ระบบการจัดการมูลค่าข้อมูลจากเกมสู่เกมด้วยบล็อกเชน

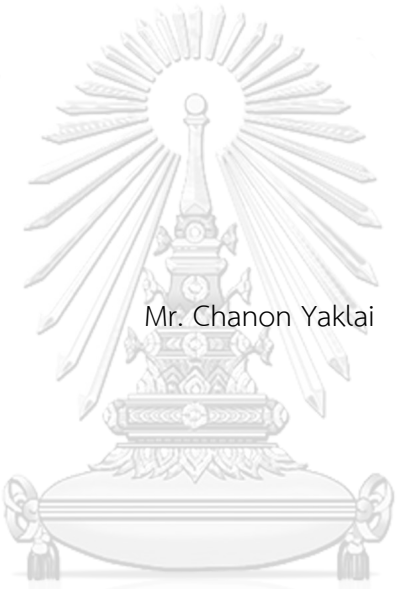
นายชานน ยาคล้าย

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2562
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

# Managing Game Data Values System from Game to Game via Blockchain

Mr. Chanon Yaklai



จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering in Computer Engineering
Department of Computer Engineering
FACULTY OF ENGINEERING
Chulalongkorn University
Academic Year 2019

Copyright of Chulalongkorn University

| | |
|---|---|
| หัวข้อวิทยานิพนธ์ | ระบบการจัดการมูลค่าข้อมูลจากเกมสู่เกมด้วยบล็อกเชน |
| โดย | นายชานน ยาคล้าย |
| สาขาวิชา | วิศวกรรมคอมพิวเตอร์ |
| อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก | รองศาสตราจารย์ ดร.วิษณุ โคตรจรัส |

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.เศรษฐา ปานงาม)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.วิษณุ โคตรจรัส)

..... กรรมการ
(อาจารย์ ดร.กุลวดี ศรีพานิชกุลชัย)

..... กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.จรัสศรี รุ่งรัตนาอุบล)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ชานน ยาคล้าย : ระบบการจัดการมูลค่าข้อมูลจากเกมสู่เกมด้วยบล็อกเชน. ( Managing Game Data Values System from Game to Game via Blockchain) อ.ที่ปรึกษาหลัก : รศ. ดร.วิษณุ โคตรจรัส

แม้ว่าในปัจจุบันบล็อกเชนจะถูกนำมาใช้ประโยชน์ในหลายอุตสาหกรรม แต่ในอุตสาหกรรมเกมนั้น บล็อกเชนไม่ได้ถูกนำไปใช้อย่างกว้างขวางมากนัก นอกจากนี้ แม้ว่าในอุสาหกรรมเกมจะมีผู้เล่นอยู่เป็นจำนวนมาก แต่ก็ยังไม่มีเกมหรือแพลตฟอร์มใดที่ให้สิทธิผู้เล่นในการเป็นเจ้าของสินทรัพย์หรือข้อมูลภายในเกมอย่างแท้จริง โดยแม้จะมีความพยายามในการระดมทุนเพื่อทำเกมหรือแพลตฟอร์มที่ให้ผู้เล่นได้มีโอกาสเป็นเจ้าของสินทรัพย์หรือข้อมูลภายในเกมอยู่บ้าง แต่ก็ยังคงอยู่ในขั้นตอนการทดลองที่ยังไม่เสร็จสมบูรณ์ และผู้เล่นยังต้องพึ่งพาระบบนิเวศน์ของแพลตฟอร์มนั้น ๆ อีกด้วย ในวิทยานิพนธ์ฉบับนี้ ผู้วิจัยจึงประสงค์ที่จะนำเสนอสถาปัตยกรรมกลางที่ทำให้ผู้เล่นเกมสามารถเป็นเจ้าของเวลาที่ตนเองใช้ภายในเกมได้โดยใช้บล็อกเชนสาธารณะ ทั้งผู้เล่นยังสามารถนำเวลาดังกล่าวไปใช้ในเกมอื่นได้ด้วย โดยใช้มาตราฐานโทเคนดิจิทัล ERC-20 บนอีเธอเรี่ยม นอกจากนี้ รูปแบบสถาปัตยกรรมที่นำเสนอดังกล่าวยังสามารถประยุกต์ใช้ได้กับทุกบล็อกเชนสาธารณะ และยังเป็นประโยชน์ต่อทุกองค์ประกอบของระบบนิเวศน์ อาทิเช่น ผู้เล่นบล็อกเชนโหนด และผู้พัฒนาเกม โดยผลการทดลองในงานวิทยานิพนธ์นี้ ยังแสดงว่าแนวความคิดดังกล่าวทำให้ผู้เล่นใช้เวลาในการเล่นเกมนานขึ้น และมีแนวโน้มที่จะอยากเล่นเกมใหม่ๆ ที่สามารถนำมูลค่าในเกมเดิมไปใช้ได้ แต่ทั้งนี้ยังมีปัจจัยหลายอย่างที่มีผล อาทิเช่น ประเภทของเกม การแลกเปลี่ยนค่าของเวลาภายในเกม เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

สาขาวิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2562 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

# # 5970145021 : MAJOR COMPUTER ENGINEERING

KEYWORD: design games blockchain data storage smart contract cryptography public ledger

Chanon Yaklai : Managing Game Data Values System from Game to Game via Blockchain. Advisor: Assoc. Prof. VISHNU KOTRAJARAS, Ph.D.

Blockchain nowadays has been utilized in several industries. However, in the game industry, blockchain has not been utilized greatly. Even though there is a large number of game players in the game industry, none of the game or platform allows users to virtually own their in-game objects or data. There were attempts to raise funds for developing a game or platform that allows players to own their in-game objects or data. However, those attempts are still in the pipeline and users are also required to use their ecosystem. In this thesis, a generic game architecture, using blockchain, that allows players to own their "spent time" in a game, is proposed. The value of this spent time can be passed on to new games as an ERC20 token on the Ethereum network. The proposed architecture can be used with any public blockchain, benefiting many roles in the game ecosystem such as players, blockchain nodes, and game developers. Experiment result shows that the proposed architecture can prolong the period that players spend in the game and make players interested in new games which can redeem the time values from old games, but there are other affecting factors such as the type of gameplay or how the spent time is exchanged in a game.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Field of Study: Computer Engineering Student's Signature .....

Academic Year: 2019 Advisor's Signature .....

# กิตติกรรมประกาศ

ขอขอบพระคุณ รศ. ดร. วิษณุ โคตรจรัส ที่ยอมเสียสละเวลามาเป็นอาจารย์ที่ปรึกษาของผู้วิจัยในการจัดทำวิทยานิพนธ์ฉบับนี้ อาจารย์ได้เมตตาและทุ่มเทเวลาให้กับการให้คำปรึกษา แนะนำแนวทาง และตรวจงานวิจัยฉบับนี้เป็นอย่างมาก หากไม่มีอาจารย์แล้วก็เชื่อได้ว่าวิทยานิพนธ์ฉบับนี้คงไม่อาจสำเร็จขึ้นมาได้

ขอขอบพระคุณ รศ.ดร.เศรษฐา ปานงาม, ผศ.ดร.จรัสศรี รุ่งรัตนาอุบล และ ดร.กุลวดี ศรีพานิชกุลชัย ที่กรุณาเสียสละเวลามาเป็นประธานกรรมการและคณะ กรรมการในการสอบวิทยานิพนธ์ครั้งนี้

ขอขอบคุณภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย สถานที่ที่เอื้ออำนวยให้ผู้วิจัยได้ศึกษาและพัฒนาความรู้ความสามารถตลอดระยะเวลาการทำวิทยานิพนธ์นี้

ขอขอบคุณพี่ๆ เพื่อนๆ และน้องๆ ในห้องปฏิบัติการเกม (Game Lab) และห้องปฏิบัติการการทำเหมืองข้อมูล (Data Mining Lab) สำหรับกำลังใจและคำแนะนำอันดีที่ช่วยให้วิทยานิพนธ์นี้สำเร็จลุล่วงไปได้

ขอขอบคุณมูลนิธิไทยเชน พี่โดม เจริญยศ พี่นเรศ เก็จรัมย์ ที่ช่วยมอบความช่วยเหลือในเรื่องบล็อกเชนสาธารณะ ไทยเชน

ขอขอบคุณพี่สำเร็จ วจนะเสถียร ที่มอบความรู้ในการเขียนสมาร์ทคอนแทรค แนวทางการนำไปใช้งาน ช่องโหว่ที่ควรระวัง

สุดท้ายนี้ ขอขอบพระคุณพ่อกับแม่ ครอบครัว และคุณนายที่รัก ที่คอยให้กำลังใจและสนับสนุนผู้วิจัยในการศึกษาต่อระดับปริญญามหาบัณฑิตตลอดมา ขอบพระคุณจากใจครับ

ชานน ยาคล้าย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# สารบัญ

**หน้า**


..... ค

บทคัดย่อภาษาไทย..... ค

..... ง

บทคัดย่อภาษาอังกฤษ..... ง

กิตติกรรมประกาศ..... จ

สารบัญ..... ช

บทที่ 1 บทนำ ..... 1

1.1 ที่มาและความสำคัญของปัญหา ..... 1

1.2 วัตถุประสงค์ของการวิจัย ..... 5

1.3 ขอบเขตของการวิจัย ..... 5

1.4 ประโยชน์ที่ได้รับ ..... 5

1.5 วิธีดำเนินการวิจัย..... 6

1.6 ผลงานตีพิมพ์จากการวิจัย ..... 6

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง..... 7

2.1 บล็อกเชน..... 7

2.2 การเข้ารหัสแบบสองทาง (Public-key cryptography, or Asymmetric cryptography) .. 8

2.3 การเข้ารหัสของข้อมูลแบบทิศทางเดียวไม่สามารถย้อนกลับได้ (hashing algorithm SHA-256)..... 9

2.4 สมาร์ทคอนแทรค (Smart contract)..... 10

2.5 ฉันทามติ (Blockchain Consensus Protocol) ..... 11

2.5.1 ฉันทามติปรู๊ฟออฟเวิร์ค (POW Concensus Protocol) ..... 11



จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

2.5.2 ฉันทามติดีลีเกตปรู๊ฟออฟสเตค (DPOS Concensus Protocol)..... 11
2.5.3 ฉันทามติปรู๊ฟออฟออธอริทิ (POA Concensus Protocol) ..... 12
2.6 สกุลเงินแบบเข้ารหัส (ERC-20)..... 13
2.7 รูปแบบสถาปัตยกรรมเกมและการเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่ายในปัจจุบัน ..... 13
2.8 รูปแบบสถาปัตยกรรมแบบกระจายศูนย์ (Decentralized Application - DApp)..... 14
บทที่ 3 งานวิจัยที่เกี่ยวข้อง ..... 17
3.1 งานวิจัยเกี่ยวกับการเก็บข้อมูลบนบล็อกเชนและสมาร์ทคอนแทรค (Blockchain Storage and Smart Contract))..... 17
3.2 งานวิจัยเกี่ยวกับเกมบนบล็อกเชน (Blockchain Games)..... 20
3.3 งานวิจัยเกี่ยวกับสถาปัตยกรรมเกมบนบล็อกเชน (Blockchain Game Infrastructure)..... 24
บทที่ 4 แนวคิดและวิธีการดำเนินงาน..... 27
4.1 รูปแบบสถาปัตยกรรมแบบผสมผสาน (Mixed Architecture) ..... 27
4.2 องค์ประกอบที่เกี่ยวข้องกับบล็อกเชน (Blockchain Components) ..... 28
4.2.1 เพลเยอร์คอมโพเน้นต์..... 29
4.2.2 บล็อกเชนโหนดคอมโพเน้นต์ ..... 29
4.2.3 นักพัฒนาเกมคอมโพเน้นต์..... 29
4.3 การทำงานร่วมกันระหว่างคอมโพเน้นต์..... 30
4.3.1 ผู้เล่นใหม่เข้ามาเป็นเพลเยอร์คอมโพเน้นต์ (Player entering blockchain architecture)..... 30
4.3.2 ผู้เล่นออกจากการเป็นเพลเยอร์คอมโพเน้นต์ (Player exiting blockchain architecture)..... 31
4.3.3 การปฏิสัมพันธ์ระหว่างเพลเยอร์คอมโพเน้นต์และนักพัฒนาเกมคอมโพเน้นต์ (Interaction between player component and game developer component)..... 32
4.3.3.1 การปฏิสัมพันธ์ขณะที่ผู้เล่นเล่นเกม (แสดงในรูปที่ 23)..... 33

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

4.3.3.2 การปฏิสัมพันธ์ขณะที่ผู้เล่นแลกเปลี่ยนไอเทม (แสดงในรูปที่ 24) ..... 34
4.3.4 การปฏิสัมพันธ์ระหว่างนักพัฒนาเกมคอมโพเน้นต์และบล็อกเชนโหนดคอมโพเน้นต์ (Interaction between game developer component and blockchain node component) ..... 34
4.3.4.1 การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นสกุลเงินดิจิทัล (แสดงในรูป 25) ..... 35
4.3.4.2 การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นสกุลเงินสด (แสดงในรูปที่ 26) ..... 36
4.4 การเข้าคิวของบล็อกเชนแทรนแซคชั่น (Blockchain Transaction Queueing) ..... 37
บทที่ 5 การพัฒนาระบบต้นแบบ ..... 38
5.1 ระบบบล็อกเชนสาธารณะ (จากรูป 29 ด้านขวา) ..... 39
5.2 อีเอ็กซ์พีโทเคน (EXPTOKEN) ..... 39
5.3 ระบบฐานข้อมูลและส่วนเอพีไอเซิร์ฟเวอร์ (จากรูป 29 ด้านซ้าย) ..... 40
5.4 เว็บบราวเซอร์ (จากรูป 29 ตรงกลาง) ..... 40
5.5 กระเป๋าเงินดิจิทัล (จากรูป 29 ตรงกลาง) ..... 41
5.6 จาว่าสคริปต์ ..... 41
5.7 การแปลงมูลค่าเวลาเป็นอีเอ็กซ์พีโทเคน ..... 42
5.8 ตัวเกมไคลเอนต์ ..... 43
5.8.1 รายละเอียดเกมไคลเอนต์ เกมที่ 1 ..... 43
5.8.1.1 การได้รับเวลาที่ก่อให้เกิดมูลค่าของเกมไคลเอนต์ เกมที่ 1 ..... 47
5.8.1.2 การแลกอีเอ็กซ์พีโทเคนเป็นไอเทมของเกมไคลเอนต์ เกมที่ 1 ..... 47
5.8.2 รายละเอียดเกมไคลเอนต์ เกมที่ 2 ..... 48
5.8.2.1 การได้รับเวลาที่ก่อให้เกิดมูลค่าของเกมไคลเอนต์ เกมที่ 2 ..... 52
5.8.2.2 การแลกอีเอ็กซ์พีโทเคนเป็นไอเทมของเกมไคลเอนต์ เกมที่ 2 ..... 52
5.9 การพัฒนาบล็อกเชนโหนดคอมโพเน้นต์และการทำงานร่วมกัน ..... 53

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

5.9.1 เกมไคลเอนต์กับเพลเยอร์คอมโพเน้นต์ ..... 54
5.9.2 เพลเยอร์คอมโพเน้นต์กับนักพัฒนาเกมคอมโพเน้นต์ ..... 54
5.9.3 นักพัฒนาเกมคอมโพเน้นต์กับบล็อกเชนโหนดคอมโพเน้นต์ ..... 55
5.9.4 เพลเยอร์คอมโพเน้นต์กับบล็อกเชนโหนดคอมโพเน้นต์ ..... 55
5.9.5 เพลเยอร์คอมโพเน้นต์กับเพลเยอร์คอมโพเน้นต์ ..... 56
5.10 กระบวนการทดสอบระบบก่อนใช้งานจริง ..... 56
5.10.1 การทดสอบแบบแยกอิสระ ..... 56
5.10.1.1 การทดสอบเครื่องคอมพิวเตอร์แม่ข่าย (Game Server - Isolation Testing) ..... 57
5.10.1.2 การทดสอบรูปแบบกรอบอ้างอิง (Framework Wrapper - Isolation Testing) ..... 57
5.10.1.3 การทดสอบระบบบล็อกเชนสาธารณะ (Public Blockchain - Isolation Testing) ..... 58
5.10.2 การทดสอบแบบบูรณาการ (Integration Testing) ..... 59
5.10.2.1 การทดสอบขณะเข้าเล่นเกม (Game Login – Intregation Testing) ..... 59
5.10.2.2 การทดสอบขณะเล่นเกม (Game Play – Intregation Testing) ..... 60
5.10.2.3 การทดสอบการแลกเปลี่ยนเวลาเป็นอีเอ็กซ์พีโทเคน (Time to Exptoken Exchange – Intregation Testing) ..... 60
5.10.2.4 การทดสอบการแลกเปลี่ยนอีเอ็กซ์พีโทเคนเป็นไอเทมภายในเกม (Exptoken to Item Exchange – Intregation Testing) ..... 61
5.10.2.5 การทดสอบการทำงานที่ผิดพลาดของระบบบล็อกเชนขณะเล่นเกม (Diagnose Blockchain Error while Play Game - Intregation Testing) ..... 62
บทที่ 6 การทดลองและผลการทดลอง ..... 63
6.1 การทดลอง ..... 63
6.2 ผลการทดลองและวิเคราะห์ผลการทดลอง ..... 64

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

6.3 รายละเอียดวิธีการเขียนสมาร์ทคอนแทรค ..... 66
6.3.1 การเขียนสมาร์ทคอนแทรคของอีเอ็กซ์พีโทเคน ..... 66
6.3.2 การเขียนสมาร์ทคอนแทรคของตัวเกม ..... 68
6.4 สรุปการนำสมาร์ทคอนแทรคที่พัฒนาขึ้นไปใช้งาน ..... 71
บทที่ 7 สรุปการวิจัยและแนวทางการวิจัยในขั้นถัดไป ..... 72
7.1 สรุปการวิจัยและอภิปรายผลการวิจัย ..... 72
7.2 ข้อจำกัดและข้อเสนอแนะ ..... 73
7.3 บทวิเคราะห์การใช้บล็อกเชนสาธารณะกับเกม ..... 75
7.4 แนวทางวิจัยในขั้นถัดไป ..... 77
บรรณานุกรม ..... 78
ประวัติผู้เขียน ..... 81

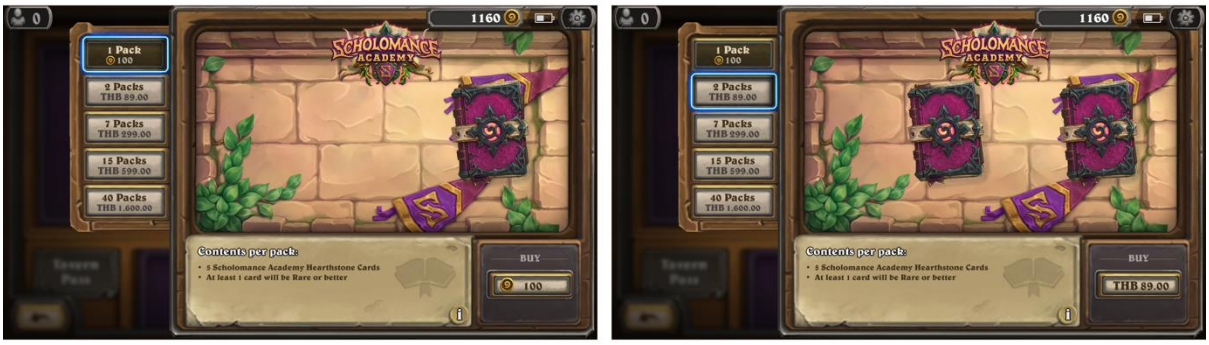
จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# บทที่ 1
# บทนำ

## 1.1 ที่มาและความสำคัญของปัญหา

อุตสาหกรรมเกมเป็นหนึ่งในอุตสาหกรรมสื่อที่มีอัตราการเติบโตสูงเป็นอันดับต้น ๆ ของสื่อทั้งหมด รายงานการคาดการณ์เกี่ยวกับอุตสาหกรรมสื่อของ PwC[1] แสดงให้เห็นว่าอัตราการเติบโตของยอดขายของธุรกิจเกมสูงเป็นอันดับสาม ข้อมูลดังกล่าวนี้สะท้อนให้เห็นถึงความสำคัญในการผลักดันให้เกิดวิธีการหรือแนวคิดใหม่ที่ช่วยให้อุตสาหกรรมเกมสามารถพัฒนาต่อไปได้อย่างยั่งยืน

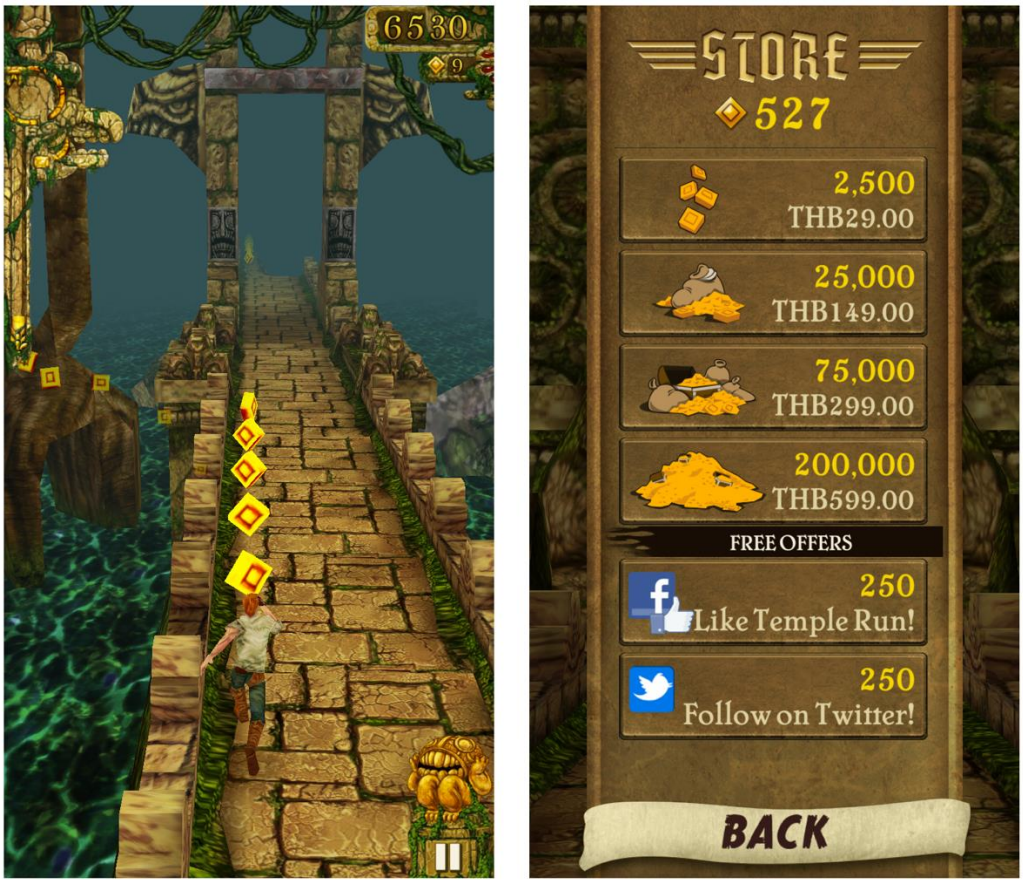
คนส่วนใหญ่เล่นเกมเพื่อความเพลิดเพลิน ซึ่งการเล่นเกมนั้นอาจเปรียบเทียบได้กับการดูภาพยนตร์สักเรื่องหนึ่ง แต่เวลาที่ใช้ในการเล่นเกมแต่ละเกมนั้นมากกว่าการดูภาพยนตร์หลายเท่าตัว มูลค่าของสะสมในเกม ซึ่งแปรตามเวลาที่ให้กับเกม เป็นสิ่งที่ผู้เล่นให้ความสำคัญ เนื่องจากต้องใช้เวลาหรือทุนทรัพย์ ในการสะสม สินทรัพย์ที่ได้ในเกมนั้นส่วนใหญ่จะได้มาจากการทำภารกิจหรือเล่นไปเป็นเวลาหนึ่ง หรือได้มาจากการใช้เงินจริง ๆ เพื่อซื้อของภายในเกม ดังแสดงในรูปที่ 1 และ รูปที่ 2




รูปที่ 1 ภาพจากเกม Hearthstone[2]
ซ้าย - แสดงการใช้เงินที่ได้รับจากการทำภารกิจภายในเกมเพื่อนำมาซื้อของภายในเกม
ขวา – แสดงการใช้เงินสดเพื่อนำมาซื้อของภายในเกม

[1] อ้างอิงจาก https://www.pwc.com/gx/en/industries/tmt/media/outlook.html

[2] อ้างอิงจาก https://playhearthstone.com/en-us/




รูปที่ 2 ภาพจากเกม TempleRun[3]
ซ้าย - แสดงการได้รับสกุลเงินภายในเกมซึ่งได้มากจากการเล่นเกม
ขวา – แสดงการได้รับสกุลเงินภายในเกมซึ่งได้มาจากการซื้อด้วยเงินสด

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

หากเกมต้องปิดตัวลง ผู้เล่นต้องสูญเสียสินทรัพย์ภายในเกมที่สะสมมา ซึ่งถือได้ว่าเป็นการสูญเสียมูลค่าทางเวลาที่ใช้ไปเช่นกัน

แนวคิดในการอนุญาตให้ผู้เล่นนำข้อมูลจากเกมที่เคยเล่น ไปใช้ในเกมใหม่ เป็นแนวคิดเพื่อช่วยให้ผู้เล่นรู้สึกว่า เวลาและทรัพยากรที่ได้ใช้ไปกับเกมที่เคยเล่นนั้น ไม่ได้หายไปเฉย ๆ มีเกมที่นำแนวคิดนี้ไปใช้อยู่จำนวนหนึ่ง ตัวอย่างเช่น เกม Metal Gear Solid (รูปที่ 3) ที่ตัวละครภายในเกมมีการพูดกับผู้เล่นโดยอ้างอิงว่าผู้เล่นคนนั้น[4] เคยเล่นเกม Castlevania มา ตัวละครนำข้อมูลมาจาก

[3] อ้างอิงจาก https://play.google.com/store/apps/details?id=com.imangi.templerun&hl=en

[4] อ้างอิงจาก http://metalgear.wikia.com/wiki/Fourth_wall

ระบบเซฟเกม ของระบบปฏิบัติการ โซนี่เพลย์สเตชั่น (Sony PlayStation หรือ PSX) ที่รับรู้ว่าผู้เล่นเคยเล่นเกมอะไรมาแล้วบ้าง

รูปที่ 3 ตัวละครภายในเกม Metal Gear Solid พูดกับผู้เล่น

อีกตัวอย่างหนึ่ง เป็นการนำตัวละครจากเกมที่เคยเล่นแล้ว มาใช้ในเกมใหม่ เกม Mass Effect 3 สามารถนำตัวละครของเกม Mass Effect 2 มาใช้ได้ รูปที่ 4 แสดงการนำเข้าตัวละครจากเกม Mass effect 2 ไปยัง Mass effect 3 โดยผู้เล่นสามารถนำตัวละครในเกมก่อนหน้าที่ถูกเก็บอยู่ในหน่วยความจำของแพลตฟอร์มที่ผู้เล่นใช้ มาใช้ในเกมที่ตนเองเล่นในปัจจุบันได้

อย่างไรก็ตาม การที่ผู้เล่นสามารถทำเช่นนี้ได้ ยังถูกจำกัดให้ทำได้แค่บนแพลตฟอร์มเดียวกัน ซ้ำยังเป็นเกมจากผู้พัฒนาเกมค่ายเดียวกันเท่านั้นอีกด้วย

