ITUPublications

International Telecommunication Union

Standardization Sector

ITU Focus Group Technical Report

(06/2024)

ITU Focus Group on metaverse
(FG-MV)

FGMV-45

Challenges to achieving trustworthy metaverse

Working Group 6: Security, Data & Personally identifiable information (PII) Protection

Technical Report ITU-T FGMV-45

Challenges to achieving trustworthy metaverse

Summary

The metaverse is an integrative ecosystem of virtual worlds, where participating entities may have one or more identities. Its essential enablers are cutting-edge technologies including Artificial Intelligence (AI), Web 3.0, Blockchain, Augmented Reality (AR), Virtual Reality (VR) and Internet of Things (IoT). When all these important and advanced technologies are applied and used in some scenarios, it will bring a serious of concerns and problems, such as the concerns of safety, security, ethics and problems of privacy, Intellectual Property Rights (IPR) and violence. In the metaverse, all these concerns and problems will occur and even other unexpected problems, and considering all these concerns and problems, trustworthiness and relevant issues become very important key issues for the metaverse and its development. Therefore, this deliverable presents key concepts, challenges and a reference model for a trustworthy metaverse including standardization landscape and roadmap.

Keywords

metaverse; trustworthy; artificial intelligence; web 3.0; blockchain; augmented reality; virtual reality.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1.0 of the ITU Technical Report on “Challenges to achieving trustworthy metaverse” approved at the 7th meeting of the ITU Focus Group on metaverse (FG-MV) held on 12-13 June 2024.

Acknowledgements

This Technical Report was researched and written by Gyu Myoung Lee (LJMU, United Kingdom), Woonjoo Park (ETRI, Korea (Republic of) and Xiao Song (China Mobile, and Xiongwei Jia (China Unicom) The development of this document was coordinated by Vincent Affleck (DSIT, United Kingdom), as Chair of Working Group 6 and Gyu Myoung Lee (LJMU, United Kingdom) as Chair of Task Group on issues on trustworthiness related to the metaverse.

Additional information and materials relating to this report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact Cristina Bueti at tsbfgmv@itu.int.

Editor & TG Chair:	Gyu Myoung Lee LJMU United Kingdom	E-mail: gyumyoung.lee@gmail.com
Editor:	Wonjoo Park ETRI Korea (Republic of)	E-mail: wjpark@etri.re.kr
Editor:	Xiaojia Song China Mobile China	E-mail: songxiaojia@chinamobile.com

Editor: Xiongwei Jia
China Unicom
China
E-mail: jiaxw9@chinaunicom.cn

WG6 Chair: Vincent Affleck
DSIT
United Kingdom
Email: Vincentaffleck2@hotmail.com

Table of Contents

Page

Technical Report ITU-T FGMV-45

Challenges to achieving trustworthy metaverse

1 Scope

This draft Technical Report focuses primarily on the metaverse that is reliable, responsible, and can be trusted completely, i.e., the trustworthy metaverse.

The scope of this Technical Report includes:

- An overview of the metaverse environment including the rationale for the need for a trustworthy metaverse.
- Core concepts and properties for a trustworthy metaverse.
- Technical challenges for a trustworthy metaverse.
- Reference model for a trustworthy metaverse.
- Standardization landscape and roadmap.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of these Technical Specifications.

[ITU-T Y.3052]	Recommendation ITU-T Y.3052 (2027), *Overview of trust provisioning for information and communication technology infrastructures and services.*
[ITU-T Y.4000]	Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

3 Terms and definitions

3.1 Terms defined elsewhere

These Technical Report use the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 Avatar [b-ISO/IEC 23005-4:2018]: Entity that can be used as a (visual) representation of the user inside the virtual environments.

3.1.3 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.4 decentralized system [b-ITU-T X.1400]: Distributed system wherein control is distributed among the persons or organizations participating in the operation of system.

3.1.5 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.6 distributed ledger technology (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

3.1.7 internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.8 ledger [b-ITU-T X.1400]: Information store that keeps final and definitive (immutable) records of transactions.

3.1.9 metaverse [b-ITU-T FGMV-20]: An integrative ecosystem of virtual worlds offering immersive experiences to users, that modify pre-existing and create new value from economic, environmental, social and cultural perspectives.

NOTE – A metaverse can be virtual, augmented, representative of, or associated with the physical world.

3.1.10 thing [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.1.11 trust [ITU-T Y.3052]: Trust is the measurable belief and/or confidence which represents accumulated value from history and the expecting value for future.

3.1.12 trustworthiness [b- ISO/IEC 22989]: ability to meet stakeholder expectations in a verifiable way.

NOTE 1– Depending on the context or sector, and also on the specific product or service, data and technology used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

NOTE 2– Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality and usability.

