Ph.D.: Byzantine-Tolerant Netcodes For Tomorrow's Metaverse

January 2023

1 Contact Information and Supervisory Team

Supervisor Team:	David Bromberg (PU, U. Rennes), François Taiani (PU, U. Rennes), Jérémie Decouchant (TU Delft)
	{david.bromberg,francois.tainai}@irisa.fr, j.decouchant@tudelft.nl
Laboratories:	Inria Centre at Rennes University
Research Group:	WIDE (the World Is DistributEd)
Location:	Rennes (France)
Funding:	three-year fixed-term work contract (with standard French health-benefits and retirement plan)
Keywords:	Metaverse, Virtual World, Decentralization, Replication, Byzantine Fault-Tolerance, Distributed Algorithms, Middleware

2 Context and Motivation

2.1 The Rise of the Metaverse

Although there is no consensus on an exact definition yet, the metaverse is generally understood as an open virtual world in which users can interact, contribute content, and engage in monetized transactions (both over user-created content and out-of-metaverse services and goods [1]). Interactions are usually understood as taking place in a three-dimensional world (possibly experienced through a virtual reality device), but earlier online experiments (including textual MMORPGs of the 80's) have shown that other modes of interactions are possible.

The potential of the metaverse has been largely popularized by Mark Zuckerberg, one of Facebook's co-founders and Meta's CEO (Facebook's parent company). In spite of this recent promotion, the metaverse has deep roots that go back several decades. Among its inspirations lie online multiplayer role-player games (MMORPG) from the 90's and early 2000's such as Habitat, Ultima Online, and World of Warcraft, as well as virtual open worlds, notably Second Life, which grew to prominence in the late 2000s.

Although the metaverse, as envisioned by its supporters, is far from being a reality, many of its core ingredients (e.g., openness, massive multiplayer interactions, and monetization) can today be found in modern and widely used games. Fortnite, for instance, is a multiplayer battle-royal free-to-play 3D game initially released in 2017, that is highly popular among teenagers. Although free, Fortnite offers an in-game currency, V-Bucks, that can be bought using real-world money or obtained by playing the game. V-bucks allow players to buy virtual content in-game (such as character outfits and virtual items). In one of its variants (Fortnite Creative), Fornite even offers a free-to-play sandbox world where users can design and shape their own island and invite other players. Both Fortnite and Fortnite Creative have been used to host virtual events, such as concerts and exhibits [2]. Similarly, Minecraft, a popular sandbox game with a multi-player version, offers an online currency (Minecoin) that can be exchanged against real-world money and can be used to buy virtual contents, such as skins, texture packs, and even entire worlds.

2.2 Replication, Consistency, and Malicious Behaviors

As these virtual experiences progressively combine gaming elements, monetary transactions, and monetized content (either provided by the game's developer, but also increasingly by other users and actors acting as content creators), the reliability of such platforms is becoming increasingly important.

Unfortunately, the robustness and fault tolerance that ensure the consistency, replication, and persistence of a metaverse's state over multiple machines have been little studied. Distributed 3D and VR games today are typically built on industrial engines (two leading examples are the Unity and Unreal engines, which power some of the most visible games in the industry). These engines typically embark some distributed logic (known as a *netcode*) to distribute a game's state across multiple machines [3, 4]. Netcodes either follow a client-server (the most common) or P2P logic [5] and rely on heuristics and optimization (such as delays and rollbacks) to ensure an acceptable level of quality of experience (e.g. high reactivity and low latency [6, 7]), even in a degraded network.

In the past, weaknesses in the security of netcodes have been exploited to obtain an unfair advantage over other players, using a variety of attacks. For instance, a lag switch allows players to temporarily degrade or even cut their internet connection to simulate a high network latency. As a result, opponents will tend to freeze locally, allowing the cheating player to overcome them more easily. To remote players, the infracting player will appear to suddenly "teleport", freeze, or become invincible. Similarly, some attacks modify network packets to include fake timestamps (e.g., in *look-ahead attacks*), allowing players seemingly to guess in advance opponent moves, while yet others exploit the game-state known the local client to reveal useful but illegitimate information to a player (e.g., removing walls, generically known as a *wallhack*).