รูปที่ 4 การนำเข้าตัวละครจากเกม Mass effect 2 ไปยัง Mass effect 3

ปัจจุบัน ยังไม่มีมาตรฐานการจัดการสินทรัพย์ต่าง ๆ ที่ได้มาจากเกม เพื่อนำไปใช้ในเกมใด ๆ อื่น ๆ ได้ แนวทางของผู้วิจัยนั้นจะมุ่งเน้นไปที่การให้ผู้เล่นได้สินทรัพย์บางอย่างที่เกิดจากการเล่นภายในเกม และผู้เล่นเป็นเจ้าของอย่างแท้จริงโดยยังสามารถนำไปใช้ในเกมอื่นที่ไม่จำเป็นจะต้องอยู่บนแพลตฟอร์มเดียวกันหรือมีผู้พัฒนาค่ายเดียวกัน

การที่จะให้ผู้เล่นเป็นเจ้าของข้อมูลของตนเองนั้น ในปัจจุบันเราสามารถทำได้โดยใช้ระบบจัดเก็บแบบศูนย์กลาง (Centralize) หรือบุคคลที่ 3 (Third-party) ในการเก็บข้อมูลของผู้เล่นไว้ ตัวอย่างเช่น การเก็บข้อมูลบนคลาวด์หรือฐานข้อมูลออนไลน์ และให้สิทธิแก่ผู้พัฒนาเกมแต่ละค่ายในการสามารถนำไปใช้ได้ แต่ผลประโยชน์ที่เกิดขึ้นก็จะตกกับบุคคลที่ 3 และอาจเกิดผลประโยชน์ทับซ้อนได้อีก ไม่เช่นนั้นจะต้องหาหน่วยงานที่น่าเชื่อถือมากำกับดูแลเพื่อให้เป็นกลางและยุติธรรม ถึงแม้จะมีหน่วยงานมากำกับดูแลแล้ว ก็ยังมีโอกาสที่จะถูกปลอมแปลงข้อมูลหรือข้อมูลสูญหายได้เช่นกัน จึงอาจกล่าวได้ว่าผู้เล่นเองหากใช้ระบบการจัดเก็บแบบศูนย์กลาง ก็ไม่อาจแน่ใจได้ว่าจะได้เป็นเจ้าของข้อมูลนั้นจริง ๆ

บล็อกเชน (Blockchain) เป็นระบบการจัดเก็บข้อมูลแบบกระจายศูนย์กลาง (Decentralize) ข้อมูลไม่ได้ถูกเก็บไว้ที่ใดที่หนึ่งและไม่ได้ถูกควบคุมโดยบุคคลใดบุคคลหนึ่ง ระบบการจัดเก็บข้อมูลชนิดนี้เป็นระบบฐานข้อมูลชนิดหนึ่งที่ถูกใช้มากในการทำธุรกรรมอิเล็กทรอนิกส์บนเครือข่ายอินเตอร์เน็ต และได้ถูกนำไปประยุกต์ใช้ในวงกว้าง ไม่ว่าจะเป็นด้านการเงินและการธนาคาร[5] การเลือกตั้ง[6] การประกันภัย[7] บล็อกเชนถูกใช้ในทุกวงการที่ต้องการให้ข้อมูลมีความปลอดภัยสูง โปร่งใส และมีเสถียรภาพ

[5] อ้างอิงจาก https://www.ibm.com/blockchain/industries/financial-services

ทางผู้วิจัยมีแนวคิดว่าเวลาและมูลค่าของสิ่งต่าง ๆ ที่ได้จากในเกม ควรเป็นสิทธิของผู้เล่นเฉก เช่นทรัพย์สินอื่นที่มีมูลค่าในโลกของความจริง อีกทั้งยังควรสามารถส่งต่อและสืบทอดให้ผู้อื่น หรือแม้แต่ซื้อขายแลกเปลี่ยนกันได้ ทางผู้วิจัยจึงประสงค์ที่จะนำเสนอแนวทางและระบบการแปลงมูลค่าของเวลาที่ผู้เล่นใช้ไปในเกม ไปเป็นมูลค่าที่สามารถส่งต่อจากเกมหนึ่งไปสู่อีกเกมหนึ่งได้ ซึ่งนอกจากประโยชน์ที่ผู้เล่นจะได้รับแล้ว ทางผู้พัฒนาเกมเองยังได้ประโยชน์อีกด้วยเนื่องจากสามารถวางแผนดึงดูดผู้เล่นจากเกมเก่ามายังเกมใหม่ได้สะดวกขึ้น โดยระบบที่นำเสนอในวิทยานิพนธ์นี้จะใช้เทคโนโลยีบล็อกเชน

## 1.2 วัตถุประสงค์ของการวิจัย

1. นำเสนอระบบที่ผู้เล่นสามารถสร้างมูลค่าจากเวลาและความเพียรที่ผู้เล่นได้ใช้ในเกมหนึ่ง ๆ เพื่อส่งผ่านไปยังเกมอีกเกมหนึ่งได้
2. พัฒนาระบบต้นแบบ เพื่อให้ผู้พัฒนาเกมสามารถใช้เป็นแนวทางเริ่มต้นในการประยุกต์ใช้กับเกมของตนได้ ตามแนวทางที่ผู้วิจัยนำเสนอ

## 1.3 ขอบเขตของการวิจัย

1. เกมที่ใช้ในการทดลองถูกสร้างจากเครื่องมือยูนิตี้ทรีดี (Untiy3d 2018) ขึ้นไป
2. เกมที่ใช้ในการทดลอง มีจำนวนสองเกม ซึ่งเลือกมาเป็นสองประเภทที่มีวิธีการเล่นแตกต่างกัน
3. ใช้เทคโนโลยีบล็อกเชนที่มีอยู่ในปัจจุบันเพื่อนำเสนอแพลตฟอร์ม
4. มีจำนวนผู้ทดสอบรวมกันทั้งหมดประมาณ 150 คน

## 1.4 ประโยชน์ที่ได้รับ

1. ได้แนวทางการส่งต่อข้อมูลจากเกมหนึ่งไปยังเกมอื่น และแนวทาง การเปลี่ยนมูลค่าเวลาในเกมเพื่อไปใช้ในเกมอื่น ซึ่งสามารถใช้เป็นต้นแบบของการถ่ายเทข้อมูลอื่น ๆ ในเกมได้ เช่น เงินภายในเกม ภารกิจที่ทำสำเร็จ และสิ่งของต่าง ๆ ที่มีภายในเกม เป็นต้น
2. ได้ระบบที่สนับสนุนแนวคิดเรื่องผู้เล่นเป็นเจ้าของข้อมูลอย่างแท้จริง

---

[6] อ้างอิงจาก https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election

[7] อ้างอิงจาก https://www.ey.com/en_gl/insurance/blockchain-marine-insurance

**1.5 วิธีดำเนินการวิจัย**

1. ศึกษางานวิจัยที่เกี่ยวข้องกับเทคโนโลยีบล็อกเชน
2. ศึกษางานวิจัยที่เกี่ยวข้องกับการให้ผลตอบแทนจากการเล่นเกม
3. ทำการทดสอบระบบบล็อกเชนในระบบปิด (Localhost)
4. สร้างส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface) ภายใน unity3d และภายในรูปแบบกรอบอ้างอิง (Framework Wrapper) ตามระบบที่เสนอในวิทยานิพนธ์นี้ เพื่อให้ผู้วิจัยและผู้พัฒนาเกมสามารถนำไปใช้ได้
5. สร้างสมาร์ทคอนแทรค (Smart Contract) เพื่อบรรจุลงบนบล็อกเชนทั้งฝั่งของผู้เล่นเกมและผู้พัฒนาเกม
6. นำสมาร์ทคอนแทรคที่สร้างทดสอบภายในระบบบล็อกเชนในระบบปิด
7. นำสมาร์ทคอนแทรคที่สร้างทดสอบภายในระบบเปิดหลักของบล็อกเชน (Main net) ที่เลือกใช้
8. เก็บผลการทดลองและสรุปผลการวิจัย
9. จัดทำวิทยานิพนธ์

**1.6 ผลงานตีพิมพ์จากการวิจัย**

ส่วนหนึ่งของวิทยานิพนธ์ฉบับนี้ ได้รับการตีพิมพ์เป็นบทความทางวิชาการ **1** เรื่อง ดังนี้

1. **“An Architecture for game to game data transfer using blockchain”** โดย ชานน ยาคล้าย และ รศ.ดร. วิษณุ โคตรจรัส ในงานประชุมวิชาการ **The 17th International Joint Conference on Computer Science and Software Engineering (JCSSE2020)** อยู่ในฐานข้อมูล **IEEE**

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# บทที่ 2
# ทฤษฎีที่เกี่ยวข้อง

ทฤษฎีที่เกี่ยวข้องกับวิทยานิพนธ์นี้ ประกอบไปด้วยเนื้อหาที่เกี่ยวข้องกับบล็อกเชนและการประยุกต์ใช้ รวมถึงนิยามศัพท์ใหม่ที่ผู้วิจัยใช้เพื่ออธิบายวิทยานิพนธ์ฉบับนี้

## 2.1 บล็อกเชน

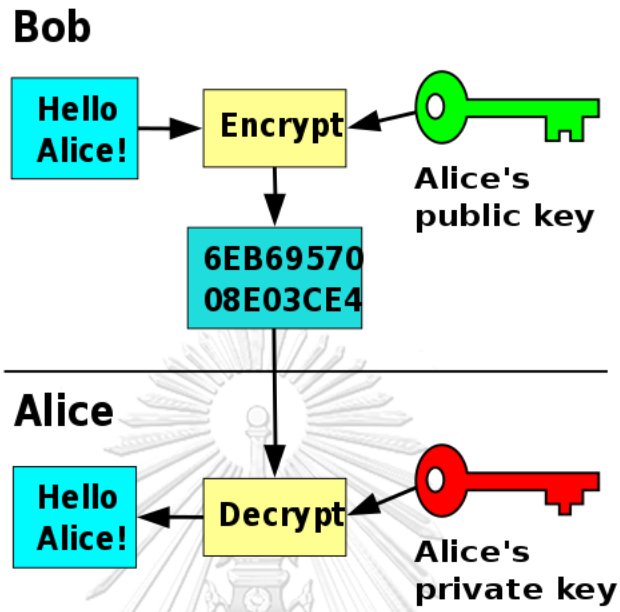
บล็อกเชนเป็นรูปแบบการเก็บข้อมูลแบบกระจายศูนย์กลาง โดยมีการอ้างอิงข้อมูลของบล็อกก่อนหน้าต่อกันเป็นสายโซ่ข้อมูล ข้อมูลจะไม่ได้ถูกเก็บไว้ที่ใดที่หนึ่ง และไม่ได้ถูกยืนยันจากบุคคลที่ 3 หากแต่จะถูกยืนยันคำสั่ง (Transaction) ที่ส่งมา ด้วยผู้ขุด (miner) หรือบางบล็อกเชนเรียกว่าผู้ยืนยัน (Validator) โดยมีมาตรการการยืนยันข้อมูลตามที่ตกลงกัน (Consensus Protocol) บล็อกเชนเป็นที่รู้จักอย่างกว้างขวางจากบทความของ Satoshi Nakamoto[8] ที่นำเสนอระบบแลกเปลี่ยนแบบอิเล็กทรอนิกส์โดยไม่จำเป็นต้องมีบุคคลที่ 3 เป็นตัวกลาง โดยเสนอสกุลเงินแบบเข้ารหัส คริปโตเคอเรนซี่ (Cryptocurrency) ที่ชื่อว่าบิทคอยน์ (Bitcoin) ในการแลกเปลี่ยนเงินตราไปมาระหว่างบุคคล ทั้งนี้การแลกเปลี่ยนดังกล่าวจะถูกยืนยันคำสั่งด้วยคนขุดภายใต้มาตรการยืนยันข้อมูลที่ตกลงกัน โดยบิทคอยน์ใช้มาตรการที่เรียกว่า Proof-of-Work หลักการคือผู้ขุดจะแข่งกันยืนยันข้อมูล โดยการแข่งกันแก้สมการคณิตศาสตร์ หากใครยืนยันได้เป็นคนแรกจะได้รางวัลเป็นสกุลเงินดิจิทัลบิทคอยน์จำนวนหนึ่ง เมื่อยืนยันคำสั่งได้แล้วข้อมูลจะถูกเข้ารหัสแบบฟังก์ชันแฮช (hash) ทั้งยังมีการสร้างชุดกุญแจส่วนบุคคล หรือไพรเวทคีย์ (Private key) และตำแหน่งที่อยู่ของบล็อก (Block Address) เสร็จแล้วจึงถูกสร้างเป็นบล็อก แล้วนำไปต่อกับบล็อกก่อนหน้าที่มี เราเรียกชุดข้อมูลที่มีบล็อกมาต่อกันนี้ว่าบัญชีสาธารณะ (Public Ledger) จะสังเกตเห็นว่าจากลักษณะของการนำข้อมูลมาต่อกันเป็นบล็อก ๆ ระบบนี้จึงถูกนิยามขึ้นว่า บล็อกเชน เมื่อบัญชีสาธารณะถูกเขียนขึ้นมาแล้วบัญชีดังกล่าวจะกระจายไปให้ทุกคนในระบบถือครองไว้ ผ่านเครือข่ายแบบโหนดต่อโหนด (Peer-to-Peer Network) เมื่อเป็นเช่นนี้แล้วทุกคนในระบบจะสามารถเข้าถึงข้อมูลของตนเองได้ด้วยชุดกุญแจส่วนบุคคลเพื่อเข้าถึงตำแหน่งที่อยู่ของบล็อกที่ถูกบันทึกไว้ในบัญชีสาธารณะ

ด้วยหลักการดังกล่าว ผู้วิจัยจึงนำบล็อกเชนมาใช้เพื่อเก็บเวลาของผู้เล่นที่ใช้ในเกมบนบล็อกเชน ตามจุดประสงค์ที่ผู้วิจัยกล่าวไว้ในบทที่ 1

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[8] อ้างอิงจาก https://bitcoin.org/bitcoin.pdf

## 2.2 การเข้ารหัสแบบสองทาง (Public-key cryptography, or Asymmetric cryptography)




รูปที่ 5 แสดงการเข้ารหัสและการถอดรหัสของหลักการ Public-key cryptography[9]

จากรูปที่ 5 การเข้ารหัสแบบสองทาง จะมีกุญแจสองดอก คือ กุญแจส่วนบุคคล (Private key) ซึ่งจะเก็บเป็นความลับที่มีเจ้าของคนเดียวเท่านั้นที่รู้ และกุญแจสาธารณะ (Public key) ซึ่งไม่จำเป็นต้องเก็บเป็นความลับ ทั้งสองตัวจะใช้งานต่างกันคือ ถ้าใช้กุญแจอันนึงเข้ารหัส จะต้องใช้กุญแจอีกตัวนึงที่เข้าคู่กันในการถอดรหัส

กุญแจส่วนบุคคลจะถูกสร้างขึ้นมาก่อนเป็นตัวเลขขนาด 256 บิต [32 ไบต์] (จำนวนบิตอาจจะต่างกันขึ้นกับมาตราฐานของบล็อกเชนสาธารณะที่ใช้) โดยใช้กลวิธีที่แต่ละเลขที่ถูกสร้างขึ้นมามีโอกาสซ้ำกันน้อยมากจนอนุมานได้ว่าไม่มีโอกาสซ้ำกันได้เลยก็ได้ และกุญแจส่วนบุคคลถือเป็นรหัสลับที่เอาไว้แทนความเป็นเจ้าของกุญแจสาธารณะ

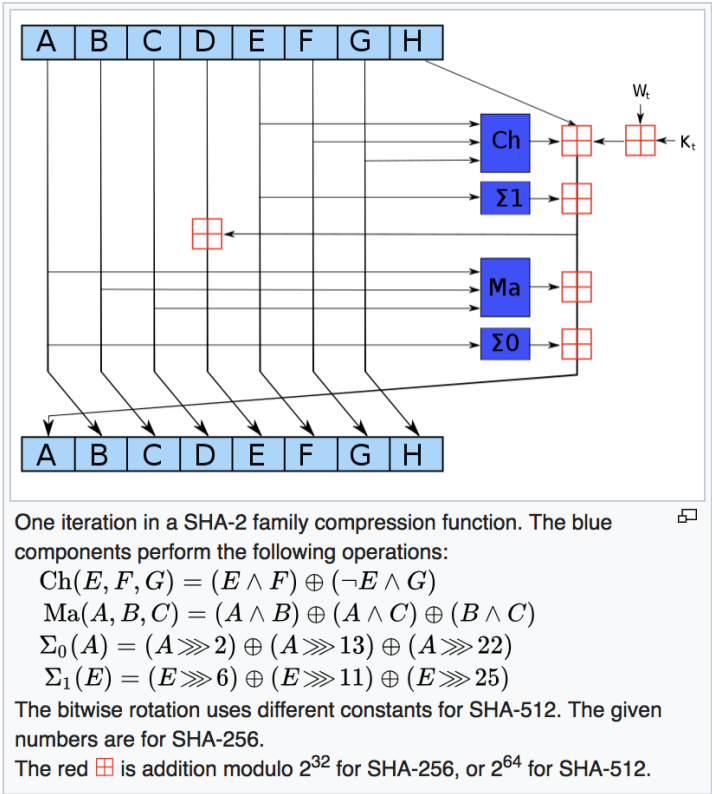
บล็อกเชนสาธารณะที่ได้รับการยอมรับส่วนใหญ่จะสร้างชุดกุญแจสาธารณะและกุญแจส่วนบุคคล โดยใช้อัลกอริทึมที่ชื่อว่า Elliptic Curve Digital Signature Algorithm (ECDSA) [1] ซึ่งจะทำให้ได้กุญแจสาธารณะที่เป็นอนุพันธ์ของกุญแจส่วนบุคคลนั้น ๆ ได้ ซึ่งแปลว่ากุญแจสาธารณะก็จะ

[9] อ้างอิงจาก https://en.wikipedia.org/wiki/Public-key_cryptography

ไม่มีโอกาสซ้ำกัน (เพราะกุญแจส่วนบุคคลไม่ซ้ำกัน) โดยกุญแจสาธารณะจะมีขนาดความยาวที่ 65 ไบต์

ด้วยหลักการที่กล่าวมาข้างต้นจะเห็นได้ว่า เราสามารถสร้างกุญแจสาธารณะได้จากกุญแจส่วนบุคคล และสามารถให้คนทั่วไปและเปิดเผยได้ ตราบใดที่ไม่มีใครรู้กุญแจส่วนบุคคลของเรา ด้วยหลักการดังกล่าวนี้ กุญแจสาธาณะจึงถูกนำมาใช้เป็นตัวแทนของกระเป๋าเงินสาธารณะ (Public Wallet) ในระบบบล็อกเชนสาธารณะที่เป็นที่นิยม อย่างเช่น อีเธอเรี่ยม[10] (ethereum) หรือ บิทคอยน์ เป็นต้น

## 2.3 การเข้ารหัสของข้อมูลแบบทิศทางเดียวไม่สามารถย้อนกลับได้ (hashing algorithm SHA-256)




รูปที่ 6 หลักการการทำงานของฟังก์ชันแฮช[11]

[10] อ้างอิงจาก https://ethereum.org/en/

[11] อ้างอิงจาก https://en.wikipedia.org/wiki/SHA-2

รูปที่ 6 แสดงการเข้ารหัสข้อมูลแบบทิศทางเดียวไม่สามารถย้อนกลับได้ ฟังก์ชันแฮช มีหลายรูปแบบ [2] ตัวอย่างเช่น MD5 ซึ่ง MD5 เป็นการเข้ารหัสที่นิยมในสมัยก่อนมาก แต่เนื่องจากมีเหตุการณ์ collision hash function[12] [3] ซึ่งเป็นกรณีที่อาจเจอผลลัพธ์ที่เกิดขึ้นเหมือนข้อมูลต้นแบบที่จะทำการแฮชได้ จึงอาจกล่าวได้ว่าข้อมูลนั้นไม่ปลอดภัย แต่หากทำการเข้ารหัสด้วย SHA-256 โอกาสที่จะเจอผลลัพธ์หลังจากการแฮชที่เหมือนข้อมูลต้นแบบเป็น $\frac{1}{2^{256}}$ ซึ่งเรียกได้ว่าน้อยมาก หรืออาจจะเป็นไปไม่ได้เลย

ผู้วิจัยได้นำหลักการของฟังก์ชันแฮช มาเพื่อแฮชข้อมูลที่ผู้เล่นสร้างจากภายในเกมเพื่อไปเก็บบนบล็อกเชนก่อนที่จะบรรจุลงในบล็อก เพื่อป้องกันข้อมูลของผู้เล่นแต่ละคนไม่ให้บุคคลภายนอกเข้าถึงได้โดยง่าย

**2.4 สมาร์ทคอนแทรค (Smart contract)**

สมาร์ทคอนแทรค [4] เป็นรูปแบบของกฎหรือสัญญา เป็นการเขียนโปรแกรมลงบนบล็อกเพื่อทำเงื่อนไขบางอย่างก่อนที่ผู้ขุดจะทำการตรวจสอบสัญญาเพื่อบรรจุข้อมูลลงบล็อก สมาร์ทคอนแทรคถูกเริ่มใช้อย่างกว้างขวางในบล็อกเชนชื่อดังอย่างอีเธอเรี่ยม โดยรูปแบบการเขียนสมาร์ทคอนแทรคก็เหมือนกับการเขียนโปรแกรมทั่วไป

ส่วนที่สำคัญของสมาร์ทคอนแทรคที่เกี่ยวข้องกับงานวิทยานิพนธ์นี้ คือ สมาร์ทคอนแทรคจะมีลักษณะเฉพาะ โดยทุกครั้งที่ทำการส่งสมาร์ทคอนแทรคขึ้นไปบนบล็อกเชน จะต้องทำผ่านผู้ที่ถือกุญแจส่วนบุคคลของกระเป๋าเงินสาธารณะ จึงทำให้สมาร์ทคอนแทรคนั้น ๆ ทราบถึงเจ้าของสมาร์ทคอนแทรค (Smart Contract’s Owner) ได้

ในงานวิทยานิพนธ์นี้ ผู้วิจัยนำสมาร์ทคอนแทรคมาเขียนโปรแกรม โดยบางฟังก์ชันในสมาร์ทคอนแทรคจะสามารถถูกเรียกได้เฉพาะเจ้าของสมาร์ทคอนแทรคเท่านั้น เช่นในส่วนที่จะให้รางวัลกับผู้เล่นเกมตามมูลค่าของเวลาที่เกิดจากการเล่น การแลกเปลี่ยนสกุลเงิน การแลกเปลี่ยนไอเทม เพราะฉะนั้นสมาร์ทคอนแทรคจำเป็นจะต้องรู้ว่าใครเป็นเจ้าของสมาร์ทคอนแทรคนั้น ๆ ในส่วนของรายละเอียดต่าง ๆ จะอธิบายในบทที่ 4 ต่อไป

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

[12] อ้างอิงจาก http://valerieaurora.org/hash.html

## 2.5 ฉันทามติ (Blockchain Consensus Protocol)

"ฉันทามติ" เป็นข้อตกลงที่ใช้ยืนยันข้อมูลที่จะนำมาต่อกับบล็อกข้อมูลใหม่ที่ถูกสร้างขึ้น เป็นข้อตกลงที่ใช้ร่วมกันภายในระบบที่ไม่มีศูนย์กลาง (Non - Centralize) หรือ ระบบแบบกระจายศูนย์ (Distributed System)

ฉันทามตินั้นมีความสำคัญเป็นอย่างมากในบล็อกเชนสาธารณะชั้นที่ 1 (Mainnet Layer 1) ตัวอย่างเช่น อีเธอเรี่ยม กล่าวคือฉันทามตินั้นเป็นตัวกำหนดความช้าหรือเร็วของแทรนแซคชั่นต่อวินาที (TPS or Transaction per sec) ยิ่ง แทรนแซคชั่นต่อวินาทีมาก ๆ แปลว่าบล็อกเชนสาธารณะนั้น ๆ สามารถรับโหลดต่อวินาทีได้มากตามไปด้วย เพราะฉะนั้นการเลือกบล็อกเชนสาธารณะใด ๆ นั้น ต้องคำนึงถึง แทรนแซคชั่นต่อวินาที ของบล็อกเชนสาธารณะนั้น ๆ ด้วย เนื่องจากโดยพื้นฐานของเกมทุกเกมจะมีการส่งค่ารับค่าตลอดเวลา ซึ่งหาก แทรนแซคชั่นต่อวินาทีของบล็อกเชนสาธารณะนั้นต่ำเกินไป จะทำให้ผู้เล่นรู้สึกได้ถึงความหน่วงและความช้าได้

### 2.5.1 ฉันทามติปรู๊ฟออฟเวิร์ค (POW Concensus Protocol)

ฉันทามติปรู๊ฟออฟเวิร์ค[13] (POW หรือ Proof-of-Work) เป็นฉันทามติที่เป็นที่รู้จักกันมากที่สุด แต่ ค่าแทรนแซคชั่นต่อวินาที ต่ำที่สุด โดยใช้กับสกุลเงินแบบเข้ารหัสที่ชื่อว่าบิทคอยน์ (Bitcoin) อาจกล่าวได้ว่า ฉันทามติแบบ POW เป็นมาตรการแรกที่ใช้ในบล็อกเชนสาธารณะ แต่ในแง่ของวิทยานิพนธ์ฉบับนี้ ผู้วิจัยเห็นว่าไม่เหมาะสมกับการใช้งานจริง เพราะช้าและค่าใช้จ่ายสูงเมื่อเทียบกับฉันทามติในแบบอื่น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

### 2.5.2 ฉันทามติดีลีเกตปรู๊ฟออฟสเตค (DPOS Concensus Protocol)

ฉันทามติดีลีเกตปรู๊ฟออฟสเตค[14] (DPOS หรือ Delegated-Proof-of-Stake) เป็นฉันทามติที่มีค่า แทรนแซคชั่นต่อวินาที สูง โดยมีตัวอย่างบล็อกเชนสาธารณะที่นำฉันทามตินี้มาใช้ ชื่อว่า อีออส[15] (EOSIO)

ฉันทามติดีลีเกตปรู๊ฟออฟสเตค ถูกพัฒนาขึ้นมาจากฉันทามติปรู๊ฟออฟสเตค (POS หรือ Proof-of-Stake) โดย ฉันทามปรู๊ฟออฟสเตค เป็นมาตรการการยืนยันข้อมูลที่ตกลงกันที่นำเสนอแนวคิดในการยืนยันข้อมูลเพื่อประหยัดพลังงานในการประมวลผลของคอมพิวเตอร์มากกว่าฉันทามติปรู๊ฟออฟเวิร์ค กล่าวคือ ปรู๊ฟออฟสเตค ไม่ได้ใช้พลังงานซีพียูและจีพียูจากผู้ขุดในการยืนยันข้อมูล

---

[13] อ้างอิงจาก https://bitcoin.org/bitcoin.pdf

[14] อ้างอิงจาก https://academy.binance.com/blockchain/delegated-proof-of-stake-explained

[15] อ้างอิงจาก https://eos.io/

หากแต่เรียกชื่อใหม่โดย จากเดิมผู้ขุดใน ฉันทามติปรู๊ฟออฟเวิร์ค เป็นผู้ยืนยันข้อมูล (Validator) โดยการยืนยันถือเอาผู้ที่ถือเหรียญแบ่งเป็นเปอร์เซ็นต์ในการยืนยัน เช่น นาย A ถือเหรียญ 50% ของระบบ นาย B ถือเหรียญ 30% ของระบบ นาย C ถือเหรียญ 20% ของระบบ โอกาสที่จะยืนยันข้อมูลที่จะบรรจุลงในบล็อก ของ นาย A นาย B และ นาย C จะเป็น 50%, 30% และ 20% ตามลำดับ จะเห็นได้ว่าไม่ได้เกิดการแข่งกันยืนยันข้อมูลโดยใช้พลังงานของซีพียูและจีพียูแต่อย่างใด หากแต่ใช้โอกาสที่ใครจะได้เป็นผู้ยืนยันข้อมูลได้เลย หากผู้ใดที่ถือเหรียญได้น้อย โอกาสที่จะยืนยันข้อมูลได้ก็น้อยตามลงไป ดีลีเกตปรู๊ฟออฟสเตคจึงมาแก้ปัญหาที่จุดนี้คือ คือทำให้โอกาสเป็นของทุกคนเท่า ๆ กัน โดยไม่สนปริมาณเหรียญมากหรือน้อย เพียงแต่ต้องมีเหรียญถือไว้จำนวนหนึ่งตามแต่ที่ระบบกำหนดไว้

