# A SURVEY ON METAVERSE : FUNDAMENTALS, SECURITY, AND PRIVACY

SECTION 7~11

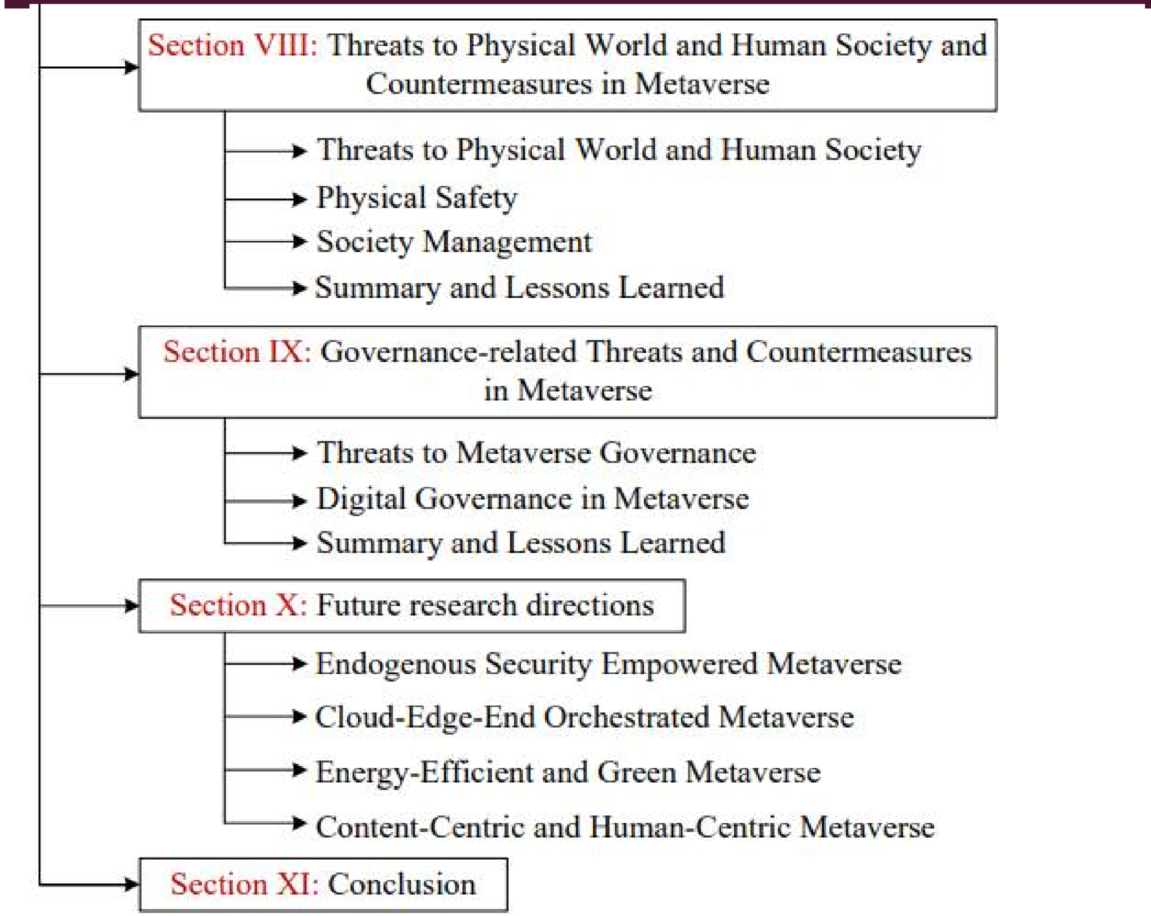
BY

ABIR EL.

SEOUL NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPT. OF COMPUTER SCIENCE AND ENGINEERING

# ORGANIZATION OF THIS PRESENTATION



Section VIII: Threats to Physical World and Human Society and Countermeasures in Metaverse

- Threats to Physical World and Human Society
- Physical Safety
- Society Management
- Summary and Lessons Learned

Section IX: Governance-related Threats and Countermeasures in Metaverse

- Threats to Metaverse Governance
- Digital Governance in Metaverse
- Summary and Lessons Learned

Section X: Future research directions

- Endogenous Security Empowered Metaverse
- Cloud-Edge-End Orchestrated Metaverse
- Energy-Efficient and Green Metaverse
- Content-Centric and Human-Centric Metaverse

Section XI: Conclusion

**Opinion**

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE (P.20)

## *A. Threats to Metaverse Economy*

- Various attacks may threaten the creator economy in the metaverse from the service trust, digital asset ownership, and economic fairness aspects. Some of these threats are summarized as follow:

  - *Service Trust Issues in UGC & Virtual Object Trading:*
    - ✓ In the open metaverse marketplace, avatars may be distrustful entities without historical interactions. There exist inherent fraud risks such as refusal-to-pay during UGC and virtual object trading among different stakeholders in the metaverse.
    - ✓ Malicious users/avatars may buy UGCs or virtual objects in Roblox and illegally sell the digital duplicates of them to others to earn profits.
    - ✓ Metaverse project Paraluni based on Binance Smart Chain (BSC) **lost over $1.7 million** in 2022 due to the reentrancy flaw in smart contracts.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *A. Threats to Metaverse Economy*

- *Threats to Digital Asset Ownership:*

  ✓ NFT offers a promising solution for asset identification and ownership provenance in the metaverse, however, NFTs also face threats such as ransomware, scams, and phishing attacks.

  ✓ Adversaries may mint the same NFT on multiple blockchains at the same time.

  ✓ Besides, evil actors may cash out their shares after inflating the value of NFTs, or they may sell NFTs to gain benefits before minting anything, where these De-Fi scams cause $129 million lost in 2020

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *A. Threats to Metaverse Economy*

- *Threats to Economic Fairness in Creator Economy:*

  ✓ In metaverse auctions, strategic avatars may overclaim its bid, instead of its true valuation, to manipulate the auction market and win the auction.

  ✓ A free-riding avatar may submit meaningless local updates in collectively training an intelligent 3D navigation model under distributed AI and unfairly enjoy the benefits from the trained metaverse model.

