

แนวทางการป้องกันและลดผลกระทบจากการตกเป็นผู้เสียหายจากเกมบล็อกเชน : กรณีศึกษา ผู้ให้ข้อมูลผ่านทาง Facebook

จุฑาทิพย์ จารึกเรียบ^{1*}

Received 19 May 2025

Revised 19 September 2025

Accepted 27 October 2025

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยและผลกระทบที่เกิดขึ้นกับผู้เสียหายจากการเล่นเกมบล็อกเชน (GameFi) เพื่อเสนอแนวทางการป้องกันและแก้ไขปัญหาที่เกิดขึ้น โดยใช้วิธีการวิจัยเชิงคุณภาพ รวบรวมข้อมูลผ่านการสัมภาษณ์กึ่งมีโครงสร้างจากกลุ่มผู้เสียหาย จำนวน 15 ราย เจ้าหน้าที่ตำรวจที่เกี่ยวข้องจำนวน 4 ราย และผู้เชี่ยวชาญเกี่ยวกับเกมบล็อกเชน โดยมีประสบการณ์มากกว่า 5 ปี จำนวน 2 ราย รวมทั้งสิ้น 21 ราย

ผลการศึกษาพบว่า ปัจจัยสำคัญของการตกเป็นผู้เสียหาย ได้แก่ ปัจจัยด้านแรงจูงใจทางการเงิน ปัจจัยด้านความรู้และความเข้าใจ และปัจจัยด้านสื่อและการตลาด ซึ่งส่งผลกระทบต่อผู้เสียหายที่เล่นเกมบล็อกเชน (GameFi) ทั้งในด้านการเงิน ที่สูญเสียทรัพย์สินจำนวนมาก ในด้านผลกระทบทางจิตใจและสังคม เช่น ผู้เสียหายเกิดความเครียดหรือซึมเศร้า อีกทั้งกระทบความสัมพันธ์กับคนรอบข้างไปด้วย และในด้านความเชื่อมั่นทางกฎหมาย ที่ผู้เสียหายไม่สามารถเรียกร้องความยุติธรรมได้โดยง่าย เนื่องจากมีข้อจำกัดของกฎหมายที่เกี่ยวข้องกับเทคโนโลยีใหม่ในการดำเนินคดีกับอาชญากร งานวิจัยนี้ได้เสนอแนวทางในการป้องกันและลดผลกระทบ โดยในระดับปฏิบัติการที่สามารถดำเนินการได้ด้วยการให้ความรู้แก่ประชาชนเกี่ยวกับความเสี่ยงและกลโกงต่าง ๆ ที่เกิดขึ้นบ่อยครั้ง รวมถึงการสร้างระบบแจ้งเตือน และช่องทางร้องทุกข์ออนไลน์ที่เข้าถึงง่ายและรวดเร็ว นอกจากนี้ในระดับนโยบาย ควรมีการออกแบบและบังคับใช้กฎระเบียบจากภาครัฐที่มีประสิทธิภาพยิ่งขึ้น เช่น จัดตั้งหน่วยงานเฉพาะด้าน GameFi ปรับปรุงหรือร่างกฎหมายหรือระเบียบเฉพาะเกี่ยวกับ GameFi รวมถึงกำหนดให้มีระบบทะเบียนเกมบล็อกเชน (GameFi Registry System) เพื่อสร้างระบบที่ปลอดภัยและลดโอกาสในการตกเป็นผู้เสียหายในอนาคต

คำสำคัญ: เกมบล็อกเชน GameFi การป้องกันอาชญากรรม ผู้เสียหาย

¹ คณะอาชญาวิทยาและการบริหารงานยุติธรรม มหาวิทยาลัยรังสิต

* Corresponding author email: Mynampeung@gmail.com

PREVENTIVE MEASURES AND MITIGATION STRATEGIES FOR THE IMPACT OF BECOMING A VICTIM OF BLOCKCHAIN GAMES: A CASE STUDY OF INFORMANTS VIA FACEBOOK

Jutatip Jaruakriab^{1*}

Abstract

This study explores the factors and impacts associated with victimization from playing blockchain-based games (GameFi) and proposes preventive and remedial measures. A qualitative research approach was used, employing semi-structured interviews with 15 victims, 4 law enforcement officers, and 2 blockchain game experts with over five years of experience, totaling 21 key informants.

The findings reveal three key contributing factors to victimization: financial motivation, knowledge and understanding, and media and marketing influences. These scams have resulted in severe consequences for victims, particularly financial loss, with many reporting the depletion of valuable assets. Psychological and social effects were also evident, including stress, depression, and strained personal relationships. Additionally, many victims reported a loss of confidence in the legal system, largely due to limitations in prosecuting crimes involving emerging technologies. This study proposes multi-level strategies to mitigate risks and prevent future victimization. At the operational level, public education on common scams and associated risks is essential, along with the development of accessible warning systems and efficient online complaint mechanisms. At the policy level, the government should enhance regulatory effectiveness by implementing stronger legal frameworks. This includes establishing a specialized agency for GameFi, revising or drafting specific laws and regulations related to GameFi, and implementing a GameFi Registry System to create a more secure environment and reduce the risk of individuals becoming victims in the future.

Keywords: Blockchain Games, GameFi, Crime Prevention, Victims

¹ Faculty of Criminology and Justice Administration, Rangsit University

* Corresponding author email: Mynampeung@gmail.com

บทนำ

ในปัจจุบัน เทคโนโลยีบล็อกเชนได้เข้ามามีบทบาทสำคัญในการพัฒนาเกมออนไลน์ โดยเฉพาะในรูปแบบที่เรียกว่า “GameFi” (Game + Finance) ซึ่งเป็นการผสมผสานองค์ประกอบของเกมเข้ากับระบบการเงินแบบไร้ตัวกลาง (Decentralized Finance: DeFi) และสินทรัพย์ดิจิทัล เช่น โทเคน และ NFT โดยเปิดโอกาสให้ผู้เล่นสามารถสร้างรายได้จริงผ่านกลไกที่เรียกว่า “เล่นเพื่อหารายได้” (play-to-earn) ซึ่งรายได้ดังกล่าวสามารถนำไปแลกเปลี่ยนเป็นสกุลเงินจริงได้ (Bitkub Academy, 2564; Proelss et al., 2023) GameFi จึงกลายเป็นทั้งเครื่องมือการลงทุนของนักพัฒนาและแพลตฟอร์มสร้างรายได้ของผู้เล่นทั่วโลก โดยเฉพาะในช่วงหลังการระบาดของโควิด-19 ที่หลายคนมองหาโอกาสทางการเงินในโลกดิจิทัล

งานวิจัยฉบับนี้ให้นิยาม “เกมบล็อกเชน” ว่า หมายถึงเกมที่มีองค์ประกอบด้านการเงินในลักษณะ GameFi เท่านั้น โดยไม่รวมเกมที่ใช้บล็อกเชนเพียงเพื่อการจัดเก็บข้อมูลหรือประวัติการเล่น ซึ่งในบริบทของประเทศไทย GameFi เติบโตอย่างรวดเร็วในช่วงปี พ.ศ. 2564–2565 โดยเฉพาะในช่วงที่เกิดการแพร่ระบาดของโควิด-19 ประชาชนจำนวนหนึ่งมองหาโอกาสสร้างรายได้จากที่บ้าน จึงหันไปเล่นเกมประเภทนี้ผ่านช่องทางโซเชียลมีเดีย เช่น Facebook และ YouTube โดยมีการสร้างกลุ่มชุมชนเพื่อแนะนำเกม วิธีลงทุน และการซื้อขายไอเทมภายในเกม (दनัย อรุณกิตติชัย, 2564; Suthiwong et al., 2022) อย่างไรก็ตาม แม้ GameFi จะถูกมองว่าเป็นนวัตกรรมทางการเงินในโลกดิจิทัลที่เปิดโอกาสให้ผู้เล่นสามารถสร้างรายได้จากการเล่นเกม แต่ในบริบทของประเทศไทย กลับพบว่ามีผู้ใช้ช่องทางนี้เป็นเครื่องมือหลอกลวงที่ซับซ้อนมากขึ้น โดยเฉพาะในกลุ่มผู้เล่นที่ขาดความรู้ทางเทคนิคเกี่ยวกับบล็อกเชน สินทรัพย์ดิจิทัล และกลไก Smart Contract สื่อมวลชนไทยได้รายงานว่า กลุ่มมิจฉาชีพใช้ GameFi เป็นช่องทางในการฉ้อโกงในลักษณะคล้ายแชร์ลูกโซ่ โดยหลอกให้ลงทุนในแพลตฟอร์มปลอม ใช้เหรียญดิจิทัลที่ไม่มีมูลค่าจริง และอ้างว่าเป็นโครงการถูกกฎหมายผ่านเอกสารและเว็บไซต์ที่น่าเชื่อถือ ซึ่งทาง Nation Thailand (2025) รายงานว่ามีการตรวจยึดทรัพย์สินมูลค่ากว่า 100 ล้านบาทจากคดีที่มีลักษณะใกล้เคียงกับ GameFi แม้จะไม่ระบุว่าเกี่ยวข้องโดยตรง แต่โครงสร้างการหลอกลวงมีความสอดคล้องอย่างชัดเจน ด้านต่างประเทศ งานของ Kell et al. (2023) วิเคราะห์กรณี Forsage ซึ่งใช้ Smart Contract สร้างโครงสร้างคล้ายแชร์ลูกโซ่โดยอาศัย GameFi เป็นฉากบังหน้า โดยพบว่ากว่าร้อยละ 88 ของผู้ขาดทุน ขณะที่ Kumar (2024) ชี้ว่ากฎหมายในหลายประเทศ รวมถึงประเทศไทย ยังไม่สามารถตามทันเทคโนโลยีการเงินแบบใหม่นี้ได้ทัน ส่งผลให้การติดตามผู้กระทำผิดที่ใช้ระบบกระจายศูนย์เป็นไปได้ยาก และยิ่งซับซ้อนขึ้นในกรณีที่ธุรกรรมเกิดในโลกเสมือน ปราบปรามการฉ้อโกงดังกล่าวสะท้อนให้เห็นว่า GameFi ในประเทศไทยมิได้เป็นเพียงทางเลือกด้านการลงทุน แต่กำลังกลายเป็นภัยไซเบอร์รูปแบบใหม่ที่แฝงอยู่ในรูปแบบความบันเทิง ผู้เสียหายจำนวนมากไม่สามารถแจ้งความหรือขอความช่วยเหลือได้ทันที่เนื่องจากไม่มีช่องทางเฉพาะด้าน ขาดกฎหมายควบคุมที่ชัดเจน และถูกตราหน้าว่า โลกหรือขาดวิจารณญาณทางการเงิน

ด้วยเหตุนี้ การศึกษาวิจัยในครั้งนี้จึงมีความจำเป็น เพื่อทำความเข้าใจปัจจัยและผลกระทบของผู้เสียหายจาก GameFi และเสนอแนวทางเชิงปฏิบัติและเชิงนโยบายที่เหมาะสมกับบริบทประเทศไทย นำไปสู่การป้องกันอาชญากรรมในโลกดิจิทัลได้อย่างเป็นระบบ