NOTE 3– Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

3.2 Terms defined in these Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AI	Artificial Intelligence
AIGC	Artificial Intelligence Generated Content
AR	Augmented Reality
GPU	Graphics Processing Unit
IoT	Internet of things
IPR	Intellectual Property Rights
LCM	Lifecycle Management
NFT	Non-Fungible Token
NLP	Natural Language Processing
PII	Personal Identifiable Information
QoE	Quality of Experience
QoS	Quality of Service
VR	Virtual Reality

XR Extended Reality

5 Conventions

None.

6 An overview of the metaverse environment

6.1 Background of metaverse

Defined as an integrative ecosystem of virtual worlds [b-ITU-T FGMV-20], the metaverse is a space where participating entities may have one or more identities. Its essential enablers are cutting-edge technologies including Artificial Intelligence (AI), Web 3.0, Blockchain, Augmented Reality (AR), Virtual Reality (VR), Internet of Things (IoT), etc. A virtual representation of the real world, everything in the metaverse is digitalized and virtualized, and “created” by companies, organizations, persons, and even by metaverse itself.

However, there are also potential risks. When all these important and advanced technologies are applied and used in some scenarios, it will bring a series of concerns and problems such as the concerns of safety, security, ethics and problems of privacy, Intellectual Property Rights (IPR), and violence. In the metaverse, all these concerns and problems will occur and even other unexpected problems, and considering all these concerns and problems, trustworthiness and relevant issues become very important key issues for the metaverse and its development.

When we discuss and study in the metaverse especially focusing on the trustworthy metaverse, there are a serious number of important topics, features and technical challenges that need to be figured out and clarified, including: core concepts, technical features, trustworthy factors, key roles, and technical challenges. Based on these, a reference model and standardization landscape should be identified. Therefore, this deliverable aims to present key concepts, challenges and a reference model for a trustworthy metaverse including standardization landscape and roadmap.

6.2 Necessities of a trustworthy metaverse

ITU’s trust-related standardization activities have addressed the complex challenges associated with emerging technologies and digital ecosystems, promoting a trustworthy environment for users, organizations, and entities participating in the evolving digital landscape. To this end, [ITU-T Y.3052] defines trust as the measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future. In the metaverse, relevant activities must continue. To address the risks identified in the metaverse, it is necessary to consider the following aspects:

- Interactions considering social-cyber-physical relationships between humans and things.
- Reliable data processing and management for monitoring, analytics, prediction, and decision making.
- Transparent sharing and exchange of digital resources including their identification.
- Safety guarantee for the digital assets which can be exchanged as currency in the virtual world(s) and directly related to the properties in the real world.
- Secure and correct operations with autonomous decision making.
- Measurable indicators and evaluation methodology for different levels of trust.

As decision-making behaviour, trust is affected by past experience and associated predictions for the future. Previously, the study of trust in systems has been a topic of psychology [b-ITU-T TR Trust]; however, with the path to the era of intelligence, i.e., with the development of intelligent technologies a series of unique changes and challenges have been occurring: the interaction between a user and a system is becoming very important. In the meantime, trust itself is a complexity-reduction mechanism, whose importance increases the less we know about the technology(-ies).

When it comes to trust relevant topics, the following issues and concerns may be considered:

- Is this metaverse is trustworthy or not? How can trustworthiness be measured, and what is the benchmark of being trustworthy?
- If it is trustworthy enough, how much it can be trusted?
- If it is not trustworthy, how it can be improved and optimized in order to be trusted?
- The standardized methods and parameters to trustworthiness of metaverse.

Above all, in the metaverse trust is an important topic and concern for the users, vendors and supervisors. Trustworthy metaverse is one of the essential and urgent topics for commercial usage of metaverse, and with this deliverable, the core concepts of trustworthy metaverse will be discussed and defined, and a series of pre-standard topics will be discussed and studied.

7 Core concepts and features for a trustworthy metaverse

7.1 Core concepts

With the study of metaverse especially focusing on its trustworthiness, it is important to clearly understand the following core and key concepts in the context of the metaverse:

- **Trustworthy metaverse**: A virtual environment or a digital world which is trustworthy enough and in which all the human beings or lives can get one or more identities to express and interact with each other.
- **Trustworthy digital identity**: A unique identity information which is secure and trustworthy enough for each avatar in a specific metaverse, and where one identity can be mapped to a human or a physical entity in the real physical world.
- **Trustworthy digital asset:** A digital asset is a digital representation of value recorded on a cryptographically secured distributed ledger or similar technology; it is supposed to be capable of being exchanged in the virtual world as a form of currency without an intermediary. A trustworthy digital asset is the digital asset which is secure and trustworthy enough.

