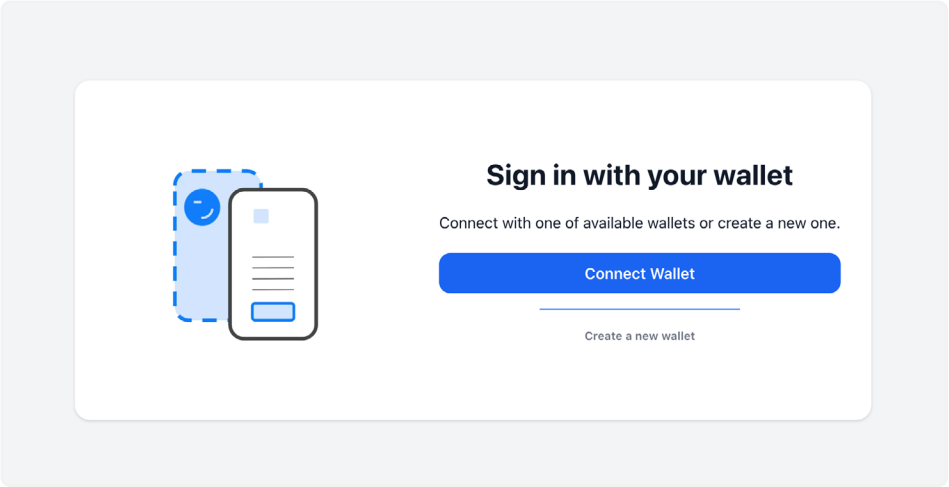
7.1 Creating a Wallet Account

A user can register and create a web wallet. This web wallet allows them to securely store and verify their credentials, as well as manage their DIDs.



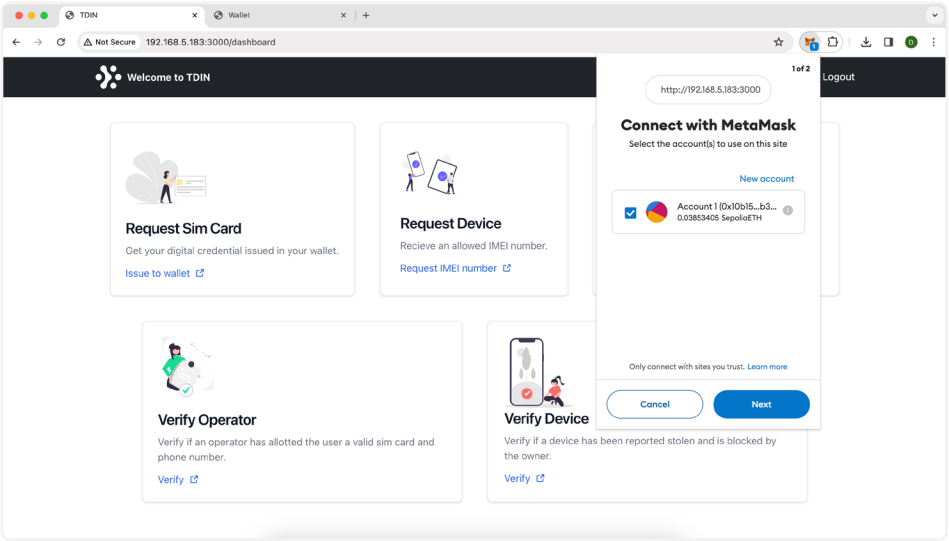
7.2 Logging into apps

Upon login, a user can use their DID instead of their user name and password for authentication to the TDIDN.