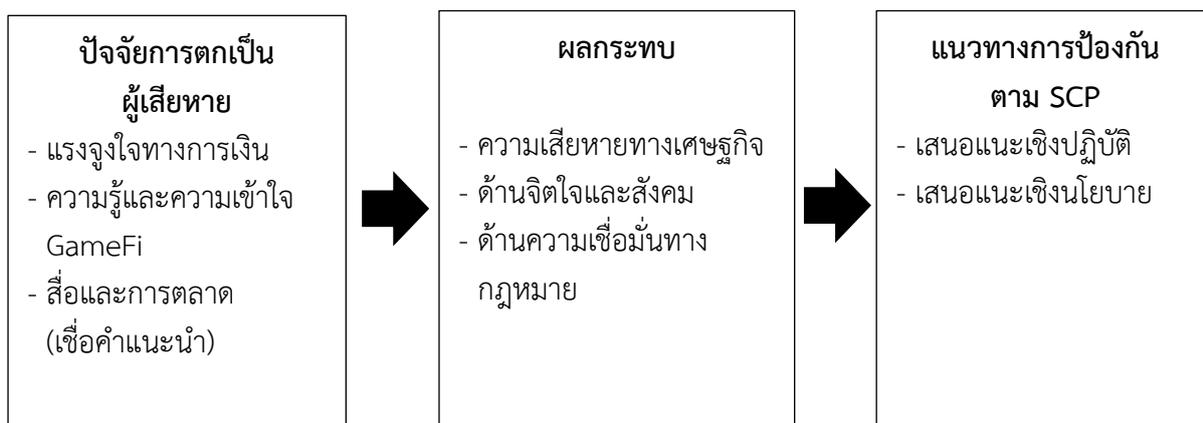
วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาปัจจัยของการตกเป็นผู้เสียหายจากเกมบล็อกเชน
2. เพื่อศึกษาผลกระทบที่เกิดขึ้นกับผู้เสียหายจากเกมบล็อกเชน

3. เพื่อเสนอแนวทางการป้องกันและลดผลกระทบจากการตกเป็นผู้เสียหายที่เกิดขึ้นจากเกมบล็อกเชน

กรอบแนวคิดการวิจัย

งานวิจัยนี้ได้ออกแบบกรอบแนวคิดจากการสังเคราะห์วรรณกรรมและทฤษฎีที่เกี่ยวข้องอย่างเป็นระบบ โดยอ้างอิงจาก 4 ทฤษฎีหลัก ได้แก่ ทฤษฎีเหยื่อวิทยา ใช้อธิบายลักษณะของผู้เสียหายทั้งบทบาทของเหยื่อเองและกลไกทางสังคม เช่น ขาดความรู้เท่าทันด้านเทคโนโลยี หรือมีการควบคุมตนเองต่ำ ทฤษฎีพฤติกรรมแห่งตามกัน ใช้อธิบายแรงจูงใจทางการเงิน และการตัดสินใจตามกระแส ทฤษฎีอาชญากรรมไซเบอร์ ช่วยระบุลักษณะของภัยในโลกดิจิทัล เช่น กลโกงทางออนไลน์ โดยเฉพาะแนวคิดของ Yar (2006) ที่แบ่งประเภทเป็นอาชญากรรมที่ใช้เทคโนโลยีเป็นเครื่องมือ โดยการหลอกลวงผู้เล่นที่ขาดความเข้าใจในเทคโนโลยีใหม่ ๆ และทฤษฎีการป้องกันอาชญากรรมโดยสถานการณ์ (SCP) นำมาใช้ในการออกแบบแนวทางการป้องกัน เช่น การจำกัดโอกาสเกิดอาชญากรรม จากทฤษฎีหลักทั้ง 4 นี้ ได้นำมาสร้างกรอบแนวคิดซึ่งเชื่อมโยง “ปัจจัยการตกเป็นผู้เสียหาย” → “ผลกระทบ” → “แนวทางการป้องกัน” โดยแนวคิดแต่ละส่วนยังถูกใช้ในการออกแบบคำถามสัมภาษณ์ให้ครอบคลุมปัจจัย ผลกระทบ และข้อเสนอแนะในการป้องกันการตกเป็นผู้เสียหายเพื่อกำหนดแนววิเคราะห์ในการศึกษากรณี GameFi ในประเทศไทยอย่างเป็นระบบและสอดคล้องกับสถานการณ์จริง



ภาพที่ 1 กรอบแนวคิดการวิจัย

การทบทวนวรรณกรรม

แนวคิดเหยื่อวิทยา (Victimology)

แนวคิดเหยื่อวิทยาเน้นศึกษาปัจจัยที่ส่งผลให้บุคคลตกเป็นเหยื่อจากเหตุการณ์ต่าง ๆ ไม่จำกัดเฉพาะอาชญากรรม แต่ยังรวมถึงโครงสร้างทางสังคม เทคโนโลยี หรือภัยพิบัติ โดยมีเป้าหมายในการลดความเสี่ยงและเยียวยาเหยื่อทั้งด้านร่างกาย จิตใจ และการสนับสนุนจากรัฐ (สุดสงวน สุธีสร, 2543)

Benjamin Mendelsohn เป็นผู้บุกเบิกว่าด้วยวิชาเกี่ยวกับเหยื่อวิทยา เสนอแนวคิดกว้างขึ้นโดยมองว่าเหยื่อไม่จำกัดเฉพาะในบริบทของอาชญากรรมเท่านั้น แต่ยังรวมถึงผู้ที่ได้รับผลกระทบจากโครงสร้างทางสังคมการเมือง เทคโนโลยีสมัยใหม่ หรือแม้แต่ภัยพิบัติ ซึ่งอาจส่งผลให้บุคคลหนึ่งกลายเป็นเหยื่อได้เช่นกัน (Mendelsohn, 1986: 195 อ้างถึงใน สุดสงวน สุธีสร, 2543)

นอกจากแนวคิดด้านเหยื่อวิทยาแล้ว ยังมีปัจจัยเชิงจิตวิทยาในการตกเป็นเหยื่อ โดยงานวิจัยของ สุกสิริ จันทรินทร์ (2565) ชี้ว่าปัจจัยเชิงจิตวิทยาที่เพิ่มความเสี่ยงในการตกเป็นเหยื่อของมิจฉาชีพมี 3 ด้าน คือ (1) พฤติกรรมชอบเสี่ยง มักตอบสนองต่อข้อเสนอที่มีผลตอบแทนสูงโดยไม่วิเคราะห์ (2) การควบคุมตนเอง ต่ำ ตัดสินใจอย่างหุนหันพลันแล่น และ (3) การจัดการอารมณ์ไม่เหมาะสม ทำให้บุคคลตัดสินใจโดยใช้อารมณ์มากกว่าเหตุผล

ทฤษฎีพฤติกรรมแห่ตามกัน (Herding Behavior)

Banerjee (1992) อธิบายพฤติกรรมแห่ตามกันว่า บุคคลมักทำตามผู้อื่นโดยไม่ใช้ข้อมูลหรือเหตุผลของตนเอง แบ่งเป็นสองแบบคือ (1) พฤติกรรมแห่ตามกันแบบมีเหตุผล (Rational Herding) เชื่อว่าผู้อื่นมีข้อมูลที่ดีกว่า และ (2) พฤติกรรมแห่ตามกันแบบไม่มีเหตุผล (Irrational Herding) เกิดจากแรงจูงใจด้านจิตวิทยา เช่น ความกลัวตกกระแส (FOMO) ส่งผลให้ตัดสินใจเสี่ยงในเกมนบล็อกเชนที่อ้างว่าจะได้กำไรสูง ระยะสั้นจนตกเป็นเหยื่อ

แนวคิดอาชญากรรมไซเบอร์ (Cybercrime)

เป็นแนวคิดที่ใช้ในการอธิบายพฤติกรรมกระทำผิดที่อาศัยเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ หรือเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือ หรือเป็นเป้าหมายของการกระทำผิด โดยครอบคลุมทั้งการแสกข้อมูล การฉ้อโกงออนไลน์ การปลอมแปลงตัวตน การกลั่นแกล้งในโลกไซเบอร์ รวมถึงการโจมตีระบบทางการเงิน หรือแพลตฟอร์มดิจิทัล โดย Yar (2006) แบ่งอาชญากรรมไซเบอร์เป็น 3 กลุ่มหลัก ได้แก่ (1) มุ่งโจมตีระบบคอมพิวเตอร์ เช่น การแสก (2) ใช้เทคโนโลยีเป็นเครื่องมือ เช่น การฉ้อโกง ฟิชซิง (Phishing) ผ่านเกมออนไลน์ และ (3) มุ่งต่อบุคคล เช่น การขโมยข้อมูลส่วนบุคคลและการกลั่นแกล้งออนไลน์ (Cyberbullying) โดยในเกมบล็อกเชน ผู้เสียหายส่วนใหญ่ตกเป็นเหยื่อกลุ่มที่สองและสาม

ในกรณีของเกมนบล็อกเชน ซึ่งมักมีลักษณะเป็นแพลตฟอร์มเปิดที่ใช้เทคโนโลยีบล็อกเชนและสัญญาอัจฉริยะ (Smart Contracts) เป็นโครงสร้างพื้นฐาน อาชญากรรมไซเบอร์อาจใช้ช่องโหว่ของเทคโนโลยี หรือการออกแบบระบบที่ขาดการควบคุม เพื่อหลอกลวงผู้ใช้งานให้โอนทรัพย์สินดิจิทัลหรือให้ข้อมูลสำคัญ เช่น private key หรือ seed phrase ซึ่งไม่สามารถเรียกคืนได้เมื่อเกิดความเสียหาย นอกจากนี้ ความเสี่ยงจากการโฆษณาชวนเชื่อผ่านโซเชียลมีเดีย ที่ใช้ข้อมูลบิดเบือนและแรงจูงใจด้านการลงทุนเป็นเครื่องมือในการชักจูงเหยื่อให้เข้าร่วมโครงการปลอม เช่น rug pull, Ponzi scheme หรือเกมที่ไม่มีการพัฒนาอย่างแท้จริง จนทำให้ผู้ใช้งานกลายเป็นเหยื่อจากการหลอกลวงทางดิจิทัลได้ง่าย และสะท้อนถึงความเปราะบางของระบบเทคโนโลยีและช่องว่างของกลไกการคุ้มครองผู้บริโภคในสังคมยุคใหม่

ทฤษฎีหน้าต่างแตก (Broken Windows Theory)

เสนอโดย Kelling and Wilson (1982) อธิบายว่าหากปัญหาหรือพฤติกรรมที่เบี่ยงเบนเล็กน้อยไม่ได้รับการจัดการในทันที จะนำไปสู่ความรู้สึกว่ากฎหมายไม่มีประสิทธิภาพ ซึ่งอาจทำให้สังคมละเลยความผิดอื่น ๆ และนำไปสู่การเสื่อมถอยของความเชื่อมั่นในระบบยุติธรรมโดยรวม ในกรณีของอาชญากรรมไซเบอร์ นำมาใช้วิเคราะห์ผลกระทบด้านความเชื่อมั่นของเหยื่อที่รู้สึกว่ารัฐไม่สามารถจัดการกับปัญหาได้ เมื่อผู้เสียหายจากเกมนบล็อกเชนต้องเผชิญกับการหลอกลวงแต่ไม่ได้รับการช่วยเหลือหรือคดีไม่คืบหน้า พวกเขาเกิดความรู้สึกว่าระบบกฎหมายไม่สามารถปกป้องตนเองได้ ส่งผลให้บางรายเลือกที่จะไม่แจ้งความ หรือปฏิเสธสถานะความเป็นเหยื่อของตนเอง

ทฤษฎีการป้องกันอาชญากรรมโดยสถานการณ์ (Situational Crime Prevention: SCP)

ทฤษฎี SCP โดย Clarke (1997) เน้นลดโอกาสเกิดอาชญากรรมด้วยการเปลี่ยนแปลงสภาพแวดล้อมผ่านกลยุทธ์ 5 ด้าน คือ (1) เพิ่มความพยายามในการก่อเหตุ (เช่น การตรวจสอบตัวตนแบบ KYC)