7.2 Technical features of a trustworthy metaverse

Considering that the metaverse is a mirror of the real world, the important issue of trust is also important, or even more important, in the metaverse. And when it comes to trust topic for metaverse, the following aspects should be considered:

- **Mirroring the real world:** In the metaverse, one of its attractive parts is that the metaverse includes the virtualized real world. In order to mirror the real world into the metaverse, it is necessary to use digital twin technologies.
- **Interaction between real world and metaverse virtual worlds:** Just as it shows that the metaverse can contain more than one “world”, the languages in the metaverse will be diverse. Natural Language Processing (NLP) will be crucial in the metaverse virtual worlds to achieve free and smooth interaction.
- **Digital copyright:** When most technologies have been taken into consideration, there may be some crucial issues to be taken seriously, one of which would be the legal issue. The virtualized worlds are full of virtual and digital lives, mirroring and virtual entities, digital images, music, and so on, each of which may have its copyright or relevant legal identity. With so many copyright and legal issues to deal with, only AI would be capable of doing it.
- **Content creation:** As the virtualized worlds, all the contents in the metaverse are virtualized and digitalized by programs or algorithms. And as the contents evolve to become richer and

richer, it is hard to design, operate, manage and maintain them by engineers alone; hence, only AI can be the way to the continuous development and evolution of metaverse, e.g., the creation of avatar(s).

- **Avatars:** Avatars are entities that can be used as (visual) representations of the user inside the virtual environments.
- **Digital identity:** Each identity in a trustworthy metaverse is supposed to have its digital identity information that is unique, safe, trustworthy and accountable, and can also be tracked to a specific owner in the real world.
- **Digital asset:** A digital asset is a digital representation of value recorded on a cryptographically secured distributed ledger or similar technology, and it is supposed to be capable of being exchanged and traded in a digital world like metaverse.

7.3 Factors of metaverse in aspects of trustworthiness

To make trust in the metaverse more intuitive and acceptable to humans in the real world and not just to specialists, the following factors should be considered for trust in the metaverse:

- **Strict Quality of Experience (QoE) requirements:** in the metaverse, all the interactions and objects are virtualized and enabled by AI, computational power and relevant technologies. It is required that metaverse should achieve immersive experience and real-time interactions, and should be capable of being accessed anytime and anywhere; these are strict QoE requirements.
- **Compliance:** as virtual worlds in which people can play different roles in different virtual scenarios and many interactions will happen in the metaverse, it is important and urgent to study, discuss and conclude that all are compliant.
- **Accountability:** the technology providers or vendors of the metaverse should take responsibility for the executive actions and interactions by AI and relevant technologies.
- **Equitability:** in the metaverse virtual worlds, intended or unintended bias(es) or unfairness(es) should be avoided, because the bias or unfairness would inadvertently cause harm, damage and loss.
- **Safety, data security and privacy:** safety, data security, privacy and all the relevant issues should be ensured in the trustworthy metaverse.

8 Technical challenges for a trustworthy metaverse

8.1 Digital identity

Digital identity is the user’s proof of identity in the metaverse, the identity proof of the ownership of digital assets, and the key to maintaining the sustainable and healthy development of the metaverse. Without digital identity, the infrastructure of the metaverse would be vulnerable. In the event of a cyberattack, weak digital identities such as user names and passwords will be stolen or used for other fraudulent activities. Digital identities in the metaverse face the following challenges:

- **Personal identification (PII)**: Digital identity information and sensitive data, such as names, e-mail addresses and phone numbers need to be handled. These data may be obtained illegally and abused. Attackers can obtain these sensitive data through various means such as network sniffing and man-in-the-middle attacks, for malicious activities such as identity theft and fraud.
- **Malicious software and attacks**: As more users and metaverses join, the network must be able to handle large-scale data exchanges and transactions while maintaining low latency and high throughput.
- **Identity interoperability**: In the metaverse, each user maps multiple identities in the metaverse platforms. Identification and interoperability between multiple identities can pose challenges.

8.2 Network connection

The metaverse integrates virtual reality, augmented reality, artificial intelligence, blockchain and other technologies, and an efficient and reliable network is a key challenge for the metaverse. In the metaverse, every detail requires a lot of computation and data transmission, and if the network is not reliable it can lead to data loss, inaccurate computation results and poor user experience. A trusted network connection faces the following challenges:

- **Interoperability**: Different metaverses have different data formats, interaction methods, and economic models. There is a lack of common standards and protocols to ensure that data and assets can be shared across metaverses.
- **Scalability**: As more users and metaverses join, the network must be able to handle large-scale data exchanges and transactions while maintaining low latency and high throughput.

