ETSI GS PDL 025 V1.1.1 (2025-05)

Permissioned Distributed Ledger (PDL); Wireless Consensus Network Composition and Organization

Disclaimer

The present document has been produced and approved by the Permissioned Distributed Ledger (PDL) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/PDL-0025_wirelessCN_compo

Keywords
network, PDL, wireless

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

List of Tables

List of Figures

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document presents the architectures and fundamentals of nodes and networks in Wireless Consensus Network (WCN) that can benefit various public and private services. Further the present document also discusses a set of recommendations that can together enable a PDL-based Wireless Consensus Network framework.

Introduction

Wireless Consensus Networks (WCNs) containing numerous PDL nodes can be organized to achieve consensus for various tasks of autonomous systems in wireless environments. While some potential use cases have been discussed in previous group reports, components such as hardware, consensus mechanisms, functions, and interfaces needed to construct each node and an integral WCN require further investigation and discussion.

The present document demonstrates fundamental specifications for node composition and network organization in WCN. Such specifications serve as a general guidance for different stakeholders assisting them to better understand the key elements required to build effective WCNs.

1 Scope

The present document defines the services of Permissioned Distributed Ledger (PDL) platform, which enable wireless distributed consensus for reliable industrial connected autonomous systems. The present document also outlines the composition of wireless consensus nodes and their organizations. Furthermore, it defines a series of consensus patterns and steps to improve reliability and enable fault tolerance.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Kim, Jung Hoon, Byung Wan Jo, Jun Ho Jo, and Do Keun Kim. 2020: "Development of an IoT-Based Construction Worker Physiological Data Monitoring Platform at High Temperatures" Sensors 20, no. 19: 5682.

[i.2] Resnati, Davide, Akira Goda, Gianluca Nicosia, Carmine Miccoli, Alessandro S. Spinelli, and Christian Monzio Compagnoni: "Temperature effects in NAND flash memories: A comparison between 2-D and 3-D arrays". IEEE Electron Device Letters 38, no. 4 (2017): 461-464.

[i.3] Chen, Fei, Bo Chen, Hongzhe Lin, Yachen Kong, Xin Liu, Xuepeng Zhan, and Jiezhi Chen: "Temperature impacts on endurance and read disturbs in charge-trap 3D NAND flash memories". Micromachines 12, no. 10 (2021): 1152.

[i.4] Wang, Zih-Song, Te-Yuan Yin, Tzung-Hua Ying, Ya-Jui Lee, Chieh-Yi Lu, Hideki Arakawa, and Chrong Jung Lin: "Impact of moisture from passivation on endurance and retention of NAND flash memory". IEEE transactions on electron devices 60, no. 1 (2012): 254-259.

[i.5] Maruf, Adnan, Sashri Brahmakshatriya, Baolin Li, Devesh Tiwari, Gang Quan, and Janki Bhimani: "Do temperature and humidity exposures hurt or benefit your SSDs?". In 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 352-357. IEEE, 2022.

[i.6] Yin, M., Malkhi, D., Reiter, M. K., Gueta, G. G., & Abraham, I. (2019): "HotStuff: BFT Consensus with Linearity and Responsiveness". In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing (PODC '19).

[i.7] Castro, M., & Liskov, B. (1999): "Practical Byzantine Fault Tolerance". In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99).

[i.8] Ongaro, D., & Ousterhout, J. (2014): "In Search of an Understandable Consensus Algorithm". In Proceedings of the 2014 USENIX Annual Technical Conference (USENIX ATC '14).

3 Definition of terms, symbols and abbreviations

3.1 Terms

access network based WCN: type of WCN where consensus nodes communicate with each other via wireless access networks such as cellular networks (4G, 5G) or Wi-Fi

Advanced Driver Assistance System (ADAS): technologies that assist drivers in driving and parking functions, often using automated technology like sensors and cameras

blockchain Trilemma: challenge of simultaneously achieving decentralization, security, and scalability in blockchain systems

Byzantine Fault Tolerance (BFT): system's ability to continue operating correctly even when some nodes are malfunctioning or acting maliciously. Distributed computing literature, originated from Leslie Lamport's Byzantine Generals Problem

Consensus Mechanism (CM): protocols used to validate transactions and organize them in a distributed ledger system

Crash Fault Tolerance (CFT): system's ability to continue operating correctly when nodes fail by crashing but do not behave maliciously

HotStuff: leader-based Byzantine fault-tolerant consensus algorithm with linear communication complexity

NOTE: As defined in Maofan Yin et al.'s 2019 paper [i.6].

Permissioned Distributed Ledger (PDL): decentralized network with restricted access where participants have to be authorized, typically governed by a consortium

Practical Byzantine Fault Tolerance (PBFT): specific consensus algorithm that provides Byzantine fault tolerance with high transaction throughput

NOTE: As defined in Miguel Castro and Barbara Liskov's 1999 paper [i.7].

Proof of Authority (PoA): consensus mechanism that relies on a set of approved validators to produce blocks and secure the network

Proof of Stake (PoS): consensus mechanism where validators are selected based on the quantity of cryptocurrency they hold and are willing to "stake"

Proof of Work (PoW): consensus mechanism that requires computational effort to validate transactions and create new blocks. Bitcoin whitepaper by Satoshi Nakamoto

raft: consensus algorithm designed to be more understandable than Paxos, providing crash fault tolerance

NOTE: As defined in Diego Ongaro and John Ousterhout's 2014 paper [i.8].