(2) เพิ่มความเสี่ยงต่อการถูกจับ (ระบบเฝ้าระวัง) (3) ลดผลตอบแทนจากการกระทำผิด (ระบบ timelock หรือ staking) (4) ลดแรงกระตุ้น (ควบคุมเนื้อหาโฆษณา) และ (5) ขจัดข้ออ้างในการกระทำผิด (แจ้งเตือนข้อควรระวังอย่างชัดเจน)

ทฤษฎีการเปลี่ยนพื้นที่ (Space Transition Theory)

ได้รับการเสนอโดย Jaishankar เพื่ออธิบายพฤติกรรมของมนุษย์ที่แปรเปลี่ยนไปเมื่อเข้าสู่โลกไซเบอร์ ทฤษฎีชี้ว่าโลกออนไลน์เป็นสภาพแวดล้อมที่มีลักษณะเฉพาะซึ่งเอื้อต่อการกระทำที่แตกต่างจากพฤติกรรมในโลกแห่งความเป็นจริง ทั้งนี้ เนื่องจากโลกไซเบอร์มีลักษณะไร้ตัวตน (Anonymity), ขาดข้อจำกัดทางกายภาพ, และมีโอกาสถูกตรวจจับน้อย ในบริบทของอาชญากรรมดิจิทัลที่นำไปสู่ความเสี่ยง (สาวตรี สุขศรี, 2560) ทฤษฎีนี้ช่วยอธิบายว่าทำไมผู้ใช้งานจึงมีแนวโน้มเชื่อถือข้อมูลจากแหล่งออนไลน์ เช่น โฆษณาเกินจริงในโซเชียลมีเดีย หรือคำบอกเล่าจากผู้ใช้คนอื่น โดยขาดการตรวจสอบข้อเท็จจริง หรือการที่บุคคลได้รับการสนับสนุนจากเสียงส่วนใหญ่ในโลกออนไลน์ที่เห็นด้วยกับลงทุน ยังส่งผลให้เกิดแรงจูงใจเชิงจิตวิทยา และลดความระมัดระวังในการตัดสินใจ ทฤษฎีนี้จึงนำมาอธิบายสาเหตุที่ผู้เสียหายมีแนวโน้มตัดสินใจลงทุนจากแรงจูงใจด้านสื่อและการตลาดมากกว่าการใช้เหตุผลเชิงวิเคราะห์ ซึ่งสะท้อนให้เห็นถึงการเปลี่ยนพฤติกรรมที่เกิดจากบริบทโลกออนไลน์ และกลายเป็นช่องทางให้ผู้ไม่หวังดีแสวงหาประโยชน์จากความไว้วางใจของผู้ใช้

ทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory – RCT)

เป็นแนวคิดที่อธิบายว่ามนุษย์จะกระทำการใด ๆ บนพื้นฐานของการชั่งน้ำหนักต้นทุนและผลประโยชน์ โดยเลือกทางเลือกที่คาดว่าจะให้ผลตอบแทนสูงสุดเมื่อเทียบกับความเสี่ยง (Cornish & Clarke, 2017) โดยเชื่อว่าบุคคลใช้เหตุผลเป็นกลไกหลักในการตัดสินใจ แต่การใช้เหตุผลนั้นขึ้นอยู่กับข้อมูลและความเข้าใจที่มีอยู่ในขณะนั้น

ในบริบทของการลงทุนในเกมบล็อกเชน ผู้เสียหายจำนวนมากเลือกลงทุนจากความเชื่อว่าจะได้รับผลตอบแทนที่สูงเกินกว่าความเสี่ยง แม้จะไม่มีข้อมูลครบถ้วนหรือไม่มีความเข้าใจในระบบเกมก็ตาม ทั้งนี้ เมื่อระบบโฆษณาหรือการบอกเล่าจากสื่อออนไลน์ส่งเสริมให้เกิดความคาดหวังเกินจริง ก็ยิ่งทำให้กระบวนการตัดสินใจมีแนวโน้มผิดพลาดสูงขึ้น

กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีและเกมบล็อกเชน

ประเทศไทยในปัจจุบันยังไม่มีกฎหมายเฉพาะที่ใช้กำกับดูแลเกมบล็อกเชนหรือแพลตฟอร์มที่มีลักษณะเป็น GameFi โดยตรง แต่การกระทำผิดที่เกี่ยวข้องกับการฉ้อโกง หลอกลวงประชาชน หรือฟอกเงินในบริบทของเกมดิจิทัล อาจเข้าข่ายความผิดตามกฎหมายที่มีอยู่ เช่น

(1) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (2560) เป็นกฎหมายหลักที่ใช้ควบคุมการกระทำผิดที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ต โดยเฉพาะในกรณีที่ผู้กระทำผิดใช้แพลตฟอร์มเกมบล็อกเชนเป็นเครื่องมือในการหลอกลวงหรือสร้างระบบฉ้อโกง เช่น การปกปิดข้อมูลหรือแสดงข้อความอันเป็นเท็จเพื่อให้ผู้ใช้งานหลงเชื่อการเข้าถึงระบบหรือข้อมูลส่วนตัวของผู้ใช้งานโดยมิชอบ, การเผยแพร่ข้อมูลปลอมหรือข้อความชักจูงให้ลงทุนในระบบที่ไม่โปร่งใส

มาตรา 14 (1) และ (2) สามารถใช้เอาผิดในกรณีที่มีการนำข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบ เพื่อหลอกลวงผู้อื่นให้เกิดความเสียหาย เช่น การโฆษณาผลตอบแทนเท็จ หรือสัญญาอัจฉริยะ (Smart Contract) ที่ออกแบบเพื่อเอาเปรียบผู้ใช้

(2) พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 (2561) เป็นกฎหมายเฉพาะที่ออกแบบมาเพื่อกำกับดูแลการประกอบธุรกิจที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล เช่น คริปโตเคอร์เรนซี โทเคนดิจิทัล และ ICO โดยเฉพาะในกรณีที่แพลตฟอร์มหรือเกมมีการออกเหรียญหรือโทเคนของตนเอง และเปิดให้ซื้อขายหรือใช้แลกเปลี่ยนภายในระบบเกม สำหรับผู้เสียหายที่ตกเป็นเหยื่อจากเกมบล็อกเชนที่มีลักษณะเป็น Ponzi scheme หรือ Rug Pull การบังคับใช้กฎหมายนี้ยังเป็นเรื่องท้าทาย เนื่องจากขอบเขตความรับผิดชอบของหน่วยงานกำกับดูแลยังไม่ครอบคลุมเกมในลักษณะกึ่งแพลตฟอร์มอย่างเพียงพอ

(3) พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 และฉบับแก้ไขเพิ่มเติม (2535) หากรูปแบบของเกมบล็อกเชนหรือการออกโทเคนในเกมมีลักษณะของการเสนอขายหลักทรัพย์ต่อประชาชนหรือเป็นการระดมทุนในลักษณะที่เข้าข่ายหลักทรัพย์ ผู้ประกอบการจะต้องได้รับอนุญาตจากสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ก่อน หากไม่มีการอนุญาตก็อาจเข้าข่ายฝ่าฝืนกฎหมาย

ประเด็นนี้มีความสำคัญเป็นพิเศษในกรณีที่เกมมีการเสนอขายโทเคนล่วงหน้า (pre-sale) เพื่อระดมทุนพัฒนาเกม หรือให้สัญญาว่าผู้ถือโทเคนจะได้รับผลตอบแทนตามสัดส่วน ซึ่งมีความคล้ายคลึงกับการถือหุ้นหรือการลงทุนในหลักทรัพย์ โดยที่ผ่านมาก.ล.ต. ได้มีการเตือนหลายกรณีเกี่ยวกับโทเคนที่ไม่มีการกำกับดูแลอย่างไรก็ตาม ความซับซ้อนของโครงสร้างโทเคนในเกม และความไม่ชัดเจนของเจตนาเชิงพาณิชย์ ทำให้การนำกฎหมายนี้มาใช้ยังมีข้อจำกัดในทางปฏิบัติ

(4) ประมวลกฎหมายอาญา มาตรา 343 (ความผิดฐานฉ้อโกงประชาชน) มาตรานี้ใช้บังคับกับการกระทำความผิดฐานฉ้อโกงโดยทั่วไป โดยเฉพาะเมื่อมีการกระทำอันเป็นเท็จต่อสาธารณชนจำนวนมาก ซึ่งตรงกับลักษณะการหลอกลวงผ่านระบบเกมที่อ้างว่าลงทุนแล้วจะได้รับผลตอบแทนสูง กรณีเกมบล็อกเชนที่ผู้จัดตั้งมีเจตนาแสวงหาประโยชน์โดยหลอกลวงให้ผู้ลงทุนโดยใช้ข้อความหรือเอกสารอันเป็นเท็จ และเมื่อมีผู้เสียหายจำนวนมากอาจเข้าข่ายฉ้อโกงประชาชน ซึ่งเป็นความผิดอาญาแผ่นดิน มีบทลงโทษที่รุนแรงกว่าการฉ้อโกงทั่วไป อย่างไรก็ตาม การพิสูจน์เจตนาและความเชื่อมโยงระหว่างผู้เสียหายกับผู้กระทำความผิดยังคงเป็นอุปสรรคสำคัญในการนำกฎหมายนี้ไปใช้กับกรณีในโลกไซเบอร์ที่มีลักษณะกระจายอำนาจและไม่ระบุตัวตน (สถาบันนิติธรรมาลัย Update กฎหมายและคำพิพากษาศาลฎีกา, (ม.ป.ป.))

งานวิจัยที่เกี่ยวข้อง

ธนวัฒน์ อภิวัฒน์นอม (2564) ได้ทำการศึกษาหัวข้อ อิทธิพลของเทคโนโลยีบล็อกเชนที่มีต่อการตัดสินใจลงทุนของนักลงทุนรายย่อย โดยมีวัตถุประสงค์เพื่อวิเคราะห์ปัจจัยที่ส่งผลกระทบต่อตัดสินใจลงทุนในอสังหาริมทรัพย์รูปแบบต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีบล็อกเชน ผลการศึกษาพบว่า ปัจจัยด้านพฤติกรรมกรรมการลงทุนอสังหาริมทรัพย์ มีอิทธิพลอย่างมีนัยสำคัญต่อการตัดสินใจลงทุนในทุกรูปแบบที่ศึกษา ในขณะที่ปัจจัยด้านการยอมรับนวัตกรรมและเทคโนโลยี มีอิทธิพลเฉพาะต่อการลงทุนในอสังหาริมทรัพย์ที่เกี่ยวข้องกับการซื้อขายด้วยคริปโตเคอร์เรนซีเท่านั้น เพื่อใช้เป็นพื้นฐานในการศึกษาแนวทางการนำเทคโนโลยีบล็อกเชนมาใช้ในอุตสาหกรรมอสังหาริมทรัพย์ รวมถึงการวิเคราะห์พฤติกรรมและปัจจัยที่ส่งผลกระทบต่อตัดสินใจลงทุนของนักลงทุนรายย่อย ซึ่งมีความเกี่ยวข้องกับงานวิจัยฉบับปัจจุบัน

พันธุ์ทิพย์ นวานุช และคณะ (2567) ทำการศึกษาเรื่อง มาตรการทางกฎหมายภัยคุกคามทางไซเบอร์ พบว่า ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มขึ้นอย่างรวดเร็วและความหลากหลาย ส่งผลให้เกิดความเสียหายทางเศรษฐกิจอย่างมหาศาล แม้ว่าจะมีกฎหมายหลายฉบับที่ใช้ในการป้องกันและปราบปราม เช่น กฎหมายมาตรการป้องกันอาชญากรรมทางเทคโนโลยี และกฎหมายความมั่นคงปลอดภัยไซเบอร์ แต่ยังไม่สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพ จึงเสนอให้มีการพัฒนากฎหมายให้ทันสมัยและเสริมสร้างทักษะบุคลากรภาครัฐและเอกชน เพื่อรับมือกับภัยไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว

Sharma et al. (2024) ได้ศึกษาเรื่องความปลอดภัยและการรักษาความปลอดภัยของผู้ใช้ใน Metaverse : ผลการวิจัยพบว่า Metaverse จินตนาการถึงอนาคตที่การโต้ตอบออนไลน์ที่สมจริงกลายเป็นบรรทัดฐาน อย่างไรก็ตาม วิทยุทัศน์นี้จะบรรลุได้อย่างปลอดภัยก็ต่อเมื่อกำหนดถึงความปลอดภัยและความเป็นส่วนตัวของผู้ใช้เป็นหลัก การตรวจสอบนี้จะประเมินผลด้านความปลอดภัยและมาตรการรักษาความปลอดภัยของผู้ใช้ที่มีอยู่ใน Metaverse อย่างมีวิจารณญาณ เน้นย้ำถึงความสามารถที่จำกัดของโซลูชันที่มีอยู่เพื่อป้องกันการคุกคาม การขโมยข้อมูลระบุตัวตน และการใช้ข้อมูลส่วนบุคคลที่รวบรวมในสภาพแวดล้อมนี้ ในทางที่ผิด มิติด้านความปลอดภัยและการรักษาความปลอดภัยของผู้ใช้ภายในโลกเสมือนจริงอย่างครอบคลุม และนำเสนออนุกรมวิธานเพื่อจำแนกภัยคุกคามและช่องโหว่เฉพาะที่ผู้ใช้ Metaverse ที่อาจพบและเผยให้เห็นช่องว่างที่สำคัญ รวมถึงการขาดกรอบการทำงานด้านความปลอดภัยที่ครอบคลุม และโมเดลการรักษาความปลอดภัยที่เป็นส่วนตัวที่สมดุลในสภาพแวดล้อมเสมือนจริงเพื่อเป็นการตอบสนอง เพื่อเสนอสถาปัตยกรรมความปลอดภัย Metaverse แบบใหม่ที่ออกแบบด้วยหลักการ Zero-Trust ที่จัดลำดับความสำคัญของผู้ใช้ในการควบคุมข้อมูล ตัวตน และประสบการณ์ นอกจากนี้ยังเน้นย้ำถึงมาตรการรักษาความปลอดภัยเชิงรุกเพื่อบรรเทาอันตรายที่อาจเกิดขึ้นในโลกเสมือนจริง และเน้นผู้ใช้เป็นศูนย์กลางในการเปิดใช้งาน Metaverse ที่น่าดึงดูด และปลอดภัยสำหรับผู้เข้าร่วมทุกคน

Kumar (2024) ได้การศึกษาเรื่อง อาชญากรรมทางไซเบอร์และกฎหมาย : ความท้าทายในการดำเนินคดีความผิดทางดิจิทัล พบว่า เทคโนโลยีดิจิทัลและอินเทอร์เน็ตที่เติบโตอย่างรวดเร็วส่งผลให้เกิดอาชญากรรมทางไซเบอร์ ซึ่งเป็นภัยคุกคามที่ซับซ้อนและเปลี่ยนแปลงตลอดเวลา แม้จะมีความพยายามในการจัดการกับอาชญากรรมทางไซเบอร์ แต่กรอบกฎหมายและระบบบังคับใช้กฎหมายยังไม่สามารถตามทันการเปลี่ยนแปลงของเทคโนโลยีได้ ทำให้เกิดช่องโหว่ที่เป็นอุปสรรคต่อการดำเนินคดี โดยมีปัญหาสำคัญ เช่น ข้อจำกัดทางกฎหมาย ปัญหาเขตอำนาจศาล และความซับซ้อนของหลักฐานดิจิทัล เพื่อรับมือกับปัญหานี้ งานวิจัยเสนอว่า จำเป็นต้องมีความร่วมมือระหว่างประเทศที่เข้มแข็งขึ้น การพัฒนาและปรับปรุงกฎหมายให้ทันสมัย เพิ่มขีดความสามารถของหน่วยงานบังคับใช้กฎหมาย และส่งเสริมการศึกษาสาธารณะ เพื่อให้สามารถต่อสู้กับอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพและรักษาความยุติธรรมในยุคดิจิทัล

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยใช้การสัมภาษณ์เชิงลึก (In-depth Interview) กับกลุ่มตัวอย่างที่มีประสบการณ์ตรงเกี่ยวกับการหลอกลวงในเกมบล็อกเชน การเลือกกลุ่มตัวอย่างใช้วิธีการแบบเจาะจง (Purposive Sampling) เพื่อให้ได้ข้อมูลเชิงลึกจากกลุ่มผู้มีบทบาทและประสบการณ์ที่เกี่ยวข้อง ได้แก่ ผู้เสียหาย เจ้าหน้าที่ และผู้เชี่ยวชาญในแวดวงเกมบล็อกเชน รวมจำนวน 21 ราย แบ่งเป็น 3 กลุ่มย่อย คือ

1. ผู้เล่นเกมบล็อกเชนที่มีประสบการณ์ในการตกเป็นเหยื่อ โดยเลือกมาจากกลุ่มผู้เล่นเกมที่ตั้งขึ้นในเฟซบุ๊ก 15 ราย แบ่งตามระดับความเสียหายด้านจำนวนเงินตามสัดส่วนที่ผู้เสียหายได้รับ แบ่งเป็น 3 กลุ่ม คือ

กลุ่มที่ 1 จำนวนเงินมากกว่าหนึ่งแสนบาท	จำนวน 5 ราย
กลุ่มที่ 2 จำนวนเงินหนึ่งหมื่นบาทแต่ไม่ถึงหนึ่งแสนบาท	จำนวน 5 ราย
กลุ่มที่ 3 จำนวนเงินหนึ่งพันบาทแต่ไม่ถึงหนึ่งหมื่นบาท	จำนวน 5 ราย

2. เจ้าหน้าที่ตำรวจ 4 ราย โดยเป็นเจ้าหน้าที่กองบัญชาการสืบสวนสอบสวนอาชญากรรมเทคโนโลยีจำนวน 2 ราย และเจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ จำนวน 2 ราย

3. ผู้เชี่ยวชาญเกี่ยวกับเกมบล็อกเชน ซึ่งมีความเข้าใจเกี่ยวกับ GameFi มากกว่า 5 ปี จำนวน 2 ราย จำนวนกลุ่มตัวอย่างทั้งหมดได้รับการพิจารณาว่าเพียงพอสำหรับการวิเคราะห์ข้อมูลเชิงคุณภาพ โดยอิงแนวคิด Data Saturation ซึ่งที่ข้อมูลเริ่มมีลักษณะซ้ำซ้อนและไม่มีประเด็นใหม่เพิ่มเติม ถือเป็นแนวทางมาตรฐานในงานวิจัยเชิงคุณภาพที่เน้นความลึกมากกว่าปริมาณ

การดำเนินการวิจัยเชิงคุณภาพในครั้งนี้ อิงตามแนวคิดของ Lincoln and Guba (1985) ที่เน้นการสร้างที่น่าเชื่อถือของข้อมูล (Trustworthiness) ผ่านกระบวนการต่าง ๆ เช่น การตรวจสอบแบบสามเส้า (Triangulation) และการตรวจสอบกับผู้ให้ข้อมูล (Member Checking) เพื่อยืนยันความถูกต้องของการตีความจากผู้วิจัย นอกจากนี้ การวิเคราะห์ข้อมูลเชิงเนื้อหา (Content Analysis) ยังใช้แนวทางของ Hsieh and Shannon (2005) ที่เน้นการสกัดประเด็นสำคัญจากคำพูดของผู้ให้สัมภาษณ์ โดยจัดกลุ่มเป็นหมวดหมู่แนวคิดที่สะท้อนปรากฏการณ์ทางสังคมอย่างมีนัยสำคัญ ซึ่งเป็นวิธีที่เหมาะสมกับงานวิจัยที่ต้องการเข้าใจประสบการณ์ของผู้เสียหายอย่างลึกซึ้ง

เครื่องมือที่ใช้ในการเก็บข้อมูล คือ แบบสัมภาษณ์กึ่งโครงสร้าง (Semi-structured Interview) โดยผู้วิจัยออกแบบแนวคำถามจากวัตถุประสงค์ของการวิจัยทั้งสามข้อ ร่วมกับการศึกษาทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องอย่างเป็นระบบ เพื่อให้แน่ใจว่าเนื้อหาและประเด็นคำถามมีความครอบคลุมและสอดคล้องกับแนวคิดและทฤษฎีที่ใช้ในการวิจัย และให้สามารถสะท้อนสาระสำคัญตามกรอบแนวคิดการวิจัยได้อย่างเหมาะสม นอกจากนี้ ได้นำแบบสัมภาษณ์ดังกล่าวไปให้ผู้ทรงคุณวุฒิตรวจสอบแล้ว โดยข้อมูลที่ได้จากการสัมภาษณ์จะถูกถอดความและนำมาวิเคราะห์ใน 2 ขั้นตอน ได้แก่ 1) การวิเคราะห์เชิงพรรณนา (Descriptive Analysis) เพื่อจัดกลุ่มข้อมูลเบื้องต้น และ 2) การวิเคราะห์เนื้อหา (Content Analysis) ซึ่งเป็นกระบวนการสกัดประเด็นหลักและแนวคิดสำคัญในเชิงลึกโดยใช้การจัดหมวดหมู่แนวคิดและเชื่อมโยงเข้ากับกรอบทฤษฎีที่ใช้เพื่อเสริมสร้าง ความน่าเชื่อถือของข้อมูล (Trustworthiness) ทั้งนี้ ผู้วิจัยดำเนินการตรวจสอบข้อมูลด้วยวิธี การตรวจสอบแบบสามเส้า (Triangulation) เพื่อวิเคราะห์เปรียบเทียบข้อมูลจากทั้ง 3 กลุ่มตัวอย่าง เพื่อหาความสอดคล้องหรือแตกต่างในประเด็นเดียวกัน อีกทั้งลดความลำเอียงจากแหล่งข้อมูลเพียงด้านเดียว และวิธีการตรวจสอบกับผู้ให้ข้อมูล (Member Checking) ที่นำผลวิเคราะห์บางส่วนกลับไปยืนยันความถูกต้องกับผู้ให้ข้อมูล เพื่อให้แน่ใจว่าการตีความของผู้วิจัยสะท้อนประสบการณ์ของผู้ให้ข้อมูลได้ถูกต้องจริง

ผลการวิจัย

1. ปัจจัยของการตกเป็นผู้เสียหายจากเกมบล็อกเชน

จากข้อมูลการสัมภาษณ์ พบว่า สามารถสรุปปัจจัยหลักที่ทำให้ผู้เล่นหลงเชื่อและตกเป็นผู้เสียหายจากเกมบล็อกเชน ได้ทั้งหมด 3 ปัจจัยหลัก ดังนี้

1.1 ปัจจัยด้านแรงจูงใจทางการเงิน คือ ความต้องการสร้างรายได้และหวังทำกำไรในระยะสั้น พบว่า ผู้เล่นจำนวนมากมองว่าเกมบล็อกเชน โดยเฉพาะในยุคที่แนวคิด Play-to-Earn กำลังเป็นกระแสนิยม เป็นโอกาสในการสร้างผลตอบแทนที่รวดเร็ว จึงตัดสินใจลงทุนจำนวนมากโดยไม่มีแผนสำรอง ไม่มีการกระจายความเสี่ยง หรือการวางแผนในการถอนทุนคืน ส่งผลให้เมื่อเกมล่มหรือขาดความน่าเชื่อถือ พวกเขาต้องสูญเสียเงินแทบทั้งหมด นอกจากนี้ ยังมีแรงผลักดันจากภาวะกลัวตกกระแส (FOMO: Fear of Missing Out)