เนื่องด้วยวิทยานิพนธ์ของผู้เขียนเห็นควรว่า ในช่วงระยะเวลาเริ่มต้น จะมีความยากเป็นอย่างมากหากใครก็ตามสามารถเป็นผู้ยืนยันแทรนแซคชั่นได้ เนื่องจากวิทยานิพนธ์ฉบับนี้ได้ออกแบบมาให้ผู้ที่ทำหน้าที่ยืนยันแทรนแซคชั่น เป็นผู้ทำหน้าที่อื่นๆ ภายในระบบนิเวศน์ด้วย เพราะฉะนั้น การที่ไม่สามารถระบุผู้ยืนยันแทรนแซคชั่นได้ จะเป็นปัญหาต่อระบบในช่วงแรกเป็นอย่างมาก งานวิทยานิพนธ์นี้จึงไม่ได้เลือกใช้ฉันทามตินี้

### 2.5.3 ฉันทามติปรู๊ฟออฟออธอริทิ (POA Concensus Protocol)

ฉันทามติปรู๊ฟออฟออธอริทิ[16] [5] (POA หรือ Proof-of-Authority) เป็นฉันทามติที่มีค่า แทรนแซคชั่นต่อวินาที สูงเทียบเท่า ฉันทามติดีลีเกตปรู๊ฟออฟสเตค หรือ ฉันทามติปรู๊ฟออฟสเตค โดยมีตัวอย่างบล็อกเชนสาธารณะที่นำฉันทามตินี้มาใช้ ชื่อว่า แบรนด์โปรโตคอล[17] (Band Protocol) และยังถูกนำไปใช้ในบล็อกเชนสาธารณะสำหรับทดสอบของอีเธอเรี่ยมอีกด้วย[18] (Ethereum Testnet)

ฉันทามติปรู๊ฟออฟออธอริทิ มีลักษณะเฉพาะตัว คือ สามารถกำหนดผู้ยืนยันแทรนแซคชั่นได้เลย จึงไม่ต้องใช้การแข่งกันคำนวณสมการคณิตศาสตร์ใด ๆ

ข้อเสียของ ฉันทามติปรู๊ฟออฟออธอริทิ คือ เป็นฉันทามติที่ค่อนข้างมีความเป็นระบบรวมศูนย์ ซึ่งมักจะนิยมใช้ในบล็อกเชนระบบปิด มากกว่าที่จะใช้ในบล็อกเชนสาธารณะ เพราะฉะนั้นหากจะนำฉันทามตินี้ไปใช้ ควรต้องมีระยะเวลาและกฎเกณฑ์ กำหนด เช่น เมื่อระบบนิเวศน์โดยรวมอยู่ตัวแล้ว จะเปลี่ยนฉันทามติเป็นแบบอื่น เป็นต้น

---

[16] อ้างอิงจาก https://academy.binance.com/blockchain/proof-of-authority-explained

[17] อ้างอิงจาก https://medium.com/bandprotocol/bandchain-phase-1-proof-of-authority-mainnet-launch-b38a354abcc

[18] อ้างอิงจาก https://github.com/ethereum/grid/issues/201

สำหรับงานวิทยานิพนธ์นี้ ต้องการความแน่นอนของผู้ยืนยันแทรนแซคชั่น อีกทั้งผู้ยืนยันยังทำหน้าที่อื่น ๆ ในระบบนิเวศน์อีกด้วย เนื่องจากเป็นระบบนิเวศน์ที่สร้างขึ้นใหม่ทั้งหมด เพื่อให้ระบบนิเวศน์อยู่ตัว ผู้วิจัยจึงได้เลือกใช้ฉันทามติปรู๊ฟออฟออธอริทิสำหรับการนำเสนอระบบที่พัฒนาขึ้นในวิทยานิพนธ์ฉบับนี้

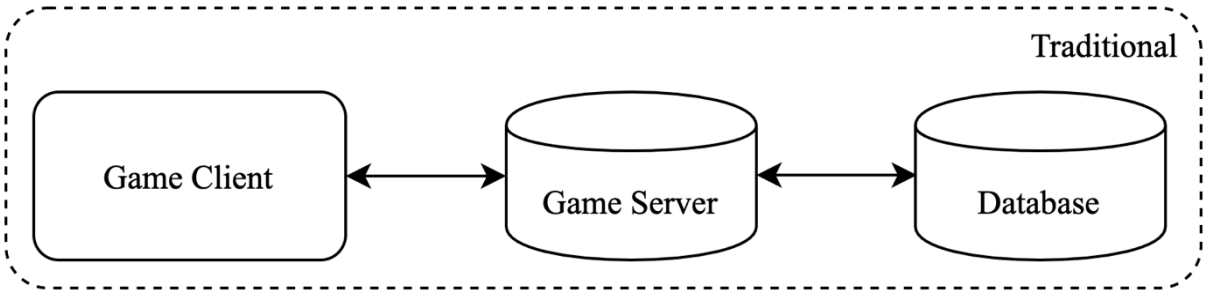
## 2.6 สกุลเงินแบบเข้ารหัส (ERC-20)

สกุลเงินแบบเข้ารหัส[19] เป็นสินทรัพย์ดิจิทัลรูปแบบหนึ่งที่ถูกแฮชข้อมูลไว้ โดยปกติแล้วเป็นที่นิยมในการใช้การระดมทุนที่เรียกว่า ไอซีโอ (ICO หรือ Intitial Coin Offering) โดยการขายโทเคนเพื่อนำเงินที่ได้ไปใช้ในการลงทุนทำกิจกรรมต่างๆ ลักษณะคล้ายกับการระดมทุนในตลาดหลักทรัพย์โดยการเสนอขายหุ้นบริษัทสู่สาธารณะที่เรียกว่า ไอพีโอ (IPO หรือ Intitial Public Offering) ความแตกต่างกันก็คือ ไอพีโอ ได้ใบหุ้นและเป็นผู้ถือหุ้นภายในบริษัท แต่ ไอซีโอ ได้เป็นสกุลเงินแบบเข้ารหัส โดยอาจจะได้รับหุ้นบริษัท หรือ ไม่ได้รับ ก็เป็นไปได้ ไม่ได้มีความเกี่ยวข้องกัน แต่ในที่นี้ผู้วิจัยนำมาอธิบายในส่วนของรางวัล (Reward) ที่ให้กับผู้ที่เล่นเกม และผู้พัฒนาเกม โดยค่าประสบการณ์ของผู้เล่นเกม หรือ มูลค่าเวลาที่เกิดจากการเล่นเกมจะถูกคำนวนและให้แก่ผู้เล่นเป็นสกุลเงินแบบเข้ารหัส ในส่วนของผู้พัฒนาเกม จะได้รับสกุลเงินแบบเข้ารหัสก็ต่อเมื่อมีผู้เล่นเกมนำ สกุลเงินแบบเข้ารหัส มาแลกเปลี่ยนกับไอเทมภายในเกม

มาตรฐาน ERC-20 นั้นถูกนำเสนอเป็นมาตรฐานที่ใช้กันสำหรับสกุลเงินดิจิทัลแบบใช้แล้วทิ้ง (Fungible Token) ซึ่งเปรียบได้เหมือนทรัพยากรธรรมชาติ ที่ใช้แล้วหมดไป เช่นน้ำมัน แก๊สธรรมชาติ เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

## 2.7 รูปแบบสถาปัตยกรรมเกมและการเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่ายในปัจจุบัน

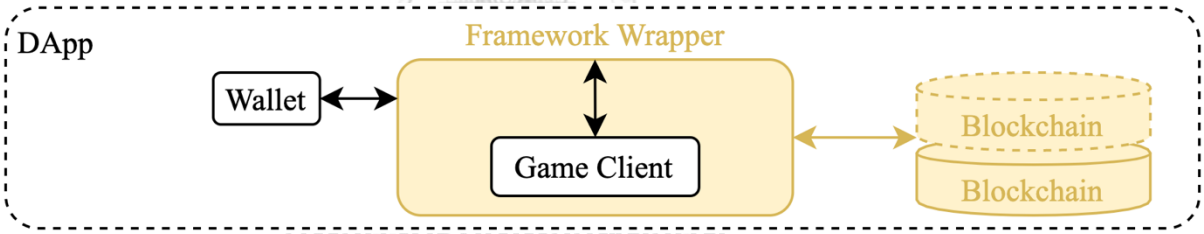



รูปที่ 7 แสดงสถาปัตยกรรมเกมในปัจจุบัน

[19] อ้างอิงจาก https://eips.ethereum.org/EIPS/eip-20

รูปแบบสถาปัตยกรรมเกมแบบดั้งเดิม (แสดงในรูปที่ 7) นั้น เกมไคลเอนต์ (Game client) จะทำหน้าที่ติดต่อกับผู้เล่นเกม หากแต่ข้อมูลเกือบทุกอย่างจะถูกเก็บอยู่ที่เกมเซิร์ฟเวอร์ (Game server) และ/หรือ ฐานข้อมูล (Database) ของผู้ผลิตเกมนั้น ๆ ซึ่งเป็นรูปแบบสถาปัตยกรรมที่ใช้โดยทั่วไปอย่างแพร่หลาย ไม่ว่าจะเป็นเกมคอนโซล (Game console) อาทิเช่น เพลย์สเตชั่น[20] (PlayStation) เอ็กซ์บ็อกซ์[21] (Xbox) หรือนินเทนโด้[22] (Nintendo) แต่ถ้าเป็นเกมออนไลน์ที่ไม่ได้ถูกผูกติดกับเกมคอนโซล ไม่ว่าจะเป็นเว็บบราวเซอร์ (Web Browser) หรือ เกมบนมือถือ ผู้พัฒนาเกมจะเป็นคนรักษาข้อมูลของผู้เล่น[23] หรือในอีกมุมหนึ่งคือ จะต้องเป็นคนจัดการและดูแลเกมเซิร์ฟเวอร์ของตนเองและฐานข้อมูลไปพร้อม ๆ กัน ซึ่งสถาปัตยกรรมในรูปแบบนี้ ผู้เล่นจำเป็นต้องเชื่อใจผู้ผลิตเกมเป็นอย่างมาก เพราะอำนาจในการจัดการข้อมูลอยู่ในมือผู้ผลิตทั้งหมด นอกจากจะทำหน้าที่รักษาข้อมูลของเกมแล้ว ผู้ผลิตยังมีอำนาจในการแก้ไขข้อมูลของผู้เล่น หากผู้ผลิตเกมถูกปิดตัวไปหรือถูกโจรกรรมข้อมูล จะทำให้ข้อมูลทุกอย่างของผู้เล่นถูกแก้ไขหรือหายไปได้

## 2.8 รูปแบบสถาปัตยกรรมแบบกระจายศูนย์ (Decentralized Application - DApp)




รูปที่ 8 แสดงสถาปัตยกรรมเกมแบบกระจายศูนย์

รูปแบบสถาปัตยกรรมแบบกระจายศูนย์[24] [4] (แสดงในรูปที่ 8) นี้ ผู้เล่นต้องเป็นผู้ถือกุญแจส่วนบุคคล (Private Key) เอง และใช้กุญแจส่วนบุคคลของตัวเองในการเซ็นแทรนแซคชั่น (Sign Transaction) เพื่อส่งข้อมูลไปเก็บไว้บนบล็อกเชน โดยกระทำผ่านกระเป๋าเงินดิจิทัล (Wallet)

[20] อ้างอิงจาก https://en.wikipedia.org/wiki/PlayStation_Network

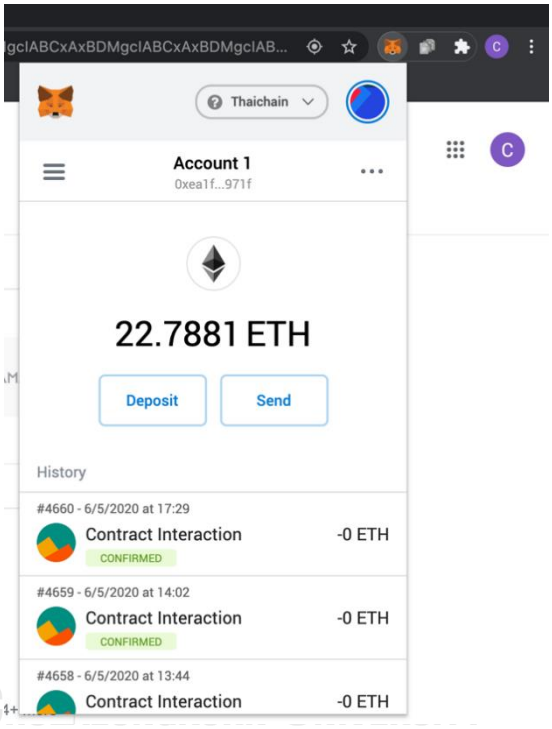
[21] อ้างอิงจาก https://en.wikipedia.org/wiki/Xbox_Live

[22] อ้างอิงจาก https://en.wikipedia.org/wiki/Nintendo_Network

[23] อ้างอิงจาก https://itch.io/games/multiplayer-server

[24] อ้างอิงจาก https://en.wikipedia.org/wiki/Decentralized_application

เกมคริปโตคิตตี้ (รายละเอียดของเกมอยู่ในบทที่ 3) ใช้สถาปัตยกรรมแบบสถาปัตยกรรมแบบกระจายศูนย์ โดยพัฒนาเกมบนเว็บบราวเซอร์ ซึ่งไม่มีความจำเป็นที่จะต้องมีเกมไคลเอนต์อยู่ที่ใด ๆ เลย เนื่องจากตัวละครภายในเกมคริปโตคิตตี้นั้นเป็นเพียงแค่ฟังก์ชันแฮช (Hash Function) ที่เกิดขึ้นจากการเซ็นแทรนแซคชั่นบนสมาร์ทคอนแทรคแล้วนำมาสร้างเป็นภาพภายในเว็บไซต์ โดยไม่ได้มีโลจิกอื่นใดภายในเกมที่สำคัญ เช่น ระบบฟิสิกส์ภายในเกม ระบบการตรวจสอบการชน เป็นต้น อย่างไรก็ดี เกมคริปโตคิตตี้นั้น หากผู้เล่นจะทำการเล่นเกม จำเป็นจะต้องมีกระเป๋าดิจิทัลที่ติดตั้งบนเว็บบราวเซอร์ โดยเกมคริปโตคิตตี้นั้นใช้กระเป๋าดิจิทัลเมต้ามาสค์ (Metamask) ซึ่งแสดงในรูปที่ 9




รูปที่ 9 ตัวอย่างกระเป๋าเงินสาธารณะของเมต้ามาร์คที่ติดตั้งบนเว็บบราวเซอร์โครม

เกมอย่างคริปโตคิตตี้นั้นสามารถถูกมองเป็นโครงสร้างเกมไคลเอนต์ที่รันอยู่บน เว็บบราวเซอร์ โดยใช้เว็บบราวเซอร์เป็นตัวสื่อสารกับองค์ประกอบภายนอกอื่น ๆ ซึ่งจะถือว่าเว็บบราวเซอร์เป็นรูปแบบกรอบอ้างอิง (Framework Wrapper)

รูปแบบกรอบอ้างอิง คือ ส่วนที่ประกอบไปด้วยเกมไคลเอนต์ และการเชื่อมต่อกับบล็อกเชน รวมถึงการส่งคำสั่งไปที่บล็อกเชนโหนด (Blockchain node) หรือนำข้อมูลจากบล็อกเชนโหนดมาแสดงผลในเกมไคลเอนต์ โดยรูปแบบสถาปัตยกรรมแบบนี้กระเป๋าเงินดิจิทัลจะอยู่ภายนอกรูปแบบกรอบอ้างอิง หรือเรียกว่ากระเป๋าเงินบุคคลที่สาม (3rd party wallet)

รูปแบบสถาปัตยกรรมแบบกระจายศูนย์นั้น นอกจากใช้กับเว็บบราวเซอร์แล้ว ก็สามารถใช้กับผู้ผลิตเกมคอนโซล หรือโมบายเกมได้เช่นกัน เพียงแต่ไส้ในของรูปแบบกรอบอ้างอิงก็จะเปลี่ยนไปตามระบบนิเวศน์บล็อกเชน (Blockchain Ecosystem) ของสถาปัตยกรรมนั้น ๆ

ผู้วิจัยไม่ได้เลือกนำสถาปัตยกรรมแบบกระจายศูนย์มาใช้ในงานวิทยานิพนธ์นี้ เนื่องจากเล็งเห็นว่า ผู้เล่นส่วนใหญ่ไม่มีกระเป๋าเงินดิจิทัลของตัวเอง เปรียบได้ว่าผู้เล่นยังไม่ได้มีความเข้าใจเรื่องบล็อกเชนมากพอ หรืออาจจะยังไม่ถึงยุคที่ผู้คนต่างก็มีกระเป๋าเงินดิจิทัลของตัวเองเหมือนอย่างที่ทุกคนมีอีเมล และเข้าใจว่าต้องมีชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) การใช้งานสถาปัตยกรรมนี้จะทำให้ผู้เล่นใช้งานจริงลำบาก ซึ่งหากเปรียบกุญแจส่วนบุคคลเป็นรหัสผ่านในการเข้าใช้งาน หากผู้เล่นทำกุญแจส่วนบุคคลหายหรือลืม ผู้เล่นจะไม่สามารถเข้าสู่กระเป๋าดิจิทัลตัวเองได้อีกตลอดกาล กระเป๋าเงินดิจิทัลนั้นเป็นอนุพันธ์ของกุญแจส่วนบุคคล และเป็นการเข้ารหัสแบบทางเดียว จึงไม่สามารถที่จะกระทำการใด ๆ กับกระเป๋าดิจิทัลได้อีก หากไม่ทราบกุญแจส่วนบุคคล เพราะฉะนั้นการจะเลือกใช้สถาปัตยกรรมแบบกระจายศูนย์ให้ได้ผลเต็มตามประสิทธิภาพนั้น ผู้ใช้งานจำเป็นต้องมีความเข้าใจบล็อกเชนเป็นอย่างดี

งานวิทยานิพนธ์นี้ ผู้วิจัยได้นำเสนอสถาปัตยกรรมใหม่ ที่ช่วยอำนวยความสะดวกกับผู้เล่นที่ยังไม่มีความเข้าใจในบล็อกเชน

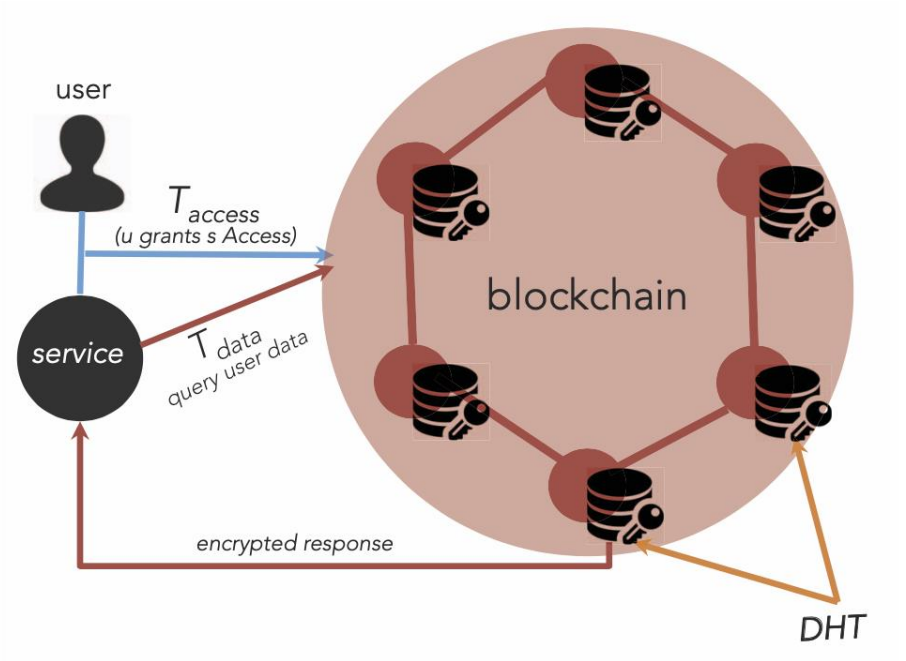
จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# บทที่ 3
# งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องในวิทยานิพนธ์นี้แบ่งออกเป็น 3 กลุ่ม ได้แก่ งานวิจัยเกี่ยวกับการเก็บข้อมูลบนบล็อกเชนและสมาร์ทคอนแทรค (Blockchain Storage and Smart Contract) งานวิจัยเกี่ยวกับเกมบนบล็อกเชน (Blockchain Games) และงานวิจัยเกี่ยวกับสถาปัตยกรรมเกมบนบล็อกเชน (Blockchain Game Infrastructure)

## 3.1 งานวิจัยเกี่ยวกับการเก็บข้อมูลบนบล็อกเชนและสมาร์ทคอนแทรค (Blockchain Storage and Smart Contract))

ในปี 2015 Zyskind และคณะ [6] กล่าวว่าข้อมูลอันเป็นส่วนตัว หรือ แม้แต่ข้อมูลทั่ว ๆ ไป ถูกบุคคลที่ 3 นำไปใช้อย่างโจ่งแจ้ง และบางทีการนำข้อมูลของผู้ใช้ไปใช้ในเชิงพาณิชย์ ก็ไม่ได้มีการขออนุญาตเจ้าของข้อมูลก่อน งานวิจัยฉบับนี้นำเสนอแนวทางในการจัดเก็บข้อมูลลงบนบล็อกเชนเพื่อการป้องกันไม่ให้บุคคลที่สามนำข้อมูลไปใช้ได้




รูปที่ 10 รูปแสดงการเก็บข้อมูลและการเรียกข้อมูล[25]

[25] อ้างอิงจาก Fig 1 ใน 6. Zyskind, G. and O. Nathan. *Decentralizing privacy: Using blockchain to protect personal data*. in *2015 IEEE Security and Privacy Workshops*. 2015. IEEE.

จากรูป 10 งานวิจัยนี้แบ่ง Role ออกเป็น 3 ส่วนคือ ผู้ใช้ (user) ส่วนบริการ (Service) ในที่นี้คือแอปพลิเคชัน ที่นำข้อมูลของผู้ใช้ไปใช้งาน และ โหนด (node) ในที่นี้คือบล็อกเชนโหนด โดยข้อมูลของผู้ใช้จะถูกจัดเก็บอยู่ภายในโหนด และเข้ารหัสด้วยกุญแจส่วนบุคคลของผู้ใช้ และถูกจัดเก็บแบบ DHT [7] คู่กับ LevelDB[26] โหนดนั้นไม่สามารถทราบถึงกุญแจส่วนบุคคลของผู้ใช้ จึงไม่สามารถอ่านข้อมูลที่ถูกเก็บอยู่ภายในบล็อกได้ DHT นั้นอยู่นอกเหนือบล็อกเชน และจะถูกบริหารโดยกลุ่มกรรมการของโหนด ซึ่งอาจจะเป็นอิสระต่อบล็อกเชนโหนดก็ได้ ผู้ใช้ซึ่งมีชุดกุญแจส่วนบุคคลสามารถเรียกดูข้อมูลของตนเองได้ตลอดเวลาผ่านฟังก์ชัน $T_{access}$ และสามารถทำการแก้ไขให้ส่วนบริการนำข้อมูลใดไปใช้งานได้บ้าง ซึ่งส่วนบริการจะนำข้อมูลไปใช้งานต้องเรียกผ่านฟังก์ชัน $T_{data}$ ซึ่งข้อมูลที่ได้รับไปมากน้อยเพียงใด ขึ้นอยู่กับผู้ใช้อนุญาต

ถึงแม้ว่างานวิจัยนี้จะพูดถึงการเก็บข้อมูลใด ๆ ของผู้ใช้ แต่ยังไม่ได้มีการกล่าวถึงการใช้สมาร์ทคอนแทรคในการเก็บข้อมูล รวมทั้งยังไม่ได้กล่าวถึงการนำไปประยุกต์ใช้กับบล็อกเชนสาธารณะ

ในวิทยานิพนธ์ฉบับนี้ ผู้วิจัยได้ทำการจัดการเก็บข้อมูลบนบล็อกเชนด้วยการใช้สมาร์ทคอนแทรค และนำหลักการไปใช้กับบล็อกเชนสาธารณะ

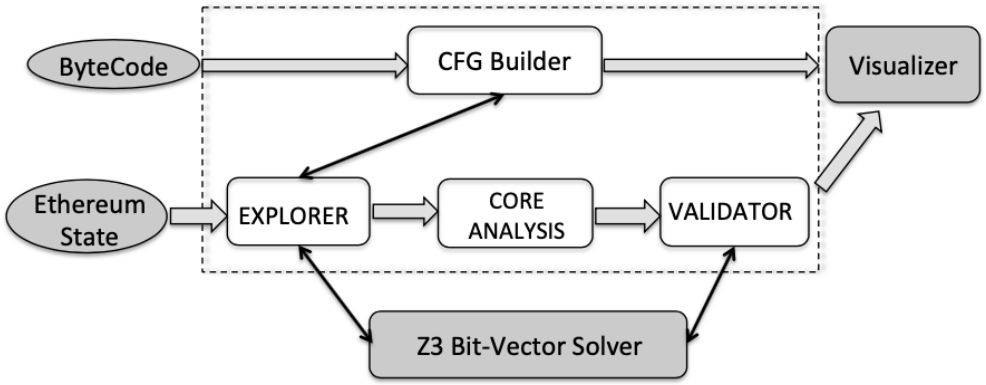
ต่อมา Delmolino และคณะ [8] จัดทำรายงานการเขียนสมาร์ทคอนแทรคด้วยภาษา solidity บนบล็อกเชนสาธารณะ อีเธอเรี่ยม งานวิจัยนี้จะชี้ให้เห็นถึงปัญหาและข้อผิดพลาดในการเขียนสมาร์ทคอนแทรค โดยยกตัวอย่างจากสมาร์ทคอนแทรคจากเกมง่าย ๆ เช่น เกม ค้อน กรรไกร กระดาษ โดยกฎง่าย ๆ คือ เล่นกัน 2 คน โดยก่อนที่จะเล่นนั้น ให้ผู้เล่นฝากอีเธอเรี่ยม เข้าในสมาร์ทคอนแทรค หากใครชนะ จะได้อีเธอเรี่ยมที่ฝากของคนแพ้ไป โดยให้นักศึกษาที่มีความรู้ในการเขียนโปรแกรมลองทำการเขียนสมาร์ทคอนแทรคขึ้นมา ค้นพบว่าแม้แต่เกมง่าย ๆ ก็ยังมีข้อผิดพลาดที่พบเยอะมาก ยกตัวอย่างเช่น การมีผู้เล่นคนที่ 3 ทำการฝากอีเธอเรี่ยม ขณะที่ผู้เล่นคนที่ 1 คนที่ 2 ทำการแข่งขันกันอยู่ อีเธอเรี่ยมที่ฝากไว้ของคนที่ 3 จะไม่สามารถได้คืนได้ ซึ่งปัญหาเหล่านี้จำเป็นต้องมีความเข้าใจในเรื่องระบบการรอคิวของแทรนแซคชั่นเป็นอย่างมาก