Such hacks have long been identified as problematic by the gaming industry, which has developed punctual countermeasures, including lag switch detectors, or by repatriating most of the game logic onto the server. The problem, however, has been little studied by the research community [8] and is poised to grow in importance with the growth of decentralized metaverse applications beyond simple gaming. In particular, we anticipate that metaverse operators will have to reconcile the need to replicate content (for reliability, availability, and performance reasons), possibly reusing earlier research on P2P games [9, 10], and the need to ensure some consistency between the copies of the world-state in spite of potentially rogue participants. Such a context directly chimes in with research on Byzantine Fault-Tolerant (BFT) algorithms that are able to withstand the corruption of a proportion of the devices they run on [11, 12, 13]. BFT replication protocols are however not usually designed with the needs of a metaverse world in mind. In particular, BFT replication protocols are usually very costly, do not scale well, and induce high delays. These limits directly conflict with the soft real-time constraints put on on metaverse virtual world in order to support seamless and high-quality user interactions.

3 Ph.D. Objectives

This PhD seeks to reconcile the performance needs of metaverse virtual worlds with a high level of protection against rogue participants by exploiting the expertise of the WIDE team in lightweight Byzantine Fault-Tolerant protocols [14, 15, 16, 17].

This PhD aims to develop novel **Byzantine-tolerant replication mechanisms** that espouse the **unique requirements of a metaverse's virtual world**, notably in terms of responsiveness and latency. In particular, the PhD will explore how Byzantine Fault-Tolerant techniques can be accelerated using two central strategies: (i) by using **adaptive levels of protection** for different parts of a meta-verse world, and (ii) by allowing for **optimistic local decisions** coupled with micro-rollbacks in case malicious discrepancies are later discovered.

3.1 Research Questions & Work Plan

More specifically, we foresee that achieving this objective requires addressing three challenges:

1. **How can adaptive levels of protection against malicious (aka Byzantine) behavior help accelerate BFT replication techniques?** Metaverse worlds often embed various data and objects (3D buildings & landscapes, recorded sounds and videos, textual information) that do

not all require the same level of protection or consistency among users. This heterogeneity offers the opportunity to develop Byzantine-tolerant replication mechanisms that adapt their guarantees to the level of protection needed by varying elements of the world in order to limit replication costs. One challenge, however, consists in developing techniques able to harmoniously coordinate these different levels of protection in a seamless experience for users, including when the world is under attack by malicious participants.

2. **How can local optimistic replication decisions be combined with short-period roll-backs to increase the reactivity of BFT redundancy algorithms?** In a second strand of research, we will explore how the cost of BFT replication protocol can be reduced by allowing local nodes to take unsafe, yet low-risk, local actions to accelerate the replication algorithm while still providing a fall-back mechanism through local roll-backs in the case of Byzantine behavior. Such an approach would essentially relax the persistence guarantees that traditional BFT algorithms provide in order to obtain performance gains and mirror some of the strategies already used in some games to mask transient network problems.

3. **In metaverses that exploit an underlying blockchain, how should the interactive state of the world be coupled with the underlying blockchain to strengthen the metaverse's overall security?** Many metaverse proposals include using an underlying blockchain (or, more generally, distributed ledger) to record and secure in-world transactions. Blockchains are usually heavy and cumbersome to use for near-real-time replication but can provide an additional opportunity to harden the replication mechanisms of the metaverse world. A straightforward yet costly approach could, for instance, include world checkpoints. We will explore how more flexible and less costly strategies could be used to benefit from the heightened guarantees of the underlying blockchain while retaining the necessary interactive reactivity required of a metaverse world.

4 Profile of the Optimal Candidate for this PhD

The candidate recruited for this Ph.D. should have a Master's Degree in Computer Science or equivalent, with **a solid algorithmic and systems background**, particularly regarding at least one of the following: distributed computer systems, distributed algorithms, and Byzantine Fault-Tolerant algorithms. Good programming skills and **a willingness to learn about new techniques** (decentralized machine learning and privacy protection) are also crucial, as well as good writing skills and the ability to propose, present, and discuss new ideas in a collaborative setting.

References

[1] E. Williams, B. Eyo, and S. Akpan. "Linden Labs Second Life: Understanding the Business Model and Sources of Commercial and Social Success or Decline of Second Life". In: *Computer and Information Science* 4.2 (2011), p. 96.

