Performance-Security Analysis in O2O Interactions in Future 6G Communications

EMANUELE BELLINI, Università di Roma Tre, Roma, Italy
ERNESTO DAMIANI, Center for Secure Cyber Physical Systems, Khalifa University, Abu Dhabi, United Arab Emirates and Dipartimento di Informatica Giovanni Degli Antoni, Università di Milano, Milano, Italy
MICHELE DI GIOVANNI and STEFANO MARRONE, Department of Mathematics and Physics, University of Campania Luigi Vanvitelli, Caserta, Italy

In traditional mobile networks, trust between subscribers and their serving networks relies on a hardware root of trust: the Subscriber Identity Module (SIM). Conversely, trust between service and home networks is established via Trusted Third Parties (TTPs), known as Clearing Houses (CHs). The 6G environment will witness a substantial increase in subscriber numbers, driven by the mass deployment of the Internet of Everything (IoE) and improvements in network performance. Simultaneously, the performance capabilities required of TTPs to manage trustworthy operator-to-operator (O2O) interactions in 6G must align with the demands of the 6G ecosystem. This work focuses on enhancing CH intermediation capabilities to support O2O trustworthy interactions within the 6G context. Given the close connection between performance and trustworthiness, this paper explores these aspects by modeling interactions between communication parties using a Petri Net model. This model is applied to analyze the quantitative relationships among the non-functional requirements of future 6G communication scenarios, considering both traditional and blockchain-based approaches.

CCS Concepts: • **Security and privacy** → *Distributed systems security*; • **Computer systems organization** → *Dependable and fault-tolerant systems and networks*; • **Networks** → *Network security*;

Additional Key Words and Phrases: Generalized Stochastic Petri Nets, Permissioned Blockchain, 6G Ecosystem, Clearing House, Roaming, Fraud Detection

ACM Reference format:
Emanuele Bellini, Ernesto Damiani, Michele Di Giovanni, and Stefano Marrone. 2026. Performance-Security Analysis in O2O Interactions in Future 6G Communications. *Distrib. Ledger Technol.* 5, 3, Article 35 (May 2026), 28 pages.
https://doi.org/10.1145/3716176

Emanuele Bellini, Ernesto Damiani, Michele Di Giovanni, and Stefano Marrone contributed equally to this research.
This publication has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936 (ELECTRON).
Authors' Contact Information: Emanuele Bellini, Università di Roma Tre, Roma, Italy; e-mail: EMANUELE.BELLINI@uniroma3.it; Ernesto Damiani, Center for Secure Cyber Physical Systems, Khalifa University, Abu Dhabi, United Arab Emirates and Dipartimento di Informatica Giovanni Degli Antoni, Università di Milano, Milano, Italy; e-mail: ernesto.damiani@unimi.it; Michele Di Giovanni, Department of Mathematics and Physics, University of Campania Luigi Vanvitelli, Caserta, Italy; e-mail: michele.digiovanni@unicampania.it; Stefano Marrone (corresponding author), Department of Mathematics and Physics, University of Campania Luigi Vanvitelli, Caserta, Italy; e-mail: stefano.marrone@unicampania.it.

ACM 2769-6480/2026/5-ART35
https://doi.org/10.1145/3716176

Table of Acronyms

Abbreviation	Description
4G	fourth generation
5G	fifth generation
6G	sixth generation
B2B	Business to Business
BC	Blockchain
CDR	Call Detail Record
CH	Clearing House
CPN	Colored Petri Net
CSP	Communication Service Provider
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
EOV	Execute-Order-Validate
eSIM	electronic SIM
FTP	File Transfer Protocol
GSPN	Generalized Stochastic Petri Net
HF	Hyperledger Fabric
HPMN	Home Public Mobile Network
HSM	Hardware Security Module
IMSI	International Mobile Subscriber Identity
IoE	Internet of Everything
IoT	Internet of Things
MNO	Mobile Network Operators
MOU	Minutes Of Use
MSP	Membership Services Provider
MVNO	Mobile Virtual Network Operator
NRTRDE	Near Real Time Roaming Data Exchange
O2O	Operator-to-Operator
PBCH	Permissionless Based Clearing House
PN	Petri Net
PoS	Proof-of-Stake
PoW	Proof-of-Work
RG	Reachability Graph
RoT	Root of Trust
SC	Smart Contract
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TAP	Transfer Account Procedure
TAP3	Transferred Account Procedure vers. 3
TTP	Trusted Third Party
TPS	Transactions per Second
UICC	Universal Integrated Circuit Card
UML-SD	Unified Modeling Language - Sequence Diagram
VPMN	Visited Public Mobile Network

1 Introduction

The rollout of **Fifth Generation (5G)** is ongoing, and the telecommunications industry is already turning its attention towards the development of the **Sixth Generation (6G)** mobile network. About 6G is expected to build upon the advancements of 5G in terms of latency and throughput, but meeting this performance challenge will become more demanding due to the expanding number of users.

In fact, the expectation is to move from about 2 billion mobile subscriptions worldwide in 2024 [Jonsson et al., 2019] to 100 billion scale in 6G [Ylianttila et al., 2020]. This is the **Internet of Everything (IoE)** scenario [Bellini et al., 2017], a further evolution of the **Internet of Things (IoT)** concept; in fact, while the term "Things" is related to connecting physical-first objects, IoE supported by 6G extends this perspective to include five elements:

—People: continuously connected mobile devices, enhanced by wearable technology;
—Things: devices such as sensors, actuators, and edge components that generate or consume information;
—Systems: encompassing industrial robots, autonomous systems, and related technologies;
—Data Intelligence: computational nodes that facilitate real-time intelligent decision-making;
—Processes: utilizing the interconnectedness of people, data, and devices.

Thus, IoE will push the performance of 5G systems to its boundaries in 10 years, as predicted by [Tariq et al., 2020]. Performance is just a starting point due to the future promise of a convergence of all mobile and fixed-mobile networks that the emergence of such IoE services and applications will require [Bariah et al., 2020]. About 6G networks are expected to realise such a convergence [Zhang et al., 2019].

Various speculative studies conducted by both researchers and industry experts aim to pinpoint the anticipated characteristics of 6G networks [Bariah et al., 2020; Saad et al., 2020; Zhang et al., 2019]. Key features under discussion include: (a) ultra-high data transfer speeds exceeding 1 Tb/s, (b) latency reduced to under 1 millisecond, (c) coverage ranges spanning hundreds to a few kilometers, (d) the ability to support user mobility at speeds of up to 1,000 km/h, and (e) advanced network features such as softwarization, virtualization, and cloudification. These advancements are projected to foster innovative business opportunities and attract new stakeholders into the industry [Yrjola, 2019], with one example being micro-operators delivering high-quality wireless services in specific localized areas [Petri et al., 2018].

Ensuring trustworthiness in the **Operator-to-Operator (O2O)** context is of a paramount importance, especially regarding roaming settlements and billing. One of the biggest sources of revenue erosion for telecommunication operators is fraudulent traffic. At an international/roaming level, **Subscriber Identity Module (SIM)** frauds involve attackers stealing or cloning a SIM in a country whose subscription plan only entitles to services on the home network and using it in another country.

Ensuring minimal delay and strong reliability when submitting Call Detail Records created from stolen SIMs is crucial for preventing legal disputes within the O2O context. Typically, O2O interactions are facilitated through Trusted Third Parties, which serve as intermediaries for O2O data **Clearing Houses (CHs)**. Whenever a user initiates a mobile call in a roaming area, the **Visited Public Mobile Network (VPMN)** requests information about the services subscribed by the mobile user from the **Home Public Mobile Network (HPMN)**. To accomplish this, CDRs are dispatched to the HPMN through a **Transfer Account Procedure (TAP)** file. Upon receiving the TAP files, the HPMN must determine charges to be billed to the VPMN in accordance with the established roaming agreement tariffs.

This system is responsible for processing these TAP files and generating invoices for its subscribers. Its primary function within the business ecosystem is to establish trustworthiness in the O2O realm by transmitting and converting (if the operator has delegated the CH for this service) the TAP files on behalf of the Communication Service Provider.

Delays in O2O communication can extend up to 36 hours. However, implementing **Near Real Time Roaming Data Exchange (NRTRDE)**[1] can shorten the timeframe for O2O interactions to just 4 hours. It is evident that these times are not acceptable for 6G: fraud in connection with billing might be detected only after 14,400 Tb (4h at 1Tb/s) of exchanged data.

To reduce the roaming fraud risk, it is necessary to find a solution that allows the VPMN to create and exchange NRTRDE files with the HPMN in real time without affecting the existing billing and mediation system of the VPMN.

A potential approach for enabling a real-time exchange of NRTRDE files within existing billing frameworks involves a gateway-based mechanism. This solution intercepts traffic at the first gateway linked to the VPMN as soon as a device initiates a call[2]. While primarily designed for fraud detection, it does not address billing or compensation processes arising from business O2O agreements. Additionally, secure communication channels between gateways are essential to mitigate potential attacks. The challenge of establishing a high-performance, reliable, and fully trustworthy mechanism for O2O interactions in roaming scenarios remains largely unresolved. A common issue in O2O disputes stems from the absence of a shared and trusted data baseline. With each party maintaining centralized, siloed records, there is a prevailing lack of mutual trust in data integrity [Shyam Prabhu et al., 2019].

This paper introduces an innovative and cost-efficient approach to building O2O trust relationships for roaming services within the 6G business ecosystem. The solution leverages a transaction-oriented permissioned **Blockchain (BC)**, **Hyperledger Fabric (HF)**, to achieve trust by consensus among 6G mobile operators. The paper defines a new transaction validation schema and models it by means of formal modelling, with the objective of exploring the possible tradeoffs between performances and security. The proposed schema, as well as the traditional one, are then modelled by Petri Nets and analyzed in order to understand the tradeoffs between performance, scalability and costs.

This paper constitutes an extension of the work published in [Bellini et al., 2023]; the extension consists in the formalization of the proposal and the definition and the analysis of the PN models.

The paper is organised as follows: traditional trust models are reviewed in Section 2; Section 3 presents a model for 6G O2O trust via BC-based consensus. Three sections deepen the fraud scenario considered in this paper by specifying (Section 4), modelling (Section 5) and analyzing the built models (Section 6). Section 7 is devoted to the discussion of the proposed contribution, while Section 8 ends the paper with the conclusions.

2 Background

The simple trust model used in mobile networks up to **Fourth Generation (4G)** involved three main actors: the *user/subscriber* using a *smart terminal* device, the *home operator*, and the *serving operator*.

Trust relations between the subscriber and the serving operator, as well as between the serving and home operators are traditionally grounded via a ***Root of Trust (RoT)***, a trustworthy source of cryptography keys used for both data encryption/decryption and for digital signature generation/verification. RoT schemes usually include ***Hardware Security Modules (HSMs)***, which hold keys and perform cryptography functions within a secure environment. A SIM is a case of HSM used to ensure trust between subscribers and serving operators.

A novel version of SIMs will be playing a key role in setting up subscriber-to-operator trust relations in 5G and 6G.