  ✓ Collusive users/avatars in the metaverse may collude with each other to perform market manipulation and gain economic benefits. For example, collusive avatars may collude to manipulate the results of metaverse auctions and earn illegal revenues.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- The metaverse economy should simultaneously achieve three goals:
  - Make data/assets from different sources mutually identifiable, trustworthy, and verifiable;
  - Design suitable incentive mechanisms for data/assets circulation to form a benign data sharing and coordination pattern;
  - Allow data subjects, data controller, data processor, and the user have the right to negotiate the rules and mechanisms of data protection and applications.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- *Trusted UGC/Asset/Resource Trading:*
  - As shown in Fig. 8, blockchain technologies such as NFT and smart contract, provide a decentralized solution to construct the sustainable creator economy.
  - NFT is the irreplaceable and indivisible token in the blockchain and is regarded as the unique tradable digital asset associated with virtual objects.
  - Besides, smart contracts enable the automatic transaction enforcement and financial settlement in trading virtual objects, items, and assets.

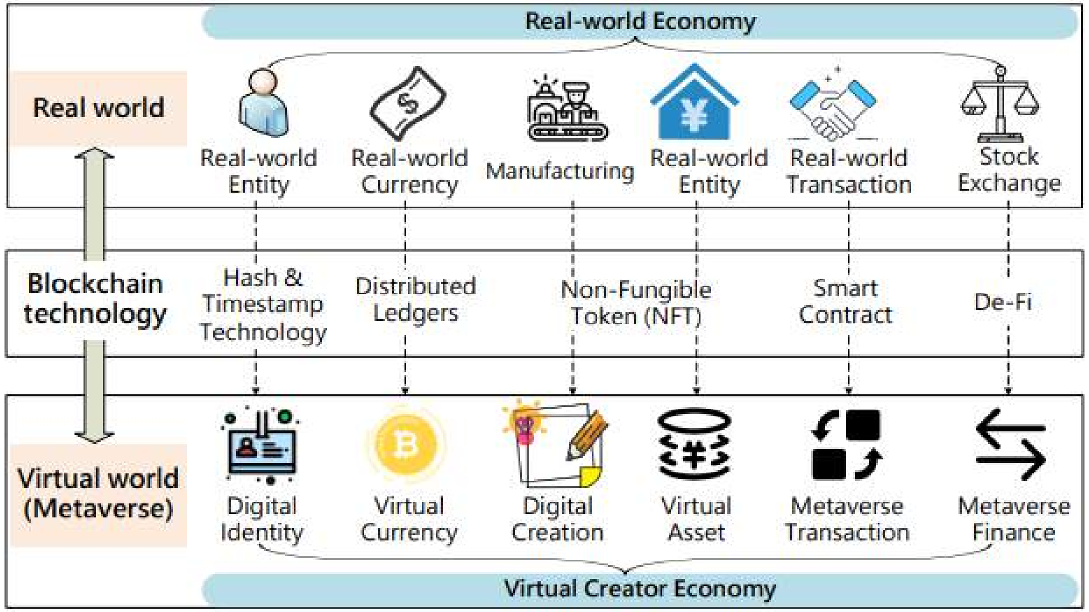


Fig. 8. The role of blockchain technologies in bridging the conventional economy and metaverse economy.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- *Trusted UGC/Asset/Resource Trading:*
  - Apart from the trust-free blockchain approaches, trust or reputation management offer a quantifiable solution to evaluate the trustworthiness of participants and services with less computation/energy consumption.
  - Multiple works has used AI, Digital Twins, Federated Learning, and other cutting-edge technologies to enhance the trust in using Blockchain for Metaverse resource trading.

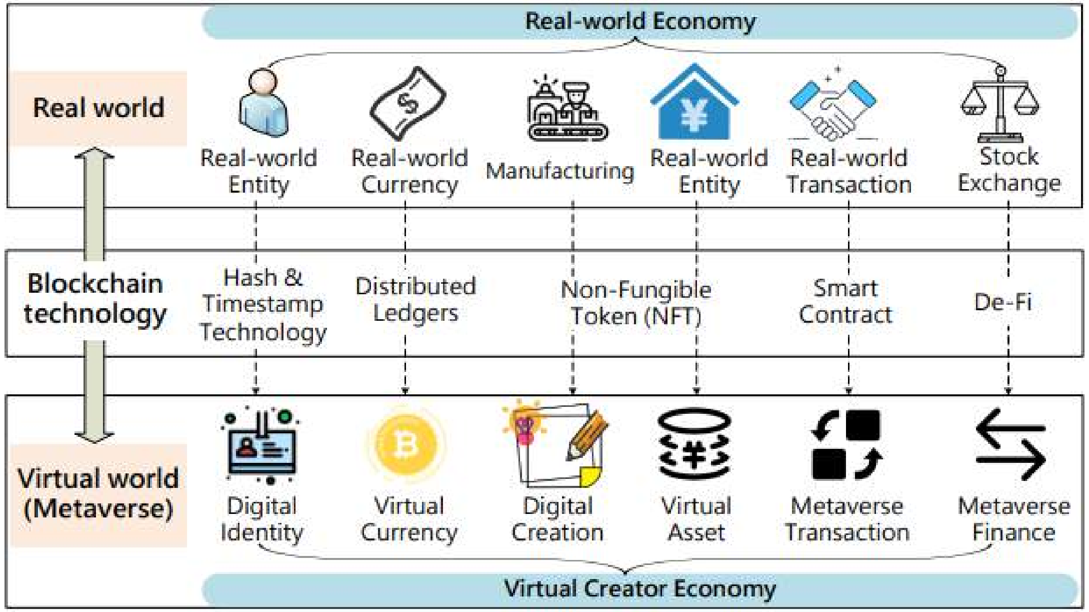


Fig. 8. The role of blockchain technologies in bridging the conventional economy and metaverse economy.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- *Economic Fairness for Manipulation Prevention:*

  - The economic fairness in metaverse markets may be violated by strategic, free-riding, and collusive users/avatars.
  - Strategy-proof incentive mechanisms, such as truthful auctions [136] and truthful contracts [137], can prevent strategic users/avatars from market manipulating. However, truthful participation also violates user's privacy, like the true bid in auctions may reveal user's true valuation on the items.

  - Existing strategy-proof and privacy-preserving auctions mainly depend on cryptographic mechanisms such as ZKP which may bring large system burdens for energy-limited wearable devices or large data utility decrease in practical metaverse applications.