งานของ Delmolino และคณะนั้น อธิบายปัญหาที่จะเจอในการเขียนสมาร์ทคอนแทรคได้ดีมากและยังเป็นงานที่เขียนลงบนอีเธอเรี่ยมโดยเฉพาะ ซึ่งผู้วิจัยสามารถนำแนวทางไปปรับประยุกต์ใช้กับงานวิทยานิพนธ์ฉบับนี้ได้

Luu และคณะ [9] ทำงานต่อยอดมาจากงานของ Delmolino และคณะ โดยงานวิจัยฉบับนี้นำเสนอแนวทางการปรับปรุงสมาร์ทคอนแทรคให้มีประสิทธิภาพมากขึ้นโดยกล่าวถึงปัญหาที่เกิดขึ้น

[26] อ้างอิงจาก https://github.com/google/leveldb

ในอีเธอเรี่ยมด้านความปลอดภัยของข้อมูล และข้อบกพร่องบางอย่าง (Bug) ที่ทำให้เกิดปัญหาได้ในการเขียนสมาร์ทคอนแทรคแบบปกติ




รูปที่ 11 รูปแบบสถาปัตยกรรม หรือ Workflow การทำงาน (Framework) ของ Oyante[27]

จากรูป 11 ผู้เขียนได้นำเสนอเครื่องมือที่ชื่อว่า Oyente เพื่อใช้ในการตรวจสอบปัญหาที่จะเกิดขึ้นในการเขียนสมาร์ทคอนแทรค และใช้ตรวจสอบกับสมาร์คอนแทรคจริง ๆ จำนวน 19,633 คอนแทรคในช่วง 1,460,000 บล็อกแรกของอีเธอเรี่ยมหลัก (Ethereum Mainnet) และพบว่ามีช่องโหว่ที่มีโอกาสทำให้ข้อมูลในสมาร์ทคอนแทรคเสียหาย หรือ เกิดการโจรกรรมในสามาร์ทคอนแทรค จำนวน 8,833 คอนแทรค โดยยกตัวอย่างเหตุการณ์จริงที่เกิดขึ้นแล้วในปัจจุบัน เช่น คริปโตเคอเรนซี่เดอะเดา (The DAO)[28] ที่เกิดการโจรกรรมขึ้นในสมาร์ทคอนแทรค มูลค่าความเสียหาย[29] ในขณะนั้นประมาณ 50 ล้านเหรียญสหรัฐ

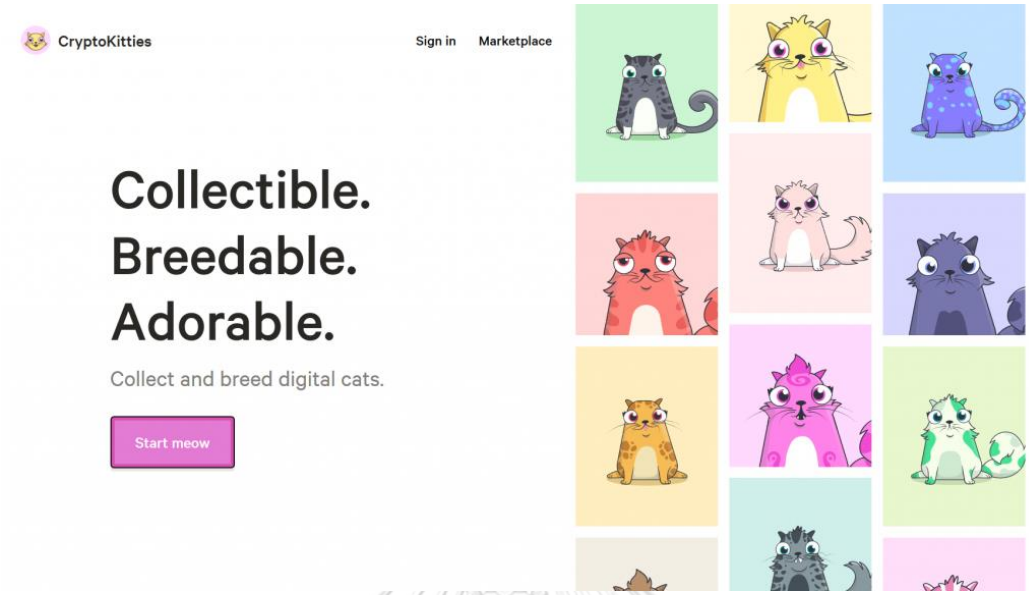
แม้ว่าในวิทยานิพนธ์ฉบับนี้จะไม่ได้นำ Oyente มาใช้เพื่อทดสอบสมาร์ทคอนแทรค แต่งานวิจัยนี้ได้ยกตัวอย่างถึงหลายกรณีศึกษา ที่แสดงให้เห็นถึงเหตุการณ์จริง ถึงความไม่ปลอดภัยของการเขียนสมาร์ทคอนแทรคที่ไม่ระมัดระวัง ซึ่งทำให้ผู้วิจัยสามารถนำไปปรับใช้ในการเขียนสมาร์ทคอนแทรคที่ป้องกันการสูญเสียดังกล่าวได้

[27] อ้างอิงจาก Fig 11 ใน 9. Luu, L., et al. *Making smart contracts smarter*. in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.

[28] อ้างอิงจาก https://en.wikipedia.org/wiki/The_DAO_(organization)

[29] อ้างอิงจาก https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

### 3.2 งานวิจัยเกี่ยวกับเกมบนบล็อกเชน (Blockchain Games)




รูปที่ 12 ภาพของเกมคริปโตคิตตี้ จาก cryptokitties.co

จากรูป 12 เกมคริปโตคิตตี้[30] (Cryptokitties) ถูกพัฒนาจากบริษัท AxiomZen ซึ่งเป็นบริษัทพัฒนาซอฟต์แวร์สัญชาติแคนาดาที่มุ่งพัฒนาด้าน VR, AR และบล็อกเชน เกมนี้เป็นเกมเพาะพันธุ์แมวแบบเสมือนจริงออกมาขาย โดยใช้อีเธอเรี่ยมในการซื้อขายแมว การเริ่มเล่นผู้เล่นต้องใช้อีเธอเรี่ยมเพื่อทำการซื้อแมวก่อน โดยแมวจะถูกแบ่งออกเป็นรุ่น (Generation) โดยเริ่มต้นที่รุ่นที่ 0 หากถูกผสมพันธุ์กัน จะมีลูกเป็นรุ่นที่ 1 เป็นอย่างนี้ต่อไปเรื่อย ๆ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

```
struct Kitty {
    uint256 genes;
    uint64 birthTime;
    uint64 cooldownEndBlock;
    uint32 matronId;
    uint32 sireId;
    uint32 siringWithId;
    uint16 cooldownIndex;
    uint16 generation;
}
```

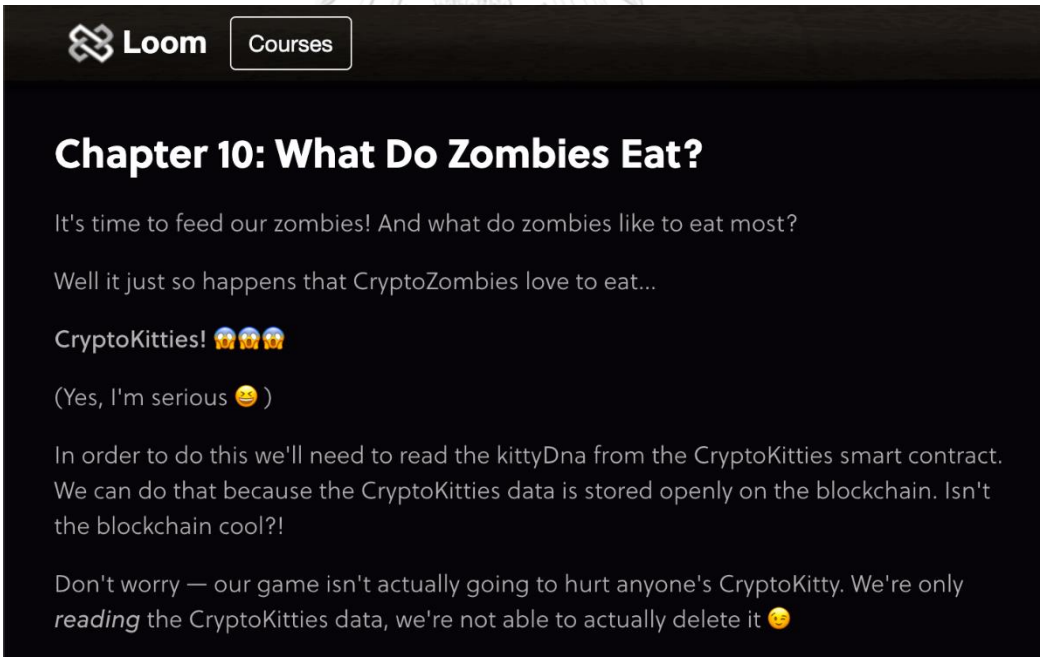
รูปที่ 13 ภาพโครงสร้างของแมวจากเกมคริปโตคิตตี้

[30] อ้างอิงจาก http://www.cryptokitties.co/

จากรูปที่ 13 แสดงโครงสร้างทั้งหมดของแมวหนึ่งตัวซึ่งเป็นเพียงตัวเลขชุดหนึ่ง เพราะฉะนั้น แมวที่ได้จากการซื้อ ขาย และผสมพันธุ์ภายในเกม จะถูกบรรจุลงในบล็อกของอีเธอเรี่ยม โดยผู้ที่ยืนยันข้อมูลการซื้อ ขาย และผสมพันธุ์จะได้ค่าธรรมเนียมในการยืนยันเป็นสกุลเงิน อีเธอเรี่ยม และผู้ที่เป็นเจ้าของแมวก็สามารถตรวจสอบแมวของตนเองผ่านทางบล็อกเชนได้เช่นกัน

สิ่งที่น่าสนใจของเกมนี้คือ การที่ผู้ใช้งานสามารถเล่นกับการผสมพันธุ์ ทำให้ได้แมวหายากออกมาหลายรูปแบบ เช่นเดียวกับการเล่นเกมหรือการเล่นของสะสม อย่างไรก็ตาม โดยสรุปแล้วการได้มาซึ่งแมวนั้นแท้จริงเป็นเพียงการโอนค่าข้อมูลชุดหนึ่งไปมาระหว่างกันเท่านั้น จะเห็นได้ว่าเป็นการประยุกต์การโอนสกุลเงินดิจิทัลและการเขียนสมาร์ทคอนแทรคได้อย่างชาญฉลาด หากแต่ก็เป็นเพียงการใช้งานอยู่ภายในตัวมันเอง ไม่ได้มีการนำแมวไปใช้ต่อในเกมหรือแอปพลิเคชันอื่น

การใช้ต่อในที่นี้หมายถึงการดัดแปลง ปรับปรุง แก้ไขตัวแมวที่เกิดจากเกม แต่เนื่องจากตัวแมวนั้นอยู่บนบล็อกเชนสาธารณะ ทุกคนจึงสามารถอ่านได้เท่านั้น (Read-Only) หมายความว่าใครก็ตามสามารถอ่านค่าแฮชของแมวนั้นได้ก็สามารถเอาแมวไปทำอะไรต่อไปภายในเกมของตนเองได้ โดยไม่มีผลกระทบต่อตัวแมวต้นฉบับ

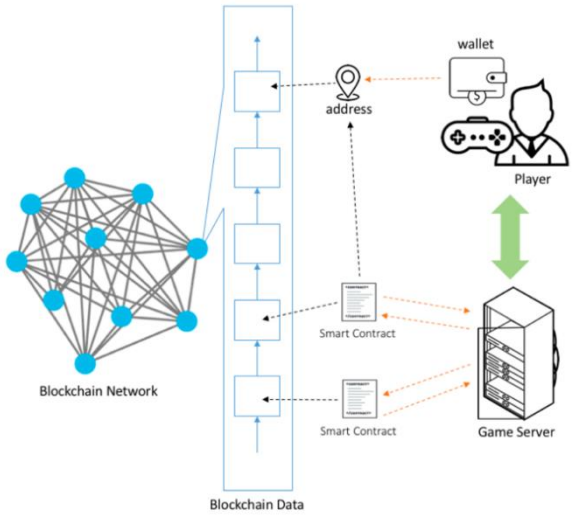



รูปที่ 14 ภาพบทเรียนจากเกมคริปโตซอมบี้[31] (Cryptozombies)

[31] อ้างอิงจาก https://cryptozombies.io/

จากรูปที่ 14 เกมคริปโตซอมบี้ เป็นเกมที่ทำขึ้นมาเพื่อสอนให้ผู้เล่นสามารถเขียนสมาร์ทคอนแทรค บนบล็อกเชนอีเธอเรี่ยม โดยผ่านการสร้างซอมบี้ และในบทเรียนหนึ่งเป็นการแสดงให้เห็นว่ามีการนำแมวจากเกมคริปโตคิตตี้มาทานเป็นอาหารของซอมบี้

จากเกมคริปโตคิตตี้ที่กล่าวถึง ในปัจจุบันได้มีเกมบนบล็อกเชนสาธารณะเกิดขึ้นเป็นจำนวนมาก ในปี 2019 Min และคณะ [10] ได้ทำการสำรวจเกมที่เป็นที่นิยมบนบล็อกเชนสาธารณะหลายเกม ซึ่งอยู่บนบล็อกเชนสาธารณะที่แตกต่างกัน




รูปที่ 15 รูปสถาปัตยกรรมเกมบนบล็อกเชนตามงานวิจัย[32]

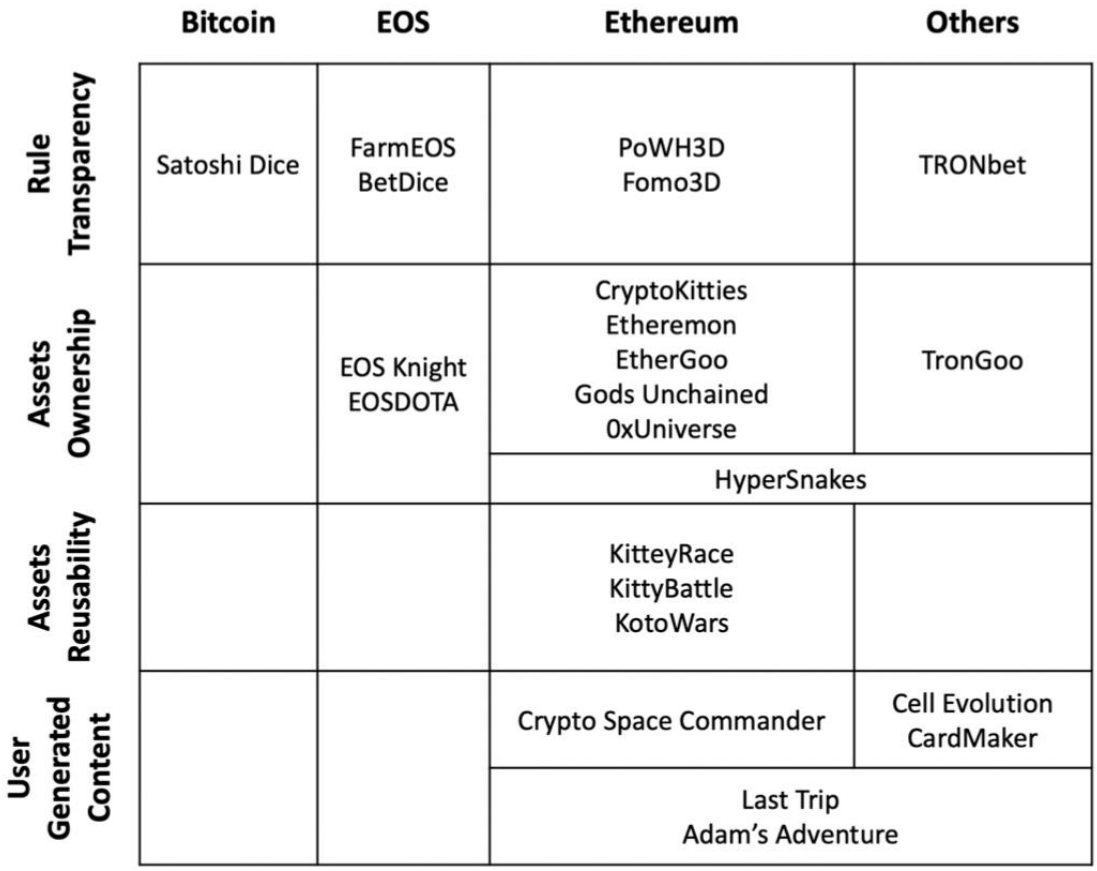
จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ในงานวิจัยฉบับนี้ สถาปัตยกรรมของเกมที่ใช้บล็อกเชนโดยส่วนใหญ่จำเป็นต้องมีเครื่องคอมพิวเตอร์แม่ข่าย (Game Server) ซึ่งอยู่นอกเหนือส่วนของบล็อกเชน และไม่มีใครสามารถตรวจสอบการคำนวณภายในเกมไคลเอนต์ที่อยู่บนเครื่องคอมพิวเตอร์แม่ข่าย หรือข้อมูลภายในเครื่องคอมพิวเตอร์แม่ นอกจากผู้พัฒนาเกมเอง จุดนี้จึงเป็นจุดอ่อนของเกมบนบล็อกเชนในลักษณะนี้ ที่จำเป็นต้องมี เครื่องคอมพิวเตอร์แม่ข่ายเพื่อให้เกมทำงานได้โดยสมบูรณ์

ในวิทยานิพนธ์ฉบับนี้ ผู้วิจัยได้แสดงให้เห็นถึงการนำคอมพิวเตอร์แม่ข่าย มาใช้เพียงเพื่อเป็นการยืนยันตัวตนของผู้เล่น และเก็บชุดกุญแจสาธารณะกับกระเป๋าเงินดิจิทัลสาธารณะ เพียงเท่านั้น ไม่ได้มีการเก็บตัวเกมไคลเอนต์ ซึ่งตัวเกมไคลเอนต์นั้น ถูกเก็บอยู่ที่ฝั่งผู้เล่นขึ้นกับแพลตฟอร์มที่นำไป

[32] อ้างอิงจาก Fig. 1 ใน 10. Min, T., et al. *Blockchain games: A survey*. in *2019 IEEE Conference on Games (CoG)*. 2019. IEEE.

พัฒนา ซึ่งเมื่อถึงเวลาที่บล็อกเชนถูกยอมรับและใช้กันอย่างเป็นที่แพร่หลาย สามารถถอดเอาเครื่องคอมพิวเตอร์แม่ข่ายออก เกมก็ยังสามารถเล่นได้ปกติ




จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

รูปที่ 16 การจำแนกประเภทของเกมตามงานวิจัย[33]

ในงานวิจัยฉบับนี้ยังได้แบ่งเกมโดยใช้เมทริกซ์ เพื่อจัดกลุ่มว่าเกมแต่ละประเภทมีอัตลักษณ์ของตัวเกมเป็นอย่างไร จากรูปที่ 16 แกนแนวตั้งแบ่งเป็น (1) ความโปร่งใสของกฎที่ตรวจสอบได้ (Rule Transpareny) (2) ความเป็นเจ้าของสินทรัพย์ภายในเกม (Asset Ownership) (3) การนำสินทรัพย์ภายในเกมมาใช้ซ้ำ (Assets Reusability) และ (4) การสร้างสิ่งของภายในเกมโดยผู้เล่นเอง (User Generated Content) ในส่วนของแกนแนวนอนเป็นชื่อของบล็อกเชนสาธารณะ

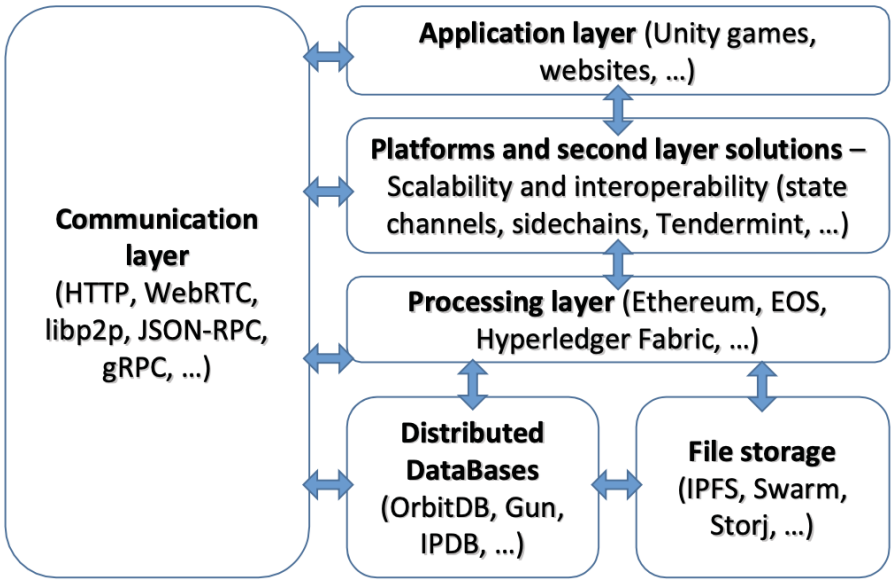
[33] อ้างอิงจาก Fig. 2 ใน 10. Min, T., et al. *Blockchain games: A survey*. in *2019 IEEE Conference on Games (CoG)*. 2019. IEEE.

แม้งานวิจัยฉบับนี้ได้กล่าวถึงลักษณะของเกมแต่ละประเภท แต่ไม่ได้นำเสนอการนำไปประยุกต์ใช้กับการพัฒนาเกมในรูปแบบเดิม และยังไม่ได้กล่าวถึงการนำมูลค่าใด ๆ ที่เกิดจากการเล่นเกมไปใช้ในเกมอื่น ๆ ภายในบล็อกเชนสาธารณะเดียวกัน

ในงานวิทยานิพนธ์นี้ ผู้วิจัยมีจุดมุ่งหมายที่จะนำเสนอรูปแบบสถาปัตยกรรมเกมที่สามารถนำมูลค่าในการเล่นเกมไปใช้ในเกมอื่นที่ผู้อ่านสามารถนำไปพัฒนากับบล็อกเชนสาธารณะที่มีอยู่ในปัจจุบัน รวมถึงพัฒนาร่วมกับเกมในรูปแบบเดิมที่ไม่ได้มีการใช้บล็อกเชนได้

### 3.3 งานวิจัยเกี่ยวกับสถาปัตยกรรมเกมบนบล็อกเชน (Blockchain Game Infrastructure)

บล็อกเชนสาธารณะได้มีการใช้อย่างแพร่หลาย และมีความพยายามที่จะพัฒนาการเก็บข้อมูลแบบกระจายศูนย์ ในปี 2019 Besancon และคณะ [11] ได้นำเสนอรูปแบบสถาปัตยกรรมเกมบนบล็อกเชน โดยมุ่งเน้นไปที่การจัดเก็บข้อมูลของเกมและตัวเกมไคลเอนต์ในแบบการกระจายศูนย์ กล่าวคือ ไม่มีข้อมูลใดๆ ที่สามารถเป็นจุดเสียหายแบบเบ็ดเสร็จ (Single point of failure) โดยใช้การจัดเก็บข้อมูลแบบกระจายศูนย์ที่เรียกว่า IPFS[34]



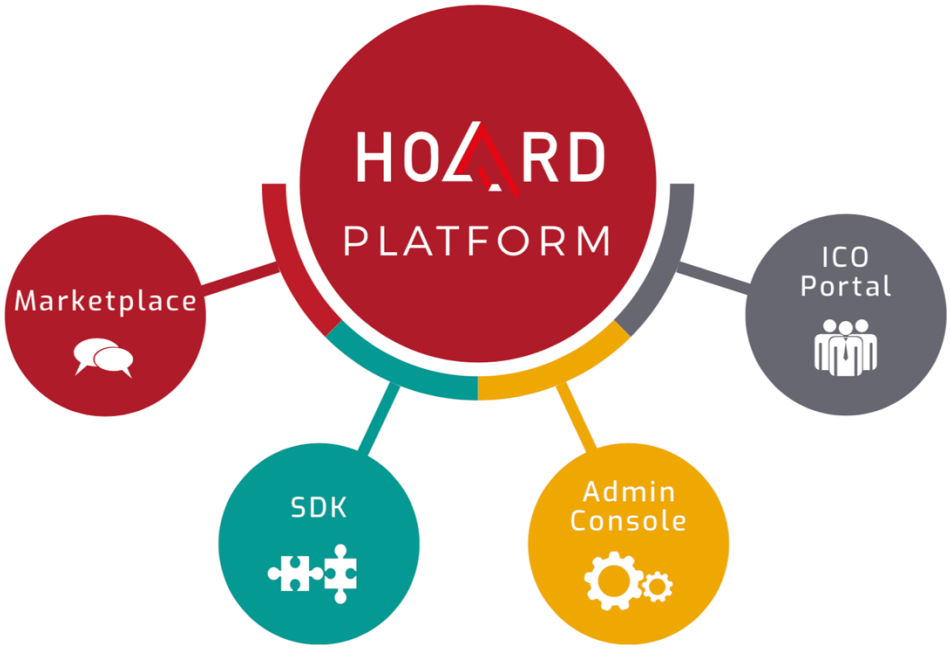

รูปที่ 17 รูปสถาปัตยกรรมเกมบนบล็อกเชนตามงานวิจัย[35]

[34] อ้างอิงจาก https://en.wikipedia.org/wiki/InterPlanetary_File_System

[35] อ้างอิงจาก Fig. 1 ใน 11. Besançon, L., C.F. Da Silva, and P. Ghodous. *Towards Blockchain Interoperability: Improving Video Games Data Exchange*. in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2019. IEEE.