Selective Edge Decision layer (SED layer): extension of ADAS's decision-making unit allowing WCN to process committed data directly under certain auto-driving conditions

self-organizing WCN: type of WCN where consensus nodes establish direct peer-to-peer connections with other nodes without relying on access points

Trusted Execution Environment (TEE): secure area within a processor that ensures confidentiality and integrity of code and data

Vehicle-to-Everything (V2X): communication technology enabling vehicles to interact with other vehicles, infrastructure, pedestrians, and networks

Wireless Consensus Network (WCN): network where PDL nodes reach consensus via wireless networks rather than traditional wired connections

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
4G	The fourth generation of mobile phone mobile communication technology standards
5G	The fifth generation of mobile phone mobile communication technology standards
ADAS	Advanced Driver Assistance System
ARM	Advanced RISC Machine
BFT	Byzantine Fault Tolerance
CFT	Crash Fault Tolerance
CM	Consensus Mechanism
CPU	Central Processing Unit
ID	Identity
IoT	Internet of Things
IP	Internet Protocol Address
LiDAR	Light Detection and Ranging
LoRa	Long Range
LTE	Long Term Evolution
NAND	NOT AND (memory)
NBIoT	Narrowband Internet of Things
OS	Operational System
PBFT	Practical Byzantine Fault Tolerance
PDL	Permissioned Distributed Ledger
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
PoX	Proof-based Algorithms
PSU	Power Supply Unit
RAM	Random Access Memory
RF	Radio Frequency
RISC	Reduced Instruction Set Computer
RREP	Routing Response Message
RREQ	Routing Request Message
TEE	Trusted Execution Environment
TPS	Transaction Per Second
UART	Universal Asynchronous Receiver and Transmitter
UWB	Ultra Wide Band
V2X	Vehicle to Everything
WCN	Wireless Consensus Network

4 Overview of Wireless Consensus Networks

4.1 Introduction

Permissioned Distributed Ledgers (PDLs), also known as permissioned blockchains, are typical decentralized networks with restricted access. A governing consortium oversees the PDL network, granting specific permissions to authorized participants. These participants identify themselves through digital certificates or other means.

In a PDL network, transactions are validated and organized through consensus among the permitted participants. The data is structured in blocks with each new block linked to the previous via a cryptographic hash. This structure ensures data integrity by creating an immutable and tamper-proof record.

Each participating node in the PDL network maintains a copy of the ledger.

Nodes can act as either:

- Miners (committing nodes): These nodes maintain the ledger and provide essential network support. They participate in the consensus process and commit new blocks of records.
- Clients: These nodes only requests transactions from miner nodes and do not participate in consensus or ledger maintenance.

Traditionally, PDL systems have been designed for stable wired communication networks, assuming sufficient and reliable communication resources. However, the emergence of Wireless Consensus Networks (WCN), where some PDL nodes reach consensus via wireless networks, may pose new challenges for consensus such as unstable wireless connections and the mobility of some PDL nodes.

While wireless networks are widely deployed using various protocols and standards, WCN introduces new challenges that may require adjustments to both network architecture and hardware, as well as to Consensus Mechanisms (CMs) deployed. The present document aims to analyse the WCN paradigm, identifying specifications for future applications. The present document discusses potential specifications and applications of WCN for PDL, covering aspects such as architecture, hardware requirements, consensus mechanisms, and protocols. It defines key components of WCN nodes and outlines how WCNs should be constructed and operated.

4.2 WCN Overall Framework

4.2.1 Background

The organization of a WCN relies on two essential elements: consensus nodes (PDL nodes) and wireless communication methods. Based on the communication methods, WCN frameworks can be categorized into two types:

1) Access network based WCN: Consensus nodes communicate with each other via access networks.
2) Self-organizing WCN: Each consensus node in this type of WCN has the ability to communicate directly with other nodes.

4.2.2 Access network based WCN framework

The first type of WCN framework involves an access network as illustrated in Figure 1. It illustrates four consensus nodes that communicate via wireless access networks such as cellular networks (4G, 5G, etc.) or Wi-Fi networks.

When a node initiates a consensus request, it sends it to other nodes through the access network. All nodes can begin executing the consensus protocol, communicating with each other via that network. Consensus can be reached according to the protocol. All nodes in this WCN can act as PDL nodes, storing the consensus results (transactions) and maintaining the PDL's integrity.

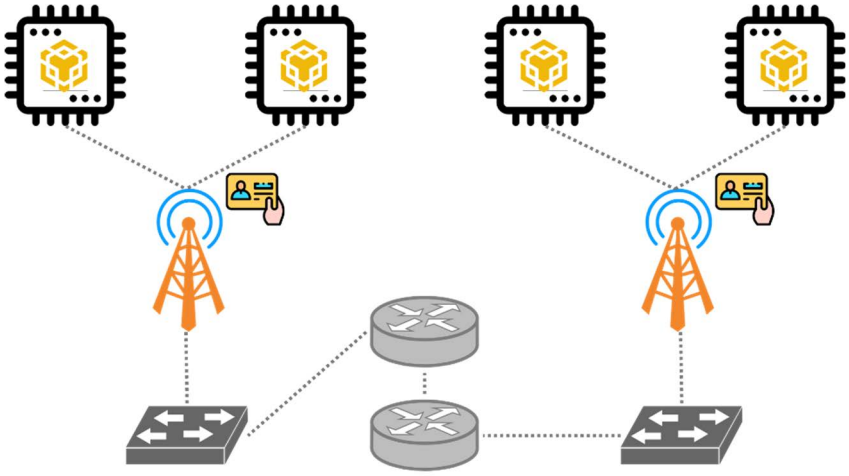

Figure 1: WCN framework based on access network

4.2.3 Self-organizing WCN framework

In a self-organizing WCN, all consensus nodes establish direct connections with other nodes to perform consensus protocol communications. Unlike the access network based framework, there is no access point or wireless communication infrastructure to support communications between consensus nodes, as illustrated in Figure 2.

In this framework, consensus nodes are expected to have peer-to-peer communication capabilities. These capabilities enable them to self-organize into WCNs and perform consensus protocols to maintain the PDL.

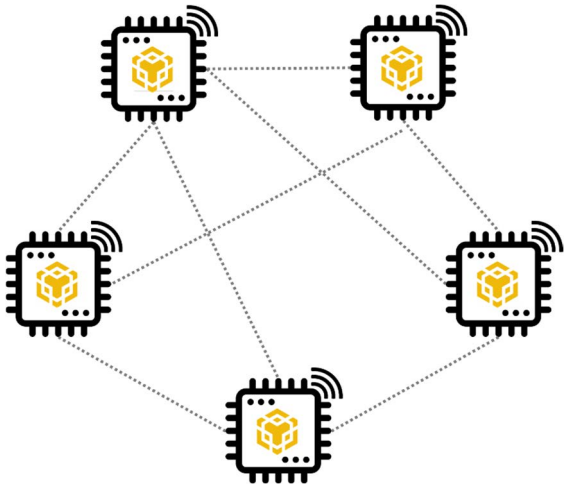

Figure 2: WCN framework based on self-organizing networks

4.3 WCN Applications

4.3.1 Autonomous driving

Wireless Consensus Networks (WCNs) have significant potential in the field of autonomous driving. Figure 3 illustrates an example scenario where WCNs can enhance road safety and vehicle coordination. In this scenario, a motorbike is driving in the blind spot of a truck. If the truck attempts to merge into the right lane without assistance, a collision could occur. However, if the truck, motorbike and three cars in Figure 3 form a WCN, they can reach a consensus regarding the occupancy of the right lane. This consensus would result in declining the truck's request to move into the right lane. Additionally, this lane occupancy information can be recorded in the PDL for nearby vehicles to access.