8.3 AI technology

In the development of the metaverse, AI technology can be applied to a wide variety of scenarios such as content generation, character modelling, speech recognition and sentiment analysis. As one of the key technologies for the realization of the metaverse, the metaverse must support the trusted AI operation in the data, modelling, analysis, prediction and decision-making process. If the AI modelling or operation process is not trusted, it will lead to the entire metaverse not being trusted, with serious consequences.

The trust challenges for AI include:

- **Lack of transparency**: The decision-making process of AI is often not transparent, which makes it difficult for people to understand and trust the decisions made by AI, and puts AI at risk of abuse.
- **Data supply**: The foundation of AI computing is data, and AI computing in the metaverse requires access to a large amount of data. As a virtual space, information and property in the metaverse are easily to be stolen and attacked in the process of AI computing.

8.4 Blockchain technology

Blockchain is one of the key foundational technologies of the metaverse, and its security, reliability, decentralization and interoperability provide a secure, trustworthy and transparent environment for the metaverse. However, blockchain technology faces a number of technical security challenges.

- **Growing data volume challenge**: With the development of blockchain, the volume of blockchain data stored by nodes is getting larger and larger, and the burden of its storage and computation is getting heavier and heavier, which will bring great difficulties to the operation of metaverse clients.
- **Low blockchain application efficiency**: Blockchain transactions require multiple confirmations, each of which creates a delay. Such efficiency does not meet the real-time requirements of the metaverse.

8.5 Trust lifecycle management

Trust Lifecycle Management (LCM) refers to a complete process of managing for trust throughout the lifecycle of a trustworthy metaverse. The general process of trust LCM is illustrated in Figure 1.

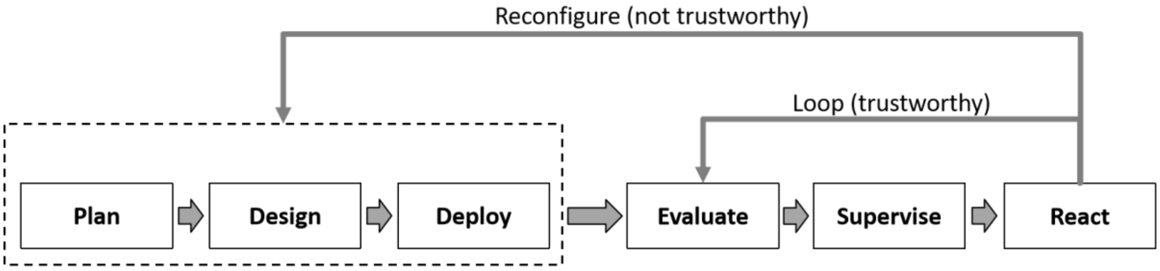

Figure 1 – General process of trust LCM

Based on Figure 1, the trust LCM can be applied in the lifecycle of the metaverse to be trusted/trustworthy. The following steps are considered, not all steps are necessary in the same lifecycle, i.e. in a lifecycle the steps depend on the specific conditions or scenarios:

- **Plan:** At the beginning of the lifecycle of trust for trustworthy metaverse, it is considered important to make plans of trust during the whole lifecycle before the relevant metaverse works.
- **Design:** After planning, the design for trustworthy metaverse is essential and necessary; it is considered that during the design, all the elements, processes, factors, and so on, are designed to be trustworthy from the very beginning or designed with the fundamental principle to be trustworthy.
- **Evaluate:** In order to be objective, measurable and quantifiable, it is considered important to compute or evaluate the trustworthiness of the relevant system in the lifecycle of the metaverse. This is so that, the operators, users, governors and supervisors can understand the levels of the trustworthiness in order to make decisions, actions, judgements and authorizations.
- **Supervise:** In the lifecycle of trust in the metaverse, after the computation/evaluation, it is considered important to monitor the fluctuation of trustworthiness in order to make sure it is trustworthy throughout the lifecycle of the metaverse.
- **React:** After the evaluation/assessment of trustworthiness, the metaverse system is considered to make appropriate reactions based on the trustworthiness, i.e. to continue working if trustworthy or to reconfigure the system if not trustworthy.
- **Loop:** Trust should be continuous and sustainable; a lifecycle should be followed by another lifecycle in the trustworthy metaverse.
- **Reconfigure:** If the metaverse system is not trustworthy enough, i.e., the evaluation results are not ideal enough to be trusted, it is considered important to reconfigure the metaverse system to make it trustworthy.

8.6 Trust indicators and measurement for computational trust

8.6.1 Indicators of computational trust

In order to make trust in the trustworthy metaverse computable, measurable and quantifiable, i.e., to make trust itself more objective and quantitative for the trustworthy metaverse, it is proposed that indicators for trust be discussed and studied carefully. With the indicators, the degree or level of trust can be computed out directly and objectively. In Table 1, there is general information for trust indicators for computational trust of trustworthy metaverse.