งานวิจัยของ Besancon และคณะ ฉบับนี้ ไม่ได้มีการกล่าวถึงการส่งผ่านข้อมูลจากเกมหนึ่งไปสู่อีกเกมหนึ่ง และยังไม่ได้กล่าวถึงการประยุกต์เพื่อพัฒนาอย่างเต็มรูปแบบ อีกทั้งยังไม่มีการกล่าวถึงบทบาทหรือส่วนประกอบภายในบล็อกเชนที่จำเป็นจะต้องใช้ในการอธิบายสถาปัตยกรรมแบบเจาะลึก

อย่างไรก็ตามในงานวิทยานิพนธ์นี้ ผู้วิจัยไม่ได้มุ่งเน้นการจัดเก็บฐานข้อมูลแบบกระจายศูนย์ ผู้วิจัยได้นำเสนอสถาปัตยกรรมแบบที่สามารถประยุกต์ใช้ทั้งกับการพัฒนาเกมในรูปแบบเดิมและรูปแบบบล็อกเชน โดยผู้วิจัยมุ่งเน้นไปที่การระบุบทบาทและหน้าที่เพื่อให้ง่ายต่อการกำกับควบคุมระบบนิเวศน์บล็อกเชนที่เกี่ยวข้อง อาทิเช่น ผู้เล่น นักพัฒนาเกม และบล็อกเชนโหนด




รูปที่ 18 ภาพแสดงฮอร์ดแพลตฟอร์มจาก Hoard.exchange

ฮอร์ดแพลตฟอร์ม[36] ถูกสร้างขึ้นมาเพื่อ 3 จุดประสงค์หลัก คือ

(1) ทำให้ของภายในเกมทุกอย่างเป็นของที่ผู้เล่นเป็นเจ้าของอย่างแท้จริง โดยจัดเก็บอยู่บนเทคโนโลยีบล็อกเชน ซึ่งเจ้าของสามารถซื้อขายแลกเปลี่ยนได้อย่างอิสระ

(2) ทำให้ผู้พัฒนาเกมทั่วไปสามารถระดมทุนผ่านแพลตฟอร์ม และผู้ที่ให้การสนับสนุนสามารถนำสกุลเงินเข้ารหัสไปใช้ในเกมที่ตนเองสนับสนุนได้

[36] อ้างอิงจาก https://hoard.exchange/

(3) ทำให้บุคคลทั่วไปสามารถนำสินค้าและบริการทั่วไปมาเข้ารหัสเหรียญข้อมูล (Tokenized) และทำการซื้อขายแลกเปลี่ยนได้ จุดประสงค์นี้เกิดเนื่องมาจากการว่างงานทางเทคโนโลยี (Technological Unemployment) กล่าวในอีกมุมหนึ่งคือเทคโนโลยีทำให้การซื้อขายแลกเปลี่ยนแบบเดิมที่มีหน้าร้านมีความนิยมน้อยลงไป

จากรูป 18 แสดงให้เห็นถึงการนำฮอร์ดแพลตฟอร์มไปใช้งาน ดังนี้ โดย

(1) **Marketplace** เป็นการใช้งานที่เกิดจากผู้ใช้งานนำสิ่งของภายในเกมมาซื้อขายแลกเปลี่ยนกัน

(2) **SDK** เป็นการใช้งานที่ผู้พัฒนาเกมนำ SDK ไปใส่ภายในตัวเกมที่ตนเองพัฒนาขึ้น

(3) **Admin Console** เป็นการใช้งานที่เกิดจากผู้พัฒนาเกมเข้ามาปรับปรุงแก้ไขค่าต่าง ๆ ภายในเกมของตัวเอง

(4) **ICO Portal** เป็นการใช้งานที่เกิดจากผู้พัฒนาเกมระดมทุนผ่านแพลตฟอร์ม

จุดประสงค์ของฮอร์ดมีความใกล้เคียงกับแนวทางที่ผู้วิจัยนำเสนอในวิทยานิพนธ์นี้ หากแต่มีประเด็นที่แตกต่างกันอยู่พอสมควร เช่น ในฮอร์ดแพลตฟอร์ม มีการนำไอเทมทุกอย่างภายในเกมมาเข้ารหัสเหรียญข้อมูลแบบใช้แล้วไม่หมดไป (ERC-721) และให้ผู้เล่นสามารถทำการแลกเปลี่ยนได้เพื่อนำสิ่งของไปใช้ แต่ผู้วิจัยนำเสนอในแนวทางที่ให้รางวัลแก่ผู้เล่นตามเวลาที่เกิดขึ้นเป็นเหรียญสกุลเงินแบบเข้ารหัสแบบใช้แล้วหมดไป ส่วนหนึ่งเพื่อให้สินทรัพย์ที่เกิดขึ้นภายในเกม ไม่เกิดการเฟ้อโดยทางอ้อม แต่ในส่วนของฮอร์ดเองไม่ได้มีการวางกลไกลการป้องกันไอเทมเฟ้อเอาไว้

ฮอร์ดแพลตฟอร์มเป็นผู้ควบคุมระบบนิเวศน์ด้วยตนเองโดยใช้เทคโนโลยีพลาสมาชั้นที่สอง (Plasma Blockchain Layer 2) หรือบล็อกเชนข้างเคียง (Sidechain) ซึ่งทำให้ต้องขึ้นกับอีเธอเรี่ยมชั้นที่ 1 (Ethereum Mainnet Layer 1)

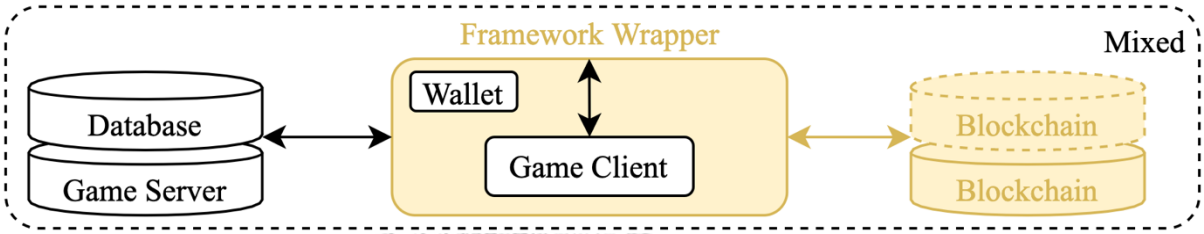
ในงานวิทยานิพนธ์นี้ ผู้วิจัยเห็นว่าการใช้เทคโนโลยีบล็อกเชนชั้นที่สองจะทำให้ผู้ที่นำระบบไปใช้งานต้องผูกติดกับบล็อกเชนสาธารณะใดสาธารณะหนึ่งเพียงเท่านั้น ทั้งยังต้องผูกติดกับเกมเอนจิ้นเนื่องจากฮอร์ดมี SDK มาให้นักพัฒนาใช้โดยอ้างอิงกับเครื่องมือที่ใช้ในการสร้างเกมโดยเฉพาะเช่น ยูนิตี้ทรีดี เป็นต้น ในทางกลับกัน ผู้วิจัยไม่ได้มุ่งเน้นไปที่เกมเอนจิ้นใดเกมเอนจิ้นหนึ่ง ทั้งนักพัฒนายังไม่จำเป็นต้องนำส่วนการเชื่อมต่อบล็อกเชนไปใส่ไว้ข้างในตัวเกม เนื่องจากผู้วิจัยนำส่วนที่ติดต่อกับบล็อกเชนไปไว้ในส่วนที่เรียกว่าระบบกรอบอ้างอิงแล้ว ซึ่งจะกล่าวต่อไปในบทที่ 4

อย่างไรก็ตาม แม้ฮอร์ดแพลตฟอร์มเองจะน่าสนใจเป็นอย่างยิ่ง แต่ก็ยังอยู่ในขั้นตอนการระดมทุน และยังไม่ได้เปิดให้ใช้จริง แนวทางดังกล่าวจึงยังคงเป็นเพียงแนวคิดที่ทางฮอร์ดแพลตฟอร์มนำเสนอสู่สาธารณชนเท่านั้น

# บทที่ 4
# แนวคิดและวิธีการดำเนินงาน

ในบทนี้เป็นการอธิบายแนวคิดของระบบทั้งหมดที่ผู้อ่านสามารถนำไปปรับใช้กับรูปแบบการพัฒนาภายในระบบนิเวศน์บล็อกเชน (Blockchain Ecosystem) ของตนเองได้

## 4.1 รูปแบบสถาปัตยกรรมแบบผสมผสาน (Mixed Architecture)




รูปที่ 19 รูปแบบสถาปัตยกรรมแบบผสมผสาน

รูปแบบสถาปัตยกรรมแบบผสมผสานเป็นรูปแบบสถาปัตยกรรมที่ผู้วิจัยนำเสนอและพัฒนามาเพื่อใช้ในงานวิจัยฉบับนี้ โดยมีจุดประสงค์เพื่อความสะดวกของผู้เล่นที่เคยชินกับระบบสถาปัตยกรรมแบบดั้งเดิม ทั้งยังสะดวกต่อผู้พัฒนาเกมในการดัดแปลงเกมจากสถาปัตยกรรมแบบดั้งเดิมที่มีอยู่แล้วได้โดยง่าย

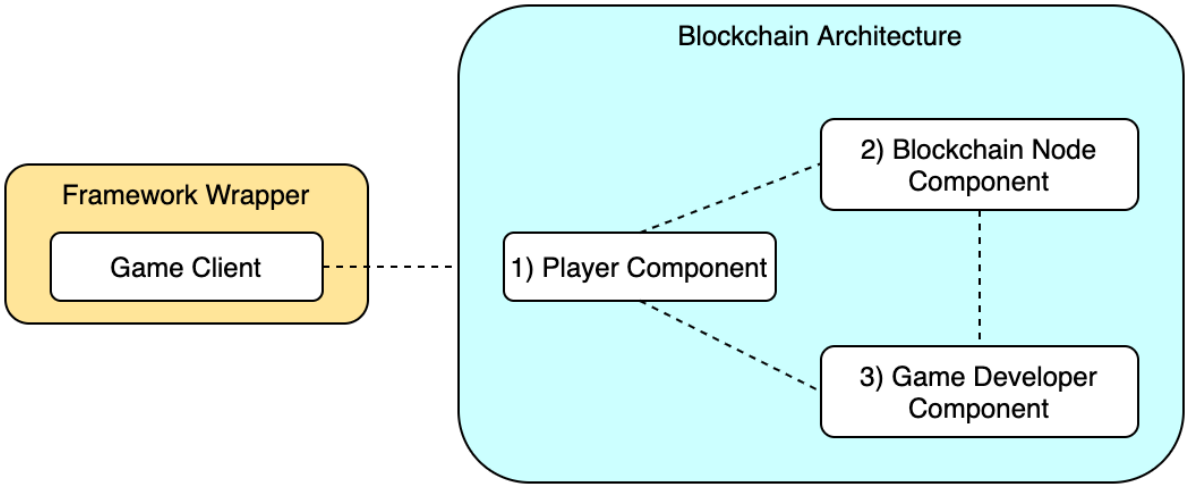
จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สถาปัตยกรรมนี้ใช้เกมเซิร์ฟเวอร์ (Game Server) และ/หรือ ฐานข้อมูล เพื่อเก็บกุญแจส่วนบุคคลของผู้เล่น และทำการเซ็นแทรนแซคชั่นเพื่อส่งขึ้นไปเก็บบนบล็อกเชน การใช้รูปแบบสถาปัตยกรรมแบบผสมผสานนี้ ทำให้ผู้เล่นไม่รู้สึกถึงความแตกต่างของการใช้งานระหว่างสถาปัตยกรรมแบบดั้งเดิมกับแบบผสมผสาน เนื่องจากการใช้สถาปัตยกรรมแบบกระจายศูนย์โดยตรงนั้น ผู้เล่นจะต้องเข้าใจถึงกุญแจส่วนบุคคล และกระเป๋าเงินดิจิทัลเสียก่อน รวมถึงหน้าที่ในการจ่ายเงินค่าเซ็นแทรนแซคชั่น หรือค่าแก๊ส (Gas Fee) นั้น จะตกเป็นหน้าที่ของผู้เล่นอีกด้วย แต่ในสถาปัตยกรรมแบบผสมผสานนั้น สามารถยกหน้าที่ดูแลกุญแจส่วนบุคคลและจัดการกระเป๋าสตางค์เหล่านี้ไปให้ผู้พัฒนาเกมหรือบริษัทผลิตเกมได้ ผ่านระบบการยืนยันตัวตน (Authentication) ซึ่งผู้เล่นที่มีความรู้เรื่องบล็อกเชนอยู่แล้ว ก็สามารถจัดการสิ่งเหล่านี้เองได้ภายหลัง การให้กุญแจส่วนบุคคลกับคนอื่นนั้นถือได้ว่าไม่ปลอดภัย แต่ผู้วิจัยมีความเห็นว่าเป็นสิ่งจำเป็นเพื่อประสบการณ์การเล่นเกมที่เข้าถึงได้ง่ายเช่นเดียวกับสถาปัตยกรรมแบบดั้งเดิมสำหรับผู้เล่นที่ยังไม่มีความรู้เรื่องบล็อกเชน

ในระบบต้นแบบของงานวิทยานิพนธ์ฉบับนี้ ผู้วิจัยทำหน้าที่เป็นผู้พัฒนาเกม และ รักษาดูแลกุญแจส่วนบุคคลด้วยตนเอง แต่หากสถาปัตยกรรมแบบผสมผสานถูกนำไปใช้อย่างแพร่หลาย การเก็บรักษาดูแลกุญแจส่วนบุคคล ควรเป็นหน้าที่ของผู้เล่นเอง เพราะหากเมื่อเกมเซิร์ฟเวอร์ ปิดตัวไป แต่ผู้เล่นมีการเก็บรักษากุญแจส่วนบุคคลด้วยตัวผู้เล่นเอง ผู้เล่นยังสามารถที่จะรักษาข้อมูลที่อยู่ภายในกระเป๋าเงินดิจิทัลของตนเองได้

สถาปัตยกรรมแบบผสมผสานนั้น จำเป็นต้องมีชั้นของรูปแบบกรอบอ้างอิงเช่นเดียวกับสถาปัตยกรรมแบบกระจายศูนย์ เพียงแต่สถาปัตยกรรมนี้ กระเป๋าดิจิทัลจะถูกผนวกเข้ามาภายในรูปแบบกรอบอ้างอิง (ซึ่งได้กล่าวถึงในบทที่ 2) ที่ผู้เล่นสามารถเข้าถึงกระเป๋าดิจิทัลได้โดยตรง โดยไม่ต้องผ่านกระเป๋าดิจิทัลของบุคคลที่สาม งานวิทยานิพนธ์นี้นำรูปแบบสถาปัตยกรรมแบบผสมผสานมาใช้ในการทดลอง เพื่อให้เห็นถึงประโยชน์ในการประยุกต์ใช้บล็อกเชนโดยที่ไม่รู้สึกว่ากำลังใช้เทคโนโลยีนี้อยู่

### 4.2 องค์ประกอบที่เกี่ยวข้องกับบล็อกเชน (Blockchain Components)




รูปที่ 20 รูปองค์ประกอบที่เกี่ยวข้องกับบล็อกเชน (Blockchain Architecture)

องค์ประกอบที่เกี่ยวข้องกับบล็อกเชนที่นำเสนอในงานวิจัยนี้ (แสดงในรูปที่ 20) สามารถนำไปใช้ได้ทั้งในสถาปัตยกรรมแบบกระจายศูนย์และสถาปัตยกรรมแบบผสมผสาน โดยมีองค์ประกอบสามส่วน (เรียกว่าคอมโพเน้นต์) คือ เพลเยอร์คอมโพเน้นต์ (Player Component) บล็อกเชนโหนดคอมโพเน้นต์ (Blockchain Node Component) และนักพัฒนาเกมคอมโพเน้นต์ (Game Developer Component) โดยการมีปฏิสัมพันธ์ระหว่างแต่ละคอมโพเน้นต์นั้น สามารถ

กระทำได้โดยผ่านสมาร์ทคอนแทรคที่อยู่ภายใต้สถาปัตยกรรมบล็อกเชน (Blockchain Architecture)

### 4.2.1 เพลเยอร์คอมโพเน้นต์

เพลเยอร์คอมโพเน้นต์นั้น เป็นส่วนของผู้เล่นที่เอาไว้เก็บมูลค่าที่เกิดขึ้นจากการเล่นเกม ซึ่งก็คือกระเป๋าเงินดิจิทัลของผู้เล่นนั่นเอง ผู้เล่นเก็บของที่มีมูลค่าของตนเองไว้ ในที่นี้คือโทเคนดิจิทัลตามมาตรฐาน ERC-20 หรือ สกุลเงินดิจิทัล ที่ใช้ในการจ่ายค่าธุรกรรมภายในสถาปัตยกรรมนี้ ตัวอย่างเช่น อีเธอเรี่ยม ซึ่งเพลเยอร์คอมโพเน้นต์นี้ เป็นช่องทางการสื่อสารระหว่างตัวเกมไคลเอนต์ ที่อยู่ภายในรูปแบบกรอบอ้างอิงกับกระเป๋าเงินดิจิทัลที่อยู่ภายในสถาปัตยกรรมบล็อกเชนจริง ๆ

### 4.2.2 บล็อกเชนโหนดคอมโพเน้นต์

บล็อกเชนโหนดคอมโพเน้นต์ทำหน้าที่มากกว่าหรือเทียบเท่าผู้ขุด (Miner) หรือ ผู้ยืนยันแทรนแซคชั่น (Validator) ในบล็อกเชนสาธารณะอื่นๆ ซึ่งทำหน้าที่ยืนยันธุรกรรมทุกธุรกรรมที่เกิดภายในสถาปัตยกรรมบล็อกเชน ไม่ว่าจะเป็นการได้รับโทเคนดิจิทัล ERC-20, จำนวนโทเคนดิจิทัลทั้งหมดของทุกคน, จำนวนกระเป๋าดิจิทัล, จำนวนสกุลเงินดิจิทัลที่อยู่ภายในกระเป๋า และอื่น ๆ อีกมากมายตามแต่จะประยุกต์ใช้ เช่น ถ้านำมาประยุกต์ใช้กับเกมก็จะเป็นการเก็บคะแนน ค่าพลังพิเศษ หรือการเก็บไอเทมพิเศษแบบเข้ารหัส (ERC-721) เป็นต้น รวมถึงยังทำหน้าที่เป็นคณะกรรมการคอยคัดเลือกเกมใหม่ ๆ เข้ามาในระบบ ป้องกันการโกง ควบคุมอัตราการแลกโทเคนดิจิทัล ERC-20 เป็นต้น บล็อกเชนโหนดคอมโพเน้นต์สามารถมีจำนวนมากน้อยเท่าใดก็ได้ ขึ้นอยู่กับความใหญ่ของระบบนิเวศน์ ตามจำนวนเพลเยอร์คอมโพเน้นต์ หรือจำนวนนักพัฒนาเกมคอมโพเน้นต์ เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สำหรับระบบความโปร่งใสในการตรวจสอบและผลประโยชน์ทับซ้อน (Conflict of Interest) นั้น อยู่นอกเหนือขอบเขตของงานวิทยานิพนธ์ฉบับนี้

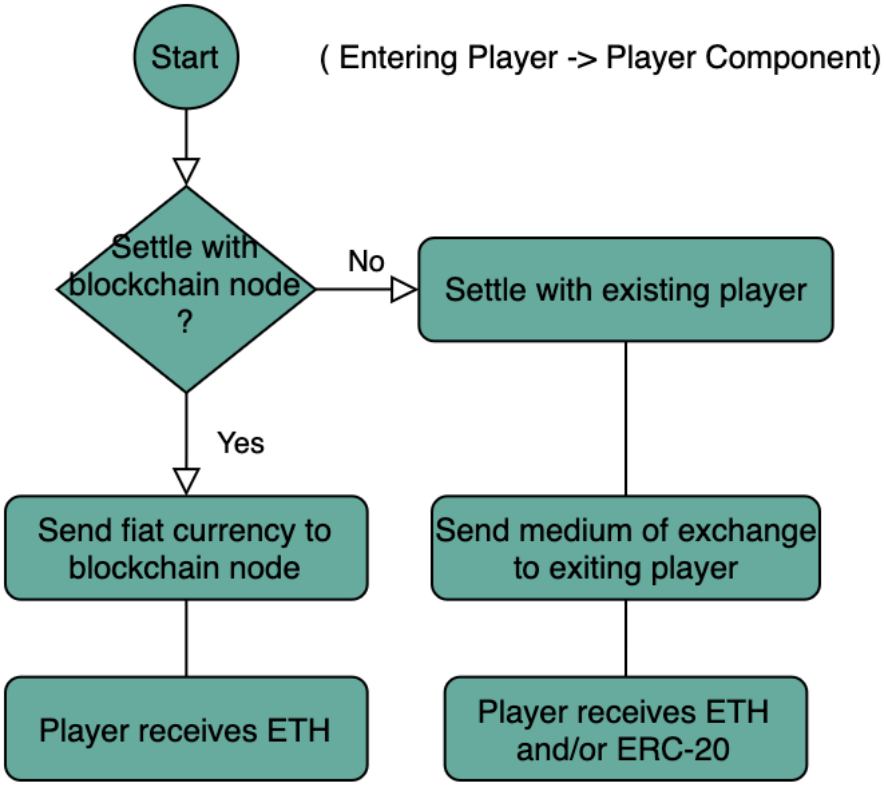
### 4.2.3 นักพัฒนาเกมคอมโพเน้นต์

นักพัฒนาเกมคอมโพเน้นต์เป็นตัวแทนของผู้พัฒนาเกม โดยหลัก ๆ จะเป็นคอมโพเน้นต์ที่แจกจ่าย ERC-20 โทเคนให้ผู้เล่นจากเงื่อนไขภายในเกม คอยดำเนินการแลกเปลี่ยน ERC-20 โทเคนเป็นของต่าง ๆ (หรือค่าพลังพิเศษต่าง ๆ) ภายในเกม ให้ผู้เล่น (เพลเยอร์คอมโพเน้นต์) รวมไปถึงอาจจะทำการสร้างไอเทมพิเศษแบบเข้ารหัสทางเดียว ERC-721 (non-fungible token) ให้ผู้เล่นได้อีกด้วย

**4.3 การทำงานร่วมกันระหว่างคอมโพเน้นต์**

หัวข้อนี้จะกล่าวถึงการทำงานร่วมกันระหว่างคอมโพเน้นต์ต่างๆ จากหัวข้อ 4.2 ซึ่งแสดงถึงปฏิสัมพันธ์ ภายในสถาปัตยกรรมบล็อกเชน

**4.3.1 ผู้เล่นใหม่เข้ามาเป็นเพลเยอร์คอมโพเน้นต์ (Player entering blockchain architecture)**




รูปที่ 21 แสดงการที่ผู้เล่นใหม่เข้าสู่ระบบสถาปัตยกรรมบล็อกเชน

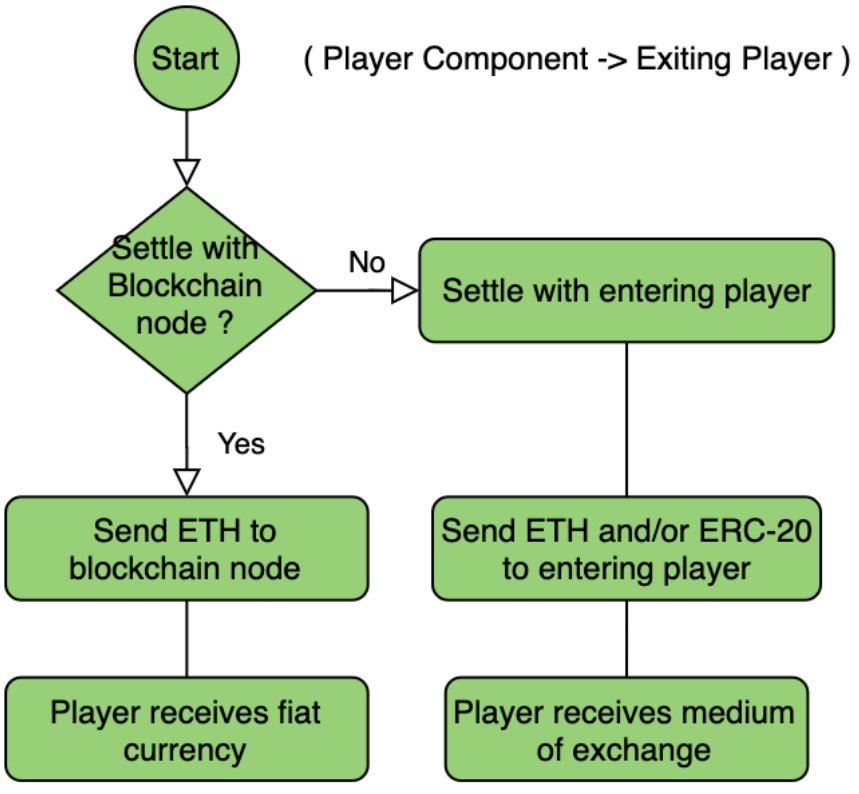
ผู้เล่นใหม่สามารถเข้าสู่สถาปัตยกรรมได้ 2 วิธี (แสดงในรูป 21) คือ การเข้าสู่ระบบกับบล็อกเชนโหนดคอมโพเน้นต์ และการเข้าสู่ระบบกับเพลเยอร์คอมโพเน้นต์

การเข้าสู่ระบบกับบล็อกเชนโหนดคอมโพเน้นต์นั้น เริ่มต้นจากการที่ผู้เล่นใหม่นำเงินสด (Fiat Currency) มาเพื่อซื้อสกุลเงินดิจิทัลที่ใช้ภายในสถาปัตยกรรมบล็อกเชนนั้น เพื่อใช้ในการจ่ายค่าแก๊สในการทำธุรกรรมภายในระบบ โดยจากรูป 21 ค่าแก๊สที่ใช้จ่ายคือสกุลเงิน ETH

ส่วนการเข้าสู่ระบบกับเพลเยอร์คอมโพเน้นต์นั้น เริ่มจากการที่ผู้เล่นใหม่นำสิ่งของที่มีมูลค่าหรือเงินสดที่ทางเพลเยอร์คอมโพเน้นต์ยอมรับ เพื่อใช้เป็นสื่อกลางการแลกเปลี่ยน (medium of exchange) โดยจะได้รับสกุลเงินดิจิทัลที่ใช้ภายในสถาปัตยกรรมนั้น และ/หรือ อาจจะได้รับโทเคน ERC-20 ที่ได้รับจากการเล่นเกมรวมถึงไอเทมพิเศษ ERC-721 ตามแต่ผู้เล่นใหม่กับเพลเยอร์คอมโพเน้นต์ตกลงกัน

อย่างไรก็ดี การแลกเปลี่ยนกับเพลเยอร์คอมโพเน้นต์โดยตรงนั้น อาจจะเกิดการโกงขึ้นได้ เพราะเป็นการกระทำที่อยู่นอกเหนือระบบสถาปัตยกรรมบล็อกเชน ซึ่งอยู่นอกเหนือวัตถุประสงค์ของงานวิจัย

### 4.3.2 ผู้เล่นออกจากการเป็นเพลเยอร์คอมโพเน้นต์ (Player exiting blockchain architecture)




รูปที่ 22 แสดงการที่เพลเยอร์คอมโพเน้นต์ออกจากสถาปัตยกรรมบล็อกเชน

หลังจากที่ผู้เล่นใหม่กลายมาเป็นเพลเยอร์คอมโพเน้นต์แล้ว หากเพลย์เยอร์คอมโพเน้นต์เองประสงค์ที่จะออกจากสถาปัตยกรรมบล็อกเชนก็ย่อมทำได้เช่นกันโดยมี 2 วิธี คือ เพลเยอร์คอมโพเน้นต์แลกเปลี่ยนกับบล็อกเชนโหนดคอมโพเน้นต์ หรือเพลเยอร์คอมโพเน้นต์แลกเปลี่ยนกับผู้เล่นใหม่ (แสดงในรูปที่ 22)

การแลกเปลี่ยนกับผู้เล่นใหม่หลักการจะเหมือนกับข้อ 4.3.1 ในการเข้าสู่ระบบโดยการแลกเปลี่ยนกับเพลเยอร์คอมโพเน้นต์ เพียงแต่การอธิบายเป็นการมองกลับด้านกัน

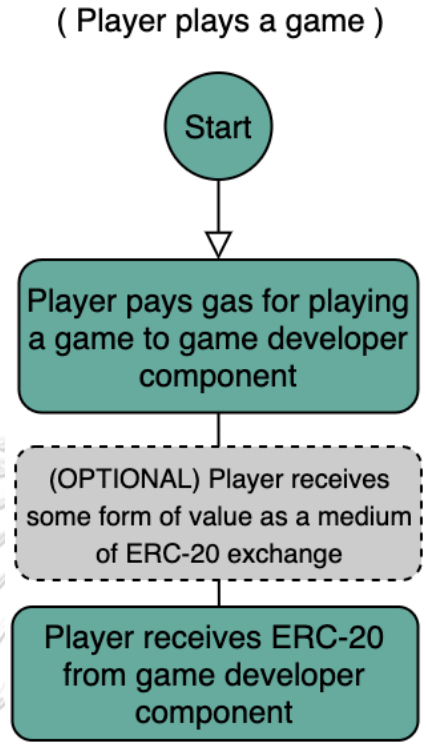
ส่วนการแลกเปลี่ยนกับบล็อกเชนโหนดคอมโพเน้นต์นั้น ผู้เล่นจะทำได้เพียงคืนสกุลเงินดิจิทัลที่ใช้ในการจ่ายค่าแก๊สในระบบสถาปัตยกรรมบล็อกเชนนั้น ๆ โดยได้รับเป็นเงินสดกลับไป อาจจะมีการหักค่าธรรมเนียมในการแลกเปลี่ยนซึ่งอยู่นอกเหนือวัตถุประสงค์ของงานวิจัย แต่เพลเยอร์คอมโพเน้นต์จะไม่สามารถนำโทเคน ERC-20 หรือไอเทมพิเศษแบบเข้ารหัส ERC-721 มาแลกกับบล็อกเชนโหนดคอมโพเน้นต์ได้ ซึ่งหากจะนำเอาโทเคนหรือไอเทมพิเศษมาแลกเป็นเงินสด จะต้องทำผ่านการแลกเปลี่ยนกับผู้เล่นใหม่ หรือตลาดรอง (Exchange) ซึ่งอยู่นอกเหนือวัตถุประสงค์ของงานวิจัยฉบับนี้