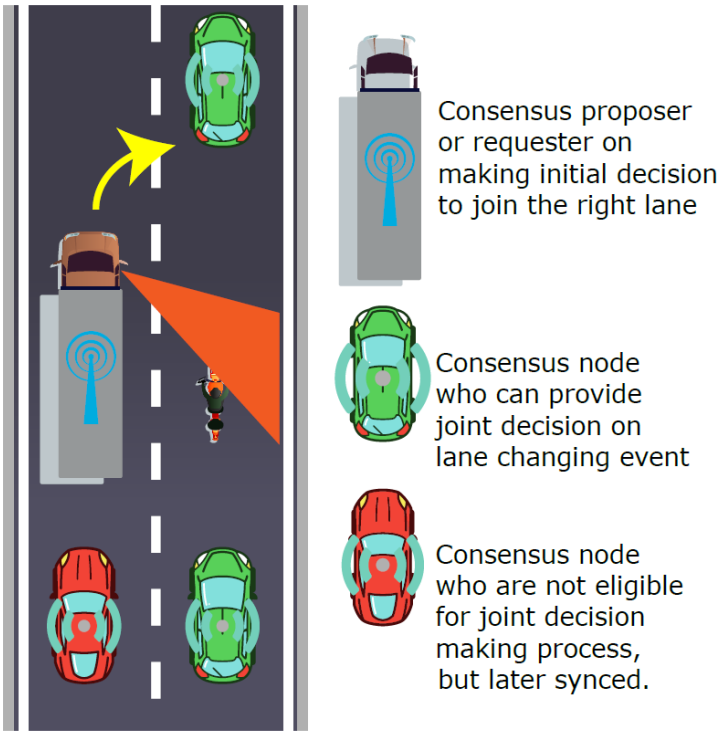

Figure 3: Wireless distributed consensus for traffic decision

The application of WCNs in autonomous driving offers several benefits:

1) **Extended Perception:** Autonomous vehicles can perceive information from other vehicles hundreds of meters away, improving safety and predictability.

2) **Data Sharing:** Vehicles can share various types of data, including:

   - Road conditions obtained after visual image processing
   - Environmental information perceived by LiDAR
   - Alarm information from unstable systems
   - Cooperative operation requests

3) **Predictable Behaviour:** When consensus is reached, the committed data can predictably influence the behaviour of each vehicle in the cluster.

4) **Advanced Driver Assistance System (ADAS) Integration:** WCNs can contribute to ADAS by enhancing environmental perception. ADAS consists of two core parts:

   a) **Perception:** Utilizes a variety of sensors (e.g. millimetre-wave radar, lidar, cameras, and satellite navigation) to sense the surrounding environment. It collects data, identifies objects, and track people and vehicles passing by at any time.

   b) **Decision-making:** Processes and analyses the perceived data.

5) **Execution:** Carries out instructions based on the decision-making process.V2X Services: In the ADAS perception, the vehicle node in the WCN can interact with the in-vehicle ADAS via embedded communication interfaces (e.g. UART or USB) to provide Vehicle-to-Everything (V2X) services under the Raft consensus mechanism.

6) **Data Flow Options:** When consensus is complete, the committed data can flow in two ways:

a) Direct transfer of raw committed data to the ADAS decision-making layer.

b) Use of WCN as a "selective edge decision layer" (SED layer) for ADAS: The SED layer is designed as an extension of the ADAS's decision-making unit. It allows the WCN to have the privilege to process the committed data directly under certain auto-driving conditions. Then, the processed data or control commands are transferred to the ADAS. Such privilege can be activated in some high-order auto-driving scenarios.

By leveraging WCNs, autonomous driving systems can enhance their environmental awareness, decision-making processes, and overall safety. The distributed nature of WCNs paves the way for more advanced and coordinated autonomous driving systems.

4.3.2 Sensor and IoT networks

The application of WCNs in sensor or IoT networks offers several benefits:

1) **Data Sharing:** Sensors or IoT devices can share various types of data, including:

   - Environmental information from sensors
   - Working progress
   - Cooperative operation requests

2) **Anomaly detection:**

   - The leader node can confirm the live status of other nodes in the network using consensus, then record and report the abnormal nodes to the system administrator. For instance, in an underwater sensor network, the administrator can retrieve the live status of each sensor from the leader sensor node instead of communicating with each sensor to confirm its working status.
   - Abnormal variance of environmental elements in the network operating environment can be detected by the WCN if some nodes achieve consensus on huge variance of certain environmental elements.

4.4 Relations between Composition and Organization

4.4.1 Aspects

The effectiveness and efficiency of Wireless Consensus Networks (WCNs) depend on two crucial aspects: the composition of individual nodes and the organization of the network as a whole. These aspects are closely interrelated and are addressed in detail in the following two clauses of the present document.

Understanding this relationship is crucial for designing and implementing effective WCNs. The following clauses explore these aspects in detail, providing a comprehensive framework for WCN development and deployment.

4.4.2 Composition

The composition of WCN nodes is critical because nodes may transfer between different WCNs. To ensure seamless integration and operation across various networks, the capabilities of each node to achieve consensus need to be standardized. Clause 5 delves into the composition specifications, covering three main aspects:

1) **Hardware:** The physical components required for a node to function effectively in a WCN.

2) **Functionality:** The software and operational capabilities that enable a node to participate in consensus mechanisms.

3) **Reliability:** The measures and features that ensure consistent and dependable node performance.