  - A trade-off mechanism between privacy and utility is needed for users/avatars with diverse preferences in the metaverse.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- *Economic Fairness for Manipulation Prevention:*

  - Existing schemes to prevent free-riders (who try to enjoy benefits of the good/service without contributing to it) mainly focus on node behavior modeling [129], cryptographic mechanism [140], [141], and contribution certification [142].

  - Li et al. [129] observe that BitTorrent systems (account for 35% of the traffic on the Internet) may fail to overcome free-riders if a large number of seeds (who have all pieces of the file) exist. To bridge this gap, the authors design a fluid model for non-free riders and free-riders in P2P file sharing systems like BitTorrent to capture and mitigate free-riding effects by designing optimal seed bandwidth allocation strategies.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- *Economic Fairness for Manipulation Prevention:*
  - Multi-user/avatar collusion prevention is also important for fairness in the creator economy. Existing collusion-resistant mechanisms mainly focus on AI-based collusion behavior detection [143], cryptographic approaches [144], game theory [128], and optimization theory [145], which can be beneficial for collusion defense in metaverse services.
  - Various works leverage game theory and learning-based methods to improve economic efficiency for metaverse services, including iterative double auction for resource pricing in DT construction [72], [133], DRL-based double Dutch auction for VR service trading [46], two-tier Q-learning for secure edge caching services [81], optimization theory for resource allocation in virtual education [146], and hierarchical game for coded distributed computing services in metaverse [147].

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Open and Decentralized Creator Economy*

- *Ownership Traceability of Digital Assets:*

  - Smart contracts offer an intelligent traceability solution by coding the ownership management logic into scripts which are run atop the blockchain.
  - Existing works have utilized blockchain technologies for food supply [148], cloud storage [69], charging pile sharing [149], and ride sharing [150].
  - In addition to private ownership, there can exist multiple types of ownership forms in the metaverse such as collective ownership and shared ownership [125], which raise extra challenges in ownership management of virtual objects and metaverse assets.
  - In current metaverse projects, there have been increasing interest in utilizing NFT for asset identification and ownership provenance.
  - Nevertheless, NFTs also face vulnerabilities such as cross-chain fraud, inflation attack, phishing, and ransomware.

# VII. ECONOMY-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *C. Summary and Lessons Learned*

- For creator economy in the metaverse, we have learned that blockchain technology is the key to build the decentralized virtual economy ecosystem from virtual currency creation and trusted UGC/asset/resource trading to economic fairness and ownership traceability.

- Moreover, the interoperability, resilience, and efficiency issues are prime concerns to construct a sustainable creator economy. A comparison of existing/potential security countermeasures to metaverse economy is presented in Table IX.

TABLE IX

Summary of Existing/Potential Security Countermeasures To Metaverse Economy

| **Ref.** | **Security Threat** | ⋆ **Purpose**<br>• **Advantages**<br>◦ **Limitations** | **Utilized Technology** |
|---|---|---|---|
| [131] | Low cooperation in creator economy | ⋆Swarm economy model for cooperative and dynamic digital resource sharing<br>•Real-world implementation of blockchain in such economy model<br>◦Non-supervisability in transaction settlement and high computational overhead | Blockchain |
| [132] | Lack supervisability on criminal transaction | ⋆Three-layer sharding blockchain for scalable and automatic transaction<br>•Enhanced system scalability and traceability of criminal transactions<br>◦Lack vulnerability analysis and large-scale real-world simulations | Blockchain sharding |
| [133] | Fraud in DT construction | ⋆Trusted and on-demand DT services in DT edge networks<br>•Transparent DT model training and resource trading<br>◦Lack efficiency and scalability analysis of their DAG blockchain | FL, DT, DAG |
| [29] | Compromised nodes/services | ⋆Intelligent trust model to quantitatively evaluate user/service trustworthiness<br>•Aggregate multi-dimensional trust attributes for high-accuracy trust computing<br>◦Lack complexity and scalability analysis, as well as cold start issues | Machine learning |
| [139] | Economic fairness, strategic users | ⋆Strategy-proof and privacy-preserving auction for heterogeneous spectrum<br>•Privacy protection, strategy-proofness, and high social welfare<br>◦Vulnerable to collusive bidders in auction | HE, auction |
| [129] | Economic fairness, free-riding attack | ⋆Mitigate free-riding effects in BitTorrent by optimizing seed bandwidth allocation<br>•Effective free-rider penalization and cooperation promotion<br>◦Lack real-world tests on robustness and lack analysis of heterogeneous peers | Fluid model |
| [141] | Economic fairness, free-riding attack | ⋆Blockchain-based fair ad delivery among connected vehicles<br>•Enable anonymity and conditional linkability<br>◦Not support batch verification of aggregated dissemination proofs | Smart contracts, ZKP |
| [128] | Economic fairness, collusion attack | ⋆Collusion-resistant auction design in cooperative communications<br>•Truthfulness, collusion-resistance, and budget-balance<br>◦Only apply to wireless cooperative communications | Game theory |

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE (P.22)

## *A. Threats to Physical World and Human Society*

- The threats occurring in the metaverse may also affect the physical world and threaten human society.
- The threats in virtual worlds also severely affect physical infrastructures, personal safety, and human society.

  ▪ *Threats to Personal Safety:*
    - ✓ In the metaverse, hackers can attack wearable devices, XR helmets, and other indoor sensors to obtain the life routine and track the real-time position of users to facilitate burglary, which may threaten their safety.
    - ✓ A report released by the XR Security Initiative (XRSI) shows that an adversary can manipulate a VR device to reset the hardware’s physical boundaries.
    - ✓ A user in metaverse can be potentially pushed toward a flight of stairs or misdirected into dangerous physical situations.
    - ✓ Due to the immersive realism of metaverse, hackers can suddenly display harmful and scary content in the virtual environment in front of the avatar, which may lead to the **death** of **fright of the corresponding user.**

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE

## A. Threats to Physical World and Human Society

- *Threats to Infrastructure Safety:*
  - ✓ By sniffing the software or system vulnerabilities in the highly integrated metaverse, hackers may exploit the compromised devices as entry points [154] to invade critical national infrastructures such as power grid systems and high-speed rail systems via APT.