Table 1 – Trust indicators for computational trust of trustworthy metaverse

Indicators	Factors
Accuracy	QoE
	QoS

	Timeliness
	Resource
Stability	Interruption
	Accident
	Maturity
	Variability
Controllability	Predictability
	Supervision
	Compliance
	Taken-over
Resilience	Backup
	Reset
Adaptability	Flexibility
	Adjustment
Security	Privacy
	Asset safety

8.6.2 Computation and measurement of trustworthiness

In order to make trust itself computable and measurable for the metaverse, it is proposed to study the general method and process for computation and measurement of trustworthiness. As the measurement of trustworthiness, it should take place in the commercial environment or the environment that is mirrored by the commercial one(s). During the evaluation/assessment of trustworthiness, all the above indicators and related factors should be taken into consideration objectively.

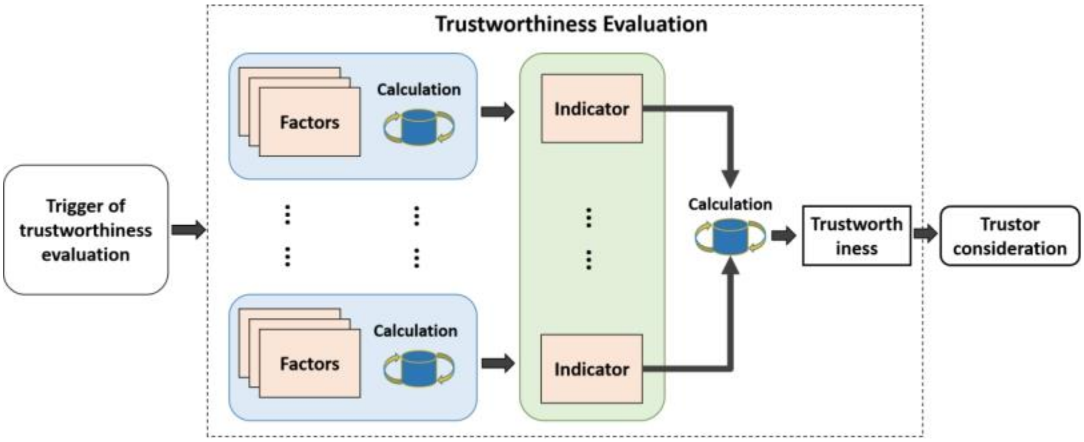

Figure 2 – General process of trustworthiness evaluation for metaverse

As shown in Figure 2, the general process of trustworthiness evaluation for metaverse has been illustrated, and trustworthiness can be evaluated/assessed/measured quantitatively and objectively. The following are the key conditions to trustworthiness evaluation for metaverse:

- **Environment of trustworthiness evaluation:** Trustworthiness of metaverse evaluation can take place in commercial networks; meanwhile, it also can take place in some test or simulation environment that is mirrored by the commercial network.
- **Trigger of trustworthiness evaluation:** Trustworthiness of metaverse evaluation can be triggered by the trustor, as well as by the trustee. The trigger includes the following situations:
  - Orders before/at the start-up of some metaverse systems.
  - Configured orders, including periodic orders and aperiodic orders at specific time points.
  - Temporary orders at random time points.

The trustor can trigger the trustworthiness of metaverse evaluation by using some original and configured/standardized input/order for different scenarios; meanwhile, the trustee can also trigger the trustworthiness of the metaverse evaluation by itself in order to gain the trust from trustor if necessary.

- **Indicators of trustworthiness evaluation:** Metrics are those parameters that are specified to make trust/trustworthiness measurable and quantifiable for metaverse (system).

  NOTE 1 – Indicator(s) in the same trustworthiness evaluation should be unified with the same unit and in a unified way.

- **Factors of trustworthiness evaluation:** Each indicator is necessary to set a series of related factors, the assessment/evaluation results of factors can perform as the calculating input for related indicators.

  NOTE 2 – Factor(s) in the same trustworthiness evaluation should be unified in the same unit with the same unified way; in the meantime, the unit and unified way of sub-metrics and metrics should be the same in a same trustworthiness evaluation.

- **Results of trustworthiness evaluation:** Trustworthiness evaluation results should be handed over to the trustor, in order to take into consideration, make decisions or cast judgement of the following authorizations or progress.

8.7 Trusted AIGC technologies

As one of the essential technologies for metaverse, artificial intelligence-generated contents (AIGC) is the main resource of continuous generative contents and creativities, all of the generated contents are supposed to be trusted or trustworthy.