ซึ่งเป็นสภาวะทางจิตใจที่เกิดจากความกลัวว่าจะพลาดโอกาสทางการเงินหรือผลตอบแทนที่ดูน่าดึงดูด เช่น โอกาสทำเงินจากการลงทุน โอกาสที่จะรวยเร็ว หรือโอกาสได้เป็นกลุ่มแรก ๆ ที่เข้าไปเล่นหรือซื้อบางสิ่งบางอย่าง กลุ่มมิจฉาชีพมักอาศัยจังหวะนี้สร้างแรงจูงใจทางอารมณ์ เช่น การชักจูงว่าหากไม่รีบลงทุนก็จะพลาดโอกาสดี ๆ ไป โดยเร่งเร้าให้รีบตัดสินใจลงทุนแบบที่ไม่ทันคิดวิเคราะห์ถึงความเสี่ยงอย่างรอบด้าน

1.2 ปัจจัยด้านความรู้และความเข้าใจ คือ การขาดความรู้และเข้าใจที่เพียงพอเกี่ยวกับเศรษฐกิจของเกมบล็อกเชน โดยการใช้เทคโนโลยีที่ซับซ้อนมาหลอกลวง อ้างว่าใช้ Blockchain, NFT, Metaverse หรือ DeFi ที่มีการสร้างระบบ Staking หรือ Yield Farming พบว่า มีผู้เสียหายหลายรายลงทุนในเกมบล็อกเชนโดยไม่เข้าใจเศรษฐกิจของเกม (Tokenomics) กลไก Smart Contract และความยั่งยืนของรายได้ในเกม ทำให้ตกเป็นเหยื่อของกลโกงในรูปแบบต่าง ๆ ได้โดยง่าย เช่น Ponzi Scheme, Pump & Dump, และ Rull Pull เป็นต้น

1.3 ปัจจัยด้านสื่อและการตลาด เกมบล็อกเชนหลายเกมใช้กลยุทธ์ทางการตลาดที่ดึงดูดนักลงทุนและผู้เล่น โดยการสร้างภาพลักษณ์น่าเชื่อถือ มีเว็บไซต์ที่ออกแบบให้ดูเป็นมืออาชีพ ใช้เอกสารขาว (Whitepaper) ที่เต็มไปด้วยศัพท์เทคนิคเพื่อแสดงข้อมูลผู้พัฒนาเกมที่ดูเหมือนเป็นบุคคลจริง พบว่า มีผู้เสียหายส่วนใหญ่หลงเชื่อในคำโฆษณาที่เกินจริง เช่น การจัดอันดับเกมในเว็บไซต์ดัง รีวิวจากผู้เล่นหรือ Streamer game คำบอกเล่าจากเพื่อนกลุ่มผู้เล่นเกมใน Facebook ที่เคยทำกำไรได้จริงในช่วงแรก ซึ่งผู้เสียหายรู้สึกว่าเป็นโอกาสที่ดี จึงลงทุนโดยไม่ทันระวังและไม่ตรวจสอบข้อมูลให้รอบคอบ ทำให้ตกเป็นเหยื่อของกลโกงที่สร้างความน่าเชื่อถือเพื่อดึงดูดผู้เล่นและนักลงทุน นอกจากนี้ พบว่า สตรีมเมอร์และ Influencer มักถูกใช้เป็นเครื่องมือทางการตลาดโดยไม่รู้ตัว ทำให้ผู้ติดตามของพวกเขาเสี่ยงต่อการลงทุนผิดพลาด

2. ผลกระทบที่เกิดขึ้นกับผู้เสียหายจากการเล่นเกมบล็อกเชน

2.1 ผลกระทบด้านการเงิน พบว่า ผลกระทบที่เกิดจากการสูญเสียเงินจากการลงทุนในเกมบล็อกเชนนั้นส่งผลกระทบต่อชีวิตประจำวันของผู้เสียหายอย่างมาก โดยเฉพาะอย่างยิ่งในด้านการเงินและการดำรงชีวิต อาทิ

(1) การสูญเสียทางการเงิน ผู้เสียหายสูญเสียเงินจำนวนมาก และไม่สามารถนำเงินกลับคืนมาได้ บางคนต้องขายทรัพย์สินหรือกู้เงินเพิ่มเพื่อใช้ชีวิตต่อไป อาจเป็นเงินที่เก็บออมไว้เพื่อใช้ในอนาคต เช่น เงินสำรองฉุกเฉิน เงินเพื่อการศึกษา หรือเงินเพื่อซื้อบ้าน ที่ถูกนำไปลงทุนในเกมบล็อกเชนและได้สูญเสียไปส่งผลกระทบต่อเกิดการขาดสภาพคล่องทางการเงิน

(2) ภาระหนี้สิน ผู้เสียหายบางรายกู้ยืมเงินจากบุคคลอื่นมาลงทุนในเกมบล็อกเชน เมื่อสูญเสียเงินลงทุนไปจึงต้องแบกรับภาระหนี้สินที่เพิ่มขึ้น อีกทั้งบางรายมีการใช้บัตรเครดิตในการซื้อสินทรัพย์ดิจิทัล และไม่สามารถชำระหนี้ได้ ทำให้เกิดปัญหาหนี้สินบัตรเครดิตตามมา

(3) ผลกระทบต่อการดำรงชีวิตประจำวัน ผู้เสียหายต้องลดค่าใช้จ่ายในชีวิตประจำวันลงเพื่อชดเชยเงินที่สูญเสียไป แผนการในอนาคต เช่น การซื้อบ้าน การเลี้ยงลูก หรือการลงทุนอื่น ๆ ต้องเลื่อนออกหรือปรับเปลี่ยนไป การสูญเสียสภาพคล่องทางการเงินทำให้เกิดความเครียด ความวิตกกังวล ส่งผลกระทบต่อสุขภาพจิตและอาจส่งผลกระทบต่อความสัมพันธ์ภายในครอบครัว

ดังนั้น ผลกระทบจากการสูญเสียเงินจากการลงทุนในเกมบล็อกเชนนั้นมีความหลากหลายและรุนแรง ขึ้นอยู่กับปัจจัยหลายประการ แม้ว่าเกมบล็อกเชนจะเป็นแหล่งสร้างโอกาสทางการเงิน แต่ก็มีความเสี่ยงสูงและอาจส่งผลกระทบต่อผู้ลงทุนโดยไม่มีการวางแผนอย่างรอบคอบ ผลกระทบ

ที่เกิดขึ้นครอบคลุมทั้งด้านการเงินหนี้สิน และการดำรงชีวิตประจำวัน ซึ่งอาจส่งผลกระทบต่อสุขภาพจิตและความสัมพันธ์ภายในครอบครัว

2.2 ผลกระทบด้านจิตใจและสังคม พบว่า การสูญเสียเงินจากการลงทุนในเกมบล็อกเชนยังส่งผลกระทบต่อสภาพจิตใจของผู้เสียหาย อาจเกิดภาวะเครียด วิตกกังวล และซึมเศร้า ผลกระทบเหล่านี้มักเป็นสิ่งที่มองไม่เห็น แต่มีผลต่อคุณภาพชีวิตและความสุขของผู้เสียหายอย่างมาก อาทิ

(1) ความเครียดและความวิตกกังวล ผู้เสียหายรู้สึกกังวลเกี่ยวกับอนาคตทางการเงินของตนเองและครอบครัว เสียหายกับเงินที่สูญเสียไป รวมถึงโอกาสที่พลาดไปจากเงินก้อนนั้นที่ได้นำไปลงทุน รู้สึกผิดหวังในตัวเองที่ตัดสินใจลงทุนโดยไม่ศึกษาข้อมูลให้ดี ความเครียดจากการสูญเสียเงินส่งผลกระทบต่ออารมณ์ ทำให้เกิดปัญหาสุขภาพตามมา

(2) ความโกรธแค้น ความโกรธเกิดขึ้นทั้งต่อผู้ที่หลอกลวง และต่อตัวเองที่ไม่รอบคอบในการลงทุน ความโกรธนี้นำไปสู่การลงโทษตัวเอง เช่น การอดอาหาร การดื่มเหล้า การสูบบุหรี่ หรือแม้แต่การหลีกเลี่ยงความสุข ทำให้สุขภาพกายและใจแย่ลง

(3) ความเสียหายต่อชื่อเสียง ผู้เสียหายรู้สึกอับอายที่ต้องบอกให้คนอื่นรู้ว่าตนเองถูกหลอก อาจส่งผลกระทบต่อภาพลักษณ์ส่วนตัวและความน่าเชื่อถือในสายตาของผู้อื่น รวมถึงกระทบความสัมพันธ์กับครอบครัว เพื่อน หรือคู่ชีวิต

ดังนั้น ผลกระทบด้านจิตใจและสังคม ส่งผลต่อคุณภาพชีวิตและสภาพจิตใจของผู้เสียหายในหลายด้าน ทั้งความเครียด ความวิตกกังวล ความโกรธ และความไม่ไว้วางใจ รวมถึงส่งผลกระทบต่อความสัมพันธ์กับครอบครัว ทำให้มีความสุขน้อยลง คุณภาพชีวิตลดลง รวมถึงประสิทธิภาพในการทำงานลดลง

2.3 ผลกระทบด้านความเชื่อมั่นทางกฎหมาย จากสัมภาษณ์ผู้เสียหาย พบว่า ผู้เสียหายที่เข้าแจ้งความส่วนใหญ่เป็นผู้ที่รับจ้างเล่นเกมหรือผู้ที่ร่วมลงทุนกับผู้อื่น ปัญหาสำคัญที่ผู้เสียหายเผชิญจากการถูกหลอกรับจ้างเล่นเกมบล็อกเชน คือ ความอ่อนแอของระบบกฎหมายไทยในการรับมือกับการหลอกลวงที่เกี่ยวข้องกับเทคโนโลยี blockchain และเหรียญ Crypto ผู้เสียหายส่วนใหญ่รู้สึกผิดหวังเนื่องจากตำรวจยังไม่มีความเข้าใจในเทคโนโลยีดังกล่าวอย่างเพียงพอ รวมถึงไม่มีแนวทางที่ชัดเจนในการดำเนินคดีกับผู้กระทำผิดที่ซ่อนตัวอยู่หลังระบบออนไลน์และการใช้บัญชี Crypto wallet ส่งผลให้คดีไม่คืบหน้าและผู้กระทำผิดยังคงลอยนวล ผู้เสียหายจึงรู้สึกไม่ได้รับความเป็นธรรม และเกิดความรู้สึกหมดหวังในระบบกฎหมายปัจจุบันของประเทศไทย