The 5G SIM—also called **Universal Integrated Circuit Card (UICC)**—and specified by the standardization body ETSI-3GPP in Release 15 UICC specification [*TS 131 121* 2019] can be fully software-implemented (i.e., the electronic SIMs) and address several issues of previous generations' SIMs, including full anonymization of subscriber identity from mobile equipment to the core network. This standard allows the load of a local network

[1] http://www.edch.com/nrtrde/

[2] https://patents.google.com/patent/US20080293409

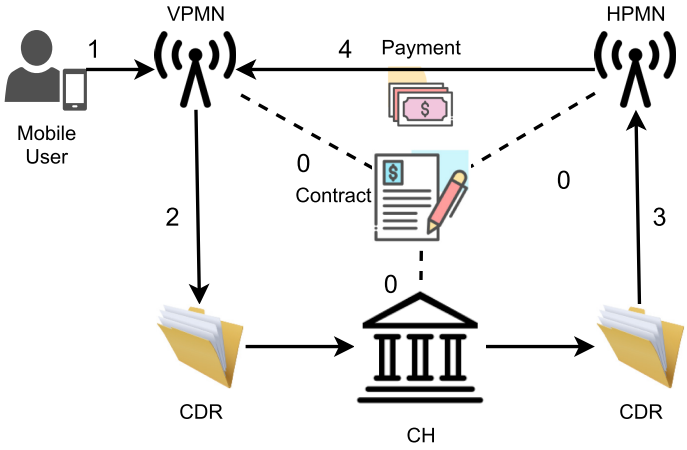

Fig. 1. Common trust solution schema based on CH intermediation.

International Mobile Subscriber Identity (IMSI) onto the device, bypassing roaming charges since the device is always local.

In O2O interaction instead, trust is established on software credentials released by TTPs, which generate and assign credentials to be used as roots-of-trust.

As a pre-requisite of this interaction scenario, VPMN and HPMN agree on a traffic transaction scheme, formalize it into a Contract and inform the CH of it. When the Mobile User starts a roaming call in the area of the VPMN, this operator prepares and sends a CDR to the CH, which checks the contract and sends payment information and related CDR to the HPMN. After receiving the data contained in the CDR, the HPMN checks the eventual fraud contained in the records or exectues the payment to the VPMN.

The problem is now to establish inter-operator trust relations in an effective and efficient manner. This "trust scalability" problem raises from the economical pressure to let new mobile operators entering into a bigger and bigger market.

In fact, 6G will dramatically increase the types and number of ***Mobile Virtual Network Operators (MVNOs)*** entities within the ecosystem. The latest data available, collected at the end of the year 2022, counted 1,986 active MVNOs, more than double the amount of traditional network operators. MVNOs, who account for more than 20% of the total mobile users, do not have their own infrastructure or an assigned frequency range. Their core business is based on reselling data and voice services to final customers purchasing **Minutes Of Use (MOU)** from physical **Mobile Network Operators (MNOs)** and reselling them customers. This traditional flow of interactions and messages the parties exchange with each other are depicted in Figure 1.

This trend is increasing the complexity (and introducing new vulnerabilities) of the 6G ecosystem and new requirements to establish O2O trustworthy interaction are emerging.

To address these issues, the following high-level requirements in the 6G scenario have been elicited in collaboration with UAE Telecommunications and Digital Government Regulatory Authority [5gw [n. d.]] toward establishing trustworthy O2O relationships:

— *Privacy*: The operational data of operators is sensitive and must be protected without compromising O2O business relationships. For instance, CDR data, NRTRDE, and billing agreements should not be shared with entities outside the O2O partnership.
— *High Performance*: The execution mechanisms of **Smart Contract (SC)** must ensure extremely low latency to prevent fraud by detecting it promptly, while also handling a high volume of **Transactions per**

Second (TPS). This is particularly crucial given the anticipated growth of network terminals in the 6G era. As such, NRTRDE data from the VPMN to the HPMN must be processed immediately upon collection.
— *Scalability*: The growing number of 6G operators entering the market will likely require TTPs to handle thousands of O2O business relationships efficiently.
— *Trusted Computing*: Trusted O2O interactions demand techniques for formally translating O2O service compensation contracts into computable processes and verifying their adherence to offline business agreements.
— *Identification*: Operators intending to engage in transactions with others must be authenticated and authorized.
— *Security*: CDRs for services provided by MVNOs to roaming users should be promptly exchanged with the home MOUs (or other MVNOs). Additionally, mechanisms for early fraud detection should be implemented and supported.
— *Auditability*: Every compensation computation (compensation transaction) must be verifiable by all parties involved in the corresponding business relationship.

Such requirements should be addressed by all 6G ecosystem actors. In this paper, we propose the adoption of BC technology to address these requirements identified effectively. In the next section, we discuss the role of BC in the 6G ecosystem and provide the motivation behind our solution.

3 BC-Based 6G Inter-Operator Trustworthy Business Interaction

3.1 BC in Telecommunications

The National Institute of Standards and Technology [Yaga et al., 2019] highlights BC technology as a distributed digital ledger that provides tamper-evident and tamper-resistant recording of transactions, emphasizing its potential to enhance trust, transparency, and data integrity in decentralized environments without requiring a central authority. BC technology has emerged as a transformative tool for addressing complex challenges in the telecommunications industry, which is increasingly characterized by its diverse stakeholders, heightened security concerns, and demand for operational efficiency. BC provides an innovative solution to the evolving trust requirements in telecommunications. Afraz et al. [Afraz et al., 2023] emphasize that, as the ecosystem transitions from single-operator systems to heterogeneous environments, traditional centralized trust mechanisms face limitations in scalability and resilience. The BC's decentralized architecture ensures secure and immutable record-keeping. The authors demonstrate the viability of BC through two critical use cases: 5G slice brokering and federated learning. These cases illustrate how private and consortium BC achieve lower latencies and higher transaction throughput compared to public alternatives, making them well-suited for telecom applications. The scalability of BC networks is a significant consideration for telecom operators. Afraz et al. highlight consortium BC like HF, which can process up to 20,000 TPS with sub-second latency. This performance far surpasses that of public BC such as Bitcoin or Ethereum, which are limited by energy-intensive consensus protocols like **Proof-of-Work (PoW)**. The authors underscore the suitability of consortium BCs in addressing the demands of 5G and beyond, where low latency and high throughput are critical. While BC offers significant advantages, Afraz et al. caution that its deployment entails substantial costs in terms of computational resources, storage, and energy consumption. They propose that cloud-native deployment models such as Blockchain-as-a-Service may offer a cost-effective alternative, albeit with potential tradeoffs in decentralization. Despite its potential, BC adoption in telecommunications remains in its infancy, as noted by Chellvamathi and Kulkarni [RS and Kulkarni, 2023]. They argue that while BC can address critical issues such as fraud, inefficiencies, and high operational costs, the technology's immaturity poses challenges in scalability, interoperability, and integration with legacy systems. The authors emphasize the need for industry-specific BC solutions tailored to telecom requirements, suggesting that strategic evaluation of use cases and further research into standards and policies are essential for widespread adoption. BC applications in telecom span diverse domains, including identity management, roaming and settlements, **Service Level Agreement (SLA)** automation, and IoT connectivity. For

instance, Chellvamathi and Kulkarni identify BC-enabled identity management as a key use case, offering secure, decentralized authentication mechanisms that reduce reliance on centralized databases and improve customer privacy. Similarly, SCs can streamline SLA enforcement, enabling automated compensation mechanisms and reducing disputes between operators.

3.2 BC-Based Trust

As said, MVNOs need to trust each other on the provenance and content of information about subscribers' access to services (e.g., the size of exchanged data, duration, and location, typically contained in CDRs)).

In general terms, we can consider this problem as a variation of the distributed agreement problem over a network, with limited trust conditions (i.e., the classic "Byzantine General's Problem" [Lamport et al., 1982]).

A *solving consensus* algorithm is a method used to reach an agreement on a statement (e.g., data value) in a multi-actor decentralized system. Any consensus algorithm has to satisfy two critical properties to ensure that an agreement is reached among actors/nodes: *safety* and *liveness*. The safety property is implemented when is guaranteed to each node of the system the same input information which must produce the same output in every node. The algorithm must have the same behavior in each node of the system that executes the transaction atomically. The liveness property is related to the fact that each non-faulty node must receive every submitted transaction. Byzantine agreement is a classic consensus mechanism for implementing atomic broadcast, guaranteeing a total ordering of all delivered messages. **Distributed Ledger Technologies (DLTs)** are natural candidates for addressing such requirements [Cachin, 2001], implementing a tamper-proof distributed ledger where not only data but also control are fully decentralized among all participants. In this scenario, every arbitrary change in the ledger is prevented unless an actor has obtained enough capacity (number of nodes) to get control of the system (33% of nodes in Practical Byzantine Fault-tolerant [Kotla et al., 2010], 50% in RAFT [Xu et al., 2020], PoW or **Proof-of-Stake (PoS)** [Nakamoto, 2008]).

The role of BC in 6G has been explored by [Hewa et al., 2020]; it is based on five pillars: [Nabil and Claus, 2018]:

- —Transactions: the nodes of the network create these pieces of information, sign them, and broadcast them to the rest of the participating nodes; then transactions are hashed and coded into a Merkle tree [Merkle, 1980]. The blocks are groups of transactions that are added to the BC after being validated;
- —Public-key Cryptography: it is used to join the blocks sequentially, making BC resistant to data alteration intentionally. Once written, data in any given block cannot be modified retroactively [Eyal et al., 2016];
- —Distributed Ledger: every node participating in the system must have the same dataset present in the ledger;
- —Consensus Mechanism: it is applied to select which blocks should be appended to the BC, following *longest chain wins* principle [Nakamoto, 2008];
- —SC: a deterministic program that comprises an executable script and a data model. It implements Read-Modify-Write operations on BC.

The rationale for using BCs to establish trustworthy O2O interaction is its capacity to dis-intermediate the interaction between Home and Service Networks [Deloitte, 2016]. BC can entirely replace TTPs while guaranteeing the required level of trust.

Figure 2 shows this solution.

In the above schema, when the subscriber generates an event when roaming to a service network, she can solicit the application of an SC corresponding to the existing business agreement between the VPMN and the HPMN. At the end of each event, the VPMN sends a batch of CDRs and billing information to the HPMN. By interacting with the BC, the HPMN verifies the request's conformance and recognizes the payment to the VPMN.

However, there are several BC implementations available with different characteristics in terms of scope, performance, privacy, consensus mechanism, costs, and so forth. Not all of them are suitable for the 6G roaming business case.

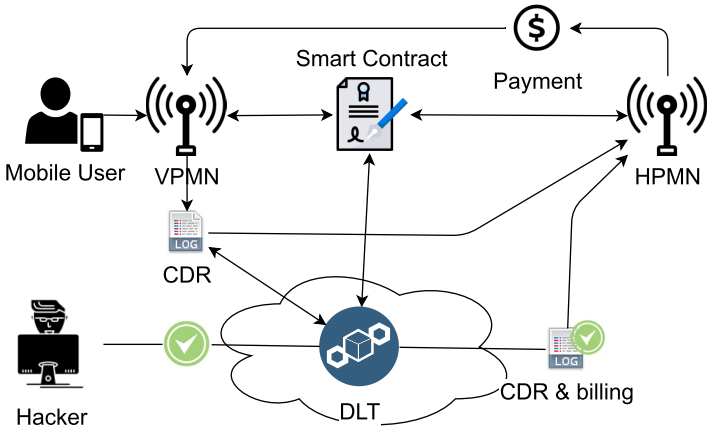

Fig. 2. The DLT-based solution schema.

Permissionless BCs face significant challenges in meeting the demands of the O2O scenario, particularly regarding the confidentiality of business-to-business billing agreements, transaction data privacy, and the enforcement of access control mechanisms. Specifically, the participants in a transaction are not fully anonymized, as all exchanged information is visible to every member of the network. While this transparency aligns with the goals of cryptocurrencies like Bitcoin, it poses a critical drawback for business-to-business interactions, where maintaining the confidentiality of agreements is fundamental to preserving competitive advantages.