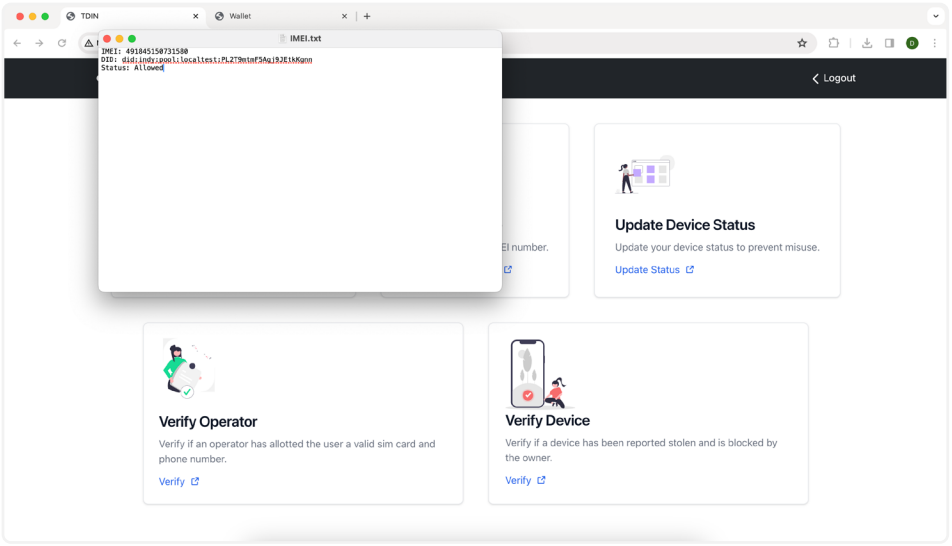
7.3 Connecting the wallet to enable transactions

When logged into the TDIDN service, a user is prompted to connect their Metamask wallet to enable transactions on the Ethereum testnet blockchain, specifically the Sophia network.



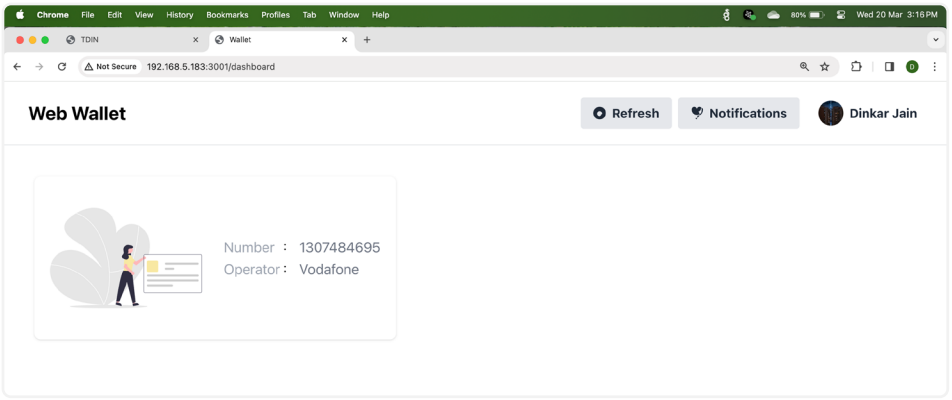
7.4 Requesting an IMEI Number

A user can generate an IMEI number by clicking the “Request IMEI Number” button. This generated IMEI number is associated with that user and stored on the IMEI blockchain.



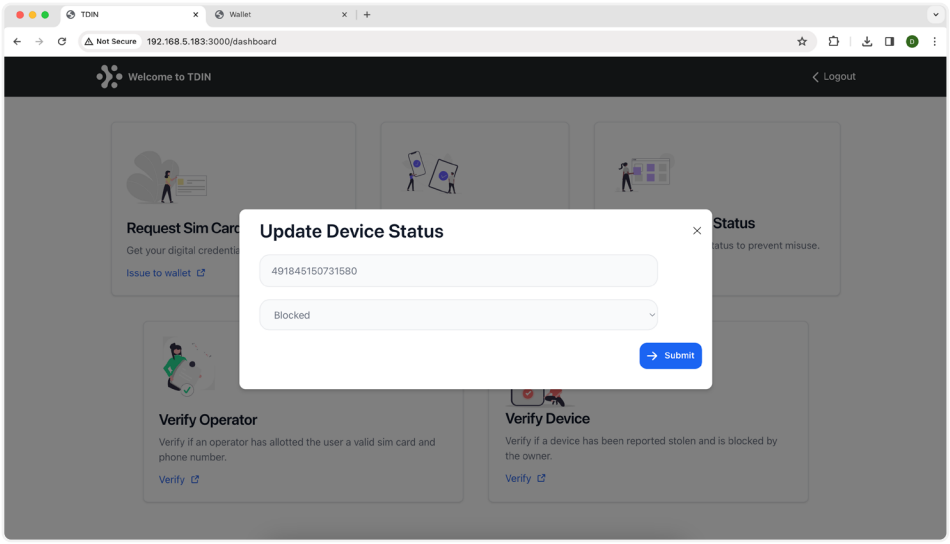
7.5 Requesting a SIM Card

A user can request a SIM card and receive a verifiable credential in their wallet by clicking the “Issue to Wallet” button.