### 4.3.3 การปฏิสัมพันธ์ระหว่างเพลเยอร์คอมโพเน้นต์และนักพัฒนาเกมคอมโพเน้นต์ (Interaction between player component and game developer component)

รูปแบบการปฏิสัมพันธ์ระหว่างเพลเยอร์คอมโพเน้นต์และนักพัฒนาเกมคอมโพเน้นต์แบ่งออกเป็น 2 รูปแบบ คือ การปฏิสัมพันธ์ขณะที่ผู้เล่นเล่นเกม และการปฏิสัมพันธ์ขณะที่ผู้เล่นแลกเปลี่ยนไอเทม

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**4.3.3.1 การปฏิสัมพันธ์ขณะที่ผู้เล่นเล่นเกม (แสดงในรูปที่ 23)**



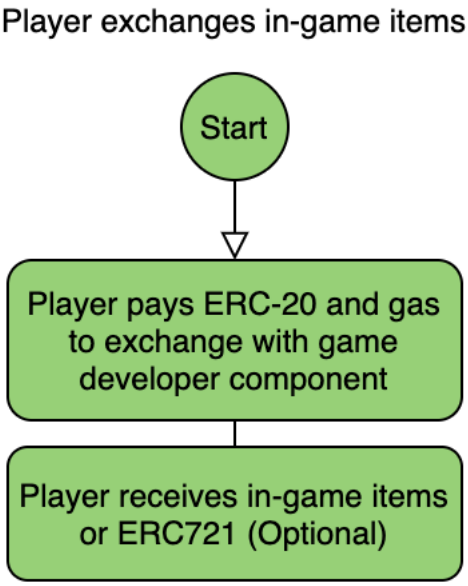

รูปที่ 23 การปฏิสัมพันธ์ระหว่างเพลเยอร์คอมโพเน้นต์และนักพัฒนาเกมคอมโพเน้นต์ขณะที่ผู้เล่นเล่นเกม

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ขณะที่ผู้เล่นเล่นเกมนั้น ผู้เล่นจะต้องจ่ายค่าแก๊สให้กับนักพัฒนาเกมคอมโพเน้นต์ในการเล่นเกมแต่ละครั้ง เพื่อได้มาซึ่งโทเคน ERC-20 โดยขึ้นอยู่กับเงื่อนไขในแต่ละเกมที่นักพัฒนาเกมคอมโพเน้นต์กำหนดขึ้น

จากรูปที่ 23 จะเห็นได้ว่าผู้พัฒนาเกมอาจจะไม่ให้ ERC-20 แก่ผู้เล่นโดยตรง อาจจะให้เป็นค่าบางอย่างที่แสดงถึงมูลค่าที่เกิดจากผู้เล่นใช้เวลาภายในเกมก่อน จึงจะสามารถแปลงเป็น ERC-20 ได้ในภายหลัง ซึ่งภายในงานวิจัยฉบับนี้ได้นำหลักการนี้มาใช้ โดยการให้เวลาแก่ผู้เล่น ก่อนการจะได้รับโทเคน ERC-20

**4.3.3.2 การปฏิสัมพันธ์ขณะที่ผู้เล่นแลกเปลี่ยนไอเทม (แสดงในรูปที่ 24)**




รูปที่ 24 การปฏิสัมพันธ์ระหว่างเพลเยอร์คอมโพเน้นต์และนักพัฒนาเกมคอมโพเน้นต์ ขณะที่ผู้เล่นแลกเปลี่ยนไอเทม

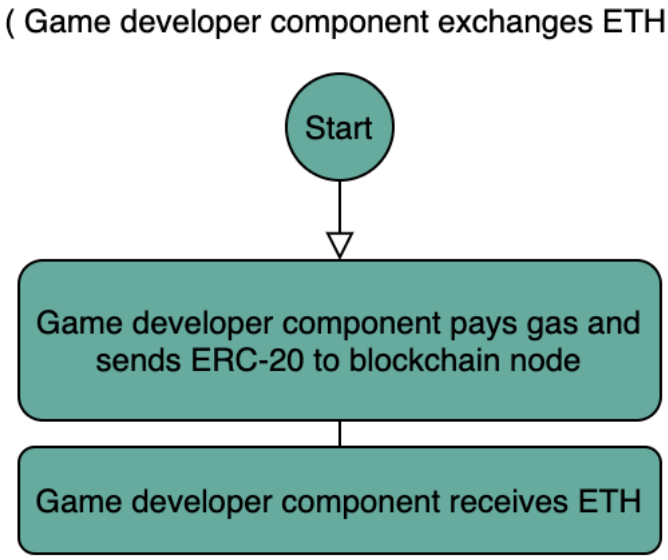
เมื่อผู้เล่นต้องการเพิ่มความสามารถบางอย่าง หรือเพิ่มคุณลักษณะพิเศษจำเพาะภายในเกม ผู้เล่นจะสามารถนำโทเคน ERC-20 ที่ได้มาจากเกมใด ๆ รวมถึงเกมปัจจุบัน มาแลกเปลี่ยนกับนักพัฒนาเกมคอมโพเน้นต์ในเกมนั้น ๆ ได้ ซึ่งผู้เล่นจำเป็นจะต้องนำโทเคน ERC-20 และสกุลเงินดิจิทัลภายในสถาปัตยกรรมบล็อกเชนนั้น ๆ มาจ่ายออกไป เพื่อแลกกับการได้รับลักษณะพิเศษจำเพาะภายในเกม หรือไอเทม หรือแม้แต่ไอเทมพิเศษแบบเข้ารหัส ERC-721 ได้

**4.3.4 การปฏิสัมพันธ์ระหว่างนักพัฒนาเกมคอมโพเน้นต์และบล็อกเชนโหนดคอมโพเน้นต์ ( Interaction between game developer component and blockchain node component)**

รูปแบบการปฏิสัมพันธ์ระหว่างนักพัฒนาเกมคอมโพเน้นต์และบล็อกเชนโหนดคอมโพเน้นต์ แบ่งออกเป็น 2 รูปแบบ คือ การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20

เป็นสกุลเงินดิจิทัล และการปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นเงินสด

**4.3.4.1 การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นสกุลเงินดิจิทัล (แสดงในรูป 25)**

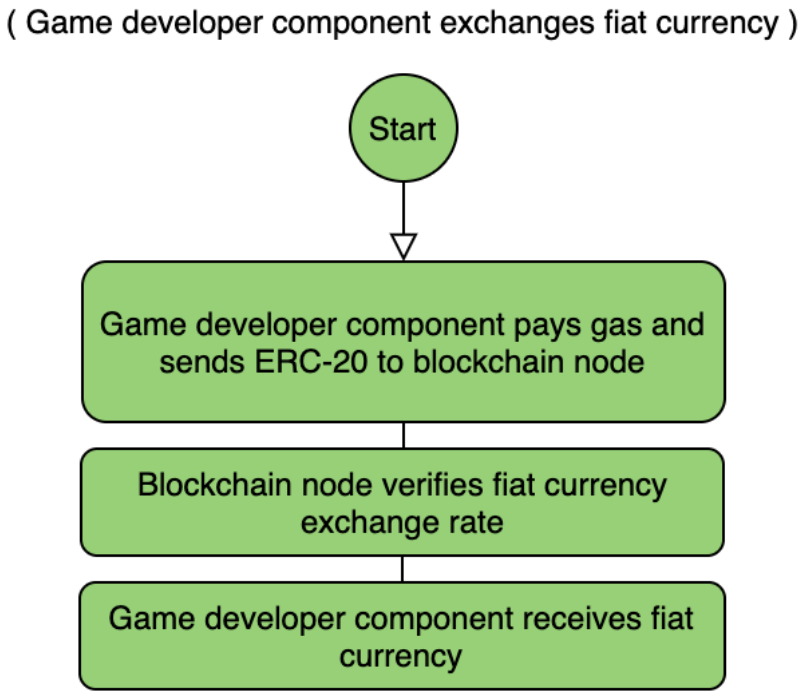



รูปที่ 25 การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นสกุลเงินดิจิทัล

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เมื่อนักพัฒนาเกมต้องการแปลงมูลค่าโทเคน ERC-20 ที่ได้รับมาจากเพลเยอร์คอมโพเน้นต์ นักพัฒนาเกมสามารถนำมาแลกเปลี่ยนกับบล็อกเชนโหนดคอมโพเน้นต์ เป็นสกุลเงินดิจิทัลในอัตราแลกเปลี่ยน ณ ขณะนั้น

**4.3.4.2 การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นสกุลเงินสด (แสดงในรูปที่ 26)**

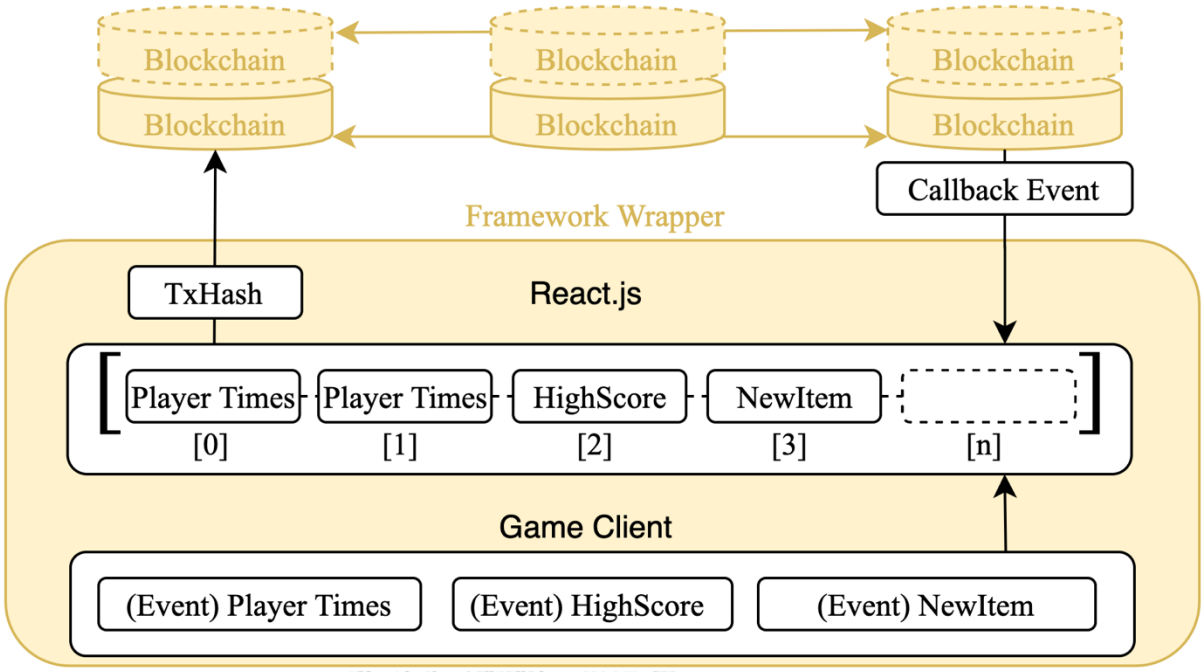



รูปที่ 26 การปฏิสัมพันธ์ขณะที่นักพัฒนาเกมต้องการแลกเปลี่ยนโทเคน ERC-20 เป็นเงินสด

เมื่อนักพัฒนาเกมต้องการแปลงมูลค่าโทเคน ERC-20 ที่ได้รับมาจากเพลเยอร์คอมโพเน้นต์ นักพัฒนาเกมสามารถนำมาแลกเปลี่ยนกับบล็อกเชนโหนดคอมโพเน้นต์ เป็นสกุลเงินสดในอัตราแลกเปลี่ยน ณ ขณะนั้น

ในขั้นตอนแรกนั้นบล็อกเชนโหนดคอมโพเน้นต์จะรวมตัวตั้งเป็นกลุ่มผู้ตัดสิน เพื่อเป็นกลุ่มคณะกรรมการที่ทำการคัดเลือกเกมเข้ามาภายในระบบนิเวศน์บล็อกเชน ซึ่งรวมถึงอัตราการแลกเปลี่ยนสกุลเงินดิจิทัลระหว่างนักพัฒนาเกมคอมโพเน้นต์ โดยอัตราการแลกเปลี่ยนนั้นขึ้นอยู่กับอุปสงค์และอุปทาน (อัตราการแลกเปลี่ยนอยู่นอกเหนือขอบเขตงานวิทยานิพนธ์ฉบับนี้)

### 4.4 การเข้าคิวของบล็อกเชนแทรนแซคชั่น (Blockchain Transaction Queueing)




รูปที่ 27 รูปแสดงกระบวนการเข้าคิวของบล็อกเชนแทรนแซคชั่น

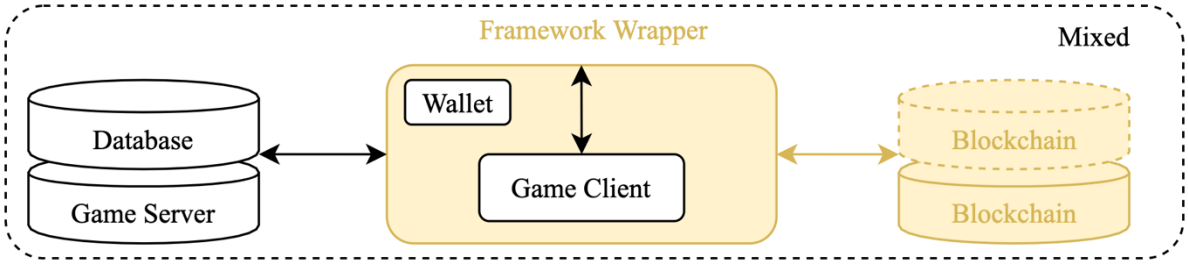
รูปที่ 27 เป็นภาพที่แสดงถึงการติดต่อระหว่างรูปแบบกรอบอ้างอิงกับบล็อกเชนโหนดคอมโพเน้นต์ โดยยกตัวอย่างจากเกมไคลเอนต์ที่อยู่บนเว็บบราวเซอร์ โดยเกมไคลเอนต์ที่อยู่ภายในรูปแบบกรอบอ้างอิงนั้น จะทำการส่งอีเว้นท์มาให้กับจาว่าสคริปต์ (Javascript) ที่เว็บบราวเซอร์ใช้โดยบรรจุเป็นอ็อบเจ็คต์ของตัวแปรอาร์เรย์ ที่ประกอบไปด้วย PlayerTimes , HighScore และ NewItem และจาว่าสคริปต์จะทำการส่งอ็อบเจ็คต์ต่อไปยังบล็อกเชนโหนดคอมโพเน้นต์ โดยก่อนที่จะทำการส่งอ็อบเจ็คต์นั้นจะต้องทำการแฮชก่อน และเมื่อแฮชอ็อบเจ็คต์นั้น ๆ ได้รับการยืนยันจากบล็อกเชนโหนด จะมีคอลแบ็คอีเว้นท์ (callback event) ตอบกลับมา หลังจากนั้นจาว่าสคริปต์จะทำการแฮชอ็อบเจ็คต์ลำดับถัดไป จนกว่าอ็อบเจ็คต์ภายในอาร์เรย์จะหมดไป

การบริหารและการจัดการการส่งข้อมูลขึ้นไปบนบล็อกเชนแบบนี้นั้นเพื่อป้องกันข้อมูลที่ซ้ำซ้อนกัน (Duplication nonce) โดยที่ผู้เล่นไม่จำเป็นที่จะต้องรอคอลแบ็คอีเว้นท์จากบล็อกเชนโหนดคอมโพเน้นต์ เนื่องจากการจัดการข้อมูลทำอยู่ในแบ็คกราวด์โพรเซส (Background process)

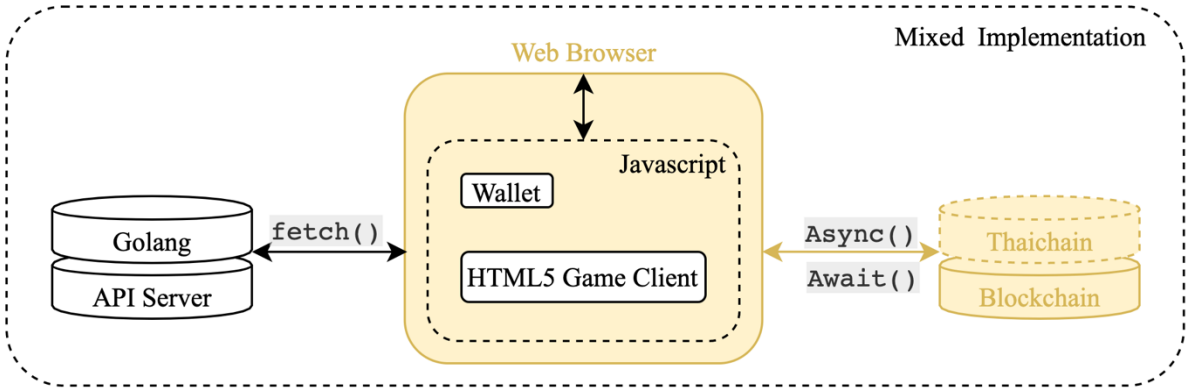
อย่างไรก็ตามถึงแม้ว่าผู้เล่นจะไม่ต้องรอข้อมูลขณะเล่นเกมอยู่ แต่ตอนจบเกมผู้เล่นจำเป็นจะต้องรอเพื่อให้อ็อบเจ็คต์ในอาร์เรย์หมดไปก่อนจึงจะสามารถออกจากเกมได้ มิเช่นนั้นแล้วข้อมูลภายในอาร์เรย์จะหายไปได้

# บทที่ 5
# การพัฒนาระบบต้นแบบ

ในบทนี้จะนำแนวคิดรูปแบบสถาปัตยกรรมแบบผสมผสาน ดังที่กล่าวไว้ในบทที่ 4 มาพัฒนาเป็นระบบนิเวศน์ที่มีองค์ประกอบต่าง ๆ ครบถ้วน ในงานวิทยานิพนธ์นี้ ผู้วิจัยใช้ “ไทยเชน”[37] ซึ่งเป็นบล็อกเชนสาธารณะมาเป็นส่วนหนึ่งของระบบนิเวศน์ รวมทั้งยังพัฒนาเกมไคลเอนต์โดยยูนิตี้ทรีดีและสร้างนักพัฒนาเกมคอมโพเน้นต์เองอีกด้วย




รูปที่ 28 รูปแบบสถาปัตยกรรมแบบผสมผสาน ซึ่งผู้วิจัยนำเสนอในบทที่ 4




รูปที่ 29 แสดงการพัฒนาระบบตามแนวทางของรูป 28

รูปที่ 29 เป็นการนำแนวคิดในบทที่ 4 มาพัฒนาเป็นระบบต้นแบบ เพื่อนำมาใช้ในการทดลอง โดยมีรายละเอียดตามหัวข้อดังนี้

[37] อ้างอิงจาก https://thaichain.io/

**5.1 ระบบบล็อกเชนสาธารณะ (จากรูป 29 ด้านขวา)**

จากรูป 29 ด้านขวา ทางผู้วิจัยได้เลือกใช้ “ไทยเชน” ที่ทำการ fork บล็อกเชนสาธารณะนำมาเปิดให้คนทั่วไปได้ใช้งาน โดยไทยเชนเป็นมูลนิธิที่จัดตั้งขึ้นในประเทศไทย เพื่อมุ่งเน้นการนำเทคโนโลยีบล็อกเชนมาใช้ในชีวิตประจำวัน โดยทางไทยเชนได้นำ GoChain มาใช้ และทำการสร้างโหนดด้วยตนเอง โดยมีฉันทามติแบบออฟออธอริทิ ซึ่งส่งผลให้ความเร็วในการทำธุรกรรมต่อหนึ่งวินาทีมีมากกว่าบล็อกเชนสาธารณะตัวอื่นๆ โดยทั่วไป

**5.2 อีเอ็กซ์พีโทเคน (EXPTOKEN)**

ในวิทยานิพนธ์ฉบับนี้ได้มีการให้รางวัลแก่ผู้เล่นเป็นสกุลเงิน อีเอ็กซ์พีโทเคน ซึ่งถูกสร้างโดยผู้วิจัย และเป็นมาตรฐาน ERC-20 ซึ่งการที่จะได้มาซึ่ง อีเอ็กซ์พีโทเคนนั้น ผู้เล่นจะต้องเล่นเกมเพื่อให้เกิดการกระทำที่มีมูลค่าขึ้น

รูปที่ 30 แสดงเกมที่ใช้ทดสอบในงานวิทยานิพนธ์ฉบับนี้

จากรูปที่ 30 ในงานวิจัยฉบับนี้จะใช้เกมตัวอย่าง 2 เกมในการทดสอบ เกมแรกจะเป็นเกมแนวแมทช์ทรี[38] ซึ่งมีการกระทำที่ก่อให้เกิดมูลค่าคือ ผู้เล่นจะต้องทำการเลื่อนสัญลักษณ์ให้ตรงกัน

[38] อ้างอิงจาก https://en.wikipedia.org/wiki/Tile-matching_video_game

อย่างน้อย 3 สีขึ้นไป ส่วนในเกมที่สองจะเป็นเกมแนวคุกกี้คลิกเกอร์[39]หรือคนทั่วไปรู้จักกันในเกมแฟลปปี้เบิร์ด (Flappy Bird) ผู้เล่นจะต้องทำการเคลื่อนที่ผ่านอุปสรรคจึงจะนับเป็นการกระทำที่ก่อให้เกิดมูลค่า ซึ่งยิ่งผู้เล่นทำการกระทำที่ก่อให้เกิดมูลค่าได้มาก ผู้เล่นก็จะยิ่งได้มูลค่าเพื่อแปลงเป็นอีเอ็กซ์พีโทเคนในลำดับถัดไปมากขึ้น

การกระทำที่ก่อให้เกิดมูลค่า (PlayerTime) นั้นจะถูกเปลี่ยนเป็นอีเอ็กซ์พีโทเคน และเก็บไว้บนบล็อกเชน อย่างไรก็ดี อัตราการแลกเปลี่ยนระหว่างการกระทำที่ก่อให้เกิดมูลค่ากับอีเอ็กซ์พีโทเคนที่ได้รับ ที่เหมาะสมสำหรับทุกเกมนั้น อยู่นอกเหนือขอบเขตงานวิจัยฉบับนี้

ผู้เล่นสามารถนำอีเอ็กซ์พีโทเคนที่ได้รับไปเปลี่ยนเป็นไอเทม หรือลักษณะพิเศษของเกมอื่น ๆ ได้ในภายหลัง เพราะถือว่าอีเอ็กซ์พีโทเคนที่ได้รับมาเปรียบเหมือนสมบัติของผู้เล่นคนนั้น ๆ

### 5.3 ระบบฐานข้อมูลและส่วนเอพีไอเซิร์ฟเวอร์ (จากรูป 29 ด้านซ้าย)

จากรูป 29 ด้านซ้าย เป็นส่วนที่ผู้วิจัยแสดงให้เห็นถึงการประยุกต์เพื่อใช้กับการพัฒนาเกมในรูปแบบดั้งเดิม ผสมผสานกับการใช้งานบนบล็อกเชน ในส่วนของเอพีไอเซิร์ฟเวอร์นั้น ผู้วิจัยได้พัฒนาขึ้นมาเพื่อเป็นการยืนยันตัวตนของผู้เล่นด้วยยูสเซอร์เนมและพาสเวิร์ด เพื่อให้ผู้เล่นไม่จำเป็นต้องจดจำกุญแจส่วนบุคคลที่เอาไว้ใช้ยืนยันตัวตนของผู้เล่น โดยในที่นี้ในส่วนของฐานข้อมูลนั้น ผู้วิจัยทำการเก็บกระเป๋าเงินดิจิทัลและกุญแจส่วนบุคคลของผู้ใช้เอาไว้ ซึ่งหากระบบบล็อกเชนได้รับการยอมรับเป็นที่กว้างขวาง ส่วนนี้จะไม่จำเป็นอีกต่อไป เพราะผู้ใช้เป็นคนเก็บกระเป๋าเงินดิจิทัลและกุญแจส่วนบุคคลด้วยตัวเอง

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

### 5.4 เว็บบราวเซอร์ (จากรูป 29 ตรงกลาง)

ผู้วิจัยได้พัฒนาตัวเกมไคลเอนต์บนเว็บบราวเซอร์ที่รองรับมาตรฐาน HTML5 ในที่นี้เว็บบราวเซอร์คือรูปแบบกรอบอ้างอิงนั่นเอง แต่หากนำแนวคิดของผู้วิจัยไปพัฒนาบนแพลตฟอร์มอื่น ๆ รูปแบบกรอบอ้างอิงก็จะแตกต่างกันไป โดยเว็บบราวเซอร์จะทำการติดต่อกับบล็อกเชน และ/หรือฐานข้อมูลผู้ใช้ด้วยฟังก์ชั่น fetch() ของเว็บบราวเซอร์และติดต่อกับบล็อกเชนโหนดด้วยฟังชั่น Async() , Await() เมื่อได้รับคำสั่งจากตัวเกมไคลเอนต์ ซึ่งการรับคำสั่งหรือส่งคำสั่งจากเกมไคลเอนต์นั้น จะกระทำผ่านฟังก์ชัน Window.postMessage() ที่เป็นมาตรฐานโดยทั่วไปของเว็บเบราว์เซอร์

[39] อ้างอิงจาก https://en.wikipedia.org/wiki/Cookie_Clicker

**5.5 กระเป๋าเงินดิจิทัล (จากรูป 29 ตรงกลาง)**

เว็บบราวเซอร์จะทำหน้าที่ไปดึงกระเป๋าเงินดิจิทัลและกุญแจส่วนบุคคลมาจากฐานข้อมูลและส่วนเอพีไอเซิร์ฟเวอร์ เพื่อทำการใช้งานต่าง ๆ ไม่ว่าจะเป็นการโอนโทเคนดิจิตอล การเซ็นต์แทรนแซคชั่น ซึ่งโดยปกติแล้ว หากบล็อกเชนได้รับการยอมรับอย่างกว้างขวาง ผู้เล่นจะเป็นคนสร้างกระเป๋าเงินดิจิทัลเอง และเก็บกุญแจส่วนบุคคลด้วยตนเอง ในงานวิจัยนี้ ผู้วิจัยได้เลือกใช้ไลบรารี่ ethers.js [40] ซึ่งเป็นจาว่าสคริปต์ไลบารี่ที่รวมคำสั่งทุกอย่างของบล็อกเชนไลบรารี่ รวมถึงการสร้างกระเป๋าเงินดิจิทัลด้วย

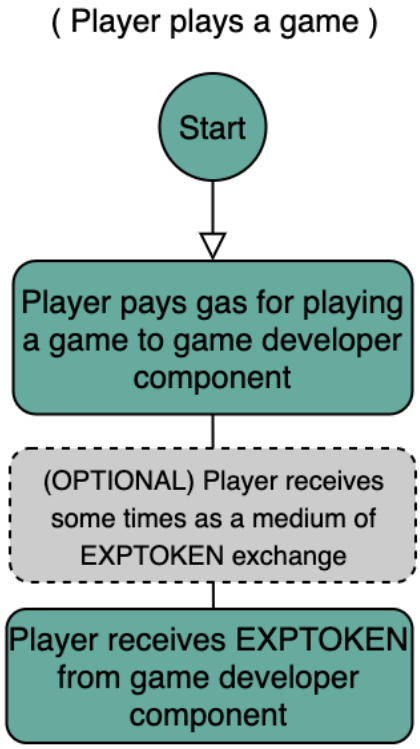
**5.6 จาว่าสคริปต์**

สำหรับการพัฒนาระบบตัวอย่างเพื่อใช้ในงานวิจัยฉบับนี้ จาว่าสคริปต์เป็นส่วนสำคัญหลักที่เอาไว้ใช้ห่อหุ้มสคริปต์ทุกอย่าง เพื่อการทำงานร่วมกัน เพราะเว็บบราวเซอร์สามารถรันจาว่าสคริปต์ได้ ทั้งนี้ได้นำ React.js มาเป็นตัวช่วยในการจัดการระหว่างบล็อกเชนไลบรารี่ อาทิเช่น ethers.js ระบบคิวที่ใช้ในการจัดเรียง (ได้กล่าวในบทที่ 4) ไลบรารี่อื่น ๆ เช่น อะซิออส (Axios) รวมถึงการรันตัวเกมไคลเอนต์ที่ถูกคอมไพล์มาเป็นสคริปต์มาตรฐาน HTML5 ด้วย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[40] อ้างอิงจาก https://docs.ethers.io/v5/