Another major limitation lies in the PoW consensus mechanism commonly used in permissionless BCs. This approach relies on a randomized process where participants compete to solve complex cryptographic puzzles [Walport, 2015]. However, the PoW protocol demands substantial energy resources [Deetman, 2016] and introduces significant latency in achieving consensus. These characteristics are incompatible with the stringent requirements of 6G networks, which necessitate near real-time O2O CDR exchanges to mitigate revenue loss and detect fraud effectively.

In BC systems, reaching a consensus on the state of the ledger typically requires approximately 10 minutes [Antonopoulos, 2017]. Alternative mechanisms, such as PoS, Delegated Proof of Stake, and Proof of Space, are still in their early stages of development.

Even if a permissionless ledger could satisfy all fundamental requirements, certain critical limitations would persist. For instance, implementing SCs to govern business relationships between operators relies on an existing "off-line" trust among the parties—something that public BCs are inherently not designed to establish.

How could an MVNO/MNO place trust in a SC developed by a counterpart? In scenarios involving the exploitation of SC vulnerabilities (e.g., the Decentralized Autonomous Organization attack [Herlihy, 2019]), identifying the malicious actor and assigning responsibility for the damage would be highly challenging.

To address this, a mapping between the trust requirements of our O2O scenario and the BCs features outlined in [Bellini et al., 2020] is presented in Table 1, aiding in the selection of the most suitable solution and configuration.

According to the mapping, the adoption of a permissioned BC seems the best option to address the O2O issues.

3.3 The Permissioned BC-Based Enhanced Intermediation for TTP/CH

A permissioned BC offers the ability to restrict access, ensuring that only authenticated and authorized peers can participate in the network. Establishing such a controlled infrastructure typically requires forming a consortium, which usually reflects an existing business network (e.g., a supply chain).

Table 1. Mapping of Trust Requirements—BC features

Requirements	**BC Feature**	**Extended features** [Bellini et al., 2020]
Privacy	B1.1 Openness: Private	O2O data transactions confidentiality
Performance	B8.5 Consensus protocol: permissioned voting-based	High transaction rate/ low latency
Trust Computing	B4.3 Data: Smart contract variables, B3.1 Business logic: On-chain	Definition of smart contract language subsets and guidelines enabling formal verification
Auditability	B5.1 Ledger distribution: Full node	Fast/Easy world state retrieval
Security	B4.3 Data: Smart contract variables, B5.1 Ledger distribution: Full node	Fast/Easy world state retrieval, External Data Analysis (fraud detection)
Identification	B2.2 Access management: Permissioned	Authoritative digital identity certification

In a permissioned BC, a leader must be designated to act as the network manager. This role is generally assigned to the primary stakeholder leading the consortium, such as an automotive manufacturer overseeing its suppliers or a neutral third party coordinating business actors. In the context of our 6G O2O trust framework, this leadership role can be fulfilled by existing CHs (**Permissionless Based CH (PBCH)**). By leveraging the permissioned BC, these CHs enable the digitization of intermediation processes rather than eliminating them, as has been proposed in some other business models [Deloitte, 2016; Paul Ridgewell, 2019].

In this setup, the PBCH assumes the role of a formal SC validator, responsible for translating and automating the legal agreements underpinning O2O transactions into reliable SCs. The PBCH also takes accountability for any flaws in SC implementation (see [Sergey and Hobor, 2017] for an in-depth discussion). Furthermore, it manages access to the BC, allowing each MVNO/MNO to handle only the subset of transactions relevant to them.

A permissioned BC can meet the low latency and high TPS requirements of the 6G scenario, enabling real-time billing and compensation. Unlike permissionless BCs, it does not rely on resource-intensive consensus mechanisms like PoW, as trust is inherently established among the identified participants. While this setup discourages malicious behavior within the consortium, it does not eliminate the risk of external attacks attempting to compromise one or more network nodes.

To address such risks, alternative consensus mechanisms are implemented in the endorsement protocols used by frameworks like Hyperledger [Androulaki et al., 2019].

3.4 PBCH Solution Schema

HF is an open, permissioned BC platform designed to support concurrent transaction execution. Participants register through a trusted authentication mechanism to interact with the BC. The system employs the **Execute-Order-Validate (EOV)** approach for transaction execution, which is structured into three distinct phases. In the execution phase, the initiator submits a transaction to an authenticated set of BC nodes, where it is executed concurrently by multiple nodes. During the ordering phase, the consensus protocol is utilized to generate blocks, which contain a totally ordered sequence of transactions to be distributed across all BC nodes. The final phase, validation, involves a subset of nodes (referred to as endorsing nodes) that verify the state changes produced by the transactions.

The EOV architecture minimizes execution overhead by limiting the transaction execution load to the endorsing peers, thereby enabling parallelism. Enhancements to the basic EOV model include FastFabric [Gorenflo et al., 2020], which distributes functional responsibilities across nodes, and Fabric++ [Sharma et al., 2019], which incorporates database optimization techniques to reorder transactions for improved performance.

When a roaming user accesses a service on a visited network, it generates a Hyperledger transaction that includes the corresponding CDR. This transaction is produced by the serving network's peer-node and can be verified immediately by the home network's peer-node.

In this context, the roaming use case is implemented between the HPMN and the VPMN using SCs. These contracts are triggered whenever a subscriber initiates an event in the VPMN. The VPMN subsequently broadcasts the raw CDR data as a transaction on the BC.

CHs utilize the **Transferred Account Procedure vers. 3 (TAP3)** protocol to facilitate the exchange of CDRs between roaming partners. TAP3 specifies the process through which the VPMN transmits billing records of roaming subscribers to their respective HPMN. It defines both the structure and content of the data to be exchanged between network operators. These files are typically transferred using a basic File Transfer Protocol connection. Efforts are underway to automate the TAP3 protocol for near real-time execution, enabling networks to efficiently support new services.

Three primary chaincodes can be identified for implementing the roaming business logic: (1) CDR conversion, (2) NRTRDE generation, and (3) Billing Computation / Ricardian Contract [Grigg, 2004]. The first chaincode addresses the transformation of the CDR format generated by the VPMN into the format used by the CH, representing a typical service offered by CHs, which can be implemented on-chain.

The second chaincode focuses on filtering and processing raw CDRs provided by the VPMN to generate NRTRDE information in real-time. This information is then sent to the HPMN for fraud detection, marking a significant improvement over traditional methods.

The third chaincode enforces the terms of roaming agreements using a formally verifiable and computable script. This contract operates on the CDRs stored in the BC, ensuring that all business partners involved in the agreement can audit the data at any time. Unlike traditional SCs, Ricardian contracts include both executable instructions and a legal framework defining the relationships between parties. These contracts specify the entities involved, potential legal consequences, and applicable regulations in case of disputes.

These SCs are deployed by a TTP, which continues to function with the added support of BC technology.

The schema illustrated in Figure 3 presents our solution based on HF, where the CH intermediates the process. CDRs generated by roaming users are transmitted to the CH, which verifies the CDRs, compiles blocks, and posts them to the BC for immediate conversion into billing evidence via the associated SCs.

Periodically, a trusted on-chain contract determines the payment from the HPMN to the VPMN based on the recorded transactions. Our solution leverages Hyperledger channels to ensure access control and confidentiality for O2O transactions. Channels in Hyperledger act as private subnets for secure communication between two or more members, enabling private and confidential transactions. Each transaction is executed within a specific channel, with all participants authenticated and authorized via credentials provided by a Membership Services Provider (MSP). In this approach, a dedicated channel is created for each operator pair with a roaming agreement. The PBCH acts as the MSP and participates in all channels, updating them (via on-chain write contracts) with blocks composed of CDRs from the service network operator. The service and home network operators use additional on-chain contracts to read and verify blocks and compute the compensation amounts.

The algorithms and schemes proposed here are specifically aimed at the fraud detection scenario in 6G networks.

4 Fraud Scenario Specification

We are now ready to deal with the fraud scenario where a malicious user connects to VPMN and the billing and validation process follows as previously described. While the literature includes different works describing fraud

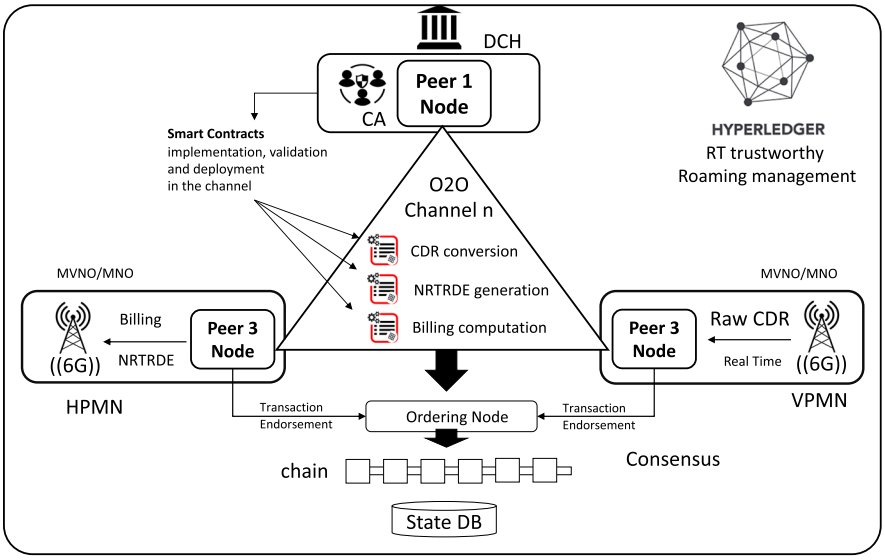

Fig. 3. The PBCH-based solution schema.

in this context, a reference benchmark [Macia-Fernandez et al., 2009] dealing with the roaming case was chosen for this research. Even if the communication technologies described in our benchmark [Macia-Fernandez et al., 2009] are 4G, general mechanisms are still current in 5G. In particular, the benchmark describes four different stages through which a system can be protected from fraud attempts. The vulnerability of the telecommunication system to fraud is related to the relations between the fraud and the response times. Regarding [Macia-Fernandez et al., 2009], this work focuses on the detection stage.

The scenario is here reported in two different configurations: a *traditional-CH* configuration, and a *PBCH* configuration.

The Traditional-CH Configuration. This CH configuration is derived from the one described in [Macia-Fernandez et al., 2009]. Figure 4 reports a **Unified Modeling Language—Sequence Diagram (UML-SD)** that represents the interactions between the parties in this configuration.

Since this scenario is exploitable through time-related flaws (Time delay in data exchange), the diagram formalizes the messages exchanged between the parties, as well as the times, involved in such a process. In particular:

- —the time that the VPMN takes to prepare the CDR to send to CH is represented by $T_{preparecdr}$;
- —$T_{sendcdr}$ is the time the network takes to deliver a CDR;
- —T_{ch} is the net time for a CH to evaluate the conformance of the received CDR to the signed contract;
- —T_{fraud} is the time needed by the HPMN to determine whether the received CDR is related or not to a fraud call.

Such interaction determines the traffic time the malicious user steals, which is represented in the figure by $T_{endcall}$. Such a time can be the "natural" duration of the call, if the fraud is not detected, or the overall time to detect the fraud, in case of detection. Here, we refer to some probabilities of detecting fraud by the HPMN: P_{fraud} and $P_{nofraud}$.