These specifications aim to create a baseline for node capabilities, allowing for interoperability and consistent performance across different WCN implementations.

4.4.3 Organization

While individual node capabilities are crucial, the way these nodes interact and form a network is equally important. Clause 6 focuses on the organizational specifications of WCNs, specifying:

1) **Behaviour:** How nodes should act within the network, including roles they may take on and how they respond to different network events.

2) **Interfaces:** The standardized ways in which nodes communicate with each other and with external systems.

These organizational specifications are essential because nodes in WCNs rely on the network structure to communicate with other nodes for consensus. A well-defined organization ensures efficient communication, robust consensus mechanisms, and effective management of the overall network.

4.4.4 Interdependence

The composition and organization of WCNs are inherently linked. The capabilities defined in the composition specifications enable the behaviours and interactions outlined in the organization specifications. Conversely, the organizational requirements inform the necessary capabilities of individual nodes.

For example, a node's hardware specifications (composition) determine its ability to handle the communication load required by the network's routing protocols (organization). Similarly, the consensus mechanism chosen for the network (organization) influences the computational resources needed in each node (composition).

5 WCN Composition Specifications

5.1 General Composition Requirements

5.1.1 Introduction to Composition

The composition of Wireless Consensus Networks (WCNs) varies depending on the type of network. This clause outlines the general requirements for both access network based WCNs and self-organizing WCNs.

5.1.2 Access network based WCN components

5.1.2.1 Consensus node (PDL node)

5.1.2.1.1 The Primary function of a Consensus node

The consensus node (PDL node) executes the consensus protocol algorithms and maintains the Permissioned Distributed Ledger through dedicated computational and communication resources. It processes transaction requests, participates in the voting process for transaction validation, and stores the agreed-upon transaction records in its local copy of the distributed ledger. This node is responsible for ensuring data consistency across the network while accommodating the constraints of wireless communications.

5.1.2.1.2 Key Components of a Consensus node

The key components of a Consensus node are:

- **Storage:** Enables the node to keep consensus status and PDL transactions.
- **Power supply:** Batteries and PSU (power supply unit from wired grids) providing power for computation, communication, and storage hardware.

5.1.2.2 Access point

An access point can accept connections from consensus nodes to allow them to join the WCN network.

5.1.2.3 Wireless communication infrastructure

The infrastructure supports communications among consensus nodes to achieve consensus.

5.1.2.4 Membership service provider

1) Issues membership certifications to consensus nodes.
2) Verifies the memberships of consensus nodes when they attempt to connect through access points.

5.1.3 Self-organizing WCN

5.1.3.1 Components of a Self-organizing WCN

5.1.3.1.1 Computational resource

Used to process consensus data and perform communication tasks.

5.1.3.1.2 Communication resource

Wireless communication hardware that performs the following functions:

- Establishes connections with other nodes.
- Facilitates joining and organizing WCN with other consensus nodes.

5.1.3.1.3 Storage

Non-volatile memory (NAND flash recommended) that stores consensus status and PDL transactions.

5.1.3.1.4 Power supply

Batteries and Power Supply Unit (PSU) providing power for computation, communication, and storage hardware.

5.2 Hardware Specifications

5.2.1 Computational Hardware

5.2.1.1 PDL node

[D1] The computational hardware of each PDL (consensus) node **SHOULD** have the capability to resolve and process consensus information and then generate consensus results.

5.2.1.2 Communication node

[D2] The computational hardware of each communication node **SHOULD** have the capability to resolve and repack data packets from/to consensus nodes, and to resolve and execute received communicating commands.

5.2.2 Communication Hardware

5.2.2.1 PDL node

[D3] The communication hardware of each PDL (consensus) node **SHOULD** have the capability to:

- send and receive data packets to/from access points or other consensus nodes;

- establish and maintain communication links with access points or other consensus nodes.

5.2.2.2 Communication node

[D4] The communication hardware of each communication node **SHOULD** have the capability to:

- send, receive and forward data packets to/from access points or other consensus nodes;
- establish and maintain communication links with access points or other consensus nodes;
- route a PDL node to another one in the same WCN network.

5.2.3 Storage Hardware

[D5] There are two types of storage hardware that each PDL node **SHOULD** contain:

- Temporary storage: used to save the temporary data generated by the computational components in communications and processing consensus.
- Persistent storage: used to store the consensus results and other essential data for the PDL node's operation.

[D6] Temporary storage **SHOULD** build on volatile memory and DRAM (dynamic random-access memory) is recommended typically.

[D7] Persistent storage **SHOULD** use non-volatile memory to ensure the stored data can be accessed permanently. Considering physical size, anti-vibration, noise, transmission speed, volume and cost, NAND flash is recommended as the persistent storage in PDL nodes.

5.3 Functional Specifications

5.3.1 Consensus Mechanism

5.3.1.1 Challenges in design of an effective consensus mechanism

The consensus mechanism is a critical component of Wireless Consensus Networks (WCNs) and blockchain systems in general. However, designing an effective consensus mechanism involves addressing the "Trilemma" problem, also known as the "impossible triangle" problem.

5.3.1.2 The Blockchain Trilemma

The blockchain trilemma refers to the challenge of simultaneously achieving three key characteristics in consensus mechanisms:

1) Decentralization
2) Security
3) Scalability

Figure 4 illustrates this concept. The following clauses explore these characteristics.

1) Decentralization:
   - **Definition:** The extent to which the system allows open participation in the production and verification processes.
   - **Implication:** A higher number of nodes typically indicates a greater degree of decentralization.
   - **Significance:** This is a core feature distinguishing blockchain from traditional centralized systems.

2) Security:

- **Definition:** The cost and difficulty of gaining control over the blockchain system.
- **Implication:** Higher computational and communication costs generally lead to increased security.
- **Significance:** Security forms the basis for reaching consensus among participants in blockchain systems.

3) Scalability:

- **Definition:** The system's capacity to process transaction information efficiently.
- **Measurement:** Often quantified by TPS (transactions per second).
- **Significance:** Scalability is crucial for the practical application of blockchain systems in real-world scenarios.