**5.7 การแปลงมูลค่าเวลาเป็นอีเอ็กซ์พีโทเคน**



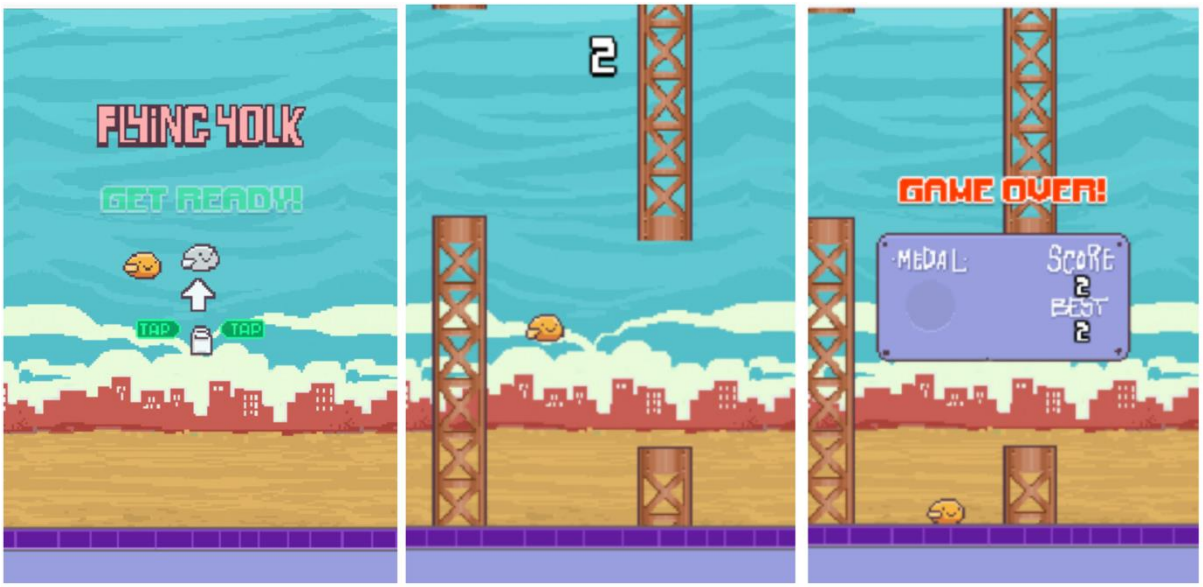

รูปที่ 30 การปฏิสัมพันธ์ระหว่างเพลเยอร์คอมโพเน้นต์และนักพัฒนาเกมคอมโพเน้นต์ขณะที่ผู้เล่นเล่นเกมในการทดลองตามวิทยานิพนธ์

ในการพัฒนาระบบต้นแบบของวิทยานิพนธ์ฉบับนี้ ได้ใช้แนวทางจากบทที่ 4 หัวข้อ 4.3.3.1 โดยจากรูปที่ 30 จะเห็นได้ว่า เมื่อผู้เล่น เล่นเกมที่ผู้วิจัยทำขึ้นมาในหัวข้อ 5.8 นั้น (รายละเอียดตัวเกมไคลเอนต์อยู่ในหัวข้อถัดไป) ผู้เล่นจะได้รับมูลค่าของเวลาเพื่อไปแลกเปลี่ยนเป็น อีเอ็กซ์พีโทเคนในภายหลัง ทั้งนี้การให้เวลาของผู้เล่นมาก่อนที่จะได้รับเป็นอีเอ็กซ์พีโทเคนโดยตรงนั้น เพื่อความสะดวกของผู้วิจัยในการกำหนดอัตราแลกเปลี่ยนเป็น อีเอ็กซ์พีโทเคนในภายหลัง อีกทั้งยังเพื่อไม่ให้ผู้เล่นได้รับ ไอเทมที่ไม่มีความเหมาะสมต่อเวลาที่ผู้เล่นใช้ไปในเกม อันเนื่องมาจากอัตราในการได้เวลาไม่เหมาะสมกับอีเอ็กซ์พีโทเคน โดยอาจจะได้มากไป หรือ น้อยไปกว่าความเป็นจริงก็เป็นได้ หากแต่ถ้าระบบบล็อกเชนได้มีการใช้งานเป็นที่แพร่หลาย และมีอัตราการแลกเปลี่ยนที่เหมาะสมตามเกมแต่ละประเภท ผู้เล่นสามารถได้รับอีเอ็กซ์พีโทเคนโดยตรง โดยไม่ต้องได้รับค่ากลางที่ผู้วิจัยทำขึ้น

### 5.8 ตัวเกมไคลเอนต์

ในงานวิทยานิพนธ์นี้ ผู้วิจัยได้พัฒนาเกมขึ้นมา 2 เกม โดยนำเกมตัวอย่างที่ทางบริษัทยูนิตี้ทรีดี ได้ทำไว้มาดัดแปลงเพื่อให้สามารถส่งผ่านมูลค่าทางเวลาไปยังเกมอื่นได้ โดยการแปลงเวลาเป็น อีเอ็กซ์พีโทเคน โดยตัวเกมไคลเอนต์ทั้ง 2 เกมจะได้มูลค่าเวลาไม่เท่ากัน ตามการกระทำที่ก่อให้เกิดมูลค่า โดยรายละเอียดการได้มาซึ่งมูลค่าเวลา และ รายละเอียดของเกมไคลเอนต์ มีรายละเอียดดังนี้

#### 5.8.1 รายละเอียดเกมไคลเอนต์ เกมที่ 1




Start game Play game Game over

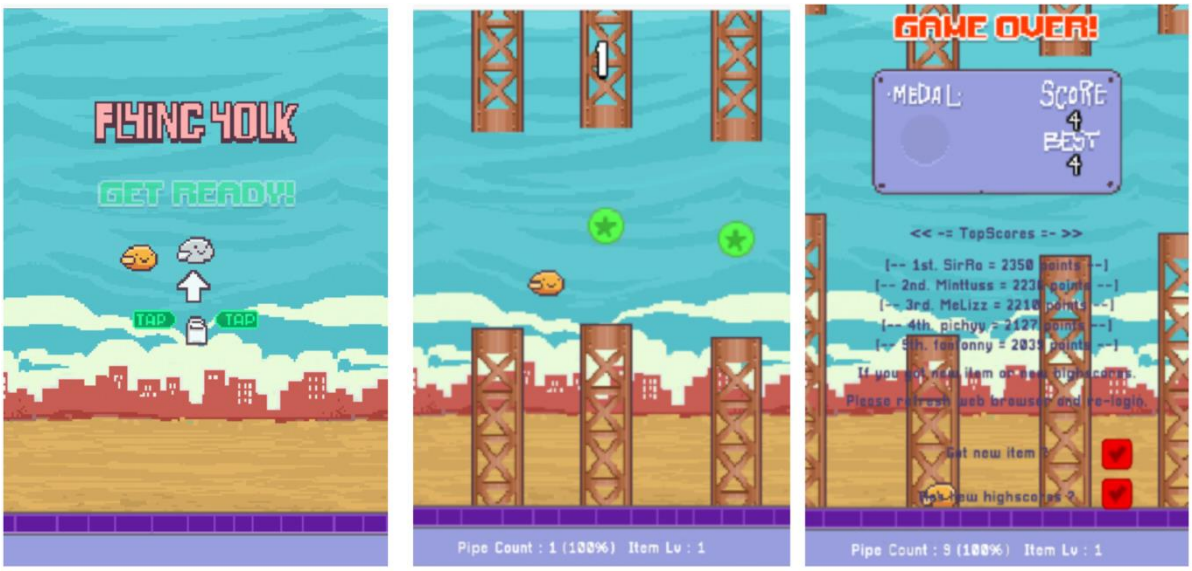
Chulalongkorn University

รูปที่ 31 ภาพแสดงตัวอย่างการเล่นเกมที่ 1 แบบดั้งเดิม ยังไม่มีการปรับแก้ไข

เกม Flappy Bird like (หรือเกมที่คล้ายกับ Flappy bird) แสดงในรูปที่ 31 ผู้เล่นสามารถเริ่มเล่นเกมได้โดยใช้นิ้วกดบนหน้าจอ เกมจะเปลี่ยนจากสถานะ Start game เป็นสถานะเล่นเกม (Play game) ทันที หากผู้เล่นกดที่หน้าจอ จะเป็นการเพิ่มแรงให้นกสามารถบินอยู่บนอากาศได้ แต่หากกดถี่เกินไป จะทำให้นกบินสูงขึ้นไปจนชนขอบบนและทำให้เข้าสู่สถานะจบเกม (Game over) ได้ อย่างไรก็ดี หากไม่กดที่หน้าจอ นกจะตกลงพื้นตามแรงโน้มถ่วงของโลก ถ้าชนพื้นจะทำให้เข้าสู่สถานะจบเกมเช่นกัน อีกทั้งยังต้องคอยหลบท่อที่เกิดมาในเกม หากกดที่หน้าจอเพื่อรักษาระดับ แต่ว่านกไปชนกับท่อเกมก็จะเข้าสู่สถานะจบเกมเช่นกัน ทั้งนี้หากเข้าสู่สถานะจบเกม ผู้เล่นก็จะทราบถึงคะแนนที่นำพาให้นกหลบสิ่งกีดขวางว่าได้กี่คะแนน (ในตัวเกมพื้นฐาน คือ หลบได้ 1 ท่อ จะได้ 1

คะแนน) และหากจบเกมทราบคะแนนที่ทำได้แล้ว ผู้เล่นประสงค์จะเล่นต่อ ก็เพียงกดที่หน้าจออีกครั้งหนึ่ง จะนำพาผู้เล่นเข้าสู่สถานะเล่นเกม อีกครั้ง เป็นอย่างนี้ไปเรื่อย ๆ จนกว่าผู้เล่นจะไม่อยากเล่นต่ออีก

เนื่องด้วยผู้วิจัยต้องการจะทำให้เกมสามารถแลกเปลี่ยนอีเอ็กซ์พีโทเคนที่ได้มาจากเกมอื่น ผู้วิจัยจึงต้องทำการแก้ไขเกมให้รองรับการแลกเปลี่ยนไอเทมพิเศษที่ได้มาจากเกมอื่น

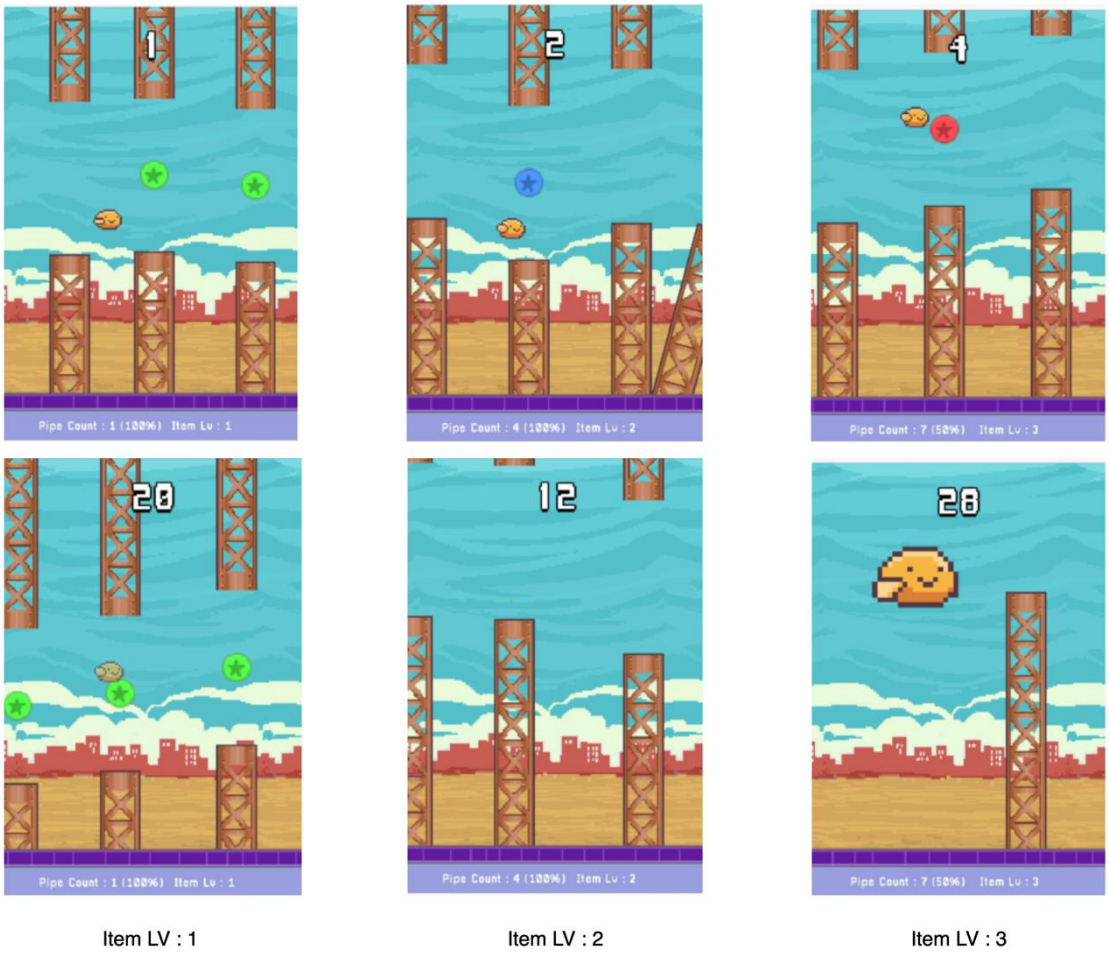



Start game | Play game with special item lv 1 | Game over with other players highscore

รูปที่ 32 ภาพแสดงตัวอย่างการเล่นเกมที่ 1 แบบมีการปรับแก้ไขเพื่อใช้ในงานวิจัย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

เกมที่ผู้วิจัยปรับแต่งเพื่อให้เข้ากับจุดประสงค์ของงานวิจัย แสดงในรูปที่ 32 ภาพตรงกลางจะมีไอเทมพิเศษที่ถ้าผู้เล่นนำนกไปเก็บ จะทำให้นกมีความสามารถพิเศษ นอกจากนี้หากเล่นจนถึงสถานะจบเกม จะพบว่าระบบจะแสดงคะแนนที่ผู้เล่นทำได้ รวมไปถึงอันดับคะแนนสูงสุดของผู้เล่นคนอื่น ๆ 5 อันดับแรก




รูปที่ 33 ไอเทมเลเวลต่าง ๆ และผลของการเก็บไอเทม

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ไอเทมพิเศษในเกมที่ปรับแก้ไขนี้มี 3 แบบ คือ

**(1) ไอเทมเลเวล 1 สีเขียว** ทำให้ทุก ๆ ครั้งที่ผ่านท่ออุปสรรคนั้น คะแนนเพิ่ม 10 คะแนน จากปกติเพิ่ม 1 คะแนน

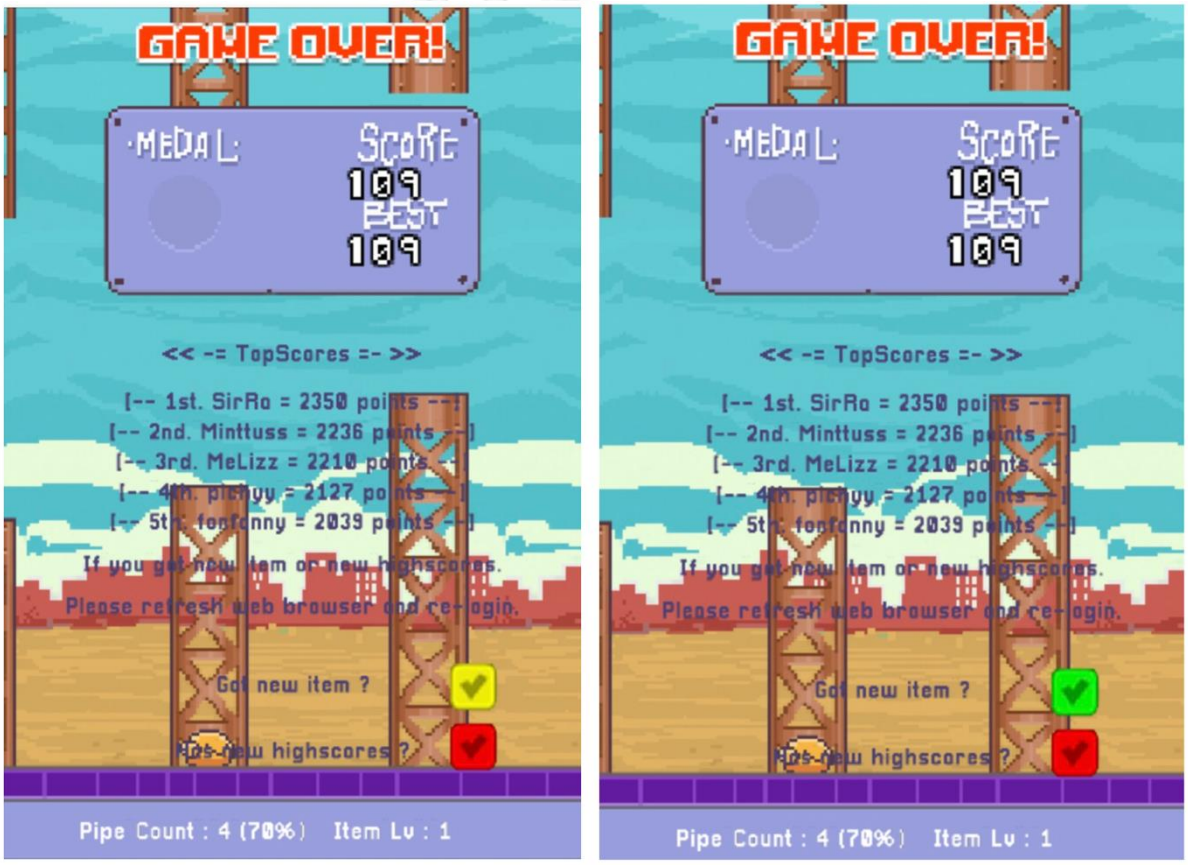
**(2) ไอเทมเลเวล 2 สีน้ำเงิน** ทำให้ทุก ๆ ครั้งที่ผ่านท่ออุปสรรคนั้น คะแนนเพิ่ม 10 คะแนน จากปกติเพิ่ม 1 คะแนน และทำให้นกตัวเล็กลงมาก ๆ จนผ่านท่ออุปสรรคได้ง่ายขึ้น

**(3) ไอเทมเลเวล 3 สีแดง** ทำให้ทุก ๆ ครั้งที่ผ่านท่ออุปสรรคนั้น คะแนนเพิ่ม 10 คะแนน จากปกติเพิ่ม 1 คะแนน และทำให้นกตัวใหญ่ขึ้น สามารถชนท่ออุปสรรคพังได้

ซึ่งการจะได้มาซึ่งไอเทมเลเวลต่าง ๆ นั้น ก็ขึ้นกับเลเวลของผู้เล่น และโอกาสในการเกิดของไอเทมภายในเกม

รูปที่ 34 แถบด้านล่างของเกม แสดงโอกาสในการเกิดของไอเทมและไอเทมเลเวล

รูป 34 แสดงหน้าจอด้านล่างของเกม ที่ให้ผู้เล่นได้เห็นว่า ทุก ๆ 5 ท่ออุปสรรคที่ผู้เล่นสามารถทำให้นกบินผ่าน จะทำให้เกิดไอเทมเลเวล 1 ด้วยอัตราการเกิด 100% ทั้งนี้โอกาสในการเกิดไอเทม และไอเทมเลเวลจะเปลี่ยนไปเป็นค่าที่ดีขึ้นทุก ๆ 100 คะแนน ที่ผู้เล่นทำได้ กล่าวคือผู้เล่นสามารถเล่นเกมเพื่อทำให้นกเก่งขึ้น เพื่อจะทำให้ผ่านด่านได้ง่ายขึ้นและได้คะแนนมากขึ้นตามไปด้วย




Waiting for new item Got new item

รูปที่ 35 รูปแสดงการเพิ่มเลเวล หลังจบเกม

จากรูป 35 หากผู้เล่นทำคะแนนได้เกิน 100 คะแนน ตอนเกมจบ จะปรากฏไอคอนสีเหลือง เพื่อแสดงให้เห็นว่าผู้เล่นกำลังจะได้ไอเทมชนิดใหม่ หรือเลเวลขึ้น ซึ่งผู้เล่นจะต้องรอจนกว่าไอคอนสีเหลืองเปลี่ยนเป็นสีเขียว ซึ่งแปลว่าผู้เล่นได้ทำการบันทึกไอเทมใหม่ หรือเลเวลขึ้น เก็บเข้าระบบบล็อกเชนเรียบร้อยแล้วนั่นเอง

**5.8.1.1 การได้รับเวลาที่ก่อให้เกิดมูลค่าของเกมไคลเอนต์ เกมที่ 1**

การได้มาซึ่งเวลาที่มีมูลค่า สำหรับเกมที่ 1 นั้น จะเกิดจากการที่ผู้เล่นสามารถบังคับตัวละครนก ผ่านอุปสรรค์ได้หนึ่งครั้ง นับเป็น 1 หน่วยเวลาที่ได้รับ โดยจะจัดเวลาที่มีมูลค่าเข้าระบบคิว (เพื่อบรรจุลงบล็อกเชน) ทุกๆ 10 ครั้งที่ผู้เล่นได้รับเวลาที่มีมูลค่า

ตารางที่ 1 แสดงตัวอย่างการแปลงเวลาที่ได้เป็น อีเอ็กซ์พีโทเคนของเกมไคลเอนต์ เกมที่ 1

| | **เวลาที่ได้รับ (หน่วย)** | **อัตราทด** | **อีเอ็กซ์พีโทเคนที่ได้รับจริงหลังปรับค่าแล้ว (หน่วย)** |
|---|---|---|---|
| **ผู้เล่นคนที่ 1** | 20 | 0.01 | 1 |
| **ผู้เล่นคนที่ 2** | 100 | 0.01 | 1 |
| **ผู้เล่นคนที่ 3** | 110 | 0.01 | 2 |

จากตารางที่ 1 มีอัตราทดจากทดสอบในกลุ่มตัวอย่างเพื่อประเมิณความเหมาะสม โดยมาจากค่าเวลาเฉลี่ยรายสัปดาห์ของผู้เล่นทุกคนในกลุ่มที่ทดสอบคำนวนมาเป็นอัตราทดที่ 0.01 แล้วนำไปคูณกับ เวลาที่ได้รับ ผลลัพธ์ที่ได้ จะได้เป็นจำนวนอีเอ็กซ์พีโทเคน โดยเศษที่ได้รับจะปัดขึ้นหลักหน่วยเสมอ

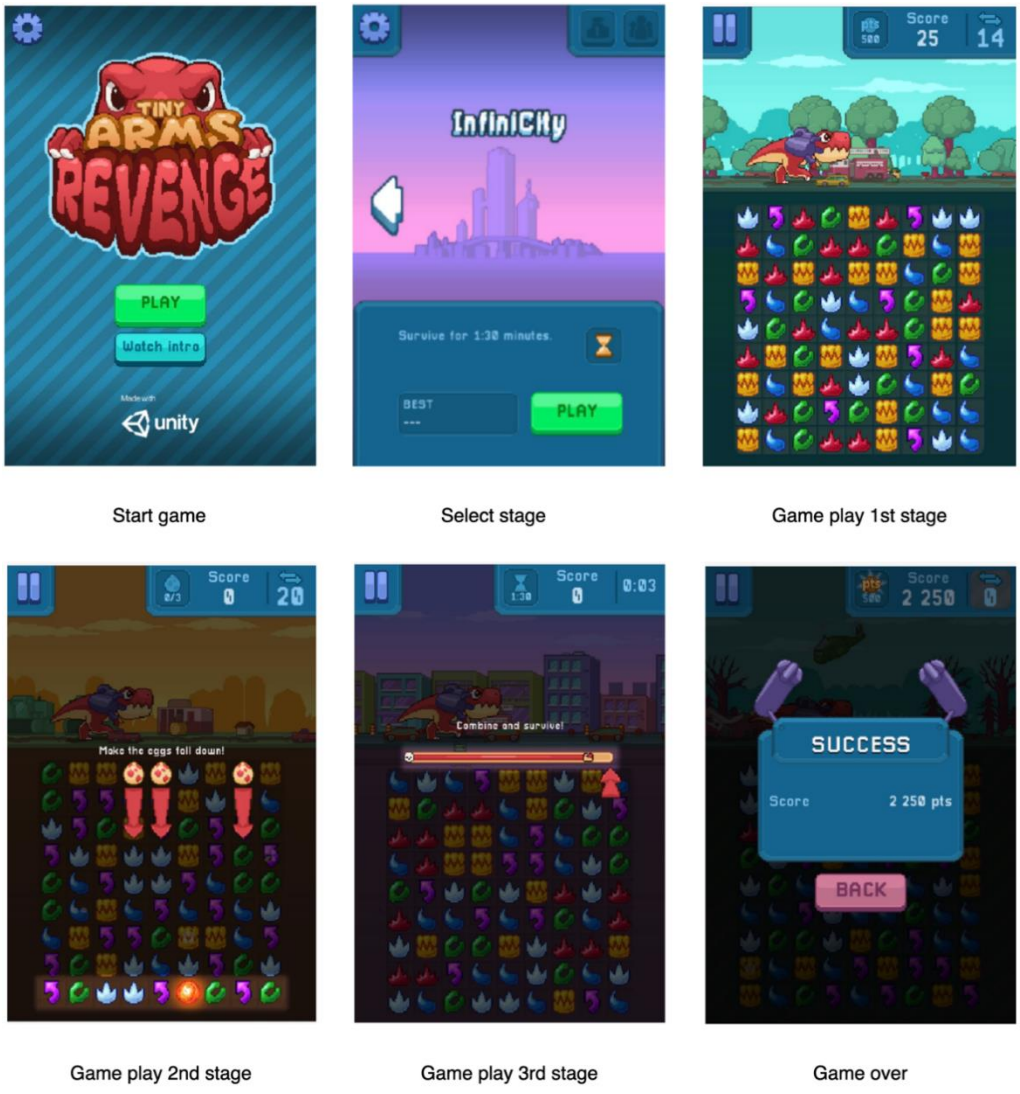
จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

**5.8.1.2 การแลกอีเอ็กซ์พีโทเคนเป็นไอเทมของเกมไคลเอนต์ เกมที่ 1**

การแลกไอเทมภายในเกมไคลเอนต์ที่ 1 นั้น เป็นการนำเอาอีเอ็กซ์พีโทเคนมาแลกกับเลเวลของผู้เล่น ซึ่งจะทำให้ผู้เล่นที่นำเอาอีเอ็กซ์พีโทเคนที่ได้มาจากเกมไคลเอนต์ที่ 2 นั้น เริ่มต้นด้วยโอกาสที่จะทำคะแนนได้สูงกว่าผู้เล่นที่เริ่มต้นโดยไม่มีอีเอ็กซ์พีโทเคน