AIGC technologies act as one of the crucial, powerful and productive enablers to the metaverse system(s), in which most of the (virtual) contents can be generated manually or automatically. Due to the need for a large number of contents in the virtual world of metaverse, AIGC technologies are supposed to be applied widely, extensively and substantially in metaverse system(s). Considering the crucial and important role of AIGC, the following aspects are supposed to be considered:

- **Trusted contents:** In trustworthy metaverse systems, the contents, especially the generated contents, should be trustworthy enough; i.e., the contents should be achieving the related requirements of trust.
- **Trusted AI technologies:** In metaverse systems, the AI technologies for content generation should be trustworthy; in the commercial environment, the AI technologies that are applied in some metaverse systems should be verified/certified in order to achieve the related requirement of trustworthiness.

- **Content verification:** In trustworthy metaverse systems, the generated contents should be verified in order to be trustworthy, so that, the users or the trustors can carry out the relevant interactions or authorizations.
- **Content traceability:** In trustworthy metaverse systems, all the generated content is supposed to be traceable with some original mark(s) or information.
- **Content security:** In trustworthy metaverse systems, the generated content is supposed to be achieving relevant security requirements.

8.8 Trusted data

As the important input and fertilizer for metaverse, data is the key enabler and fuel for most processes of metaverse. Trustworthy data and dataset need to be further studied and specified to make metaverse trusted and trustworthy. To make it more detailed and concrete for trusted data of metaverse, the following are the key aspects suggested to take consideration:

- **Compliance:** All the data of trustworthy metaverse no matter the input or the output should be compliant within the specific metaverse (system) for specific rules and related specifications and even laws.
- **Traceability:** The trusted data of metaverse are supposed to be traceable, and the trusted data or dataset may configure with identity or mark to make the trace possible.
- **Privacy:** It is important for all the trusted data to achieve the requirement of user's privacy, and the trusted data include the input data and the output data.

8.9 Trusted digital asset

A digital asset is a digital representation of value recorded on a cryptographically secured distributed ledger or similar technology, and it is supposed to be capable of being exchanged and traded in a digital world like metaverse without an intermediary. As in the trustworthy metaverse, the digital assets should be trustworthy enough to do the relevant exchanges and trades in the digital world as metaverse. The following are the essential aspects that should be taken into consideration for the trusted digital assets:

- **Decentralization:** With numerous nodes distributed in the digital world, each node has highly autonomous characteristics, the nodes can freely connect to each other and form new connection units. Each node can become a periodic centre, but does not have mandatory central control functions. The influence between nodes will form a nonlinear causal relationship through the network. Thus, in order to be trusted of the digital asset, "decentralization" should be one of the essential properties of a trusted digital asset.

- **Encryption:** Encryption is the process of converting data into a message that no one can understand without the correct key through cryptographic arithmetic; for the trusted digital asset, it should be encrypted all the time in the digital world.

- **Traceable:** All the traces of the digital asset should be recorded, so that they can be traced back if necessary.

- **Immutable:** Based on the traceability, all the recorded traces should be immutable, i.e., they cannot be falsified.

- **Privacy:** All the private information, especially the assets, should be well protected.

- **Security:** The physical security, network security, data encryption, identity authentication, and so on, should be ensured, so that exchanges are protected from attack and illegal access.

- **Trusted exchange/payment:** All the exchanges or payments should be trustworthy enough whether in peer-to-peer, real-time or offline scenarios.

9 Reference model for a trustworthy metaverse

As shown in Figure 3, to build a trustworthy virtual world, related technical enablers should be supported on top of the infrastructure for a trustworthy metaverse. In addition, related applications will be made available across different domains in a trustworthy manner.