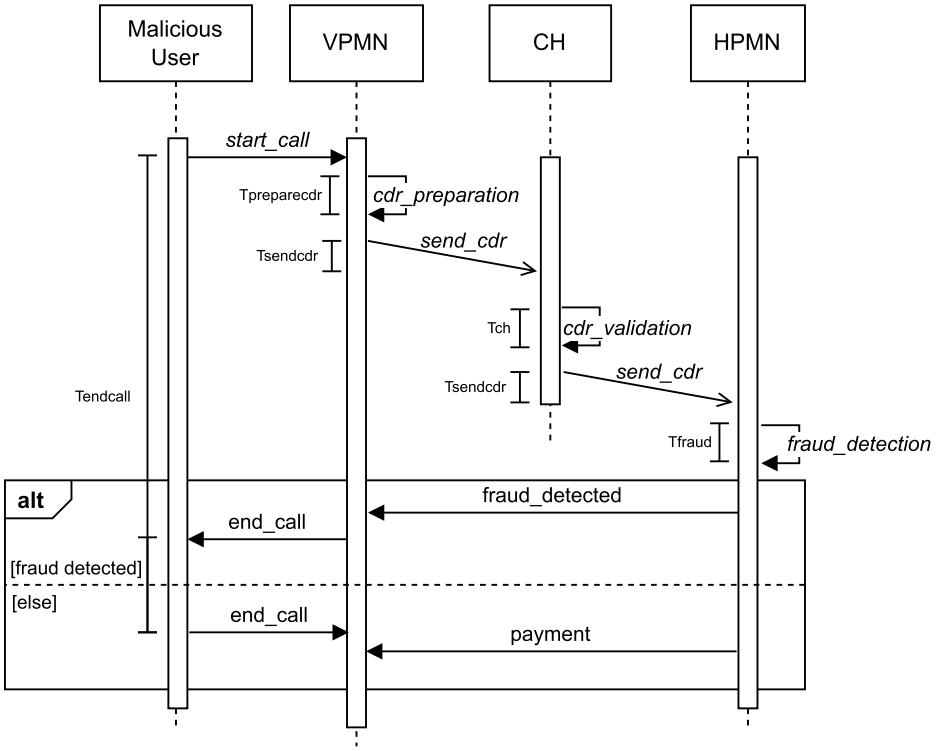

Fig. 4. The fraud UML-SD scenario.

In this configuration, we also consider the presence of different VPMNs which concur with the one the malicious user connects to use the resources of the CH. It is a classic case of concurrence that does not add any further information to the diagram already depicted and that is detailed in Section 5.

The PBCH Configuration. In this configuration, the DLT-based CH is reported, extending the previous one, according to the UML-SD reported in Figure 5.

The initial and the final steps of the sequence are the same as the previous configuration, while the central part—the fraud detection mechanism—is delegated to a permissioned BC. The PBCH object receives the *send_cdr* message from the VPMN, as in the previous configuration but, it selects a number of validators over a total amount of possible DLT-participants[3]. The four main steps are:

- *select_validators*: when the PBCH invites $N_{validators}$ validators to participate in the consensus (the action consumes $T_{sendcdr}$ time;
- *detection*: when the invited validators detect if a fraud is on going. This action lasts T_{fraud} that can span from a few seconds (as in permissioned BC) to some minutes (as in permissionless chains);
- *return*: when each validator returns its response on the nature of the transaction (fraudulent / non-fraudulent);
- *fraud_detection*: when the PBCH evaluates the different responses to decide the final nature of the transaction. The action consumes T_{voting} time.

[3]Even if not explicitly marked in the diagram, these numbers are two model parameters: $N_{validators}$ and $N_{partcipants}$.

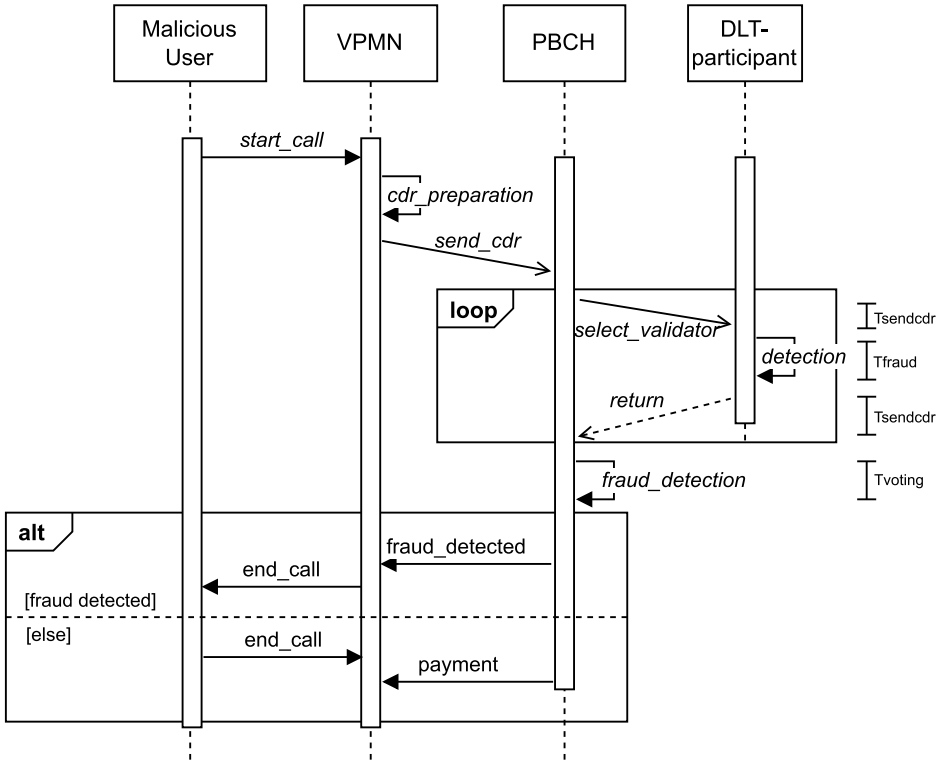

Fig. 5. The fraud UML-SD scenario—the *PBCH* configuration.

5 Fraud Scenario Modelling

Starting from the scenario and the configurations reported in Section 4, this section is devoted to formalizing such interactions.

The final aims of the paper are to show possible tradeoffs between security and performance in the design and the construction of the proposed PBCH schema, the comparison with the traditional CH validation, and the quantitative impact of one or more parameters on some defined performance indices. Hence, one of the most widespread formalisms able to depict a concurrent distributed system to obtain quantitative analysis is the one of Generalized Stochastic Petri Nets.

Among formal verification techniques for BC consensus mechanisms, model checking has received a lot of interest due to the possible goal of a "push-button" technology able to verify security properties without human intervention. Belonging to this category, there are the following works: [Liu and Liu, 2019], which models SCs using Colored Petri Nets; [Osterland and Rose, 2020], which translates Solidity in Promela to verify them by SPIN; [Lahbib et al., 2020], where the Event-B framework is used for both modelling and analyzing SC using both model checking and simulation; [Nehaï et al., 2018], that models SCs with NuSMV. Other PN-related papers are also reported [Chu et al., 2024; He et al., 2023; Zaitsev et al., 2023] witnessing the generic applicability of these formalisms to the DLTs modelling and analysis.

To the best of our knowledge, most of these papers introduce simple GSPN models for security-performance tradeoffs, and none of them focuses on fraud detection in the mobile phone context.

The rationale behind the construction of the model, and its inherent structure, are based on our previous work [Flammini et al., 2013]. In that work, the authors consider a similar problem—i.e., the construction of a PN model

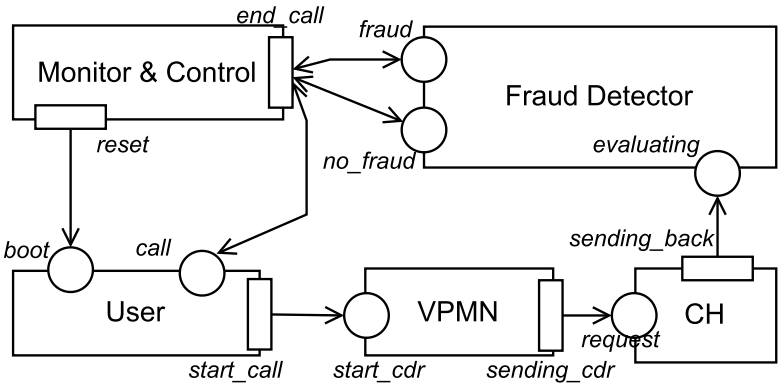

Fig. 6. The GSPN model schema.

Table 2. PN Submodel Interconnections

From	To	Nature	Reference
Monitor and Control	User	Message	-
User	VPMN	Message	start_call
VPMN	CH	Message	send_cdr
CH	Fraud Detector	Message	send_cdr
Fraud Detector	Monitor and Control	State Sharing	-
User	Monitor and Control	State Sharing	-

to evaluate the physical vulnerability of a critical infrastructure. The present paper shares the motivation—i.e., finding a model able to predict if a given attack would be successful—and the final objective—i.e., evaluating the vulnerability of a protection system as a probability. Our fraud scenario fits well into the modelling and analysis framework of the cited work. In both cases, the success of an attack is mainly based on detection probability and on the latency of both attacking and defending processes. Valuable references for this modelling framework are [Hennessey et al., 2006; Garcia, 2006].

To construct the GSPN model, a compositional method has been chosen. Figure 6 represents the main model structure, highlighting the main GSPN submodels.

These models are interconnected by arcs. The nature of these interconnections, and their relation with the high-level UML-SDs previously described, are reported in Table 2. When present, a value in the `Reference` column reports the name of the message in the UML-SD to which the interaction is related.

When the interconnection nature is `Message`, it means that the compositional semantics of GSPN submodels refers to the asynchronous message-passing mechanism, as the one reported in Sibertin-Blanc's cooperative networks [Sibertin-Blanc, 2001]. On the contrary, `State Sharing` means that the Monitor and Control subnetwork can read/write from input places to alter the state of the other networks.

The *Monitor and Control model*, in fact, is responsible for resetting the network when a call is ended in both the detection and non-detection cases. This subnet is reported in Figure 7.

The *User model* is depicted in Figure 8 and represents the behavior of the malicious user.

The *VPMN model* is depicted in Figure 9 and represents the behavior of the VPMN, preparing and transmitting the CDR to be validated.

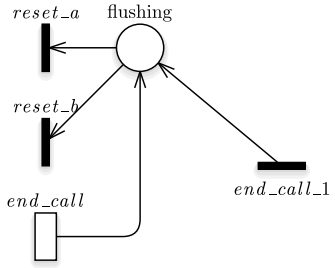

Fig. 7. The Modelling and Control GSPN submodel.

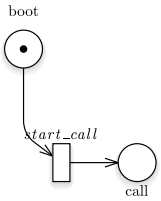

Fig. 8. The User GSPN submodel.

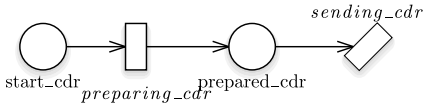

Fig. 9. The VPMN GSPN submodel.

Regarding the two considered configurations, some differences occur when designing the other sub-models.

The Traditional-CH Configuration. This configuration presents two distinct models for CH and Fraud Detector, depicted in Figure 10 and in Figure 11, respectively.

In the *CH model*, when a request arrives, the start_serving transition fires to represent the CH considers the sent CDR. For the sake of realism, the *clients* place contains a number of generators of external requests that concur with the fraudulent one in getting the resources of the CH. Such resources are limited and are represented by the $CH_{resources}$ place and its initial marking, i.e., the $CH_{parallel}$ parameter.

The *Fraud Detector model* simply computes the fraud detection algorithm (using the *DetectingFraud* timed transition) and determines whether the call is related to a fraud or not (i.e., by the *detecting_fraud* and the *undetecting_fraud* transitions).

As a result, the composed GSPN network related to this configuration is reported in Figure 12.