[2] B. Francis. "Epic and Time Magazine debut interactive MLK Jr. exhibit in Fortnite". In: *Game Developer* (Aug. 2021). Accessed January 23, 2022.

[3] A. Lioret, L. Diler, S. Dalil, and M. Mota. "Hybrid Prediction for Games' Rollback Netcode". In: *SIGGRAPH Posters*. ACM, 2022, 3:1–3:2.

[4] M. Ahmed, S. Reno, M. R. Rahman, and S. H. Rifat. "Analysis of Netcode, Latency, and Packet-loss in Online Multiplayer Games". In: *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*. 2022, pp. 1198–1202.

[5] T. Walker, B. Gilhuly, A. Sadeghi, M. Delbosc, and S. L. Smith. "Predictive Dead Reckoning for Online Peer-to-Peer Games". In: *IEEE Transactions on Games* (2023).

[6] K.-T. Chen, Y.-C. Chang, H.-J. Hsu, D.-Y. Chen, C.-Y. Huang, and C.-H. Hsu. "On the quality of service of cloud gaming systems". In: *IEEE Transactions on Multimedia* 16.2 (2013), pp. 480–495.

[7] P. Quax, P. Monsieurs, W. Lamotte, D. De Vleeschauwer, and N. Degrande. "Objective and subjective evaluation of the influence of small amounts of delay and jitter on a recent first person shooter game". In: *Proceedings of 3rd ACM SIGCOMM workshop on Network and system support for games*. 2004, pp. 152–156.

[8] A. Yahyavi, K. Huguenin, J. Gascon-Samson, J. Kienzle, and B. Kemme. "Watchmen: Scalable Cheat-Resistant Support for Distributed Multi-player Online Games". In: *IEEE 33rd International Conference on Distributed Computing Systems, ICDCS 2013, 8-11 July, 2013, Philadelphia, Pennsylvania, USA*. IEEE Computer Society, 2013, pp. 134–144.

[9] R. Diaconu, J. Keller, and M. Valero. "Manycraft: Scaling Minecraft to Millions". In: *Annual Workshop on Network and Systems Support for Games, NetGames '13, Denver, CO, USA, December 9-10, 2013*. IEEE/ACM, 2013, 1:1–1:6.

[10] J. Gascon-Samson, B. Kemme, and J. Kienzle. "Lamoth: A Message Dissemination Middleware for MMOGs in the Cloud". In: *Annual Workshop on Network and Systems Support for Games, NetGames '13, Denver, CO, USA, December 9-10, 2013*. IEEE/ACM, 2013, 9:1–9:2.

[11] L. Lamport, R. E. Shostak, and M. C. Pease. "The Byzantine Generals Problem". In: *ACM Transactions on Programming Languages and Systems* 4.3 (1982), pp. 382–401.

[12] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song. "The Honey Badger of BFT Protocols". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS '16. Vienna, Austria: ACM, 2016, pp. 31–42. ISBN: 978-1-4503-4139-4.

[13] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and M. Yin. "Sync HotStuff: Simple and Practical Synchronous State Machine Replication". In: *IEEE Symposium on Security and Privacy (S&P)*. 2020, pp. 106–118.

[14] T. Albouy, D. Frey, M. Raynal, and F. Taïani. "Good-Case Early-Stopping Latency of Synchronous Byzantine Reliable Broadcast: The Deterministic Case". In: *DISC*. Vol. 246. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 4:1–4:22.

[15] D. Frey, L. Guillou, M. Raynal, and F. Taïani. "Consensus-Free Ledgers When Operations of Distinct Processes are Commutative". In: *PaCT*. Vol. 12942. Lecture Notes in Computer Science. Springer, 2021, pp. 359–370.

[16] T. Albouy, D. Frey, M. Raynal, and F. Taïani. "Byzantine-Tolerant Reliable Broadcast in the Presence of Silent Churn". In: *SSS*. Vol. 13046. Lecture Notes in Computer Science. Springer, 2021, pp. 21–33.

[17] A. Auvolat, D. Frey, M. Raynal, and F. Taïani. "Byzantine-tolerant causal broadcast". In: *Theor. Comput. Sci.* 885 (2021), pp. 55–68.