- *Social Effects:*
  - ✓ Although metaverse offers an exciting digital society, severe side effects can also raise in human society such as user addiction [155], rumor prevention [156], child pornography, biased outcomes, extortion, cyberbullying, cyberstalkers [11], and even simulated terrorist camps [157].
  - ✓ The immersive metaverse can provide future potentials for extremists and terrorists by making it easier to recruit and meet up, offering new ways for training and coordination, and lowering costs for finding new targets.

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE

## *B. Physical Safety*

- *Cyber Insurance-based Solutions:*
  - ✓ Cyber insurance offers a financial instrument for risk mitigation of critical infrastructures in cyberthreats.
  - ✓ To resolve the high premium stipulation in traditional insurance offered by insurance companies, Lau et al. [158] propose the coalitional insurance in power systems where the coalitional premium is computed by considering loss distributions, vulnerabilities, and budget compliance in an insurance coalition.
  - ✓ Feng et al. [159] integrate cyber insurance into blockchain services for prevent potential damages under attacks, where a sequential game theoretical framework is developed to model the interactions among users, blockchain platform, and cyber-insurer. The user's optimal demand of blockchain service, blockchain platform's optimal pricing strategy, and cyberinsurer's optimal investment strategy are analytically derived by solving the joint market equilibrium problem.

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE

## *B. Physical Safety*

- *CPSS-based Solutions:*
  - ✓ Apart from the single cyber perspective, existing CPSS-based solutions afford lessons for cyberthreat defense and physical safety protection in the metaverse from the perspective of interactions between cyber and physical worlds.

  - ✓ Vellaithurai et al. [154] introduce cyber-physical security indices for security measurement of power grid infrastructures. The cyber probes (e.g., IDS) are deployed on host systems to profile system activities, where the generated logs along with the topology information are to build stochastic Bayesian models using belief propagation algorithms.

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE

## *C. Society Management*

- *Human Safety and Cyber syndromes:*
  - ✓ Casey et al. [152] investigate a new attack named **human joystick attack** in immersive VR systems such as Oculus Rift and HTC Vive. In their work, adversaries can modify VR environmental factors to deceive, disorient, and control immersed human players and move them to other physical locations without consciousness.
  - ✓ Valluripally et al. [155] present a novel cybersickness mitigation method and several design principles in social VR learning scenarios via threat quantification and attack-fault tree model construction.
  - ✓ However, the ethical issues and adaptations to different attack-defense strategies are not considered in their work, which is an important factor for future metaverse construction. Besides, more research efforts are required on the mitigation of other immersion risks to human body and human society.

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE

## *C. Society Management*

- *Society Acceptance Advances in Industry:*

  ✓ To enforce age-appropriate interactions within its platforms, Meta has enhanced its age certification mechanism with GDPR-compliance, where a tool named Transfer Your Information (TYI) is developed in 2021 [162].

  ✓ In TYI, users are allowed to retract their personal information from Meta whenever they intend.

# VIII. THREATS TO PHYSICAL WORLD AND HUMAN SOCIETY AND COUNTERMEASURES IN METAVERSE

## *D. Summary and Lessons Learned*

- For physical safety and social effect in the metaverse, we have learned that existing cyber-insurance and CPSS based approaches can offer some insights for protecting physical devices.
- More related technological and sociological efforts in this field considering the characteristics of metaverse are required.
- A comparison of existing/potential security countermeasures to physical safety and social effect in the metaverse is presented in Table X.

TABLE X

SUMMARY OF EXISTING/POTENTIAL SECURITY COUNTERMEASURES TO PHYSICAL AND SOCIAL THREATS IN METAVERSE

| **Ref.** | **Security Threat** | ⋆ **Purpose**<br>• **Advantages**<br>◦ **Limitations** | **Utilized Technology** |
|---|---|---|---|
| [159] | Threats to cyber insurance | ⋆Game theoretical modeling among users, blockchain platform, and cyber-insurer<br>•Analytically derive the market equilibrium with all participants' optimal strategies<br>◦Lack scalable and dynamic insurance coalition formation and fair premium design | Sequential game |
| [154] | Stochastic risk on power system | ⋆Cyber-physical security indices for security measurement of power systems<br>•Efficient indices computing under actual attacks in real-world test-bed<br>◦Lack merging other cutting-edge technologies into this framework | Graph theory |
| [158] | High premium stipulation | ⋆Coalitional insurance with budget compliance for risk control in power grids<br>•High defense level with long-term reduced premiums<br>◦Lack dynamic insurance design and dependence analysis of cyberthreats | Cyber-insurance |
| [156] | Butterfly effect in information spreading | ⋆Minimize misinformation influence via dynamic node blocking in OSNs<br>•Low misinformation spreading value and misinformation interactions<br>◦Challenging to be applied to the dynamic and time-varying metaverse | Heuristic greedy |
| [152] | Human joystick attack | ⋆Construct human joystick attack model in immersive VR systems<br>•Deceive and move immersed players to intended physical locations unconsciously<br>◦Lack effective defense design | HCI, VR |

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE (P.24)

## *A. Threats to Metaverse Governance*

- In analogy to the social norms and regulations in the real world, the interactions among avatars in the metaverse should align with the digital norms and regulations to ensure compliance.
- In the supervision and governance process of metaverse, the following threats may deteriorate system efficiency and security:
  - *New Laws & Regulations for Virtual Crimes:*
    - ✓ Essentially, it is difficult to decide whether a virtual crime is the same as a real one. Thereby, it is hard to directly apply the laws and regulations in real life to enforce penalization for criminal actions such as abusive language, virtual harassment, virtual stalking/spying, and so on.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *A. Threats to Metaverse Governance*

- *Misbehaving Regulators:*

  - ✓ Regulators may misbehave and cause system paralysis, and their authorities also need supervision.
  - ✓ Dynamic and effective punishment/reward mechanisms should be enforced for misbehaving/honest regulators, respectively.
  - ✓ To ensure sustainability, punishment and reward rules should be maintained by the majority of avatars in a decentralized and democratic manner.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *A. Threats to Metaverse Governance*

- *Threats to Collaborative Governance:*

  ✓ To avoid the concentration of regulation rights, collaborative governance under hierarchical or flat mode is more suitable for large-scale metaverse maintenance.

  ✓ Nevertheless, collusive regulators may undermine the metaverse system even under collaborative governance scenarios.