The PBCH Configuration. On the contrary, this configuration considers just one submodel covering both Fraud Detection and CH. Figure 13 depicts this case.

The model represents the workflow of activities executed in a permissioned BC validation task:

—Selection of the Validators: the *select_validators* extract from the *participant's* place *Nvalidators* peers;
—Validation: each selected peer enables in parallel the validate transition and then decides whether the transaction is valid or not (i.e., the *detecting_fraud* and *undetecting_fraud* transitions);

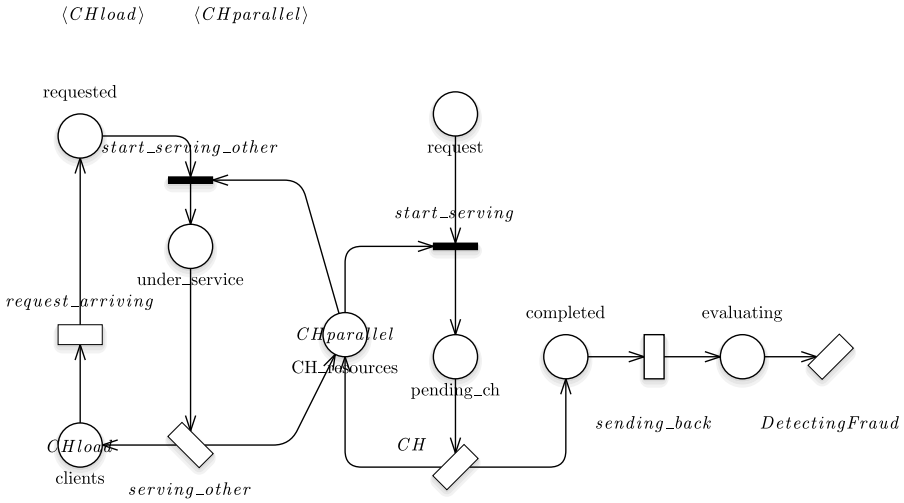

Fig. 10. The CH GSPN submodel.

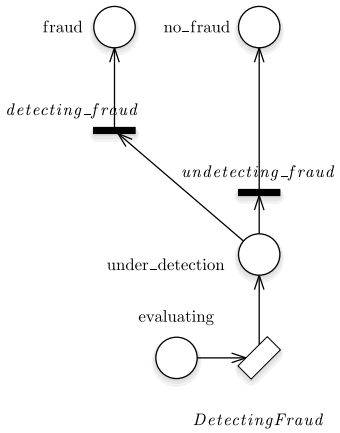

Fig. 11. The Fraud Detector GSPN submodel.

—Decision and Restoring: the *voting* and *flushing_bc* places rule this phase, oriented to the determination of the most voted case and the restoring of the validators into the participant's pool;
—Voting: once the vote has been determined, two timed transitions represent the time needed by the voting algorithm to make the decision.

The composed GSPN network related to this configuration is reported in Figure 14.

6 Fraud Scenario Analysis

This section is devoted to analyzing the GSPN models presented in the previous section. First, let us start with the high-level metrics to compute and then translate them into GSPN performance indices. From a system point of view, two metrics fit well into a risk-oriented process, supporting the decision to adopt or not a PBCH fraud detection scheme; they are: the cost of the solution itself; the cost the solution has, in terms of stolen MOUs, in case of non-detection or late detection of the fraud.

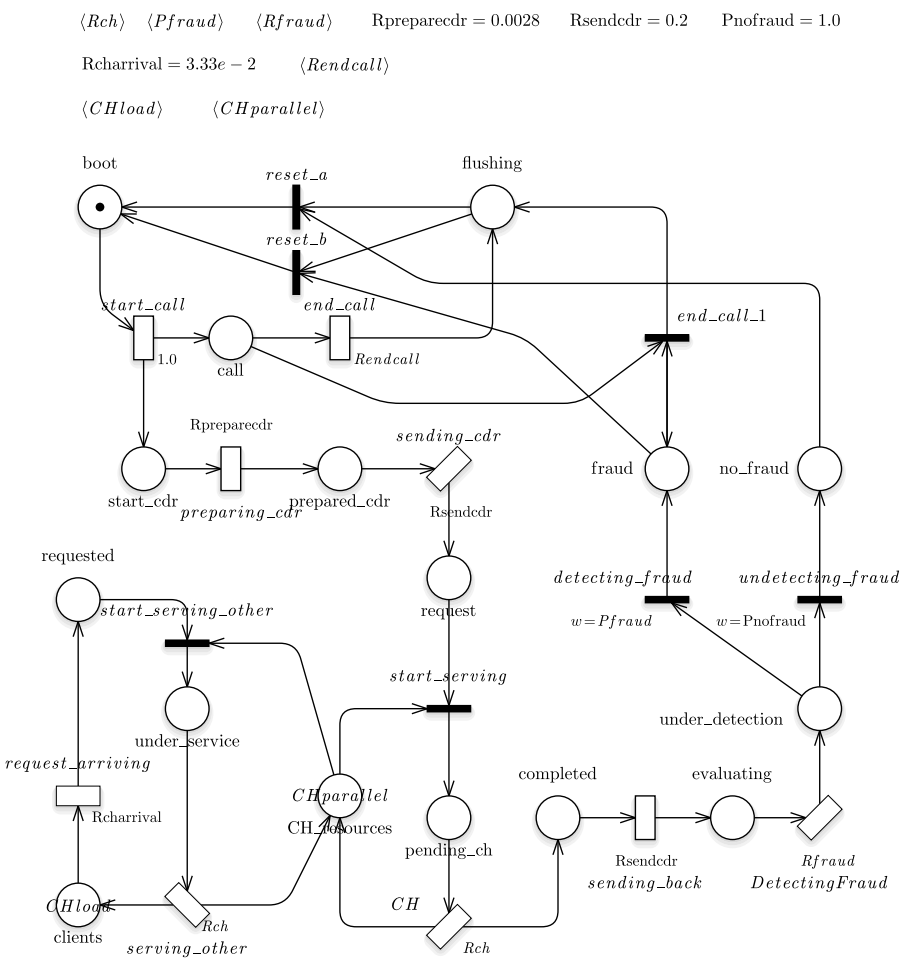

Fig. 12. The traditional-CH GSPN composed model.

This section focuses on the second item. Since it is not possible to exactly evaluate the first item, Section 7 reports some considerations on its estimation.

The measure of how much money the HPMN loses from a fraud call can be translated by computing the following GSPN performance indices:

—the mean sojourn time of the token in the *call* place T_{call};
—the overall probability of detecting a fraud, $P\{detection\}$.

Both metrics can be computed by using the throughputs of the transitions end_call and end_call_1. According to [Ajmone Marsan et al., 1984] and related bibliography, T_{call} can be computed by using Equation (1) while $P\{detection\}$ using Equation (2).

$$T_{call} = \frac{1}{th(end\_call) + th(end\_call\_1)} \tag{1}$$

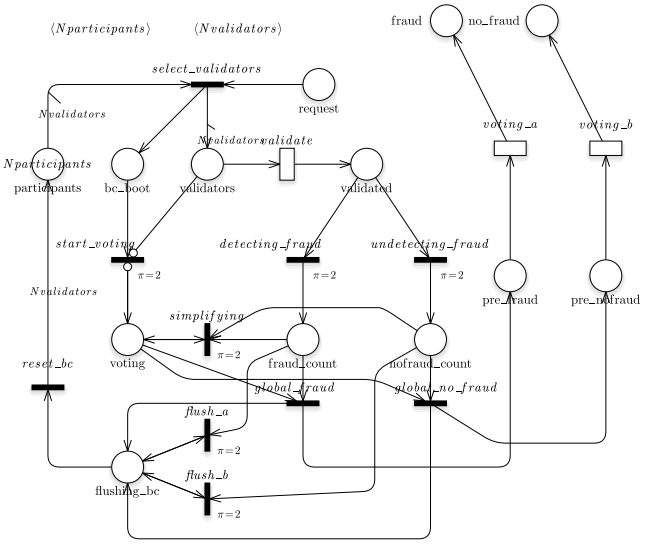

Fig. 13. The Fraud Detector GSPN submodel.

$$P_{detection} = \frac{th(end\_call\_1)}{th(end\_call) + th(end\_call\_1)}. \tag{2}$$

Equation (1) computes the inverse of the sum of the throughputs of all the transitions whose firing removes a token from the *call* place. This set is constituted by the *end_call* and by the *end_call_1* transitions.

On the other hand, the whole process ends with two different outcomes: fraud detection (represented by the firing of the *end_call_1* transition) and non-detection (represented by the firing of the *end_call* transition). Hence, in Equation (2), the detection is computed by considering the frequency of the positive event over the summation of all the possible events.

These indices are computed in the context of a parametric analysis made by varying the values of the parametric variables of the model. Tables 3 and 4 respectively represent the variables whose value are kept constant and the variables that are subject to a parametric analysis. All the times in both the tables are expressed in seconds. As the paper just proposes a sensitivity analysis, the parameter values are not chosen starting from a concrete case study or from a pilot project. Instead, they span into a large range to demonstrate the performance-trustworthiness differences between the two modelled approaches.

For these last group of variables, nominal values are considered. These values are used to simplify the analysis. While a parameter value is varied, the others are kept at their nominal values; hence, the parametric analysis is made by varying one parameter variable at a time. Even if this analysis does not allow identifying the parameter values that optimise the performance indices, this approach highlights to which parameters the performance indices are most sensitive.

The models have been implemented with the GreatSPN tool [Amparore et al., 2016] and the performance indices are derived by computing the steady state analysis. Both the complete GSPN models are analyzed on a 16-core AMD Ryzen 7 5800H, equipped with 16 GB of RAM, and running Linux Mint 21.1 Cinnamon (kernel 5.15.0-79-generic). The biggest Reachability Graph has been obtained in the case of 37 validators per transaction in the PBCH model, and it counts around 4500 states. All the analyses have been executed in a few seconds up to a minute. The following analyses are conducted.

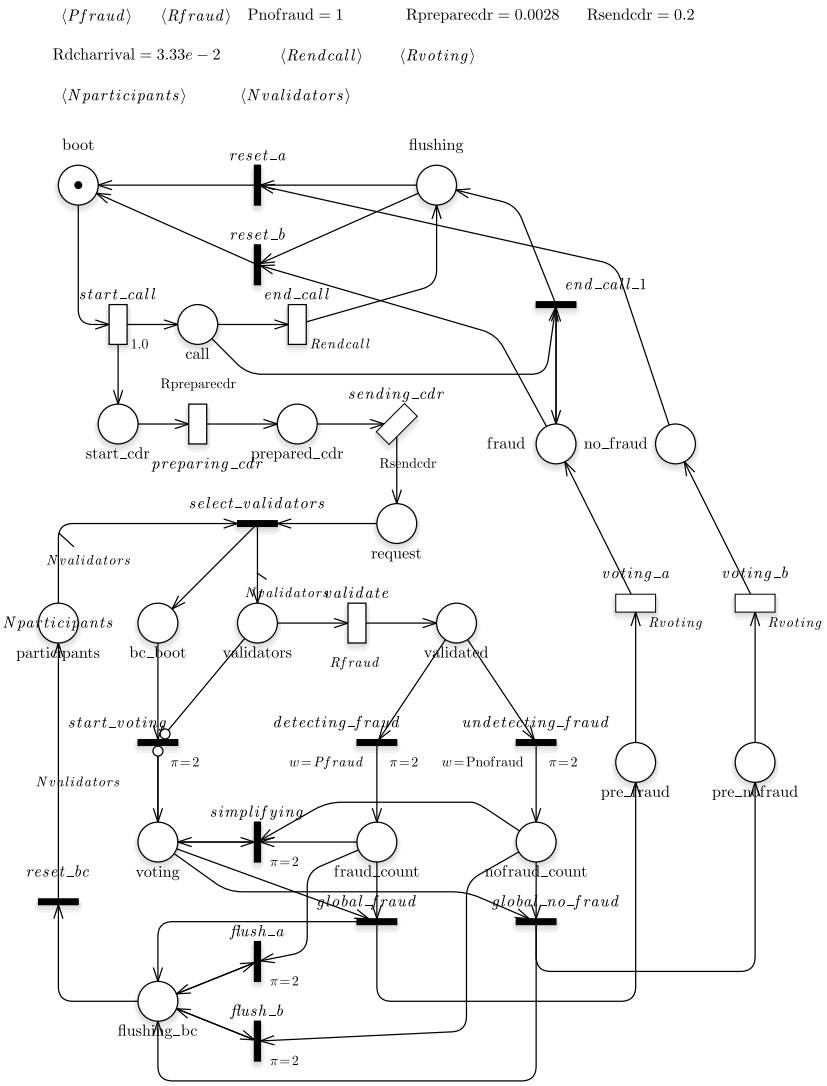

Fig. 14. The PBCH-based GSPN composed model.