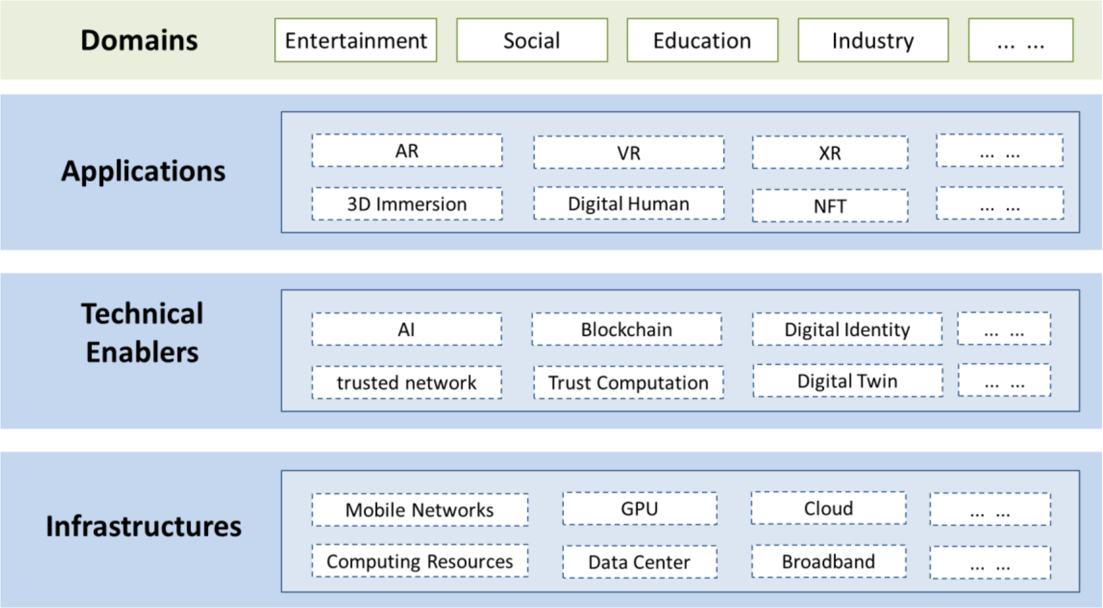

Figure 3 – A reference model for a trustworthy metaverse

For a trustworthy metaverse, it can be applied in entertainment, social, educational or even in various industrial domains with the applications of extended reality (XR), avatars, digital twin, and so on. In addition, the main enablers of trustworthy metaverse are, for example, trustworthy AI technologies, digital identity, and relevant technologies for safety and security. The trustworthy metaverse should be built or initiated on mobile networks and computing resources to efficiently support data processing, communications and computing.

- **Infrastructures:** As a digitalized “world”, the metaverse system is built on a number of infrastructures, including the mobile networks, data centres, computing resources, broadband, graphics processing unit (GPU), and cloud computing, all these infrastructures act as the foundations for the metaverse system.
- **Technical enablers:** Based on the infrastructures, the metaverse system is enabled by, for example, the trusted networks, AI technologies, blockchain, trust computation, digital identity, and digital twin, all of which are required to enable the metaverse system to be trustworthy enough.
- **Applications:** The users of the metaverse who are in the real world need software and hardware to make access to the virtual world of the metaverse. The applications of the metaverse are essential for users to gain access, so the applications can be software and also hardware, e.g., AR, VR, XR, 3D immersion, avatars, and non-fungible tokens (NFT) NFT.
- **Domains:** A trustworthy metaverse can be used in many different domains, including the entertainment, social, educational and industrial domains, where users can work, socialize and entertain themselves in the virtual world.

10 Standardization landscape and roadmap

10.1 Standardization landscape

Figure 4 shows (draft) Recommendations on trustworthy networking and services developed in ITU-T SG13. Meanwhile, as an emerging topic, although most SDOs are starting their work on the metaverse and related topics, the work for a trustworthy metaverse has not yet been formally started for standardization. Therefore, current work on trust-related standardization should be extended to the metaverse.