  ✓ For example, they can collude to make a certain regulator partitioned from the network via wormhole attacks.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *A. Threats to Metaverse Governance*

- *Threats to Digital Forensics:*

  ✓ Digital forensics in the metaverse means the virtual reconstruction of cybercrimes by identifying, extracting, fusing, and analyzing evidences obtained from both real and virtual worlds.

  ✓ Nevertheless, due to the high dynamics and interoperability issues of various virtual worlds, it is challenging for efficient forensics investigation including 25 entity-behavior association, identification, and tracing among anonymous users/avatars with diverse behavior patterns in the metaverse.

  ✓ Bad actors may produce fake news, faces, audios, and videos via AI algorithms to mislead the public, just like the recent Deepfake event.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Digital Governance in Metaverse*

- Almeida et al. [163] highlight three principles in the digital governance of content moderation ecosystems:
  - open, transparent, and consensus-driven,
  - respect human rights, and
  - publicly accountable
- This subsection review existing potential solutions to metaverse governance from the following three fields.

  - *AI Governance:*

    - ✓ With the pervasive fusion of perception, computing, and actuation, AI will play a leading role to allow digital self-governance of individuals and society in the metaverse in a fully automatic manner.
    - ✓ AI approaches can be employed for detecting misbehaving entities and abnormal or Sybil accounts in the metaverse.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Digital Governance in Metaverse*

- *Decentralized Governance:*

  - ✓ For governance in the largescale metaverse maintenance, centralized regulatory can face multiple technical and standard obstacles and difficulty in the compatibility of transnational regulations.
  - ✓ Blockchain technologies offer potential decentralized solutions for collaborative governance in the metaverse, where smart contracts offer a straightforward approach for decentralized governance in an automatic manner.
  - ✓ Febrero et al. [164] present a blockchain-based decentralized framework in digital city governance to encourage users' active engagement and witness in all administrative processes. In their approach, a verifier group is dynamically selected from digital citizens for transaction verification in the hybrid blockchain.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Digital Governance in Metaverse*

- *Decentralized Governance:*
  - ✓ Based on SDN, Bai et al. [166] design a decentralized data lifecycle governance architecture, where UGC owners can implement customized governance rules for data usage to VSPs, aiming to promote an open environment to satisfy users' diverse requirements.
  - ✓ Li et al. [171] study a Dirichlet-based probabilistic detection model to detect compromised local agents in decentralized power grid control systems by evaluating their reputation levels using historical operating observations.
  - ✓ The implementation of AI governance under decentralized architectures is a future trend for metaverse governance.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Digital Governance in Metaverse*

- *Trusted Digital Forensics:*

  - ✓ Digital forensics is an enabler for accountability in the metaverse under disputes, which has been widely investigated in images and videos.
  - ✓ Swaminathan et al. [172] develop a general forensic mechanism for digital camera images, according to the observation that in-camera and post-camera image processing leaves a series of distinct fingerprint traces on the digital camera image. The estimated post-camera fingerprints can be employed to validate image authenticity.
  - ✓ However, the use of anti-forensics makes trusted digital forensics challenging. An obstacle of digital forensics in the metaverse lies in trustworthiness and labor cost especially for cross-platform operations. Blockchain can offer a decentralized solution to establish trust and enhance automation in multi-party cross-platform digital forensics.

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *B. Digital Governance in Metaverse*

- *Trusted Digital Forensics:*

  ✓ Digital forensics can also be utilized for accountability of privacy violations.

  ✓ Zou et al. [174] propose a privacy leakage forensics scheme with taint analysis and RAM mirroring to obtain digital evidences without touching user’s privacy data in a simulated virtual environment.

  ✓ More research efforts are required in terms of resilience, collaboration, QoS enhancement, and privacy preservation in the implementation of digital forensics for metaverse applications

# IX. GOVERNANCE-RELATED THREATS AND COUNTERMEASURES IN METAVERSE

## *C. Summary and Lessons Learned*

- For digital governance in the metaverse, we have learned that AI-enabled governance and decentralized governance are two trends for future metaverse regulation.

- Moreover, trusted digital forensics offers a promising tool to regulate the metaverse.

- Besides, it is important to leverage AI and blockchain technologies to promote the self-governance capabilities of metaverse communities, where each community forms an autonomous code of conduct and users can report the violation behavior according to the terms.

- More research efforts are required from both technological and sociological perspectives. Advanced security solutions tailored to the metaverse setting are needed. A comparison of existing/potential security countermeasures to metaverse governance is presented in Table XI