Table 3. Constant Model Parameters

Name	Configuration	Description	Value
Tpreparecdr	Both	Mean time to prepare CDR	360
Tsendcdr	Both	Mean sending time of CDR	5
Tcharrival	Both	Mean arrival time of external CH requests	30

Table 4. Variable Model Parameters

Name	Configuration	Description	Nominal Value	Variation
Pfraud	Both	Weight of fraud detection	9	{1, 3, 9, 19, 99}
Tch	Traditional	Mean time of CH computation	14,400	from 7,200 to 28,800 with step 1800
Tfraud	Both	Mean time to detect fraud	100	from 30 to 180 with step 30
Tendcall	Both	Mean call duration	600	from 100 to 3,600 with step 500
Chload	Traditional	Number of concurring clients	15	from 5 to 45 with step 5
Chparallel	Traditional	Number of CH resources	5	from 3 to 9 with step 2
Nvalidator	PBCH	Number of validators in the DLT	7	from 5 to 37 with step 4
T_{voting}	PBCH	Mean time to reach consensus	1	from 1 to 73 with step 8

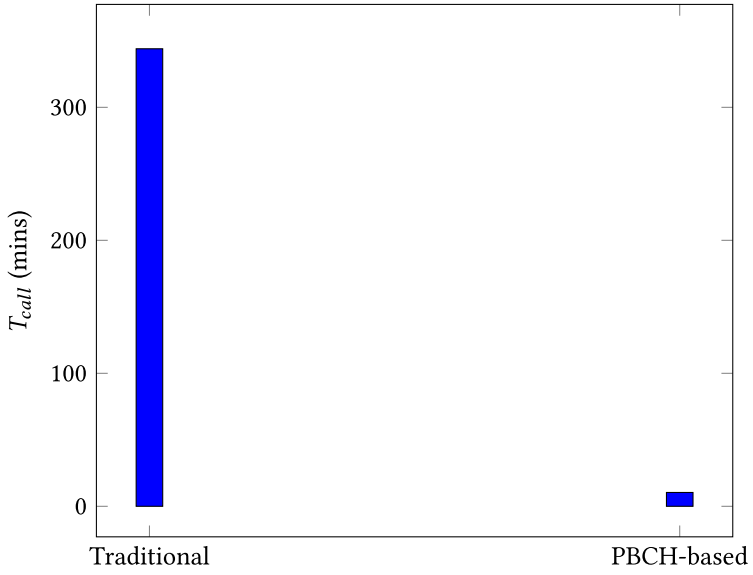

Fig. 15. Traditional vs PBCH-based solutions (T_{call}).

Solution Comparison. Figures 15 and 16 respectively report T_{call} and $P_{detection}$ variables for both the traditional and PBCH-based solutions.

The analysis—conducted in the nominal cases, i.e., with the same values for the common parameters—reveals a net superiority of the PBCH-based approach in both the measures. In fact, the detection time of the PBCH case is around 3% of the traditional one, while the probability of detection is increased by a 228× factor.

Traditional Solution. Regarding the traditional approach, the sensitivity analysis on the variation of the considered parameters are conducted; their results are here reported. For the sake of brevity, only the plots reporting T_{call} are shown.

Figure 17 shows T_{call} w.r.t. changes in the *Chparallel* parameter when the external load is 15 concurrent external clients: the biggest gain is to reach 5 parallel executors to the centralized CH.

Figure 18 changes instead *Chload*, showing that the system reaches the saturation when the number of the clients served by the CH is around twice the computing resources of the CH itself.

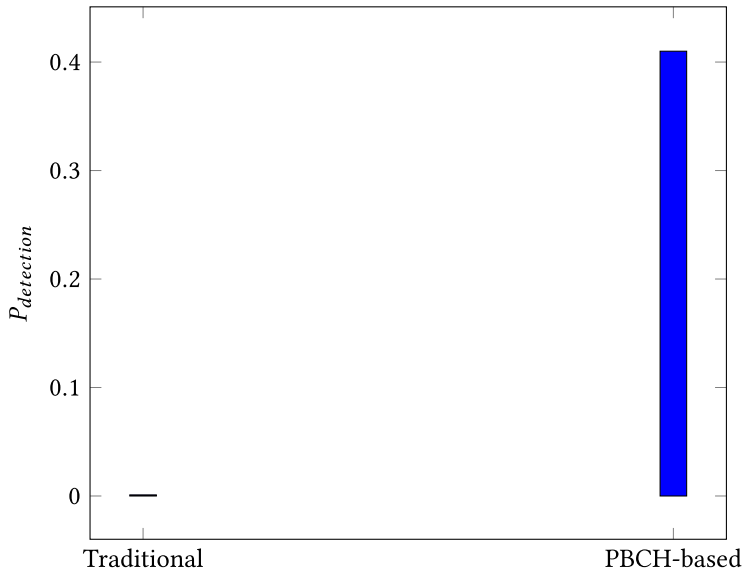

Fig. 16. Traditional vs PBCH-based solutions ($P_{detection}$).

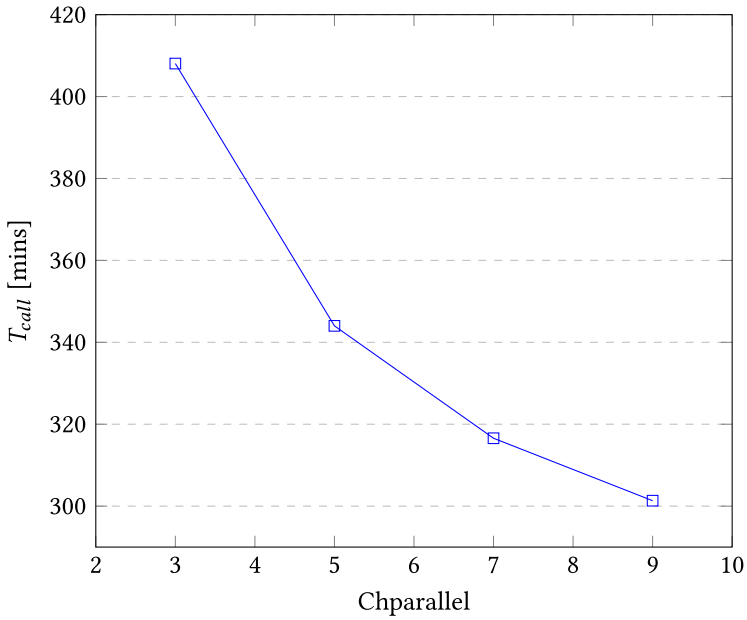

Fig. 17. Traditional solution—T_{call} variations w.r.t. *Chparallel*.

Figure 19 changes instead *Tch*, highlighting a linear dependency from this parameter to the overall duration of the call.

PBCH-Based Solution. As for the traditional solution, some plots are reported, analyzing the sensitivity of the T_{call} values to the changes in the values of specific parameters.

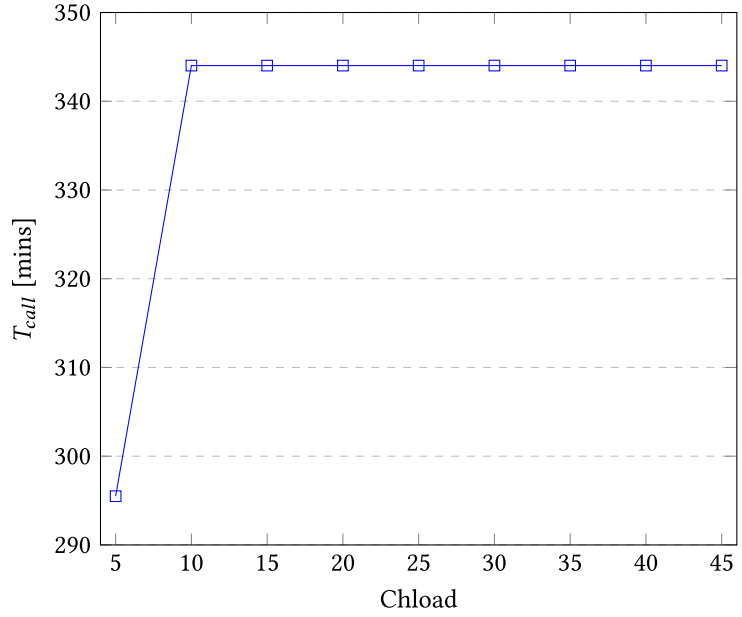

Fig. 18. Traditional solution—T_{call} variations w.r.t. *Chload* .

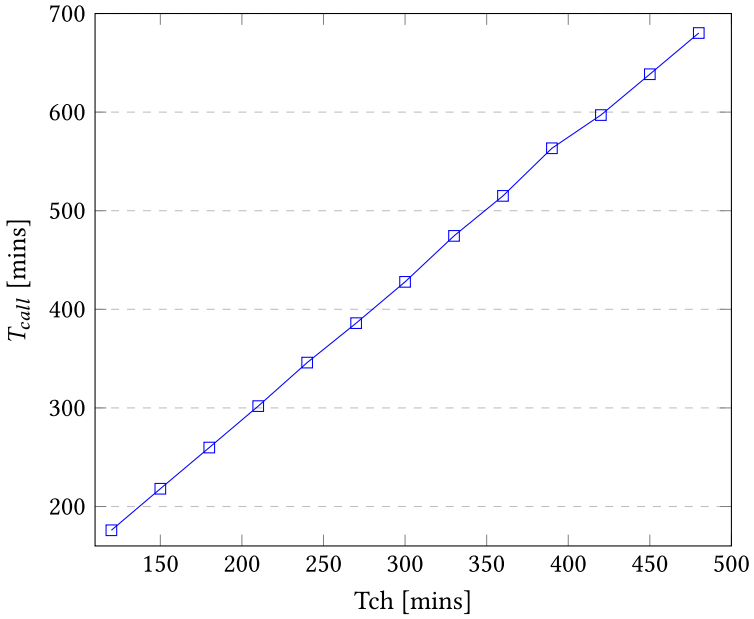

Fig. 19. Traditional solution—T_{call} variations w.r.t. *Tch.*

Figure 20 considers the changes in the number of the validators, while Figure 21 considers the changes in the time to vote.