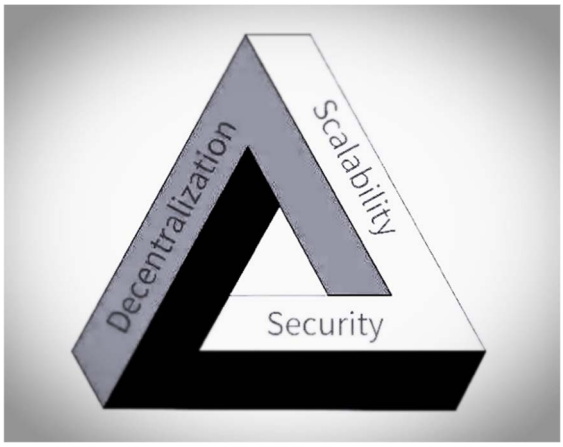

Figure 4: Consensus trilemma: decentralization, scalability and security

5.3.1.3 Challenges and Trade-offs

The trilemma posits that optimizing all three characteristics simultaneously is extremely challenging. Current blockchain systems often struggle to achieve high levels of scalability while maintaining strong decentralization and security.

Key points to consider:

1) **Independence of characteristics:** Each characteristic has its own technological development path. Sacrificing one does not automatically enhance another.

2) **Fundamental requirements:** Decentralization and security are essential for constructing a viable blockchain system. Without them, the system risks becoming insecure or autocratic.

3) **Focus on scalability:** Many blockchain systems prioritize improving TPS to enhance overall system performance, as scalability often presents the most significant barrier to practical applications.

4) **Ongoing research:** The blockchain community continues to explore innovative solutions to break through the trilemma, aiming to create systems that balance all three characteristics effectively.

For WCNs, addressing the trilemma is particularly important due to the unique challenges posed by wireless environments. Designers of WCN consensus mechanisms should carefully consider these trade-offs and strive to optimize the balance between decentralization, security, and scalability based on the specific requirements of their application.

5.3.2 Security

5.3.2.1 Software Security

5.3.2.1.1 System and Application

[R1] The components of the deployed systems in WCN **SHALL** have security precautions in both design and implementation against malicious exploitations via stacks and heaps in memory.

[D8] The applications used in the system **SHOULD** have security precautions against malicious exploitations to avoid sabotage of applications and privilege escalations leading to the compromise of the system.

5.3.2.1.2 Run-time and Execution Environment

[D9] The run-time environments of applications **SHOULD** have security precautions against malicious exploitations to avoid sabotage of the run-time environments and privilege escalations leading to the compromise of the system.

[D10] The execution environments of instructions for computation and communication SHOULD have security precautions against insertion of illegal instructions and unauthorized instruction manipulations.

5.3.2.1.3 Vulnerability Fixing

[D11] The system and applications **SHOULD** have the capability to update the components of themselves to fix internal vulnerabilities or cope with emerging security threats.

5.3.2.2 Hardware Security

[D12] On-chip Trusted Execution Environment (TEE) **SHOULD** be implemented on each WCN node to protect other hardware components in bootstrap and support run-time and execution environments for system components and applications.

[D13] Hardware debug interfaces **SHOULD** be pre-set on each WCN node for the use of factory test and in-use debug by technicians.

[O1] Physical protection of the hardware of WCN nodes **MAY** be considered to avoid unauthorized break or disassembling of hardware.

5.4 Reliability

5.4.1 Reliability of Individual Component

5.4.1.1 Computation Working Conditions

WCN nodes are designed to operate reliably under specified computation working conditions.

a) **Electromagnetic interference:**

[R2] The WCN nodes **SHALL** comply with applicable Electromagnetic Compatibility (EMC) requirements. The equipment **SHALL** operate as intended in the presence of electromagnetic disturbances and **SHALL NOT** generate electromagnetic disturbances that may affect other equipment.

[O2] Extra precautions **MAY** be required for WCN nodes deployed in certain extreme environments such as nuclear environments to prevent strong EMC.

b) **Temperature**:

[R3] The WCN nodes **SHALL** be capable of operating within a temperature range of -40 °C to +70 °C for outdoor deployments, and 0 °C to +45 °C for indoor deployments [i.1].

[O3] Extra precautions **MAY** be required for WCN nodes deployed in certain extreme environments such as extreme high-temperature environments to ensure proper operation of WCN nodes.

5.4.1.2 Communication Working Conditions

[R4] The WCN communication subsystem **SHALL** maintain reliable operation under specified communication working conditions.

[R5] The communication subsystem **SHALL** be designed to operate within specified limits for conducted and radiated emissions. It shall also demonstrate immunity to electrostatic discharge, radiated Radio-Frequency (RF), electromagnetic fields, and electrical fast transients.

In the case the WCN is intended for uses in specific industries, standards of the applied industry should be adopted to provide better electromagnetic protection.

5.4.1.3 Storage Working Condition

[R6] The storage components of WCN nodes **SHALL** be designed to operate reliably under specified storage working conditions to reflect its working condition for critical missions.

a) **Electromagnetic interference:**

[R7] Storage systems **SHALL** be protected against electromagnetic disturbances that could affect data integrity or system performance.

b) **Temperature:**

[D14] Storage components **SHOULD** operate within a temperature range of -30 °C to +40 °C [i.2], [i.3].

[O4] Extra precautions **MAY** be required to ensure the usability of the storage device in extreme temperature environments e.g. temperature below -30 °C or over 40 °C [i.2].

c) **Humidity:**

[D15] Storage systems **SHOULD** be designed to operate in relative humidity conditions ranging from 0 % to 100 %, and suitable for naval uses [i.4], [i.5].

[O5] Extra precautions **MAY** be required to ensure the usability of the storage device in extreme humidity environments e.g. humidity over 80 % [i.5].

d) **Vibration and pressure:**

[D16] Storage components **SHOULD** withstand mechanical vibration with a frequency range from low to very high frequency mechanical vibrations and a peak acceleration of the maximum value from applied use case.

[O6] They **MAY** also operate at altitudes up to 3 000 m above sea level with extra precautions.

e) **Power supply resilience:**

1) Power loss protection:

[R8] The data storage system **SHALL** maintain data integrity and accessibility in the event of an unexpected power loss.