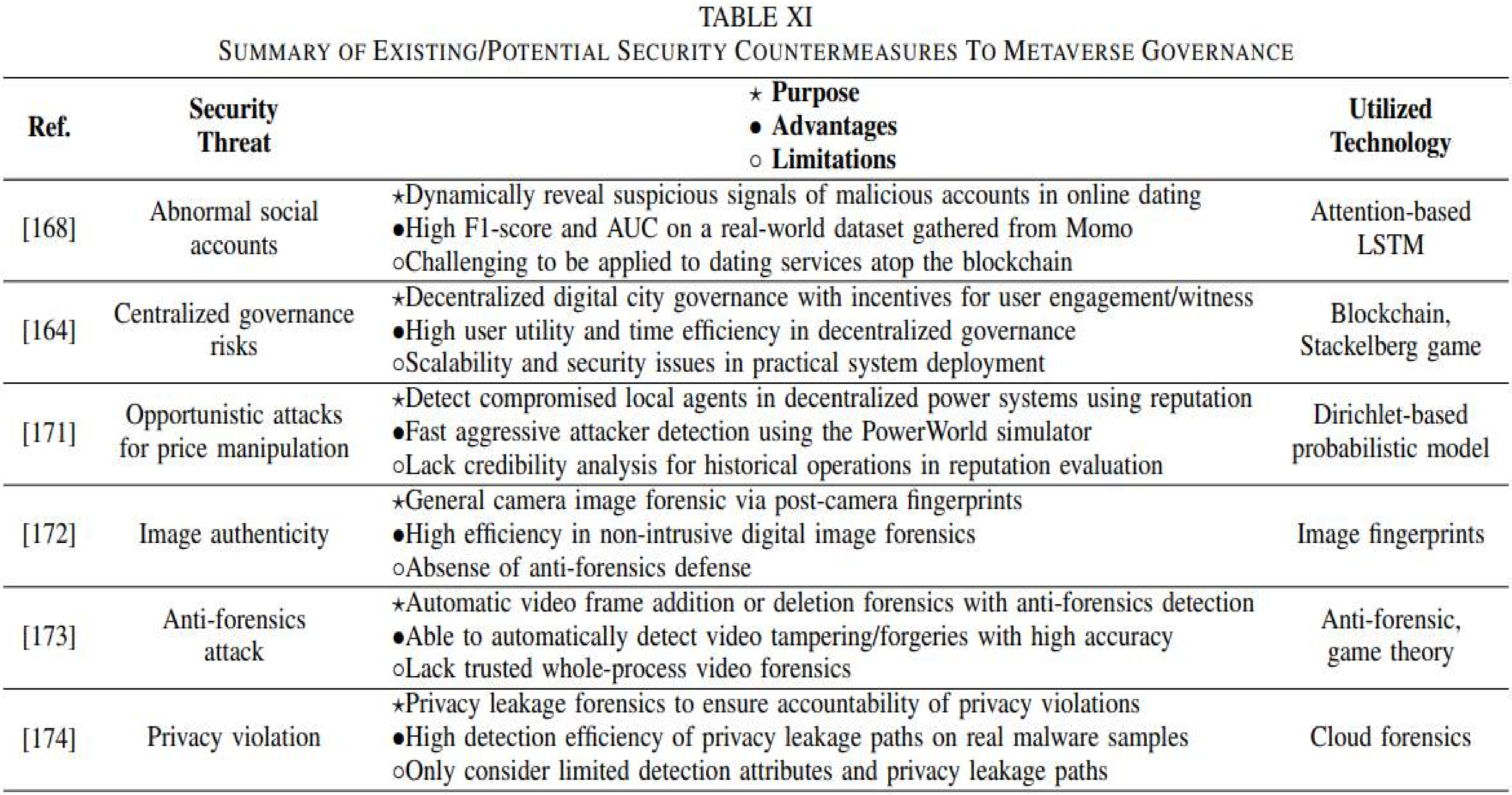


TABLE XI

SUMMARY OF EXISTING/POTENTIAL SECURITY COUNTERMEASURES TO METAVERSE GOVERNANCE

| Ref. | Security Threat | ⋆ Purpose<br>• Advantages<br>◦ Limitations | Utilized Technology |
|---|---|---|---|
| [168] | Abnormal social accounts | ⋆Dynamically reveal suspicious signals of malicious accounts in online dating<br>•High F1-score and AUC on a real-world dataset gathered from Momo<br>◦Challenging to be applied to dating services atop the blockchain | Attention-based LSTM |
| [164] | Centralized governance risks | ⋆Decentralized digital city governance with incentives for user engagement/witness<br>•High user utility and time efficiency in decentralized governance<br>◦Scalability and security issues in practical system deployment | Blockchain, Stackelberg game |
| [171] | Opportunistic attacks for price manipulation | ⋆Detect compromised local agents in decentralized power systems using reputation<br>•Fast aggressive attacker detection using the PowerWorld simulator<br>◦Lack credibility analysis for historical operations in reputation evaluation | Dirichlet-based probabilistic model |
| [172] | Image authenticity | ⋆General camera image forensic via post-camera fingerprints<br>•High efficiency in non-intrusive digital image forensics<br>◦Absense of anti-forensics defense | Image fingerprints |
| [173] | Anti-forensics attack | ⋆Automatic video frame addition or deletion forensics with anti-forensics detection<br>•Able to automatically detect video tampering/forgeries with high accuracy<br>◦Lack trusted whole-process video forensics | Anti-forensic, game theory |
| [174] | Privacy violation | ⋆Privacy leakage forensics to ensure accountability of privacy violations<br>•High detection efficiency of privacy leakage paths on real malware samples<br>◦Only consider limited detection attributes and privacy leakage paths | Cloud forensics |

# X. FUTURE RESEARCH DIRECTIONS (P.26)

## *A. Endogenous Security Empowered Metaverse*

- Existing commercial metaverse systems mainly depend on the brought-in security such as frequent security patch upgrades after the system deployment. Although security upgrades can enhance system security to an extent, the passive defense mechanisms built on security patching strategies inevitably result in the curse of being continuously broken.

- Endogenous security theory offers a promising solution for provisioning built-in security or called secure by design mechanisms with self-protection, self-evolution, and autoimmunity capabilities [175], which takes security and privacy factors into account before the system design.

- An example of endogenous security is the quantum key distribution (QKD) [176], which utilizes channel-based secret keys to resolve information disclosure in wireless transmissions via quantum entanglement properties. Besides, quantum-resistant cryptography (QRC) for quantum secure metaverse applications is another promising research direction.

# X. FUTURE RESEARCH DIRECTIONS

## *B. Cloud-Edge-End Orchestrated Secure Metaverse*

- In the metaverse, different users/services have distinct QoE/QoS requirements, which incurs huge difficulty for the metaverse network to simultaneously offer these holographic services for massive users/avatars.

- The orchestration of cloud-edge-end computing offers a potential solution by collaboratively and dynamically sharing computation, communication, and storage resources among various entities, thereby enhancing the QoE for users/avatars and QoS for metaverse services, as shown in Fig. 16.