While the second plot reveals that the time to detect the fraud is not sensitive to T_{voting}, the number of the validators can be the basis of performance-security tradeoffs. Since the overall security of the approach grows as

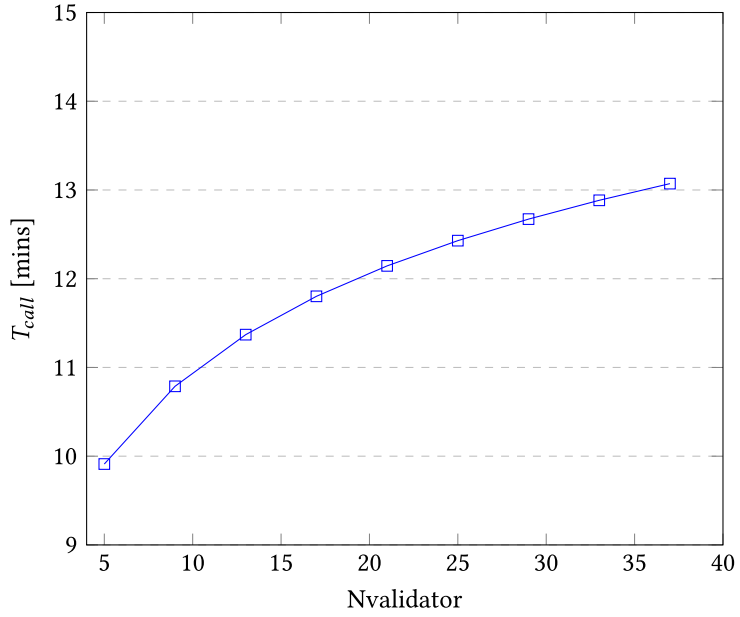

Fig. 20. PBCH solution—T_{call} variations w.r.t. *Nvalidator*.

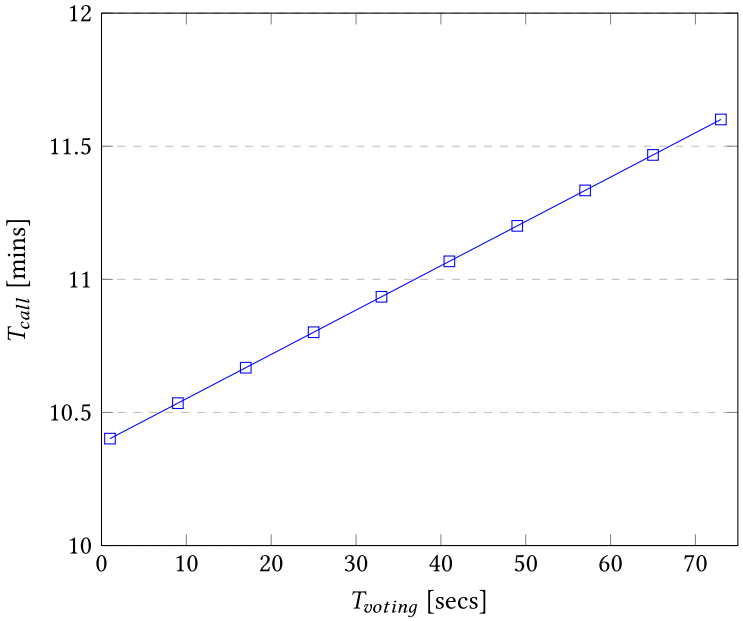

Fig. 21. PBCH solution—T_{call} variations w.r.t. T_{voting}.

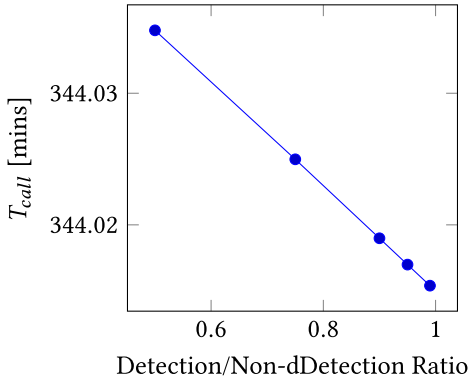

Fig. 22. *Pfraud* sensitivity (Traditional).

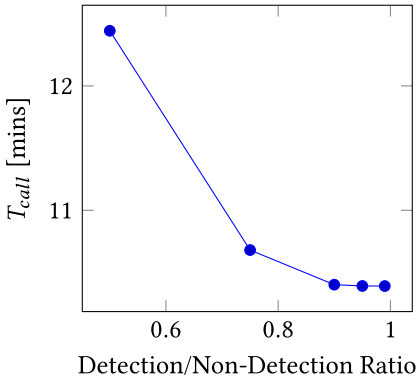

Fig. 23. *Pfraud* sensitivity (PBCH-based).

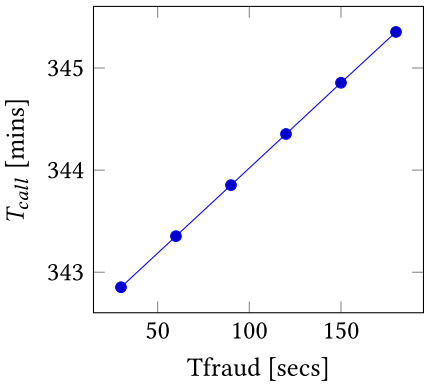

Fig. 24. *Tfraud* sensitivity (Traditional).

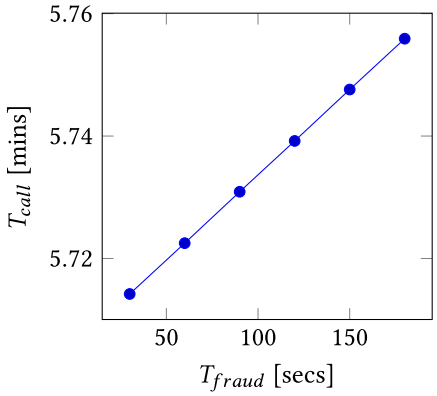

Fig. 25. T_{fraud} sensitivity (PBCH-based).

the number of the involved validators is high, keeping low the probability that a malicious agent can corrupt the decision of the majority of the validators, keeping high this number, does not bring to an explosion of T_{call}.

Joint Sensitivity Analysis. The final set of analyses is devoted to a joint sensitivity analysis of both the scenarios regarding changes in the same parameters according to the same values, since some parameters affect both models. Figures 22 and 23 respectively report the variation of T_{call} w.r.t. changes in the values of the ration of fraud detection by analyzing the CDRs. In both the scenarios, the variations are small and in the case of PBCH-based scenario, there is a saturation effect when approaching the perfect detection.

The next two groups of analyses—Figures 24 and 25 for *Tfraud*, and Figures 26 and 27 for *Tendcall*—present two similar variation patterns between the two scenarios, i.e., the shapes of the figures. The analysis regarding *Tfraud* is linear, while the second one seems quadratic. This notwithstanding, both the analyses are quite rigid since all the variations of the T_{call} are small.

7 Discussion

The quantitative analysis described in Section 6 reveals a technical superiority of the PBCH-based solution even if, from a managerial point of view, the final decision of which solution to adopt depends on some cost-oriented factors: the cost of the solution itself ($C_{solution}$) and the cost of the late detection of the fraud (C_{fraud}).

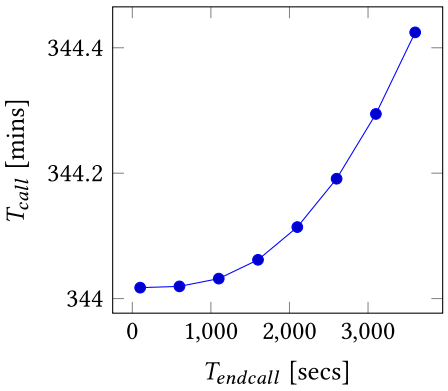

Fig. 26. *Tendcall* sensitivity (Traditional).

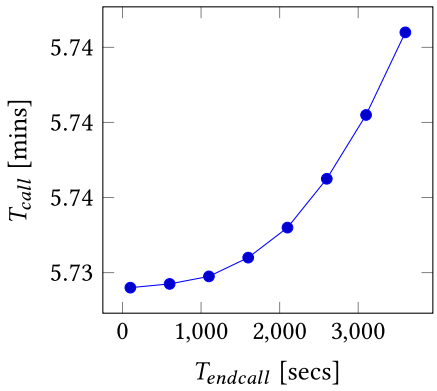

Fig. 27. $T_{endcall}$ sensitivity (PBCH-based).

As an accurate evaluation of these costs is out of the scope of this paper, the following considerations can be done. Equation (3) describes a formula computing such C_{fraud}.

$$C_{fraud} = \begin{cases} C_{min} * T_{call} * \iota & \text{in case of detection} \\ C_{min} * T_{call} & \text{in case of missed detection} \end{cases}, \tag{3}$$

where C_{min} is the cost per minute of roaming traffic, and ι represents the possible (partial) compensation from an insurance service in case of detected fraud[4]. This formula can be synthetized into Equation (4).

$$C_{fraud} = C_{min} * T_{call} * (P_{detection} * \iota + 1 - P_{detection}) = C_{min} * T_{call} * [1 + (\iota - 1) * P_{detection}]. \tag{4}$$

This equation hides an intrinsic complexity that makes the estimation of the overall costs a hard task, due to these reasons:

- —according to both the models considered in Section 5 and analyzed in Section 6, T_{call} depends on $P_{detection}$ since early detection allows HPMN and VPMN to hang up the communication and to shorten the loss of money;
- —ι may depend on the adopted technology on the specific parameters chosen and on the performance in terms of fraud detection the O2O operator demonstrates to achieve to the insurance company;
- —furthermore, a greater ι is often coupled to a greater cost, affecting $C_{solution}$;
- —$P_{detection}$ and T_{call} are affected by several parameters, which have their own costs, contributing to the calculation of the overall $C_{solution}$ value.

Regarding this last point, all the analyses conducted in Section 6 can be used to find the (sub)optimal tuning of the parameter values under able to maximize performance parameters and minimize costs at the same time. An exhaustive discussion of all the possible considerations is out of the scope of this paper; to mention a few about the PBCH-based solution:

- —as the number of the validators increases, the T_{call} does not explode, and it suggests using a considerable number of validators, also according to security requirements (see Figure 20);
- —as P_{fraud} does not impact on the global T_{call} when it is bigger than 0.8 (see Figure 25), the advantage of a more reliable (and consequently slower and more expensive) detection algorithm is not obvious;
- —in this last scenario, also T_{fraud} would increase, but the impact on the global T_{call} is limited.

[4] ι is a non-dimensional factor between 0 and 1 where 1 means no cost coverage and 0 means total cost coverage.

As a final consideration, this paper assumes the presence of a fraud, and the focus on the analysis is on the economic impact of a fraud. To complete the risk-oriented analysis, also considerations on the occurrence of such frauds should be considered since in a country with a high probability of fraud attempts, a more sophisticated (and expensive) system would be economically justified, while in a country with a low probability of fraud, traditional detection systems could be enough.

8 Conclusion

To conclude, the use of permissioned BCs to establish the trustworthiness of some specific actors represents a great opportunity for CH to continue to play a crucial role in the 6G era. Our work proposes a scheme based on HF, and PBCH, for BC-enabled CH operation. PBCH radically transforms CH intermediation to ensure its scalability while continuing to support O2O trust in the new 6G ecosystem.

The conducted analysis demonstrates the advantages of the proposed PBCH-based solution to detect roaming fraud attempts. This demonstration is supported by a quantitative analysis of a GSPN model where parametric analysis can support the network designer and project managers in their decisions.

Future research will improve the adherence of the proposed models to reality by comparing the model with laboratory-sized Hyperledger infrastructures and/or with real-world data. This research stage would assess the GSPN models.