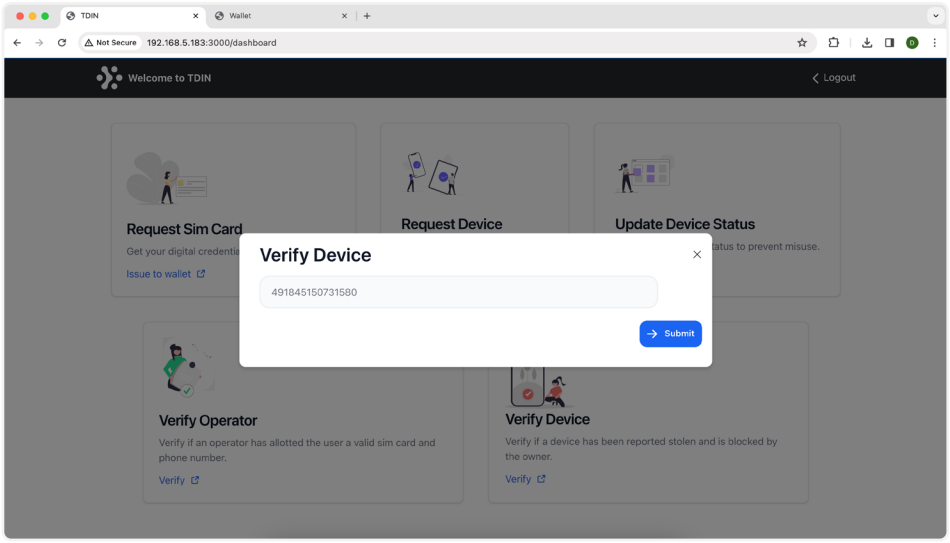
7.6 Updating the Status of a Device

If a user's device is lost or stolen, the user can change the status of a device on the ledger, through the "Update Device Status" feature.



7.7 Verifying the Status of a Device by a Third Party

A third party can verify the status of a mobile device by using the "Verify Device" feature to view the IMEI numbers on the IMEI blockchain. A third party can also validate the verifiable credential with the "Verify Operator" feature.



8. CONCLUSIONS

This solution brief introduced the TDIDN architecture as a significant step forward for identity management by telecom operators. TDIDN uses decentralized identifiers (DID) and blockchain technology to streamline identity management.

This innovative approach improves management of essential items such as IMEI numbers, SIM cards, and CDRs. Making a paradigm shift from a siloed and centralized approach to a shared and decentralized philosophy will provide many concrete benefits to telecom operators: more robust security, lower costs, enhanced privacy, and fewer disputes with their partners and customers.

ACKNOWLEDGEMENTS

The Hyperledger Telecom Special Interest Group would like to thank the following people who contributed to this solution brief: David Boswell, Dinkar Jain, and Vipin Rathi.

HOW TO GET INVOLVED

The Hyperledger Telecom Special Interest Group is focused on technical and business-level conversations about appropriate use cases for blockchain technology in the telecom industry. The SIG is open to anyone in the world.

To find out more or to join the SIG, visit **wiki.hyperledger.org/TCSIG**

To download the repo and documentation for the TDIDN reference application, visit **https://github.com/hyperledger-labs/TDIDN**

SOURCES

1 C. David Hylender, Philippe Langlois, Alex Pinto, and Suzanne Widup, "Verizon 2023 Data Breach Investigation Report," May 2023, page 8. **https://www.verizon.com/business/resources/reports/dbir/**

2 "Decentralized Identifiers (DIDs) v1.0," 19 July 2022, World Wide Web Consortium (W3C). **https://www.w3.org/TR/did-core/**

3 Hyperledger Aries, Hyperledger Foundation. **https://www.hyperledger.org/projects/aries**

4 Hyperledger Indy, Hyperledger Foundation. **https://wiki.hyperledger.org/display/indy/Hyperledger+Indy**

5 Tim Berners-Lee et al, "Uniform Resource Identifier (URI): Generic Syntax," The Internet Society, 2005. **https://datatracker.ietf.org/doc/html/rfc3986**