ในด้านเจ้าหน้าที่ตำรวจ ปัญหาในกระบวนการยุติธรรมที่ผู้เสียหายจากเกมบล็อกเชนต้องเผชิญ พบว่า เกมบล็อกเชนเป็นช่องทางที่มีฉ้อโกงใช้หาประโยชน์จากความไม่รู้ของผู้เล่น และกระบวนการยุติธรรมใช้เวลานาน เนื่องจากการดำเนินคดีที่เกี่ยวข้องมีความซับซ้อน กฎหมายที่เกี่ยวข้องยังไม่ครอบคลุมสรุปประเด็นสำคัญจากการสัมภาษณ์ ได้ดังนี้ (1) ความซับซ้อนของเทคโนโลยี บล็อกเชนเป็นระบบที่ซับซ้อน ทำให้การสืบสวนติดตามตัวผู้กระทำผิดเป็นไปได้ยาก (2) การฉ้อโกงข้ามประเทศ หลายคดีเกิดจากโครงการเกมที่มีทีมพัฒนาอยู่ในต่างประเทศ ทำให้การดำเนินคดีใช้เวลานานและมีข้อจำกัด ด้านกฎหมายและข้อกฎหมายเกี่ยวกับคริปโตฯ และ NFT ยังไม่ชัดเจน ทำให้ผู้เสียหายไม่รู้ว่าต้องดำเนินการอย่างไร (3) ขาดหลักฐานที่ชัดเจน ผู้เสียหายมักไม่มีเอกสารหรือหลักฐานที่เพียงพอในการดำเนินคดี เนื่องจากธุรกรรมเกิดขึ้นบนบล็อกเชนที่ไม่สามารถแก้ไขย้อนหลังได้ และ (4) การขาดหน่วยงานกำกับดูแล ไม่มีหน่วยงานที่สามารถควบคุมหรือกำกับดูแลแพลตฟอร์มเกมบล็อกเชนได้อย่างมีประสิทธิภาพ อีกทั้งกฎหมายไทยยังไม่มีบทบัญญัติที่สามารถดำเนินคดีเกี่ยวกับเกมบล็อกเชนได้โดยตรง

แม้ว่าภาครัฐได้มีการดำเนินการที่เจาะจงต่อปัญหาของเกมบล็อกเชน (GameFi) โดยเฉพาะในมิติที่เกี่ยวข้องกับการหลอกลวงทางการเงินและอาชญากรรมไซเบอร์ ปัจจุบันรัฐบาลไทยจะมีมาตรการในการควบคุมและปราบปรามอาชญากรรมทางเทคโนโลยีที่เกี่ยวข้องกับภาพรวมของอาชญากรรมไซเบอร์ เช่น การผลักดันพระราชกำหนดมาตรการปราบปรามอาชญากรรมทางเทคโนโลยี ที่มีบทบัญญัติให้สามารถระงับบัญชีม้า ระงับซิมที่เกี่ยวข้องกับการหลอกลวง และให้หน่วยงานที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล ธนาคาร และผู้ให้บริการโทรคมนาคมมีหน้าที่เฝ้าระวังและรายงานธุรกรรมที่น่าสงสัย รวมถึงมีการจัดตั้งศูนย์ปฏิบัติการเฉพาะทางด้านอาชญากรรมไซเบอร์แล้วนั้น อย่างไรก็ตาม ผู้ให้ข้อมูลสะท้อนว่า มาตรการที่กล่าวมายังไม่มีส่วนที่มุ่งเน้นเฉพาะไปที่ GameFi ซึ่งเป็นระบบเกมที่มีลักษณะคล้ายการลงทุน มีความเสี่ยงต่อการถูกฉ้อโกงในรูปแบบใหม่ที่แตกต่างจากอาชญากรรมไซเบอร์ทั่วไป เช่น การเปิดตัวเกมหลอกลวงโดยไม่มีการเปิดเผยเจ้าของ การถอนตัวกลางคันของผู้พัฒนาโดยไม่รับผิดชอบ และการสร้างแรงจูงใจให้ลงทุนในโทเคนที่ไร้มูลค่า เป็นต้น

3. ข้อเสนอแนะจากผู้ให้ข้อมูล

จากการศึกษาข้อมูลของกลุ่มผู้เสียหาย เจ้าหน้าที่ตำรวจ และผู้เชี่ยวชาญในวงการเกมบล็อกเชน พบว่า สามารถจัดกลุ่มข้อเสนอแนะจากผู้ให้ข้อมูลทั้ง 21 ราย โดยจัดกลุ่มตาม “แนวคิดที่ใกล้เคียงกัน” เพื่อให้เห็นภาพชัดเจนว่าข้อเสนอแนะมีน้ำหนักในด้านใดบ้าง ดังนี้

กลุ่มที่ 1 : การตรวจสอบข้อมูลก่อนลงทุน

(1) ก่อนลงทุนควรหาข้อมูลเชิงลึกเกี่ยวกับเศรษฐกิจของเกมก่อนเสมอ และควรตรวจสอบระบบของเกมว่ามีการควบคุมตลาดหรือไม่ ถ้าหากไม่มีการกำกับดูแลอาจเป็นโครงการปั่นราคาหลอกลวงลงทุน

(2) ศึกษาข้อมูลและความน่าเชื่อถือของเกมก่อนลงทุน เช่น ตรวจสอบทีมพัฒนา หรือ Roadmap อ่านข้อกำหนดและเงื่อนไขให้ละเอียดก่อนตัดสินใจลงทุน หากเกมไม่เปิดเผยข้อมูลที่ทีมงานหรือให้ข้อมูลคลุมเครือ อาจเป็นสัญญาณการโกง

(3) ควรศึกษาตัวเกมและตัวผู้ว่าจ้างให้ละเอียด และควรเก็บหลักฐานหรือทำสัญญาเอาไว้

(4) อย่าหลงเชื่อโฆษณาที่ให้ผลตอบแทนสูงเกินจริง คิดไตร่ตรองให้รอบด้าน

กลุ่มที่ 2 : การจัดการเงินทุนและลดความเสี่ยง

(1) ถ้าหากลงทุน จะต้องจำกัดวงเงินลงทุนที่เหมาะสม ไม่ลงทุนเงินทั้งหมดในเกมเดียว ที่สำคัญอย่าใช้เงินก้อนใหญ่หรือเงินที่จำเป็นมาต่อยอด และต้องมีแผนสำรองที่ชัดเจนว่าจะถอนทุนเมื่อไหร่

(2) ถ้ามีคนเร่งให้รีบลงทุน ต้องไตร่ตรองให้ดี และอย่ารีบตัดสินใจ

กลุ่มที่ 3 : ความรู้และเทคนิคด้านความปลอดภัย

(1) ใช้กระเป๋าเงินดิจิทัลที่ปลอดภัย และอย่าคลิกลิงก์หรือดาวน์โหลดไฟล์แนบจากแหล่งที่ไม่รู้จัก และตรวจสอบให้ละเอียดว่าเป็นเว็บของทางการ

(2) ควรเข้าร่วมเฉพาะแพลตฟอร์มที่ได้รับการรับรองจากหน่วยงานที่เชื่อถือได้ และหลีกเลี่ยงการให้ข้อมูลส่วนตัวหรือรหัสผ่าน (Seed Phrase) กับบุคคลอื่น

(3) ก่อนทำข้อตกลงกับใคร ต้องตรวจสอบประวัติบุคคลนั้นให้ดีเพื่อลดความเสี่ยงที่จะเสียหาย

(4) ควรเข้าร่วมชุมชนเกมบล็อกเชน เช่น กลุ่มผู้เล่นเกมใน Facebook, Discord ของเกมนั้น ๆ เพื่อติดตามข่าวสาร การแจ้งเตือน และตรวจสอบสัญญาณของโครงการที่อาจหลอกลวงของเกมบล็อกเชนอยู่เสมอ

และจากการสัมภาษณ์ผู้ให้ข้อมูลในกลุ่มเจ้าหน้าที่ตำรวจและผู้เชี่ยวชาญ พบว่า มาตรการที่มีอยู่ยังไม่เพียงพอหรือไม่ตรงกับลักษณะเฉพาะของเกมบล็อกเชน (GameFi) โดยเฉพาะที่มีองค์ประกอบทางการเงินและสื่อสารข้ามแพลตฟอร์ม ทำให้ผู้เสียหายจำนวนมากไม่ได้รับความช่วยเหลือหรือไม่สามารถ

ร้องเรียนได้ทันเวลา และมีข้อเสนอว่า ภาครัฐควรจัดตั้งระบบทะเบียนเกมบล็อกเชน (GameFi Registry System) เพื่อถ่วงดุลและติดตามเกมที่ดำเนินกิจกรรมทางการเงิน ควบคู่กับการกำกับดูแลด้านการโฆษณา และเปิดเผยความเสี่ยงก่อนใช้งาน โดยเฉพาะอย่างยิ่งในกลุ่มเป้าหมายวัยรุ่นที่มีแนวโน้มตกเป็นเหยื่อในสื่อออนไลน์ และควรมีการกำกับดูแลในระดับนโยบาย ได้แก่ การตั้งหน่วยงานเฉพาะด้าน GameFi การออกกฎหมายรองรับ การสร้างฐานข้อมูลเตือนภัยเกม เป็นต้น

อภิปรายผล

จากผลการศึกษานำผลการวิจัยมาอภิปรายผล โดยมีรายละเอียดดังต่อไปนี้

ปัจจัยของการตกเป็นผู้เสียหายจากเกมบล็อกเชน

1. ปัจจัยด้านแรงจูงใจทางการเงิน ผู้เสียหายจำนวนมากมีแรงจูงใจจากความคาดหวังในการได้รับผลตอบแทนที่สูงและรวดเร็วจากการลงทุนในเกมบล็อกเชน โดยเฉพาะในช่วงที่กระแสการลงทุนเพื่อหารายได้กำลังได้รับความนิยมอย่างกว้างขวาง เป็นการสร้างแรงดึงดูดให้เกิดการลงทุนอย่างขาดความระมัดระวัง ทั้งยังตัดสินใจลงทุนด้วยจำนวนเงินที่สูงโดยไม่มีแผนสำรองหรือการประเมินความเสี่ยงทางการเงินอย่างเหมาะสม แม้จะอยู่ในระบบที่ตนไม่เข้าใจอย่างแท้จริง ส่งผลให้เกิดความเสียหายทางการเงินร้ายแรงเมื่อระบบเศรษฐกิจในเกมล้มลงหรือเมื่อเกิดการหลอกลวงในรูปแบบต่าง ๆ สอดคล้องกับทฤษฎีพฤติกรรมแห่ตามกันแบบไม่มีเหตุผลที่อธิบายว่าผู้เล่นตัดสินใจโดยไม่ไตร่ตรองและตามกระแสเนื่องจากกลัวตกกระแส (Fear of Missing Out – FOMO) นอกจากนี้ ยังสอดคล้องกับแนวคิดเหยื่อวิทยาของ Benjamin Mendelsohn (อ้างถึงในสุดสงวน สุธีสร, 2543) ที่ชี้ว่าผู้เสียหายบางส่วนมีบทบาทเชิงรุกในการเข้าร่วมกิจกรรมเสี่ยงด้วยตนเอง (เหยื่อโดยสมัครใจ) รวมทั้งตรงกับงานวิจัยของ สุภสิริ จันทรินทร์ (2565) ที่อธิบายว่าบุคคลที่มีลักษณะชอบเสี่ยงและควบคุมตนเองต่ำ มักตัดสินใจอย่างหุนหันพลันแล่นเมื่อเจอข้อเสนอที่มีผลตอบแทนสูงโดยไม่ได้วิเคราะห์ถึงผลเสียที่จะตามมา อีกทั้งข้อมูลจากงานวิจัยของ ธนวัฒน์ อภิวัฒน์ม (2564) ยังพบว่า นักลงทุนรายย่อยมีแนวโน้มได้รับอิทธิพลจากแรงจูงใจทางเทคโนโลยีและผลตอบแทนใหม่ ๆ ซึ่งสะท้อนพฤติกรรมการตัดสินใจลงทุนในสิ่งที่ไม่เข้าใจอย่างแท้จริง เพราะเชื่อมั่นว่าจะได้ผลตอบแทนสูงจากกระแสใหม่ทางเทคโนโลยี