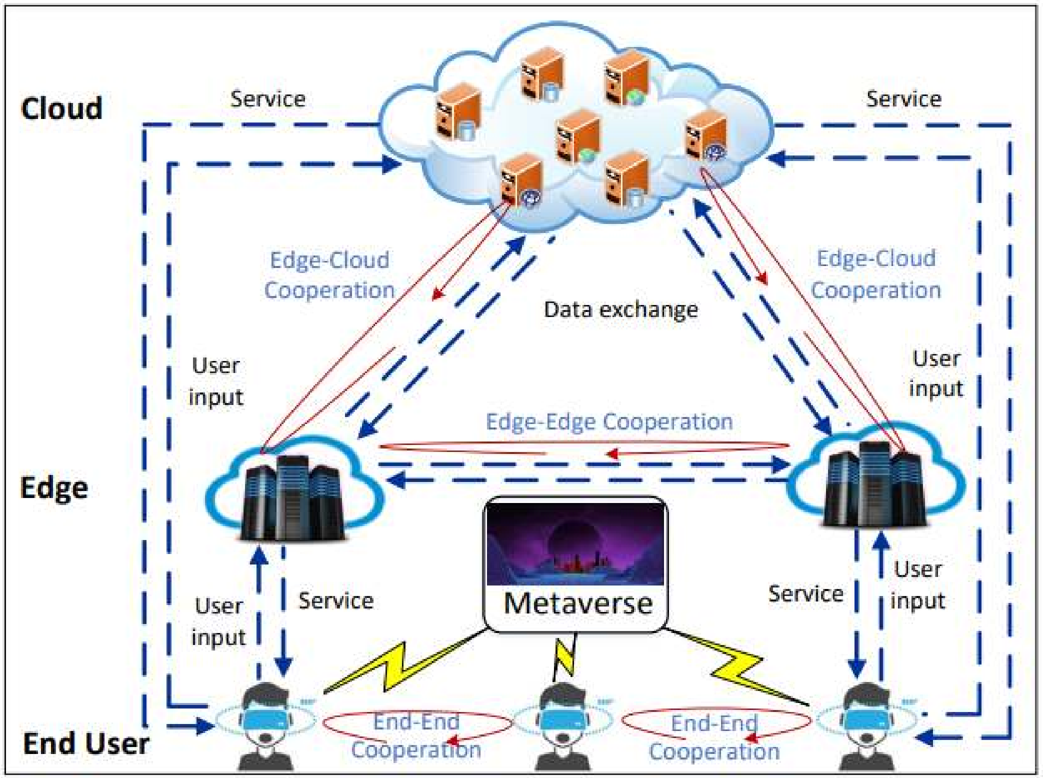


Fig. 16. Illustration of cloud-edge-end computing in metaverse service offering.

# X. FUTURE RESEARCH DIRECTIONS

## *B. Cloud-Edge-End Orchestrated Secure Metaverse*

- Besides, cloud-edge-end computing can assist edge intelligence and user privacy protection by aggregating and processing users' private data at edge devices (e.g., home gateways) via federated edge learning.

- In addition, by analyzing the metaverse system as a whole, the cooperation among various sub-metaverses is essential to facilitate seamless security provision and privacy protection and requires further investigation.

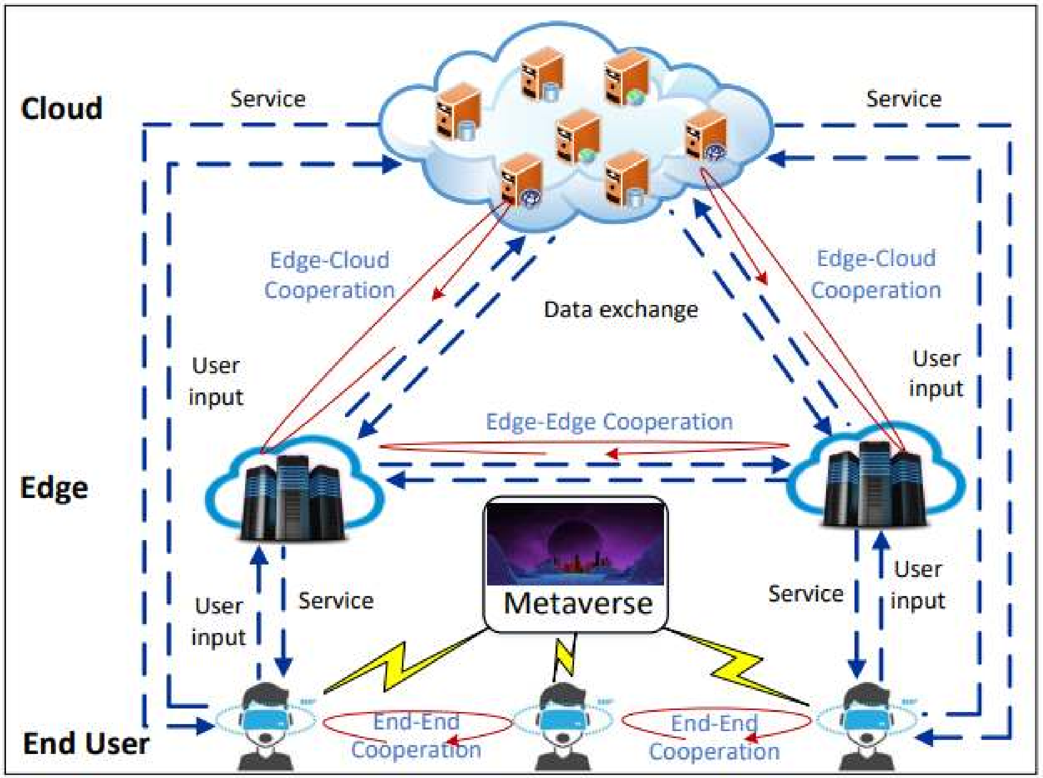


Fig. 16. Illustration of cloud-edge-end computing in metaverse service offering.

# X. FUTURE RESEARCH DIRECTIONS

## *C. Cross-Chain Interoperable and Regulatory Metaverse*

- By getting rid of trusted third parties, blockchain is recognized as the underlying technology to build the future trust-free economy ecosystem in the metaverse.
- However, distinct sub metaverses may deploy services on heterogeneous blockchains such as using different transaction formats, block structures, and consensus protocols to meet QoS requirements, resulting in severe interoperability concerns.
- As shown in Fig. 17, efficient cross-chain authentication and governance are essential to ensure the security and legitimacy of digital asset-related activities across different sub-metaverses built on heterogeneous blockchains.