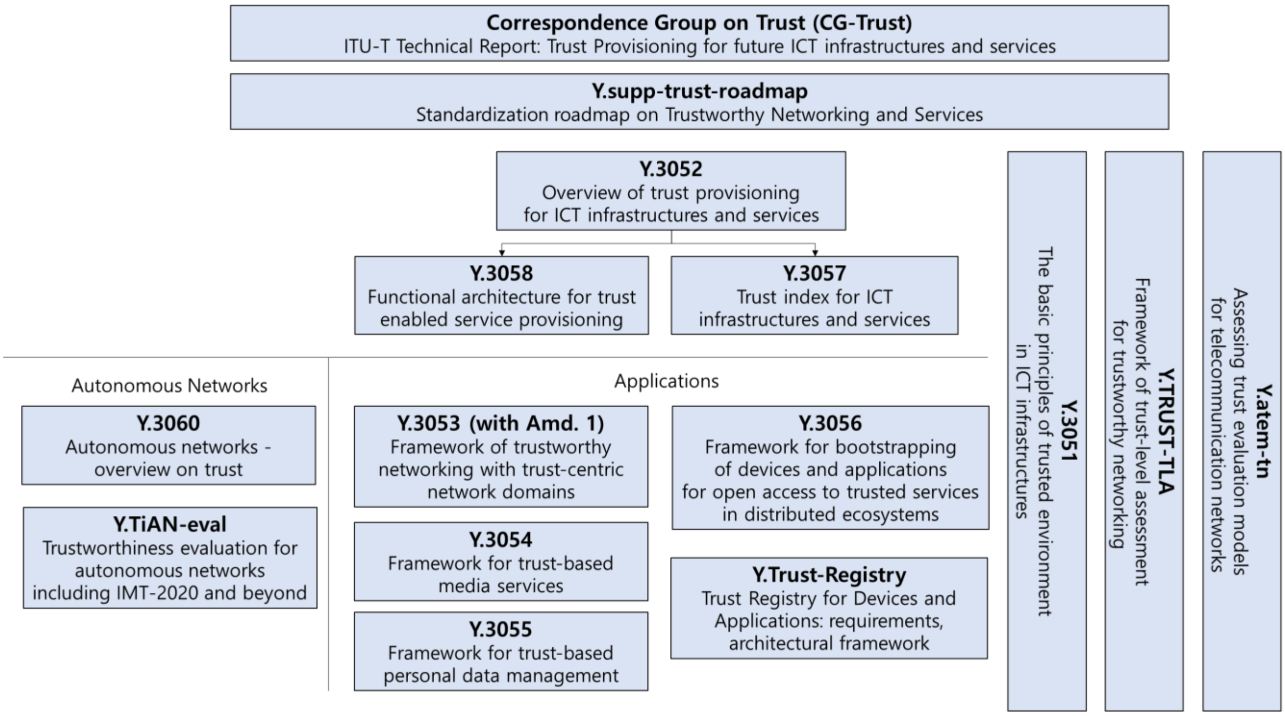
Correspondence Group on Trust (CG-Trust)
ITU-T Technical Report: Trust Provisioning for future ICT infrastructures and services
Y.supp-trust-roadmap
Standardization roadmap on Trustworthy Networking and Services
Y.3052
Overview of trust provisioning for ICT infrastructures and services
Y.3058
Functional architecture for trust enabled service provisioning
Y.3057
Trust index for ICT infrastructures and services
Y.3051
The basic principles of trusted environment in ICT infrastructures
Y.TRUST-TLA
Framework of trust-level assessment for trustworthy networking
Y.atem-tn
Assessing trust evaluation models for telecommunication networks
Autonomous Networks
Y.3060
Autonomous networks - overview on trust
Y.TiAN-eval
Trustworthiness evaluation for autonomous networks including IMT-2020 and beyond
Applications
Y.3053 (with Amd. 1)
Framework of trustworthy networking with trust-centric network domains
Y.3054
Framework for trust-based media services
Y.3055
Framework for trust-based personal data management
Y.3056
Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems
Y.Trust-Registry
Trust Registry for Devices and Applications: requirements, architectural framework

Figure 4 – ITU-T (draft) Recommendations on trustworthy networking and services in SG13

As shown in Figure 4, trust-related standardization has been published or is underway in applications and autonomous networks, and it is believed that trust needs to be standardized in more areas for the development and evolution of, for example, intelligent technologies, digitalization and virtualization. With this draft technical report, one of the important topics has been focused and discussed, namely the trustworthy metaverse. Further and more detailed studies should be made and discussions for standardization of the trustworthy metaverse held, although there will be many obvious challenges.

10.2 Standardization roadmap

In order to develop standards for a trustworthy metaverse, it is necessary to reach a consensus on the right direction, taking into account the needs of industry and users. This will help to create a positive atmosphere and technical foundations. The following are some suggestions and advice for the standardization roadmap and development:

- Develop a trusted/trustworthy framework and architecture to provide guidelines and roadmap for the standardization of the key technical enablers.

- Develop standards for trustworthy technical enablers, i.e., the enabling technologies for trustworthy metaverse systems, based on the existing or evolving infrastructure standards.

- Develop standards for the essential aspects of the trustworthy metaverse, e.g., performance, interface (with hardware), protocols, application scenarios and security.

- Develop details of specific technical requirements and specifications, including the QoS requirements, QoE requirements, the (virtual world) mirroring requirements, and the “rules” in the virtual world.
- In order to make the trustworthy metaverse more objective, it is also necessary to study the measurement and evaluation of the trustworthiness of the metaverse or relevant systems/solutions and develop relevant standards.
- The commercial applications and services of trustworthy metaverse should also be trustworthy, it is necessary to develop standards for relevant trustworthy applications or services.
- General considerations for the security, data and PII protection are taken into account in any standardization for a trustworthy metaverse.

Bibliography

[b-ITU-T Y.supp.trust-roadmap] Draft new Supplement ITU-T Y.supp.trust-roadmap: “Standardization roadmap on trustworthy networking and services” (in progress).

[b-ITU-T FGMV-20] ITU Focus Group Technical Specification ITU-T FGMV-20 (2023), *Definition of metaverse.*

[b-ITU-T TR Trust] ITU-T Technical Report -- Trust in ICT (2017).

[b-ISO/IEC 22989] ISO/IEC 22989: (2022) *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology.*

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology.*

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks.*