2) Backup power duration:

[R9] The storage system **SHALL** be equipped with a backup power source (e.g. capacitors, batteries) capable of supplying power for a duration not less than T, where $T = T_c + T_a$, T_c is the time required to complete the current system synchronization, and T_a is the time required to perform a graceful abortion action.

[R10] The values of T_c and T_a **SHALL** be configurable based on the current consensus group requirements and system characteristics.

3) Synchronization completion:

[R11] The system **SHALL** ensure that all ongoing write operations and data synchronizations are completed before initiating the abortion action.

4) Graceful shutdown:

[R12] In the event of extended power loss beyond the backup power duration, the storage system **SHALL** perform a graceful shutdown procedure to prevent consensus disruption by initiating Leave Group procedure.

5) Recovery mechanism:

[R13] Upon power restoration, the storage system **SHALL** implement a recovery mechanism to verify data integrity of current node by comparing the record on the PDL and update the latest PDL records before resuming normal operations.

5.4.2 Reliability of Systems

5.4.2.1 Consensus Tolerance

The reliability of the WCN system depends on the consensus tolerance of the applied consensus mechanism. Specifically, the number of failed nodes or malicious nodes that the WCN system can tolerate determines the different levels of system reliability.

The reliability of the WCN system depends on the consensus tolerance of the applied consensus mechanism.

[R14] The WCN system **SHALL** define and implement a consensus mechanism that specifies the maximum number of failed or malicious nodes that can be tolerated while maintaining system reliability.

[R15] The consensus mechanism **SHALL** ensure that the system remains operational and maintains data consistency in the presence of the specified number of faulty nodes.

[R16] The choice between CFT and BFT **SHOULD** be based on the threat model and reliability requirements of the specific WCN deployment.

5.4.2.2 Crash Fault Tolerance vs. Byzantine Fault Tolerance

[R17] The WCN system **SHALL** implement either Crash Fault Tolerance (CFT) or Byzantine Fault Tolerance (BFT) based on security requirements of deployment scenarios. Some prevalent consensus mechanisms and their comparisons are listed below shown in Table 1.

a) Crash Fault Tolerance (CFT):

[R18] A CFT-based system **SHALL** tolerate faulty nodes in a network of $n = 2f + 1$ total nodes.

[R19] The system **SHALL** maintain liveness and safety properties as long as a majority of nodes are operational.

b) Byzantine Fault Tolerance (BFT):

[R20] A BFT-based system **SHALL** tolerate Byzantine faulty nodes in a network of $n = 3f + 1$ total nodes.

[R21] The system **SHALL** maintain liveness and safety properties as long as at least two-thirds of the nodes are honest and operational.

Table 1: Performance comparison of commonly used CMs

CM	Ledger type	Transaction throughput	Scalability	Security bound	Communication complexity	Spectrum requirement	Representative project	Latency	Sensitivity to communication fault
PBFT	Permissioned	High	Low	$3f+1$	$2N^2+N$	$2N+1$	Hyperledger Fabric	Medium	Low
HotStuff	Permissioned	High	Medium	$2f+1$	$2N$	$N+1$		Low	Medium
Raft	Permissioned	Very high	Medium	$2f+1$	$2N$	$N+1$	Quorum	Low	Medium
PoW	Permissionless	Low	High	$2f+1$	$2N$	2	Bitcoin, Ethereum	High	High
PoS	Permissionless	Low	High	$2f+1$	$2N$	2		High	High
PoA	Permissioned	Medium	High	$2f+1$	$2N$	2		High	High

5.4.2.3 Tolerance Analysis for Reliability

[D17] The WCN system **SHOULD** undergo a comprehensive tolerance analysis to ensure reliability.

[D18] The analysis **SHOULD** consider:

1) The expected failure rate of individual nodes.
2) The network topology and communication patterns.
3) The consensus mechanism employed (CFT or BFT).
4) The required system availability and consistency guarantees.

[D19] Based on the tolerance analysis, the WCN **SHOULD** implement appropriate redundancy measures including:

1) Node replication.
2) Data replication across multiple nodes.
3) Backup communication channels.

[D20] The system **SHOULD** provide mechanisms for graceful degradation in case of partial system failure, maintaining essential functionalities even when operating with a reduced number of nodes.

6 WCN Organization Specifications

6.1 General Organizational Requirement

6.1.1 Introduction to organization

The organization of Wireless Consensus Networks (WCNs) varies depending on the type of network. This clause outlines the general requirements for both access network based WCNs and self-organizing WCNs.

6.1.2 Access network based WCN

6.1.2.1 Group management

For each WCN node, the following requirements of group management are considered:

- Creating and discovering a group
- Joining and leaving a group
- Modifying and removing a group
- Node behaviour of leader and followers in a group

6.1.2.2 Interface

For each WCN node, the following requirements of interface are considered:

- Peer synchronization
- Consensus state synchronization

6.1.3 Self-organizing WCN

6.1.3.1 Group management

For each WCN node, the following requirements of group management are considered:

- Creating and discovering a group
- Joining and leaving a group
- Modifying and Removing a group
- Node behaviour of leader and followers in a group

6.1.3.2 Interface

For each WCN node, the following requirements of interface are considered:

- Peer routing
- Peer synchronization
- Consensus state synchronization

6.2 Group Management Specifications

6.2.1 State Description

[D21] The node state of consensus **SHOULD** include:

a) Persistent state on all nodes:

T: Current Term of consensus

VF: Candidate ID that this node vote for

LOG: Log entries which contain the commands and corresponding term

b) Volatile state on all states of nodes/candidates:

CI: Index of highest log entry that is committed

AI: Index of highest log entry applied to state

c) Volatile state on leader (Reinitialized after the stage of election):

NI: Index of next log entry send to nodes

MI: Index of highest log entry replicated on server (matched)

6.2.2 Discovering and Creating a Group

6.2.2.1 For consensus nodes in access network based WCN

[R22] A consensus node **SHALL** have the capability to discover existing consensus groups via the access point.

[R23] A consensus node **SHALL** have the capability to create a consensus group and broadcast this group to the whole network via the access point.

6.2.2.2 For consensus nodes in self-organizing WCN

[R24] A consensus node **SHALL** have the capacity to discover the current consensus group via its neighbour nodes.