2. ปัจจัยด้านความรู้และความเข้าใจ ผู้เสียหายส่วนใหญ่มีข้อจำกัดในความเข้าใจที่เกี่ยวข้องกับเศรษฐกิจของเกมบล็อกเชน กลไกการทำงานของระบบเทคโนโลยีสมัยใหม่ เช่น Blockchain, NFT, Smart Contract และ Tokenomics การขาดความเข้าใจในเรื่องเหล่านี้ ทำให้ผู้เล่นไม่สามารถประเมินความเสี่ยงของการลงทุนในเกมได้อย่างเหมาะสม ส่งผลให้ตกเป็นเป้าของกลโกงที่ซับซ้อนทางเทคนิค ปัจจัยนี้มีความสอดคล้องกับทฤษฎีด้านอาชญากรรมไซเบอร์ (Cybercrime) โดยเฉพาะแนวคิดของ Yar (2006) ที่ใช้เทคโนโลยีเป็นเครื่องมือ (Cyber-enabled Crime) เนื่องจากอาชญากรมักอาศัยการขาดความรู้ของเหยื่อในการก่อเหตุ นอกจากนี้ ยังตรงกับทฤษฎีการป้องกันอาชญากรรมโดยสถานการณ์ (Situational Crime Prevention – SCP) ของ Clarke (1997) ที่ชี้ให้เห็นว่าการให้ข้อมูลและความรู้ที่ถูกต้องจะสามารถลดโอกาสที่บุคคลจะตกเป็นเหยื่อจากการหลอกลวงได้อย่างมีประสิทธิภาพ

3. ปัจจัยด้านสื่อและการตลาด เป็นอีกหนึ่งแรงผลักดันสำคัญที่นำไปสู่การตกเป็นผู้เสียหายจากการเล่นเกมบล็อกเชน โดยเฉพาะอย่างยิ่งในยุคที่การสื่อสารผ่านแพลตฟอร์มออนไลน์มีความแพร่หลายและรวดเร็ว ผู้เสียหายเชื่อข้อมูลจากสื่อและโฆษณาเกินจริงผ่านช่องทางออนไลน์ รวมถึงการบอกเล่าจากผู้เล่นกลุ่มแรก ๆ ในกลุ่ม Facebook ว่าเคยทำกำไรได้จริง ส่งผลให้เกิดการตัดสินใจลงทุนโดยขาดการตรวจสอบข้อเท็จจริง ซึ่งสอดคล้องกับทฤษฎีการเปลี่ยนพื้นที่ (Space Transition Theory) ของ Jaishankar (อ้างถึงใน

สาวตรี สุขศรี, 2560) ที่อธิบายว่าบุคคลมักเปลี่ยนพฤติกรรมเมื่อเข้าสู่โลกออนไลน์ เนื่องจากรู้สึกปลอดภัย และเชื่อถือข้อมูลที่ได้รับการยืนยันจากคนจำนวนมากในโลกเสมือน ทำให้มีแนวโน้มเชื่อข้อมูลง่ายขึ้นและลดความระมัดระวังลงเมื่อเทียบกับโลกแห่งความเป็นจริง

ผลกระทบที่เกิดขึ้นกับผู้เสียหายจากเกมบล็อกเชน

จากการวิเคราะห์ข้อมูลจากกลุ่มผู้เสียหาย เจ้าหน้าที่ตำรวจ และผู้เชี่ยวชาญในวงการเกมบล็อกเชน เกี่ยวกับผลกระทบจากเกมบล็อกเชนต่อผู้เสียหาย พบว่า ผลกระทบที่เกิดขึ้นกับผู้เสียหายมีความหลากหลาย และซับซ้อน และมีความรุนแรงแตกต่างกันไปทั้งในด้านการเงิน ด้านจิตใจและด้านสังคม รวมถึงด้านความเชื่อมั่นทางกฎหมาย ซึ่งเชื่อมโยงกับลักษณะเฉพาะของเกมบล็อกเชนที่มีทั้งความไม่โปร่งใส การขาดการควบคุม และความซับซ้อนของเทคโนโลยี ส่งผลให้ผู้เล่นจำนวนมากไม่สามารถประเมินความเสี่ยงได้อย่างแม่นยำ ก่อนตัดสินใจลงทุน ดังนี้

ด้านการเงิน ผู้เสียหายสูญเสียเงินลงทุนจำนวนมากจากการลงทุนที่ขาดการวิเคราะห์ความเสี่ยง โดยเกิดจากการประเมินผิดพลาดว่าผลตอบแทนที่สูงจะคุ้มค่างับความเสี่ยงที่เกิดขึ้น สอดคล้องกับ ทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory – RCT) ของ Cornish and Clarke (2017) ที่อธิบายว่าบุคคลจะตัดสินใจกระทำโดยคำนึงถึงผลตอบแทนที่คาดว่าจะได้รับเมื่อเทียบกับความเสี่ยง ทำให้ผู้เล่นตัดสินใจลงทุนเพราะเชื่อมั่นผิดๆ ว่าผลตอบแทนที่ได้รับจะมีมากกว่าความเสียหายที่อาจเกิดขึ้น

ด้านจิตใจและด้านสังคม เป็นอีกด้านหนึ่งที่ปรากฏชัดในข้อมูลจากผู้ให้สัมภาษณ์ ผู้เสียหายจำนวนมากรู้สึกเสียใจ เครียด ซึมเศร้า และอาจเกิดความขัดแย้งในครอบครัวด้วย ความรู้สึกเหล่านี้ สอดคล้องกับ งานวิจัยของ Sharma et al. (2024) ซึ่งศึกษาความปลอดภัยในโลก Metaverse และพบว่าความเสี่ยงในโลกเสมือนจริงไม่ได้จำกัดแค่ภัยคุกคามทางเทคนิค แต่ยังรวมถึงผลกระทบต่อสภาวะจิตใจของผู้ใช้เมื่อรู้สึกสูญเสีย การควบคุมหรือถูกหลอกลวงในสภาพแวดล้อมที่มีความสมจริงสูง เช่นเดียวกับเกมบล็อกเชนที่มีภาพลักษณ์ของโอกาสใหม่ แต่กลับนำมาซึ่งความเสียหายรุนแรงทั้งด้านเศรษฐกิจและจิตใจ ซึ่งข้อมูลของผู้เสียหายที่พบในงานศึกษานี้ เน้นว่าการขาดระบบควบคุมความเป็นส่วนตัวและการคุ้มครองผู้ใช้ในโลกเสมือนนั้น นำไปสู่ ภาวะทางอารมณ์เชิงลบ ความรู้สึกเปราะบาง และการโดดเดี่ยว เป็นต้น

ด้านความเชื่อมั่นทางกฎหมาย ผู้เสียหายหลายรายระบุว่าเมื่อเกิดเหตุการณ์หลอกลวงหรือ ถูกเอาเปรียบจากการลงทุนผ่านเกมบล็อกเชน ระบบกฎหมายที่มีอยู่กลับไม่สามารถให้ความยุติธรรม ได้ทันที่หรือมีประสิทธิภาพเพียงพอ ผลกระทบดังกล่าวก่อให้เกิดความรู้สึกไม่ปลอดภัยและไม่เชื่อมั่น ต่อระบบกฎหมายและหน่วยงานรัฐ ขณะที่ผู้เสียหายหลายรายไม่แจ้งความ เพราะเชื่อว่าตำรวจไม่สามารถ ดำเนินคดีได้ หรือเคยแจ้งความแล้วไม่ได้รับการติดตามต่อ ทั้งนี้ ความเปราะบางของผู้ใช้ในระบบเทคโนโลยี ที่เปลี่ยนแปลงรวดเร็ว ที่สะท้อนให้เห็นข้อค้นพบในงานวิจัยของ Kumar (2024) ซึ่งศึกษาปัญหา ในการดำเนินคดีอาชญากรรมทางดิจิทัล โดยพบว่ากฎหมายและกระบวนการยุติธรรมยังตามไม่ทันเทคโนโลยี ที่ซับซ้อน ส่งผลให้ทั้งเหยื่อและเจ้าหน้าที่ขาดความร่วมมือในการรับมือ ทำให้ผู้ใช้งานในระบบดิจิทัลตกอยู่ใน ความเสี่ยงซ้ำซ้อน และไม่เพียงพอเพราะความรู้เทคโนโลยีไม่เพียงพอ แต่ยังไม่มียุทธศาสตร์สนับสนุนจากรัฐ ที่ตอบสนองอย่างทันเหตุการณ์ ข้อมูลจากงานวิจัยของผู้วิจัยจึงไม่เพียงชี้ว่าผู้เล่นขาดความรู้เท่านั้น แต่ยังสะท้อนถึงช่องว่างเชิงโครงสร้างที่รัฐและหน่วยงานที่เกี่ยวข้องยังไม่สามารถสร้างความเข้าใจ ความตระหนักรู้ และระบบช่วยเหลือที่เพียงพอสำหรับประชาชนในยุคดิจิทัล และสอดคล้องกับงานวิจัย ของพันธุ์ทิพย์ นวานุช และคณะ (2567) ที่ศึกษาภัยคุกคามทางไซเบอร์และเสนอว่า ภัยในโลกออนไลน์มีความหลากหลายและเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งสอดคล้องกับงานวิจัยนี้เช่นกัน โดยเฉพาะในรูปแบบภัย คุกคามเชิงสื่อสาร เช่น การโฆษณาชวนเชื่อ ข้อมูลหลอกลวง และข่าวปลอม ซึ่งทำให้ผู้ใช้งานหลงเชื่อและ

ตัดสินใจอย่างผิดพลาดได้ง่าย และข้อเสนอยังระบุชัดเจนว่าปัจจุบันกฎหมายยังไม่สามารถตามทันการพัฒนาเทคนิคการสื่อสารในโลกไซเบอร์ได้อย่างมีประสิทธิภาพ ทำให้ผู้บริโภคอยู่ในสถานะเปราะบาง โดยเฉพาะเมื่อระบบการตรวจสอบและกำกับดูแลโฆษณาดิจิทัลยังไม่มีความชัดเจน

ข้อเสนอแนะแนวทางการป้องกันและลดผลกระทบจากการตกเป็นผู้เสียหายที่เกิดขึ้นจากเกมบล็อกเชน

1. ข้อเสนอแนะเชิงปฏิบัติ

1.1 สำหรับประชาชน/ผู้เล่นเกม

(1) ศึกษาข้อมูลอย่างละเอียด ให้ตรวจสอบโครงการที่พัฒนา และ Roadmap ของเกมก่อนตัดสินใจลงทุน

(2) พิจารณากลไกเศรษฐกิจของเกม ให้เลือกลงทุนในเกมที่มีระบบควบคุมอุปทานของ NFT และโทเคนอย่างชัดเจน เพื่อป้องกันการปั่นราคาเหรียญและ NFT

(3) หลีกเลี่ยงคำโฆษณาเกินจริง จะต้องระวังการโฆษณาที่การันตีผลตอบแทนสูงหรือสามารถทำกำไรได้เร็ว

(4) บริหารความเสี่ยงในการลงทุน ไม่ควรนำเงินออมหลักหรือเงินจำเป็นมาลงทุน ควรลงทุนเฉพาะเงินที่สามารถรับความเสี่ยงได้เท่านั้น

(5) รักษาข้อมูลส่วนตัวให้ปลอดภัย เช่น Seed Phrase wallet ไว้เป็นความลับและไม่กดลิงค์แปลกปลอม

(6) ติดตามข่าวสารอย่างสม่ำเสมอ ให้เข้าร่วมชุมชนออนไลน์ เช่น Facebook Groups, Discord เพื่อคุนแนวโน้มของเกมและตรวจสอบการร้องเรียนหรือปัญหาของโครงการอย่างต่อเนื่อง