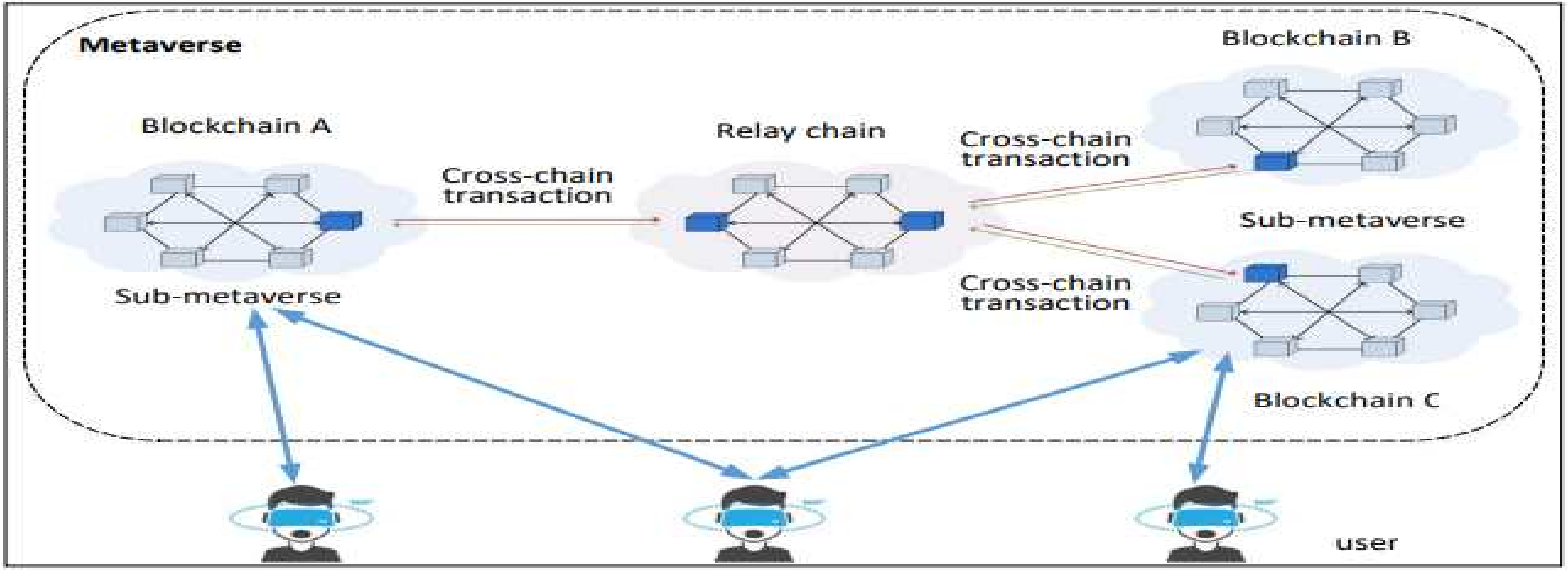


Fig. 17. Illustration of cross-chain services among three sub-metaverses which are built on three different blockchains. A relay chain is established to support cross-chain transactions [177], where the relay chain synchronies the information of source blockchain $A$ to allow destination blockchains $B$ and $C$ to verify the correctness of transactions on source blockchain $A$.

# X. FUTURE RESEARCH DIRECTIONS

## *C. Cross-Chain Interoperable and Regulatory Metaverse*

- The implementation, efficiency, and security of identity authentication across various domains and blockchains in the metaverse need to be further investigated.
- Moreover, novel decentralized, hierarchical, and penetrating cross-chain governance mechanisms need further research efforts in the metaverse.
- Besides, efficient metaverse specific consensus mechanisms, redesigned block structures, as well as well-designed user incentives are required for distinct metaverse applications.
- Open challenges include application-specific governance rule design, programmable and scalable cross-chain governance architecture design, on-chain entity identification and risk assessment, dynamic and collaborative cross-chain governance

# X. FUTURE RESEARCH DIRECTIONS

## *D. Energy-Efficient and Green Metaverse*

- The future metaverse design should be energy-efficient and green to attain sustainability.
- Users/avatars' cooperation can offer a possible solution for green metaverse in terms of UGC/AIGC dissemination, cooperative networking, and cooperative computation.
- Apart from user cooperation and new green technology design, other possible solutions include new architecture design, new green edge-cloud computing design, new energy-efficient consensus protocol design, etc., to support green networking and computing in the metaverse.

# X. FUTURE RESEARCH DIRECTIONS

## *E. Content-Centric and Human-Centric Metaverse*

- In the future metaverse, a surge of UGC is expected to be created, requested, and delivered across various sub-metaverses.
- Existing IP-based content transmissions can face critical challenges in securing UGC dissemination to massive heterogeneous end devices over the large-scale metaverse across virtual worlds.
- Content-centric networking (CCN) stands for a paradigm shift of current Internet architecture.
- In contrast to current IP-based and host-oriented Internet architecture, contents are addressed and routed directly by their naming information in CCN instead of IP addresses.
- In CCN-based metaverse, the UGC consumer can request the desired UGC object by sending an interest message to any CCN node that hosts the matched UGC.

# X. FUTURE RESEARCH DIRECTIONS

## *E. Content-Centric and Human-Centric Metaverse*

- The deployment of CCN can offer a more flexible, scalable, and secure network in the metaverse.
- However, CCN also brings new security concerns in the metaverse and one of them is content poisoning, in which adversaries can contaminate the cache space of metaverse nodes by injecting poisoned UGCs and further cause the delay and even failure in retrieving valid UGCs via flooding attacks.
- In addition, the design of metaverse should be human-centric.
- For example, users/avatars' personalized privacy preferences should be ensured in developing privacy-preserving approaches in metaverse environments.

# XI. CONCLUSION (P.27)

- This paper presented an in-depth survey of the fundamentals, security, and privacy of metaverse.
- The security and privacy threats, as well as the critical challenges in security defenses and privacy preservation, have been investigated under the distributed metaverse architecture.
- The authors reviewed the existing/potential solutions in designing tailored security and privacy countermeasures for the metaverse.

# OPINION

- With the fast development of AI, XR, VR, AR, Blockchain, and Digital Twin technologies, Metaverse is expected to be the next internet generation in the near future.
- Multiple large companies such as Microsoft and Meta are currently investing billions of dollars into Metaverse applications (Software and Hardware development) to make it available to the average user.
- However, as mentioned before, Metaverse is a fusion of multiple cutting-edge technologies, thus the security and privacy issues and threats are more critical.
- The current industrial and academic are mainly focusing on the development of Metaverse applications and its utilization and implementation is real world, yet, very few approaches has been done to enhance its security.
- Based on the possible security threats discussed in this paper, I believe that more work should be done regarding the security and privacy perspective before any further development of Metaverse application (before a mass distribution and implementation of Metaverse applications).

# A SURVEY ON METAVERSE : FUNDAMENTALS, SECURITY, AND PRIVACY

**THANK YOU!**