[R25] When a consensus node is the leader node, it **SHALL** have the capacity to create a consensus group and broadcast the group in the network.

6.2.3 Joining and Leaving a Group

6.2.3.1 For consensus nodes in access network based WCN

[D22] A consensus node **SHOULD** have the capability to send messages to request to join a consensus group via the access point.

[R26] A consensus node **SHALL** have the capability to send messages to:

1) leave the current consensus task;
2) not participate in a new consensus task;
3) leave the current consensus group via the access point.

[R27] For the leader node, it **SHALL** have the capability to send messages to:

1) start the leader election process when it leaves the current group or joins another group;
2) cancel the current consensus task or hand over the current consensus task to the new leader;
3) not start a new consensus task;
4) leave the current consensus group via the access point.

6.2.3.2 For consensus nodes in self-organizing WCN

[R28] A consensus node **SHALL** have the capacity to join the current consensus group via its neighbour nodes.

[D23] When a leader node is leaving, it SHOULD have the capacity to broadcast messages to:

1) start the leader election process;
2) cancel the current consensus task or hand over the current consensus task to the new leader;

3) not start a new consensus task;

4) leave the current consensus group.

6.2.4 Modifying and Removing an Existing Group

6.2.4.1 For leader nodes in access network based WCN

[R29] A leader node **SHALL** have the capability to broadcast messages to allow new nodes to join its managed consensus group via the access point.

[R30] A leader node **SHALL** have the capability to broadcast messages to remove the current consensus group if:

1) there is no on-going consensus task;

2) there are no other consensus nodes in the current group.

6.2.4.2 For leader nodes in self-organizing WCN

[R31] A leader node **SHALL** have the capacity to allow new nodes to join the current consensus group by the broadcasted joining messages from the new node and its neighbour nodes.

[R32] A leader node **SHALL** have the capability to broadcast messages to remove the current consensus group if:

1) there is no on-going consensus task;

2) there are no other consensus nodes in the current group.

6.2.5 Contingency Group Management

6.2.5.1 Access network based WCN

[R33] When a node loses the connection to the access network, it **SHALL** save the state of the current consensus task and the peer status and wait for the next state and peer synchronizations.

[R34] When a node received the notification of leader exiting or cannot receive the response from the leader node in a pre-set time interval, it **SHALL** save the state of the current consensus task and the peer status and wait for the next state and peer synchronizations.

[R35] If the state synchronization cannot recover the current consensus task or the leader is changed after the peer synchronization, a node **SHALL** response a disapproval of the current consensus task to the leader and wait for the next state synchronization.

[R36] Each node **SHALL** have a consist strategy to select a new leader based on the current peer status when the new leader election process is interrupted.

6.2.5.2 Self-organizing WCN

[R37] When a node received the notification of leader exiting or cannot receive the response from the leader node in a pre-set time interval, it **SHALL** save the state of the current consensus task and the peer status and wait for the next state and peer synchronizations.

[R38] If the state synchronization cannot recover the current consensus task or the leader is changed after the peer synchronization, a node **SHALL** response a disapproval of the current consensus task to the leader and wait for the next state synchronization.

[R39] Each node **SHALL** have a consist strategy to select a new leader based on the current peer status when the new leader election process is interrupted.

6.2.6 Organizational Security

[R40] In the access network based WCN, the access network **SHALL** have the capability to authorize the nodes to join the WCN.

[R41] The self-organizing WCN **SHALL** block new nodes using duplicated identifiers within the current WCN to join to avoid sybil attack.

[D23] In the access network based WCN, the access network **SHOULD** have the capability to reject nodes with duplicated identifiers to join to avoid sybil attack.

[R42] A WCN **SHALL** have the capability to detect nodes with duplicated identifiers and remove them except the oldest one based on the existing time.

[D24] A node **SHOULD NOT** change its identifier after joining a WCN.

6.3 Interface Specifications

6.3.1 Peering Interface

6.3.1.1 Access network based WCN

[R43] Each node **SHALL** implement the interface to organize the peering information for broadcast.

[R44] Each node **SHALL** implement the interface to resolve the received peering information and update the peering status.

6.3.1.2 Self-organizing WCN

[R45] Each node **SHALL** implement the interface to forward the received broadcasting peer information to its neighbour nodes and the two interfaces mentioned in clause 6.3.1.1).

6.3.2 Routing Interface

6.3.2.1 Routing protocols

Routing protocols in Wireless Consensus Networks (WCNs) play a crucial role in two specific scenarios:

a) New Node Integration: when a new node aims to join the WCN but cannot establish a direct connection to the current leader.

b) Failed Node Synchronization: when a node that failed during log replication needs to synchronize its state after the replication process.

In both cases, routing protocols enable nodes to connect with the leader through intermediate nodes, as illustrated in Figure 5.

6.3.2.2 Routing (RREQ) Initiation Process

When a new node (the source node in example a in the diagram below) wants to join the WCN but cannot directly connect to the current leader it initiates the routing process by broadcasting a Routing Request (RREQ) message to its neighbouring nodes.

The RREQ message contains the following components:

- **SA:** Source Address - the address of source node
- **PR:** Permission Request - Details of the request to join the network
- **HN:** Hop Number - The number of hops the message has travelled

- **RID:** RREQ Identity - A unique identifier for the request

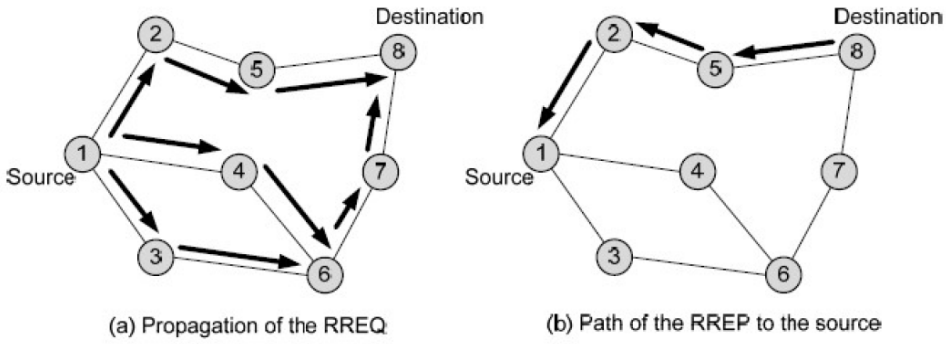

Figure 5: Routing protocol

6.3.2.3 RREQ Handling by Intermediate Nodes

When a node receives an RREQ:

1) It checks if this is the first time it has received this particular request by examining the RID.
2) If it is a new request, the node:
   - Records the routing information (SA, RID).
   - Increments the HN by 1.
   - Forwards the updated RREQ to its neighbouring nodes.
   - Sends a Routing Response (RREP) message back to the node that sent the RREQ, establishing a temporary reverse routing path.
3) If it is a duplicate request, the node ignores it.