(7) เก็บหลักฐานธุรกรรม ข้อความสนทนา และเอกสารที่เกี่ยวข้องในการลงทุน เมื่อกรณีจำเป็นต้องแจ้งความดำเนินคดี และแจ้งความทันทีเมื่อถูกโกง

ดังนั้น การเล่นเกมบล็อกเชนอาจเป็นทั้งโอกาสและความเสี่ยง หากผู้เล่นขาดความรู้และความระมัดระวัง จะตกเป็นเหยื่อของมิจฉาชีพได้ง่าย แนวทางป้องกันที่ดี คือ ให้ศึกษาข้อมูลอย่างรอบครอบ มีสติ และไม่หลงเชื่อคำโฆษณาที่เกินจริง

1.2 สำหรับหน่วยงานรัฐ

(1) พัฒนา “ระบบรับแจ้งเหตุเฉพาะด้าน GameFi” ที่แยกจากระบบร้องเรียนทั่วไป โดยควรออกแบบให้ใช้งานสามารถรายงานเหตุได้ง่ายผ่านแพลตฟอร์มดิจิทัล เช่น เว็บไซต์หรือแอปพลิเคชัน พร้อมระบบแนบหลักฐานที่เกี่ยวข้อง เช่น ธุรกรรมคริปโทฯ หรือลิงก์หน้าเว็บ เพื่อให้การวิเคราะห์เหตุการณ์มีความรวดเร็วและแม่นยำ

(2) ภาครัฐควรจัดทำ “สื่อการเรียนรู้เกี่ยวกับ GameFi” เพื่อให้ประชาชนมีความรู้เท่าทันในลักษณะเกมที่มีความเสี่ยง โดยเน้นรูปแบบที่เข้าถึงง่าย เช่น คลิปวิดีโอสั้น อินโฟกราฟิก หรือสื่ออินเทอร์แอกทีฟ โดยกลุ่มเป้าหมายควรรวมถึงเยาวชน ผู้สูงอายุ และผู้ที่สนใจลงทุนในโลกดิจิทัล รวมถึงควรบรรจุความรู้เหล่านี้ไว้ในหลักสูตรการศึกษาขั้นพื้นฐานและระดับอุดมศึกษา

(3) ควรจัดตั้งระบบ “ช่วยเหลือผู้เสียหายเชิงลึกแบบเฉพาะด้าน” โดยบูรณาการความร่วมมือระหว่างนักจิตวิทยา นักกฎหมาย และผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล เพื่อให้ความช่วยเหลือทั้งในด้านสุขภาพจิต และแนวทางในการดำเนินคดี ซึ่งผู้เสียหายส่วนใหญ่มักรู้สึกอับอาย ไม่กล้าแจ้งความ หรือไม่เข้าใจกระบวนการทางกฎหมาย

(4) ส่งเสริมให้มี “หลักสูตรรู้เท่าทัน GameFi” อย่างเป็นทางการ ทั้งในระบบการศึกษาและการอบรมของรัฐ โดยหลักสูตรควรออกแบบให้เข้าใจง่าย ครอบคลุมเรื่องความเสี่ยง พฤติกรรมการหลอกลวง และสิทธิของผู้บริโภคในยุคดิจิทัล อาจบรรจุในรายวิชาคอมพิวเตอร์ เศรษฐศาสตร์ หรือหน้าที่พลเมือง และจัดอบรมให้แก่ครู นักเรียน เจ้าหน้าที่รัฐ และประชาชนทั่วไปอย่างต่อเนื่อง

2. ข้อเสนอแนะเชิงนโยบาย

(1) จัดตั้ง “หน่วยงานเฉพาะด้าน GameFi” หรือ “ศูนย์เฝ้าระวังเกมบล็อกเชน” ภายใต้อำนาจของหน่วยงานรัฐที่มีอำนาจ เช่น กองบัญชาการตำรวจไซเบอร์ หรือสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) โดยหน่วยงานดังกล่าวจะมีหน้าที่ในการรวบรวม วิเคราะห์ และติดตามเกมที่มีความเสี่ยงต่อการฉ้อโกง รวมถึงจัดทำฐานข้อมูลเกมที่มีพฤติกรรมหลอกลวงเพื่อแจ้งเตือนสาธารณชน

(2) ปรับปรุงหรือร่าง “กฎหมายหรือระเบียบเฉพาะเกี่ยวกับ GameFi” โดยเสนอให้มีการนิยามสถานะทางกฎหมายของเกมที่มีลักษณะ Play-to-Earn และมีการหมุนเวียนของสินทรัพย์ดิจิทัล เพื่อให้ครอบคลุมถึงความรับผิดชอบของผู้พัฒนาเกม การควบคุมการโฆษณา การเปิดเผยความเสี่ยง รวมถึงกระบวนการในการเอาผิดผู้กระทำความผิด

(3) กำหนดให้มี “ระบบทะเบียนเกมบล็อกเชน” (GameFi Registry System) สำหรับเกมที่เปิดให้บริการในประเทศไทย โดยผู้ให้บริการต้องลงทะเบียนพร้อมข้อมูลพื้นฐาน เช่น รูปแบบรายได้ ทีมพัฒนา ระบบธุรกรรม และ Smart Contract เพื่อให้ภาครัฐสามารถติดตาม ตรวจสอบ และออกคำเตือนสาธารณะได้ทันทั่วทั้งที่ยังเป็นการสร้างแรงจูงใจให้ผู้พัฒนาเกมดำเนินธุรกิจด้วยความโปร่งใส

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

1. ควรศึกษาเพิ่มเติมเกี่ยวกับปัจจัยการยอมรับเทคโนโลยีของผู้ใช้เกมบล็อกเชน โดยมุ่งเน้นวิเคราะห์ว่าเหตุใดผู้เล่นถึงมีการยอมรับหรือไม่ยอมรับเทคโนโลยีใหม่ ๆ ในเกมบล็อกเชน เพื่อช่วยในการพัฒนากลยุทธ์ทางการตลาดและการออกแบบเกมที่ปลอดภัยและมีความน่าเชื่อถือมากขึ้น

2. การวิจัยครั้งต่อไปควรมีการศึกษาในเชิงปริมาณควบคู่ไปด้วย เช่น การสำรวจทัศนคติ พฤติกรรม และความรู้ของผู้เล่นเกมบล็อกเชนในวงกว้าง เพื่อวิเคราะห์รูปแบบพฤติกรรมที่มีความเสี่ยงและแนวโน้มของปัญหาที่อาจเกิดขึ้นในอนาคต

3. ควรศึกษากลไกทางกฎหมายเชิงเปรียบเทียบระหว่างประเทศที่ประสบความสำเร็จในการจัดการและควบคุมเกมบล็อกเชนและอาชญากรรมไซเบอร์ เพื่อนำมาเป็นแนวทางในการปรับปรุงและพัฒนานโยบายและกฎหมายของประเทศไทยให้สามารถป้องกันและจัดการกับอาชญากรรมประเภทนี้ได้มีประสิทธิภาพมากขึ้น

เอกสารอ้างอิง

दनัย อรุณกิตติชัย. (2564, 9 พฤศจิกายน). *GameFi กับผลตอบแทนที่ไม่ใช่แชร์ลูกโซ่*. กรุงเทพธุรกิจ.

<https://www.bangkokbiznews.com/blogs/columnist/970614>

ธนวัฒน์ อภิวัฒน์นอม. (2564). อิทธิพลของเทคโนโลยีบล็อกเชนที่มีต่อการตัดสินใจลงทุนของนักลงทุนรายย่อย [การค้นคว้าอิสระปริญญาโท]. คลังสารสนเทศดิจิทัล มหาวิทยาลัยธรรมศาสตร์.

https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:299503

พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561. (2561, 13 พฤษภาคม). *ราชกิจจานุเบกษา*.

เล่ม 135 ตอนที่ 33 ก. หน้า 43-70.

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560. (2560, 24 มกราคม).
ราชกิจจานุเบกษา. เล่ม 135 ตอนที่ 10 ก. หน้า 24-35.
- พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 และฉบับแก้ไขเพิ่มเติม. (2535, 16 มีนาคม).
ราชกิจจานุเบกษา. เล่ม 109 ตอนที่ 22. หน้า 1-82.
- พันธุ์ทิพย์ นวานุช, อัมพล กองเขียว, และทองเลื่อน วิเชียรผลา. (2567). มาตรการทางกฎหมายภัยคุกคามทางไซเบอร์. *วารสารวิชาการวิทยาลัยสันตพล*, 10(1), 158-166.
- สถาบันนิติธรรมมาลัย Update กฎหมายและคำพิพากษาฎีกา. (ม.ป.ป.). *หมวด 3 ความผิดฐานฉ้อโกง (มาตรา 341-348)*. <https://www.drthawip.com/criminalcode/1-53>
- สาวตรี สุขศรี. (2560). อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา. *วารสารนิติศาสตร์*, 46(2), 415-432.
- สุดสงวน สุธีสร. (2543). *เหยื่ออาชญากรรม*. พิมพ์ดี
- สุภสิริ จันทรินทร์. (2565, 5 กันยายน). *จิตวิทยาของการตกเป็นเหยื่อมิจฉาชีพ (Victim of scams)*.
คณะจิตวิทยา จุฬาลงกรณ์มหาวิทยาลัย. <https://www.psy.chula.ac.th/th/feature-articles/victim-of-scams>
- Banerjee, A. V. (1992). A Simple Model of Herd Behavior. *The Quarterly Journal of Economics*, 107(3), 797–817. <https://doi.org/10.2307/2118364>
- Bitkub Academy. (2564, 10 พฤศจิกายน). *GameFi คืออะไร?*.
<https://www.bitkubacademy.com/th/blog/what-is-gamefi>
- Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Harrow and Heston.
- Cornish, D. B., & Clarke, R. V. (2017). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Routledge.
- Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- Kell, T., Yousaf, H., Allen, S., Meiklejohn, S., & Juels, A. (2023). Forsage: Anatomy of a Smart-Contract Pyramid Scheme. In Baldimtsi, F., Cachin, C (Eds.), *Financial Cryptography and Data Security. FC 2023. Lecture Notes in Computer Science*, 13951. (pp. 241-258) Springer. https://doi.org/10.1007/978-3-031-47751-5_14
- Kumar, C. R. (2024). Cybercrime and the Law: Challenges in Prosecuting Digital Offenses. *Indian Journal of Law*, 2(5), 20-25. <https://doi.org/10.36676/ijl.v2.i5.53>
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Sage.
- Nation Thailand. (2025, March 1). *Over 100 million baht assets seized in crackdown on gambling website*. <https://www.nationthailand.com/news/general/40046910>
- Proelss, J., Sévigny, S., & Schweizer, D. (2023). GameFi: The perfect symbiosis of blockchain, tokens, DeFi, and NFTs?. *International Review of Financial Analysis*, 90, 102916. <https://doi.org/10.1016/j.irfa.2023.102916>
- Sharma, S., Singh, J., Gupta, A., Ali, F., Khan, F., & Kwak, D. (2024). User Safety and Security in the Metaverse: A Critical Review. *IEEE Open Journal of the Communications Society*, 4(5), 5467-5487. <https://doi.org/10.1109/OJCOMS.2024.3397044>

Kelling, G. L., & Wilson, J. Q. (1982). Broken windows: The police and neighborhood safety.

The Atlantic, 249. <https://unbrokenwindows.queensmuseum.org/index/atlantic>

Suthiwong, S., Wongwatcharapaiboon, J., Thienthaworn, A., & Tapracharoen, K. (2022, June 27). An investigation of expanding the market factors in the gaming industry based

on a blockchain system in Thailand. In *The 13th Built Environment Research Associates Conference* (pp.902-913). Thammasat University, Pathum Thani.

Yar, M. (2006). *Cybercrime and Society*. Sage.