ETSI GR PDL 020 V1.1.1 (2023-06)

Permissioned Distributed Ledger (PDL); Wireless Consensus Network

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
DGR/PDL-0020_Wireless_consens

Keywords
network management, PDL, wireless,
wireless ad-hoc network

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

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

Modal verbs terminology

In the present document "**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 fundamentals and potential applications of decentralized identification that can benefit various public and private services. Further present document also discusses a set of PDL services that can together enable a PDL based Wireless Consensus Network framework.

Introduction

Consensus is a fundamental component of PDL, critical when updating ledgers with new transactions and ensuring ledgers are synchronized and consistent. Current studies related to PDL and consensus have not considered the network infrastructure (i.e. wired or wireless) and assume network communications is reliable and error-free [i.3]. However, in practical terms communication errors may occur during consensus process because of network infrastructure conditions especially when wireless networks are in use. Wireless networks are less stable and less reliable than wired networks due to interferences and obstacles in space. Meanwhile, compared with wired networks, wireless networks can be more dynamic since wireless nodes (such as mobile devices) can join or leave a network without the need for physical connections or disconnection of devices. Therefore, the use of Wireless Consensus Networks (WCNs) for consensus between nodes (which can be a mix of mobile and static devices) could pose challenges. This study provides an overview of wireless consensus network approaches that can offer benefits to certain services. Various factors such as the requirements and architectures of WCNs, consensus mechanisms, hardware, protocols used to realize WCNs are analysed. In addition, this study also demonstrates some use cases based on WCNs.

A consensus network is used to achiever two primary goals:

a) to ensure a consensus on content of data among nodes in a distributed system exists; and

b) to reach an agreement on a proposal.

It is expected to be fault tolerant, scalable, secure, democratic, and privacy-preserving to serve as an auditable tool in scenarios where data integrity should be preserved and recorded (e.g. when investigating events related to autonomous driving). Furthermore, a consensus network also serves as the backbone of distributed systems such as PDL. The present document discusses the challenges of maintaining sufficient quality of the above metrics when the consensus network is operated over fully or partially wireless infrastructure, hence becoming a WCN.

1 Scope

The present document investigates the following aspects related to wireless consensus network:

- Use cases of wireless consensus networks.
- Wireless consensus network architecture.
- Methods to construct wireless consensus networks:
  - MAC and physical layers.
  - Decentralized/Centralized communication.
- Performance metrics of consensus mechanisms/protocols.
- Protocols to construct wireless consensus networks.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Xu H., Fan Y., Li W. & Zhang L. (2022): "Wireless Distributed Consensus for Connected Autonomous Systems". IEEE™ Internet of Things Journal, doi: 10.1109/JIOT.2022.3229746.

[i.2] Sae International (2018): "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles".

[i.3] Shi Y., Zhou Y., & Shi, Y. (2021, July): "Over-the-air decentralized federated learning". In 2021 IEEE International Symposium on Information Theory (ISIT) (pp. 455-460). IEEE™.

[i.4] Hu Z., Shen J., Guo S., Zhang X., Zhong Z., Chen Q. A. & Li K. (2022, January): "Pass: A system-driven evaluation platform for autonomous driving safety and security". In NDSS Workshop on Automotive and Autonomous Vehicle Security (AutoSec).

[i.5] Feng C., Xu Z., Zhu X., Klaine P. V. & Zhang L. (2023): "Wireless Distributed Consensus in Vehicle to Vehicle Networks for Autonomous Driving", IEEE™ Transactions on Vehicular Technology.

[i.6] Sun Y., Zhang L., Feng G., Yang B., Cao B. & Imran M. A. (2019): "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment", IEEE™ Internet of Things Journal, 6(3), 5791-5802.

[i.7] Zhang L., Xu H., Onireti O., Imran M. A. & Cao, B. (2021): "How much communication resource is needed to run a wireless blockchain network?", IEEE™ network, 36(1), 128-135.

[i.8] Li W., Feng C., Zhang L., Xu H., Cao B. & Imran M. A. (2020): "A scalable multi-layer PBFT consensus for blockchain", IEEE™ Transactions on Parallel and Distributed Systems, 32(5), 1146-1160.

[i.9] Williamson T. & Spencer N. A. (1989): "Development and operation of the traffic alert and collision avoidance system (TCAS)", Proceedings of the IEEE™, 77(11), 1735-1744.

[i.10] Isermann R., Schwarz R. & Stolzl S. (2002): "Fault-tolerant drive-by-wire systems", IEEE™ Control Systems Magazine, 22(5), 64-81.

[i.11] Patterson D. A., Gibson G. & Katz R. H. (1988, June): "A case for redundant arrays of inexpensive disks (RAID)". In Proceedings of the 1988 ACM SIGMOD international conference on Management of data (pp. 109-116).

[i.12] Vukadinovic V., Bakowski K., Marsch P., Garcia I. D., Xu H., Sybis M., ... & Thibault I. (2018): "3GPP C-V2X and IEEE™ 802.11 p for Vehicle-to-Vehicle communications in highway platooning scenarios". Ad Hoc Networks, 74, 17-29.

[i.13] McKeen F., Alexandrovich I., Anati I., Caspi D., Johnson S., Leslie-Hurd R. & Rozas C. (2016): "Intel® software guard extensions (intel® sgx) support for dynamic memory management inside an enclave". In Proceedings of the Hardware and Architectural Support for Security and Privacy 2016 (pp. 1-9).