References

5G Roles in Industry Digitalization in the UAE. Retrieved December 30, 2023 from https://tdra.gov.ae/-/media/TDRA-Media/Resources/English/White-Paper-v271012.ashx

Nima Afraz, Francesc Wilhelmi, Hamed Ahmadi, and Marco Ruffini. 2023. Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. *IEEE Access* 11 (2023), 95653–95666. DOI: https://doi.org/10.1109/ACCESS.2023.3309423

Marco Ajmone Marsan, Gianni Conte, and Gianfranco Balbo. 1984. A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems. *ACM Transactions on Computer Systems (TOCS)* 2, 2 (1984), 93–122. DOI: https://doi.org/10.1145/190.191

Elvio Gilberto Amparore, Gianfranco Balbo, Marco Beccuti, Susanna Donatelli, and Giuliana Franceschinis. 2016. 30 years of GreatSPN. In *Principles of Performance and Reliability Modeling and Evaluation*. Springer, 227–254.

Elli Androulaki, Angelo De Caro, Matthias Neugschwandtner, and Alessandro Sorniotti. 2019. Endorsement in Hyperledger Fabric. In *Proceedings of the IEEE International Conference on Blockchain (Blockchain)*, 510–519. DOI: https://doi.org/10.1109/Blockchain.2019.00077

Andreas M. Antonopoulos. 2017. *Mastering Bitcoin*. O'REILLY.

Lina Bariah, Lina Mohjazi, Sami Muhaidat, Paschalis C. Sofotasios, Gunes Karabulut Kurt, Halim Yanikomeroglu, and Octavia A. Dobre. 2020. A prospective look: Key enabling technologies, applications and open research topics in 6G networks. *IEEE Access* 8 (2020), 174792–174820. DOI: https://doi.org/10.1109/ACCESS.2020.3019590

Emanuele Bellini, Paolo Ceravolo, and Paolo Nesi. 2017. Quantify resilience enhancement of uts through exploiting connected community and internet of everything emerging technologies. *ACM Trans. Internet Technol.* 18, 1 (Oct. 2017), Article 7, 34 pages. DOI: https://doi.org/10.1145/3137572

Emanuele Bellini, Ernesto Damiani, and Stefano Marrone. 2023. Blockchain-based trustworthy O2O interaction in the next 6G ecosystem. In *Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR '23)*, 92–98. DOI: https://doi.org/10.1109/CSR57506.2023.10224977

Emanuele Bellini, Youssef Iraqi, and Ernesto Damiani. 2020. Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access* 8 (2020), 21127–21151.

Christian Cachin. 2001. Distributing trust on the internet. In *Proceedings of the International Conference on Dependable Systems and Networks*, 183–192. DOI: https://doi.org/10.1109/DSN.2001.941404

Liangyong Chu, Jingru Ding, and Yiyi Xie. 2024. Modeling and analysis of Petri nets for multimodal transport "single contract. *Systems Based on Blockchain. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering* 10, 1 (2024). DOI: https://doi.org/10.1061/AJRUA6.RUENG-1094

Sebastiaan Deetman. 2016. Bitcoin Could Consume as Much Electricity as Denmark by 2020. http://motherboard.vice.com/read/bitcoin-couldconsume-as-much-electricity-as-denmark-by-2020

Deloitte. 2016. Blokchain @ telco—How Blockchain can impact the telecommunications industry.

Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert van Renesse. 2016. Bitcoin-NG: A scalable blockchain protocol. In *Proceedings of the Usenix Conference on Networked Systems Design and Implementation*, 45–59.

Francesco Flammini, Stefano Marrone, Nicola Mazzocca, and Valeria Vittorini. 2013. Petri net modelling of physical vulnerability. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. LNCS, Vol. 6983, 128–139. DOI: https://doi.org/10.1007/978-3-642-41476-3_11

Mary Lynn Garcia. 2006. Vulnerability assessment of physical protection systems. In *Vulnerability Assessment of Physical Protection Systems*.

Christian Gorenflo, Stephen Lee, Lukasz Golab, and Srinivasan Keshav. 2020. FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second. *International Journal of Network Management* 30, 5 (2020), 455–463.

Ian Grigg. 2004. The Ricardian contract. In *Proceedings of the 1st IEEE International Workshop on Electronic Contracting, 2004*, 25–31. DOI: https://doi.org/10.1109/WEC.2004.1319505

Yaqiong He, Hanjie Dong, Huaiguang Wu, and Qianheng Duan. 2023. Formal analysis of reentrancy vulnerabilities in smart contract based on CPN. *Electronics (Switzerland)* 12, 10 (2023), 1–20. DOI: https://doi.org/10.3390/electronics12102152

Brian Hennessey, Bradley Norman, and Robert B. Wesson. 2006. Security simulation for vulnerability assessment. In *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, 46–50. DOI: https://doi.org/10.1109/CCST.2006.313428

Maurice Herlihy. 2019. Blockchains from a distributed computing perspective. *Communications of the ACM* 62, 2 (2019), 78–85.

Tharaka Hewa, Gürkan Gür, Anshuman Kalla, Mika Ylianttila, An Bracken, and Madhusanka Liyanage. 2020. The role of blockchain in 6G: Challenges, opportunities and research directions. In *Proceedings of the 2nd 6G Wireless Summit (6G SUMMIT '20)*, 1–5. DOI: https://doi.org/10.1109/6GSUMMIT49458.2020.9083784

Peter Jonsson, Stephen Carson, Andres Torres, Per Lindberg, Kati Öhman, and Athanasios Karapantelakis. 2019. Ericsson Mibility Report. Retrieved from https://www.ericsson.com/49d1d9/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf

Ramakrishna Kotla, Lorenzo Alvisi, Mike Dahlin, Allen Clement, and Edmund Wong. 2010. Zyzzyva: Speculative Byzantine fault tolerance. *ACM Transactions on Computer Systems* 27, 4 (2010), Article 7, 39 pages. DOI: https://doi.org/10.1145/1658357.1658358

Asma Lahbib, Abderrahim Ait Wakrime, Anis Laouiti, Khalifa Toumi, and Steven Martin. 2020. An event-B based approach for formal modelling and verification of smart contracts. In *Proceedings of the 34th International Conference on Advanced Information Networking and Applications*, 1303–1318.

Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems* 4, 3 (1982), 382–401.

Zhentian Liu and Jing Liu. 2019. Formal verification of blockchain smart contract based on colored petri net models. In *Proceedings of the IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC '19), Vol.* 2, 555–560. DOI: https://doi.org/10.1109/COMPSAC.2019.10265

Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, and Jesus Diaz-Verdejo. 2009. Fraud in roaming scenarios: An overview. *IEEE Wireless Communications* 16, 6 (2009), 88–94. DOI: https://doi.org/10.1109/MWC.2009.5361183

Ralph C. Merkle. 1980. Protocols for public key cryptosystems. In *Proceedings of the IEEE Symposium on Security and Privacy*, 122–134.

El Ioini Nabil and Pahl Claus. 2018. A review of distributed ledger technologies. In *Proceedings of the Conference On the Move to Meaningful Internet Systems (OTM '18)*.

Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical Report.

Zeinab Nehaï, Pierre-Yves Piriou, and Frédéric Daumas. 2018. Model-checking of smart contracts. In *Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 980–987. DOI: https://doi.org/10.1109/Cybermatics_2018.2018.00185

Thomas Osterland and Thomas Rose. 2020. Model checking smart contracts for Ethereum. *Pervasive and Mobile Computing* 63 (2020), 101129. DOI: https://doi.org/10.1016/j.pmcj.2020.101129

Contributing Analyst Paul Ridgewell. 2019. Blockchain: Where's the value for telecoms?

Ahokangas Petri, Matinmikko-BlueMarja, Yrjola Seppo, Seppanen Veikko, Hammainen Heikki, Jurva Risto, and Matti Latva-aho. 2018. Business models for local 5G micro operators. In *Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN '18)*, 1–8.

Chellvamathi RS and Prasanna Kulkarni. 2023. Blockchain in telecom: Challenges and the way forward. In *Proceedings of the International Conference on Innovative Data Communication Technologies and Application (ICIDCA '23)*, 661–667. DOI: https://doi.org/10.1109/ICIDCA56705.2023.10099882

Walid Saad, Mehdi Bennis, and Mingzhe Chen. 2020. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network* 34, 3 (2020), 134–142. DOI: https://doi.org/10.1109/MNET.001.1900287

Ilya Sergey and Aquinas Hobor. 2017. A concurrent perspective on smart contracts. In *Financial Cryptography and Data Security*. Brenner M. (Ed.), Lecture Notes in Computer Science, Vol. 10323, Springer, Cham, 478–493.

Ankur Sharma, Felix Martin Schuhknecht, Divya Agrawal, and Jens Dittrich. 2019. Blurring the lines between blockchains and database systems: The case of hyperledger fabric. In *Proceedings of the 2019 International Conference on Management of Data (SIGMOD '19)*. ACM, New York, NY, 105–122. DOI: https://doi.org/10.1145/3299869.3319883

Gunasekaran Shyam Prabhu, Barbara Muscara, Vipin Rathi, Bilal Saleh, Amandeep Singh, Mathews Thomas, Paulo Zanotto, Sunay Zelawat, Afraz Nima, and Vinay Chaudhary. 2019. Hyperledger-based Solution for Reducing the Cost of Settling Inter-carrier Charges. Retrieved from https://wiki.hyperledger.org/pages/viewpage.action?pageId=16326816

Christophe Sibertin-Blanc. 2001. Cooperative Objects: Principles, Use and Implementation. (2001).

Faisal Tariq, Muhammad R. A. Khandaker, Kai-Kit Wong, Muhammad A. Imran, Mehdi Bennis, and Merouane Debbah. 2020. A speculative study on 6G. *IEEE Wireless Communications* 27 (2020), 118–125. DOI: https://doi.org/10.1109/MWC.001.1900488

ETSI. 2019. *TS 131 121*. Technical Report.

Mark Walport. 2015. Distributed Ledger Technology: Beyond Blockchain. Technical Report. Government Office for Science.

Hao Xu, Lei Zhang, Yinuo Liu, and Bin Cao. 2020. RAFT based wireless blockchain networks in the presence of malicious jamming. *IEEE Wireless Communications Letters* 9, 6 (2020), 817–821. DOI: https://doi.org/10.1109/LWC.2020.2971469

Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. 2019. Blockchain technology overview. arXiv:1906.11078. Retrieved from http://arxiv.org/abs/1906.11078

Mika Ylianttila, Raimo Kantola, Andrei Gurtov, Lozenzo Mucchi, Ian Oppermann, Zheng Yan, Tri Hong Nguyen, Fei Liu, Tharaka Hewa, Madhusanka Liyanage, et al. 2020. 6G White paper: Research challenges for Trust, Security and Privacy. arXiv:2004.11665 [cs.CR]. Retrieved from http://arxiv.org/abs/2004.11665

Seppo Yrjola. 2019. Decentralized 6G business models. In *Proceedings of the 6G Wireless Summit*.

Dmitry A. Zaitsev, Tatiana R. Shmelevaand Zeyu Zhou, and Ding Liu. 2023. Verification of cryptocurrency consensus protocols: reenterable colored Petri net model design. *International Journal of Parallel, Emergent and Distributed Systems* (2023), 32–50. DOI: https://doi.org/10.1080/17445760.2023.2273452

Zhengquan Zhang, Yue Xiao, Zheng Ma, Ming Xiao, Zhiguo Ding, Xianfu Lei, George K. Karagiannidis, and Pingzhi Fan. 2019. 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Vehicular Technology Magazine* 14, 3 (2019), 28–41. DOI: https://doi.org/10.1109/MVT.2019.2921208

Received 31 December 2023; revised 6 December 2024; accepted 7 January 2025