6.3.2.4 Leader Node Response

When the RREQ reaches the current term leader:

1) The leader verifies if the source node has permission to join the network.
2) If approved, the leader:
   - Registers the source node in the current distributed network for the next round of log replication.
   - Sends back an acknowledgment.

6.3.2.5 Direct Leader Communication

It is important to note that in the Raft consensus protocol, followers maintain direct connections to the leader. Therefore:

- If any follower receives an RREQ, it can forward the request directly to the leader and establish a valid path.
- This direct communication helps maintain the network's efficiency and responsiveness.

6.3.2.6 Fault Tolerance Consideration

[D25] To maintain the fault tolerance properties of the Raft protocol, the number of nodes implementing routing protocols **SHOULD NOT** exceed half of the total number of nodes in the network.

By implementing this routing interface, WCNs can efficiently handle node integration and synchronization, even when direct connections to the leader are not immediately available. This approach enhances the network's flexibility and resilience while maintaining the integrity of the consensus process.

6.3.3 State Synchronization Interface

6.3.3.1 Leader node

[R46] To process a consensus task, the leader node **SHALL** implement different interfaces to broadcast voting messages in different consensus phases.

[R47] To conclude a consensus task, the leader node **SHALL** implement an interface of collecting voting results to determine the final consensus result.

[R48] To continue a consensus task after interruption or involve new follower nodes, the leader node **SHALL** implement an interface of state synchronization to synchronize the consensus state of the current task with other follower nodes or synchronize the consensus ledgers with new followers.

[R49] The leader node **SHALL** implement the following interfaces for role switch between leader and follower:

- Notification of changing leader
- Broadcasting messages of new leader election
- Collecting response of new leader election messages from followers and determining the new leader
- Switching node roles and updating peer status

6.3.3.2 Follower node

[R50] To process a consensus task, the follower node **SHALL** implement different interfaces to receive the voting messages from the leader in different consensus phases.

[R51] To conclude a consensus task, the follower node **SHALL** implement an interface to respond its voting decision to the leader node based on the received voting messages.

[R52] The follower node **SHALL** implement the following interfaces for role switch between leader and follower:

- Receiving notification of changing leader
- Responding messages of new leader election to the leader node
- Switching node roles and updating peer status

6.3.4 Communication Interface

6.3.4.1 General

[R53] A WCN node **SHALL** have the communication interface to transfer data to other nodes.

[R54] A WCN node **SHALL** have the communication interface to receive data from other nodes.

[R55] The communication interface for broadcasting the change of the node's identifier **SHALL NOT** be provided in WCNs.

6.3.4.2 Self-organizing

[R56] For nodes in self-organizing WCNs, the communication interfaces **SHALL** be implemented to:

- Broadcast and receive routing information;
- Broadcast and receive peering information;

- Broadcast, forward and receive state synchronization information.

[D26] For nodes in self-organizing WCNs, the communication interfaces **SHOULD** be implemented to transmit other essential data/information for the WCN operation.

6.3.4.3 Access Network based Organizing

[R57] For nodes in access network based WCNs, the communication interfaces **SHALL** be implemented to:

- Broadcast and receive peering information;
- Broadcast and receive state synchronization information.

[R58] The communication interface for node authentication **SHALL** be implemented to authorize the node's identification when it is joining the access network based WCN.

[D27] For nodes in access network based WCNs, the communication interfaces **SHOULD** be implemented to transmit other essential data/information for the WCN operation.

6.3.5 Time Synchronization Interface

6.3.5.1 General

[D28] A general time synchronization interface **SHOULD** be implemented for the operational system (OS) of the WCN node to synchronize time with the clock generator in the node.

6.3.5.2 Self-organizing

[D29] The time synchronization interface **SHOULD** be implemented for WCN nodes to synchronize time with other nodes via communication.

6.3.5.3 Access Network based Organizing

[D30] The time synchronization interface **SHOULD** be implemented for WCN nodes to synchronize time with the time servers through the access network.

[O7] The time synchronization interface **MAY** be implemented for WCN nodes to synchronize time with other nodes via communication.

7 Conclusion and Recommendation

7.1 Conclusion

The present document discusses the specifications of constructing wireless consensus networks. It first describes the background and two use cases of WCN with two WCN architectures presented. Then, the composition and organization of WCN nodes and networks with consideration to their functionalities are specified. The hardware conditions and consensus protocols that may be involved in WCNs are discussed. Finally, recommendations for the next step are included.

Overall, each WCN node should have the capable computational resources to process data for the system operation and consensus communication. For instance, some CPUs with ARM architecture or other RISC/CISC architectures and enough RAM can be considered as the capable computational resources for the WCN node. As for the communication to achieve wireless consensus, numerous measurements can be considers including Wi-Fi, LoRa, UWB, NearLink, NBIoT, etc. depending on the communication distance in the practical environment for WCN deployments. The employed consensus mechanism should be lightweight for resource-constrained WCN node to use such as Raft and Hotstuff.

7.2 Recommendations for the Next Step

Since different consensus protocols and hardware for wireless networks with different computing and communication overhead are still evolving, it is out of the scope of ETSI ISG PDL to define a particular wireless consensus network with specific technology. More creative and lightweight approaches should be developed for PoS based consensus, such as Proof of Honesty (putting reputation as stake) and PBFT consensus such as PBFT with multiple layers. However, the following aspects could be considered for standardization by ETSI ISG PDL:

- Specifications on the protocols of wireless consensus network could be developed.
- Specifications on the access control of wireless consensus network could be developed.

History

Document history		
V1.1.1	May 2025	Publication