[i.14] Gervais A., Karame G. O., Wüst K., Glykantzis V., Ritzdorf H. & Capkun, S. (2016, October): "On the security and performance of proof of work blockchains". In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 3-16).

[i.15] Menon A. A., Saranya T., Sureshbabu S. & Mahesh A. S. (2022): "A Comparatıve Analysis on Three Consensus Algorithms: Proof of Burn, Proof of Elapsed Time, Proof of Authority". In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021 (pp. 369-383). Springer Singapore.

[i.16] Samuel C. N., Glock S., Verdier F. & Guitton-Ouhamou P. (2021, May): "Choice of ethereum clients for private blockchain: Assessment from proof of authority perspective". In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-5). IEEE™.

[i.17] IEEE 802.11p™: "IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments".

[i.18] IEEE 802.15.4™: "IEEE Standard for Low-Rate Wireless Networks".

[i.19] DSRC vs. C-V2X for Safety Applications.

[i.20] ARINC 629: "Airlines Electronic Engineering Committee, 629 Part 2-2 Multi-Transmitter Data Bus, Part 2-Application Guide", February 1999.

[i.21] ARINC 659: "Airlines Electronic Engineering Committee, 659 Backplane Data Bus", December 1993.

[i.22] ARINC 664: "Airlines Electronic Engineering Committee, 664P4-2 Aircraft Data Network, Part 4 - Internet-Based Address Structure Assigned Numbers", December 2007.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
4G	4th Generation of mobile communication technology standards
5G	5th Generation of mobile communication technology standards
AI	Artificial Intelligence
API	Application Programming Interface
BFT	Byzantine Fault Tolerance
CA	Collision Advisory
CAN	Controller Area Network
CFT	Crash Fault Tolerance
CM	Consensus Mechanism
CP	Consensus Protocol
CPU	Central Processing Unit
CSMA	Carrier-Sense Multiple Access
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
CSS	Chirp Spread Spectrum
DCN	Distributed Consensus Network
DDoS	Distributed Deny of Service
DSRC	Dedicated Short Range Communication
FIFO	First In First Out
GPS	Global Positioning System
ID	Identity
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPFS	InterPlanetary File System
ITS	Intelligent Transportation Systems
LoRa	Long Range
LTE	Long Term Evolution
MAC	Medium Access Control
MCU	MicroController Unit
NAND	Not AND
OFDM	Orthogonal Frequency Division Multiplexing
PBFT	Practical Byzantine Fault Tolerance
PCDA	Perception-Collection-Decision-Action
PDL	Permissioned Distributed Ledger
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
PoX	Proof-based Algorithms
PSU	Power Supply Unit
QoS	Quality of Service
RAID	Redundant Arrays of Independent Disks
RAM	Random Access Memory
RF	Radio Frequency
RISC	Reduced Instruction Set Computer
ROP	Return Oriented Programming
RREP	Routing Response message
RREQ	Routing Request message
SAE	Society of Automotive Engineers
SC-FDMA	Single-Carrier Frequency-Division Multiple Access
SGX	Software Guard eXtensions
SNR	Signal to Noise Ratio

SPOF	Single Point Of Failure
TCAS	Traffic Collision Avoidance Systems
TEE	Trusted Execution Environment
TPM	Trusted Platform
TPS	Transaction Per Second
UAF	Use After Free
URLLC	Ultra-Reliable and Low Latency Communication
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
WCN	Wireless Consensus Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
XGS	intel Software Guard eXtensions

4 Overview of Wireless Consensus Networks

4.1 Background

Permissioned Distributed Ledger (PDL) is built on a decentralized network that relies on frequently direct communications between distributed nodes. Compared with centralized data records as presented in Table 1, PDL is more receptive to enabling numerous participants to share data in an autonomous and uncoordinated manner. The Consensus Mechanisms (CMs), which play a pivotal role in PDL, are resource-demanding both in terms of computation and in terms of communication overheads. The CMs would often determine security requirements (i.e. fault tolerances, identity) and other key performance metrics such as transaction throughput, latency thresholds and scalability to achieve the data consistency required for proper PDL functions.

Table 1: Comparison of centralized vs. decentralized

Property	Centralized	Decentralized
Meaning	The retention of power and authority with respect to planning and decisions, with the top management, is known as centralized or centralization.	The dissemination of authority, responsibility, and accountability to the various management levels, is known as decentralized or decentralization.
Geographical Distribution	Located at a centralized location (with possible mirrors/replication).	Geographically distributed.
Node Ownership	All nodes are owned by a single entity.	Each node is owned by a different entity.
Involves	Systematic and consistent preservation of authority.	Disintermediation. Systematic dispersal of authority.
Communication	Vertical.	Open and Free.
Decision Making	Made by single entity - SPOF. Fast.	Consensus by participants to prevent SPOF. May be slow depending on consensus mechanism.
Advantage	Clear coordination and leadership.	Sharing of burden and responsibility.
Power of decision making	Managing authority (not necessarily the operator of the ledger).	Decentralization. Disintermediation. Multiple participants have the power of decision making.
Best suited for	Small-sized networks/organizations. Data that is owned by a single entity.	Large-sized networks/organizations. Data that is shared between multiple entities.
Authority	Single entity.	Multiple (all) participants.