โดยอัตราการแลกเปลี่ยนของ 1 อีเอ็กซ์พีโทเคน ต่อ 1 เลเวล ที่ผู้เล่นจะได้รับ

### 5.8.2 รายละเอียดเกมไคลเอนต์ เกมที่ 2




รูปที่ 36 ภาพแสดงตัวอย่างการเล่นเกมที่ 2 แบบดั้งเดิม ซึ่งตัวเกมยังไม่มีการปรับแก้ไข

เกม Tiny arms revenges (หรือเกมที่คล้ายกับแมทช์ทรี) แสดงในรูปที่ 36 ผู้เล่นสามารถเริ่มเล่นเกมได้โดยกดปุ่ม Play บนหน้าจอ เกมจะเปลี่ยนจากสถานะ Start game เป็นสถานะ Select Stage โดยผู้เล่นสามารถเลือกด่านที่ตนเองอยากจะเล่นได้ แต่จะต้องเคยผ่านด่านก่อนหน้านั้นมาก่อน ตัวอย่างเช่น ไม่สามารถเล่นด่านที่สามได้ หากไม่เคยผ่านด่านที่สองมาก่อน

ด่านแรก (1st stage) ผู้เล่นจะต้องทำคะแนนให้ถึงค่าที่กำหนด โดยมีการจำกัดการเคลื่อนที่ของวัตถุเป็นจำนวนครั้งที่กำหนด จะเป็นด่านที่ผู้เล่นจะต้องทำการสลับสับเปลี่ยนวัตถุ

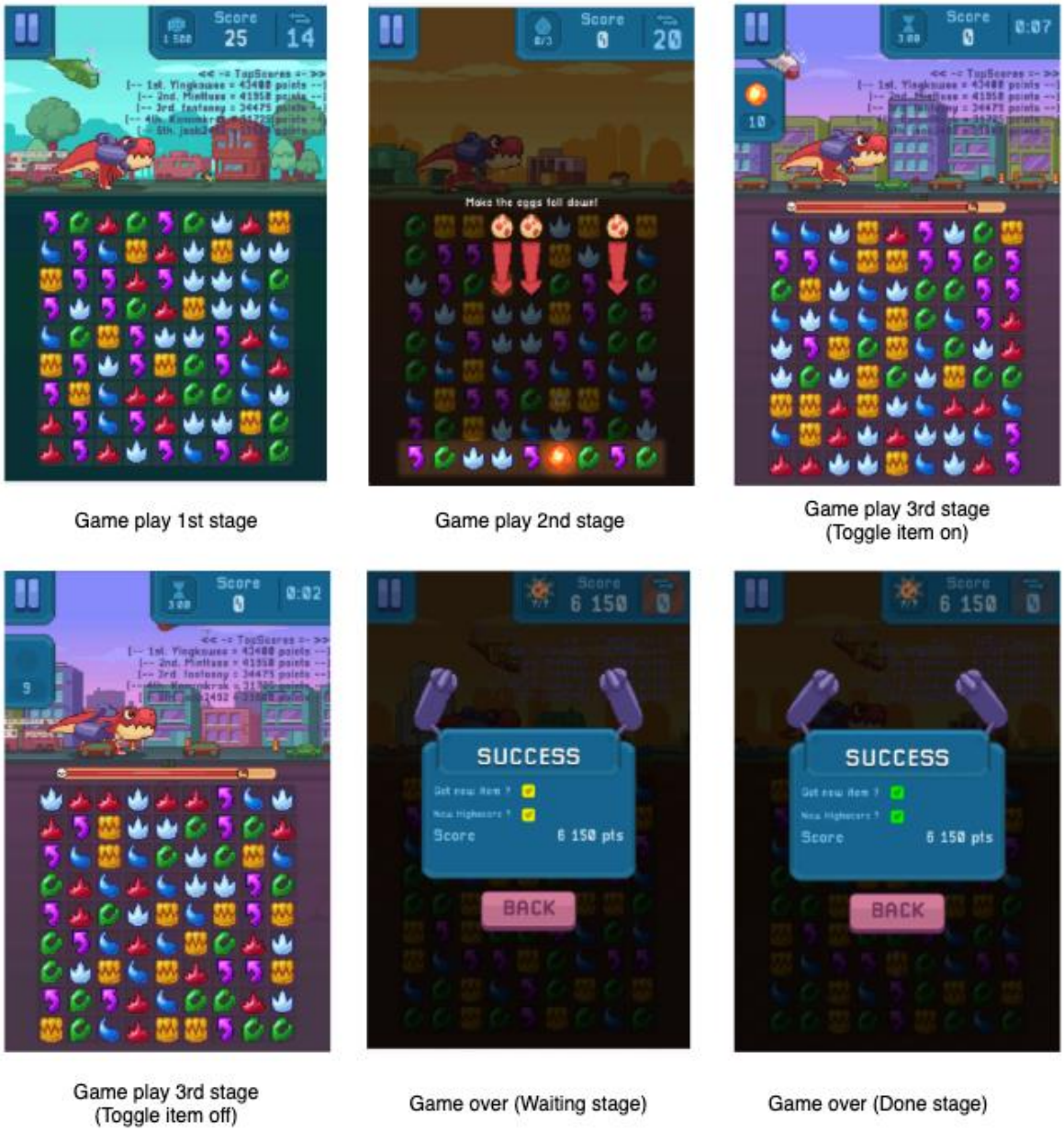
ด่านที่สอง (2nd stage) ผู้เล่นจะต้องทำให้วัตถุรูปไข่หล่นลงข้างล่างให้ครบทุกอัน โดยมีการจำกัดการเคลื่อนที่ของวัตถุเป็นจำนวนครั้งที่กำหนด

ด่านที่สาม (3rd stage) ผู้เล่นจะสามารถเล่นไปได้เรื่อย ๆ ตราบใดที่แถบเวลายังไม่หมด โดยไม่มีการจำกัดการเคลื่อนที่ของวัตถุ

การเล่นเกมในทุก ๆ ด่าน จะต้องทำให้วัตถุเรียงเหมือนกันอย่างน้อย 3 วัตถุ ต่อกัน โดยผู้เล่นสามารถ สลับสับเปลี่ยนวัตถุได้แค่ทิศทางขึ้น ลง ซ้าย ขวา เท่านั้น โดยจะเริ่มทำกับวัตถุใดก่อนก็ได้ และทุกครั้งที่มีการเคลื่อนที่วัตถุ จำนวนครั้งที่กำหนดก็จะลดลงตาม หากผู้เล่นสามารถเรียงวัตถุให้เหมือนกันอย่างน้อย 3 วัตถุ ได้ วัตถุนั้นจะหายไป และผู้เล่นจะได้คะแนนเพิ่มขึ้น หากผู้เล่นเล่นในด่านแรกหรือด่านที่สองจนจำนวนครั้งที่กำหนดลดลงจนเหลือ 0 เกมจะเข้าสู่สถานะจบเกม (Game over) ทันที แต่หากเป็นด่านที่สาม เกมจะเข้าสู่สถานะจบเกม ก็ต่อเมื่อแถบเวลาหมดลง โดยผู้เล่นจะต้องผ่านด่านแรกก่อน จึงจะสามารถเล่นด่านที่สองต่อไปได้ และเช่นเดียวกันจะต้องผ่านด่านที่สองก่อนจึงจะสามารถเล่นด่านที่สามได้ซึ่งเป็นด่านสุดท้าย และผู้เล่นสามารถกลับมาเล่นใหม่ซ้ำได้เรื่อย ๆ เพื่อให้คะแนนของผู้เล่นมีค่าสูงขึ้นเพื่อแข่งกับผู้เล่นคนอื่น ๆ โดยระบบจะแสดงผลคะแนนเฉพาะผู้เล่นที่มีคะแนนสูงสุด 5 อันดับแรกเท่านั้น

เนื่องด้วยผู้วิจัยต้องการจะทำให้เกมสามารถแลกเปลี่ยนอีเอ็กซ์พีโทเคนที่ได้มาจากเกมอื่น ผู้วิจัยจึงต้องทำการแก้ไขเกมให้รองรับการแลกเปลี่ยนไอเทมพิเศษที่ได้มาจากเกมอื่นโดยเกมที่แก้ไขเป็นดังนี้

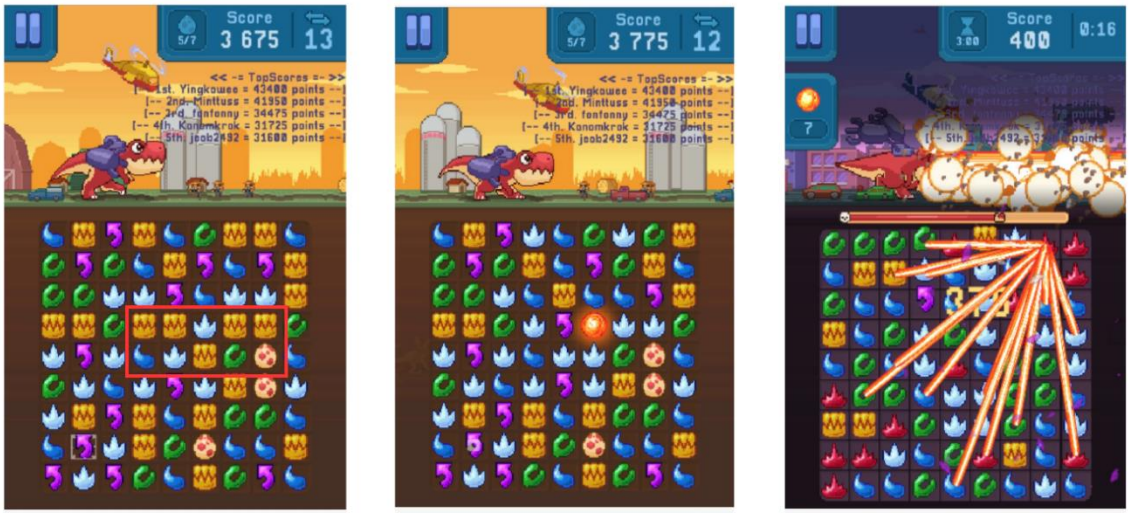
จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University




รูปที่ 37 ภาพแสดงตัวอย่างการเล่นเกมที่ 2 แบบมีการปรับแก้ไขเพื่อใช้ในงานวิจัย

รูปที่ 37 แสดงเกมที่ผู้วิจัยปรับแต่งเพื่อให้เข้ากับจุดประสงค์งานวิจัย โดยเกมเพลย์ในทุก ๆ ด่าน จะมีคะแนนสูงสุด 5 อันดับแรกของผู้เล่นแสดงอยู่ ความพิเศษจะอยู่ในด่านที่ 3 โดยผู้เล่นสามารถกดเปิดหรือปิดไอคอนลูกไฟภายในด่านที่ 3 ได้ โดยหากเปิดไอคอนลูกไฟอยู่ (รูปขวาบน ในรูปที่ 37) และผู้เล่นทำการสลับสับเปลี่ยนวัตถุใดก็ได้ให้เหมือนกัน 3 วัตถุ จะเกิดลูกไฟพิเศษขึ้นมาให้ใช้ในเกม แต่ก็จะทำให้จำนวนลูกไฟที่ใช้ได้ในไอคอนลูกไฟลดลง หากผู้เล่นไม่อยากใช้ไอคอนพิเศษนี้ก็สามารถกดปิดได้ (รูปซ้ายล่างภายในรูปที่ 37) ซึ่งการเล่นก็จะกลับมาเป็นแบบปกติ แต่โดยปกติการ

ที่จะได้ลูกไฟมานั้น ผู้เล่นจะต้องทำการสลับสับเปลี่ยนวัตถุให้เหมือนกันถึง 6 วัตถุ ลูกไฟจึงจะเกิดขึ้นได้




Game play, before forming fireball | Game play, after forming fireball | Game play, using fireball

รูปที่ 38 ภาพเกมเพลย์ที่แสดงลูกไฟพิเศษ

การเปิดความสามารถพิเศษของลูกไฟ ทำให้ผู้เล่นสามารถอยู่ในด่านที่ 3 ได้นานขึ้น เนื่องจากลูกไฟสามารถสลับกับวัตถุใดก็ได้ จะทำให้วัตถุสีนั้น ๆ หายไปทั้งฉาก ส่งผลให้ค่าเวลาในด่านที่ 3 กลับขึ้นมา ทำให้ผู้เล่นอยู่ในด่านที่ 3 ได้นานขึ้น และส่งผลให้มีโอกาสทำคะแนนได้สูงมากขึ้นด้วย ดังแสดงในรูปที่ 38

จากรูป 37 (กลางล่าง และ ขวาล่าง) หากผู้เล่นเล่นจนจบเกม จะพบกับสัญลักษณ์กล่องสี่เหลี่ยม โดยถ้าสัญลักษณ์ขึ้นสีแดงแปลว่าในการเล่นของผู้เล่นครั้งนั้น ๆ ไม่ได้ทำ High score ของตัวเองใหม่ หรือไม่ได้มีการได้มาซึ่งไอเทมลูกไฟ โดยไอเทมลูกไฟจะได้เพิ่มมา 1 ลูก หากผู้เล่นทำคะแนนในด่านนั้น ๆ ได้เกิน 5000 คะแนน แต่ถ้าหากสัญลักษณ์เป็นสีเหลือง (รูปกลางล่างของรูป 38) แสดงว่าผู้เล่นทำ High score ได้ โดยผู้เล่นจะต้องรอจนกว่าสัญลักษณ์กลายเป็นสีเขียว ซึ่งแสดงว่าได้มีการบันทึก High score แล้ว ผู้เล่นจึงจะได้รับไอเทมลูกไฟ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**5.8.2.1 การได้รับเวลาที่ก่อให้เกิดมูลค่าของเกมไคลเอนต์ เกมที่ 2**

การได้มาซึ่งเวลาที่มีมูลค่าสำหรับเกมที่ 2 นั้น จะเกิดจากการที่ผู้เล่นทำให้วัตถุเรียงเหมือนกันอย่างน้อย 3 วัตถุ นับเป็น 1 หน่วยเวลาที่ได้รับ โดยจะจัดเวลาที่มีมูลค่าเข้าระบบคิว เพื่อบรรจุลงบล็อกเชน ทุกๆ 5 ครั้งที่ผู้เล่นได้รับเวลาที่มีมูลค่า

ตารางที่ 2 แสดงตัวอย่างการแปลงเวลาที่ได้เป็น อีเอ็กซ์พีโทเคนของเกมไคลเอนต์ เกมที่ 2

| | **เวลาที่ได้รับ (หน่วย)** | **อัตราทด** | **อีเอ็กซ์พีโทเคนที่ได้รับจริงหลังปรับค่าแล้ว (หน่วย)** |
|---|---|---|---|
| **ผู้เล่นคนที่ 1** | 20 | 0.01 | 1 |
| **ผู้เล่นคนที่ 2** | 100 | 0.01 | 1 |
| **ผู้เล่นคนที่ 3** | 110 | 0.01 | 2 |

จากตารางที่ 2 มีอัตราทดจากทดสอบในกลุ่มตัวอย่างเพื่อประเมิณความเหมาะสม โดยมาจากค่าเวลาเฉลี่ยรายสัปดาห์ของผู้เล่นทุกคนในกลุ่มที่ทดสอบคำนวนมาเป็นอัตราทดที่ 0.01 แล้วนำไปคูณกับ เวลาที่ได้รับ ผลลัพธ์ที่ได้ จะได้เป็นจำนวนอีเอ็กซ์พีโทเคน โดยเศษที่ได้รับจะปัดขึ้นหลักหน่วยเสมอ

**5.8.2.2 การแลกอีเอ็กซ์พีโทเคนเป็นไอเทมของเกมไคลเอนต์ เกมที่ 2**

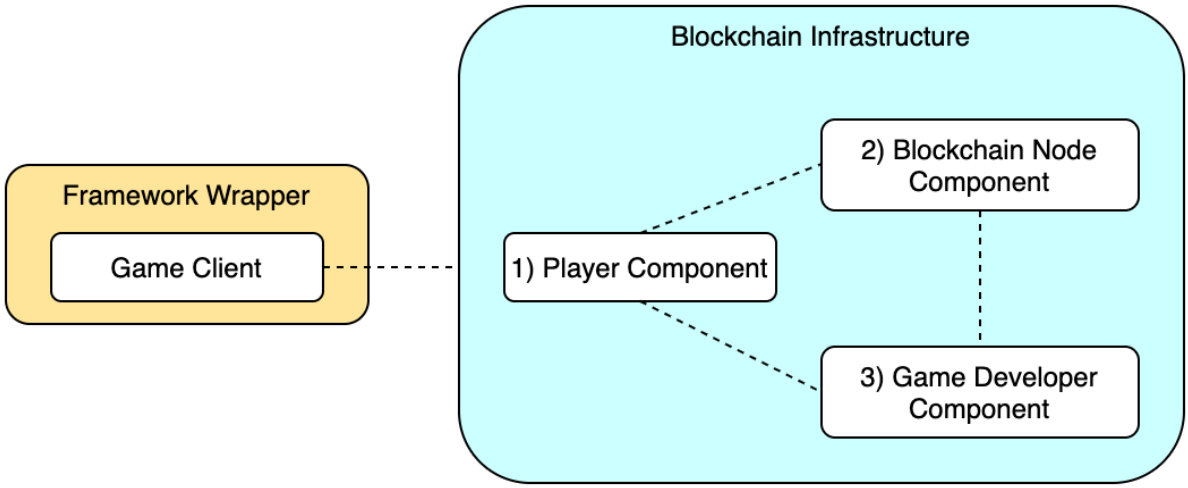
การแลกไอเทมภายในเกมไคลเอนต์ที่ 2 นั้น เป็นการนำเอาอีเอ็กซ์พีโทเคนมาแลกกับไอเทมลูกไฟภายในเกมเพื่อใช้ในด่านที่ 3

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

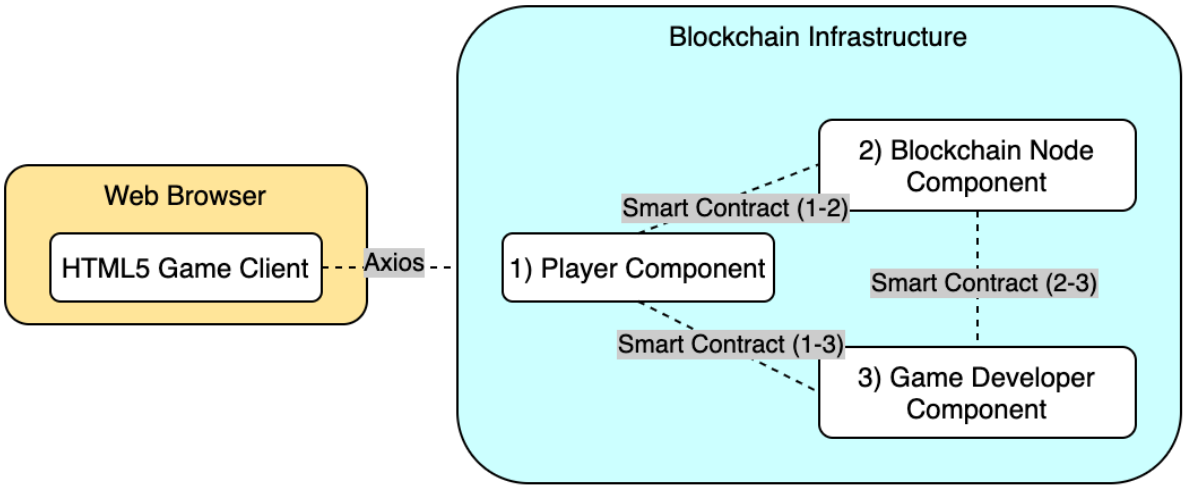
ซึ่งจะทำให้ผู้เล่นที่นำเอาอีเอ็กซ์พีโทเคนที่ได้มาจากเกมไคลเอนต์ที่ 1 นั้น เริ่มต้นด้วยจำนวนลูกไฟที่มากกว่า ส่งผลให้คะแนนที่ทำได้ในด่านที่ 3 สูงกว่าผู้เล่นที่เริ่มต้นโดยไม่มีอีเอ็กซ์พีโทเคน เนื่องจากสามารถใช้ลูกไฟพิเศษได้เป็นจำนวนมาก

โดยอัตราการแลกเปลี่ยนของ 1 อีเอ็กซ์พีโทเคน ต่อ 1 เลเวล ที่ผู้เล่นได้รับ

**5.9 การพัฒนาบล็อกเชนโหนดคอมโพเน้นต์และการทำงานร่วมกัน**




รูปที่ 39 (จากบทที่ 4) รูปองค์ประกอบที่เกี่ยวข้องกับบล็อกเชน (Blockchain Components)




รูปที่ 40 (บทที่ 5) รูปองค์ประกอบที่เกี่ยวข้องกับบล็อกเชนที่พัฒนาเพื่อใช้ในงานวิทยานิพนธ์ฉบับนี้

รูปที่ 39 แสดงหลักการทำงานร่วมกันของแต่ละคอมโพเน้นต์ ส่วนรูปที่ 40 แสดงระบบตัวอย่างที่ได้พัฒนาตามรูปที่ 39 โดยมีการทำงานร่วมกันของคอมโพเน้นต์ต่างๆ โดยในที่นี้จะพูดถึงรายละเอียดการพัฒนาที่เพิ่มเติมเข้ามาจาก บทที่ 4 เท่านั้น

### 5.9.1 เกมไคลเอนต์กับเพลเยอร์คอมโพเน้นต์

จากรูปที่ 40 เกมไคลเอนต์มีอยู่ 2 หน้าที่ คือ

**(1) รับค่าจากบล็อกเชนเพื่อมาใช้ภายในเกม**

การรับค่าต่าง ๆ มาจากบล็อกเชนเพื่อใช้ในการแสดงผลภายในตัวเกม จะกระทำโดยเกมไคลเอนต์ส่งอีเว้นท์มาที่จาว่าสคริปต์ภายในเว็บบราวเซอร์ ผ่านไลบารี่ อะซิออส เพื่อทำการเรียกขอรีเควสค่าต่าง ๆ และรอรับค่าต่าง ๆ นั้นกลับมาผ่านฟังก์ชัน Promise() ได้แก่ ค่าไอเทมพิเศษต่าง ๆ ที่เก็บไว้บนบล็อกเชน ตัวอย่างเช่นคะแนนสูงสุด ค่าพลังพิเศษติดตัว (เช่น เลเวลของเกมแฟลปปี้เบิร์ด) จำนวนไอเทมพิเศษ (เช่น จำนวนลูกไฟของเกมแมทช์ทรี) ซึ่งจะถูกบันทึกอยู่ในสมาร์ทคอนแทรคของนักพัฒนาเกมคอมโพเน้นต์ โดยอ้างอิงจากกระเป๋าเงินดิจิทัลของเพลเยอร์คอมโพเน้นต์

**(2) ส่งค่ากลับไปเพื่อบันทึกลงบล็อกเชน**

การบันทึกค่าต่าง ๆ บนบล็อกเชนภายในสมาร์ทคอนแทรคของนักพัฒนาเกมคอมโพเน้นต์ของเกมใด ๆ เริ่มจากการที่ภายในเกมไคลเอ้นต์เกิดเหตุการณ์ต่าง ๆ ขึ้น เช่น เมื่อผู้เล่นเล่นถึงจุดที่กำหนด (ในที่นี้คือการบันทึกเวลาเพื่อแปลงเป็น อีเอ็กซ์พีโทเคน) ทำคะแนนสูงสุดใหม่ หรือได้รับค่าพลังสถานะพิเศษ เกมไคลเอ้นต์จะทำการส่งอีเว้นท์มาที่จาว่าสคริปต์ และนำอีเว้นท์นั้น ๆ เซ็นแทรนแซคชั่นด้วยกุญแจส่วนบุคคลของผู้เล่นโดยไลบารี่ ethers.js และทำการส่งขึ้นไปที่เพลเยอร์คอมโพเน้นต์ เพื่อให้เพลเยอร์คอมโพเน้นต์ได้ทำการบันทึกอีเว้นต์ที่เกิดขึ้นที่สมาร์ทคอนแทรคของนักพัฒนาเกมคอมโพเน้นต์

### 5.9.2 เพลเยอร์คอมโพเน้นต์กับนักพัฒนาเกมคอมโพเน้นต์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

เพลเยอร์คอมโพเน้นต์ติดต่อกับนักพัฒนาเกมคอมโพเน้นต์ โดยผ่านสมาร์ทคอนแทรค (จากรูป 40 Smart Contract (1-3) ) ตามที่ได้กล่าวไว้ในบทที่ 4

ในส่วนนี้ผู้วิจัยได้พัฒนาสมาร์ทคอนแทรคเพื่อจุดประสงค์ดังนี้คือ

**(1) เพลเยอร์คอมโพเน้นต์ได้รับค่าเวลาในการเล่น**

จากบทที่ 4 การที่จะได้รับค่าตัวแทนกลางซึ่งใช้ในการแลกเปลี่ยนจากการเล่นเกมนั้น ไม่จำเป็นจะต้องทำ ถ้าหากระบบนิเวศน์บล็อกเชนที่ใช้ได้รับการยอมรับและมีการตรวจสอบเป็นอย่างดี เพลเยอร์คอมโพเน้นต์จะสามารถได้รับอีเอ็กซ์พีโทเคนโดยตรงได้เลย ไม่ต้องรับค่าตัวแทนกลาง แต่ในงานวิทยานิพนธ์ฉบับนี้ เนื่องจากเป็นการทดลองที่ยังไม่ได้ปรับอัตราการได้มาซึ่งอีเอ็กซ์พีโทเคน ผู้วิจัยจึงให้ผู้เล่นได้รับค่าตัวแทนกลางขณะที่เล่นเกม และจะนำไปแลกเปลี่ยนเป็นอีเอ็กซ์พีโทเคนในภายหลัง

**(2) เพลเยอร์คอมโพเน้นต์แลกอีเอ็กซ์พีโทเคนกับไอเทมพิเศษต่าง ๆ**

จากบทที่ 4 การที่จะแลกเปลี่ยนอีเอ็กซ์พีโทเคนกับไอเทมพิเศษภายในเกมนั้น หากระบบได้มีการใช้งานอย่างแพร่หลายแล้ว ผู้เล่นจะสามารถแลกเปลี่ยนได้ด้วยตนเอง ในงานวิทยานิพนธ์นี้ ผู้วิจัยจะทำหน้าที่แลกเปลี่ยนแทนผู้เล่น โดยเอาเวลาที่ได้จากการเล่นเกมหนึ่ง ซึ่งก็คือค่าตัวแทนกลางนำมาแลกเป็นอีเอ็กซ์พีโทเคน และจึงเปลี่ยนเป็นไอเทมพิเศษแต่ละเกมต่อไป

### 5.9.3 นักพัฒนาเกมคอมโพเน้นต์กับบล็อกเชนโหนดคอมโพเน้นต์

นักพัฒนาเกมคอมโพเน้นต์ติดต่อกับบล็อกเชนโหนดคอมโพเน้นต์ โดยผ่านสมาร์ทคอนแทรค (จากรูป 40 Smart Contract (2-3) ) ตามที่ได้กล่าวไว้ในบทที่ 4

ในส่วนนี้ผู้วิจัยไม่ได้ทำในงานวิจัย เนื่องจากผู้วิจัยทำหน้าที่เป็นนักพัฒนาเกมคอมโพเน้นต์เองจึงไม่ได้มีความจำเป็นจะต้องนำเอาอีเอ็กซ์พีโทเคนที่ได้รับมาจากผู้เล่น ไปแลกคืนเป็นสกุลเงินดิจิทัลหรือสกุลเงินสดแต่อย่างใด

### 5.9.4 เพลเยอร์คอมโพเน้นต์กับบล็อกเชนโหนดคอมโพเน้นต์

เพลเยอร์คอมโพเน้นต์ติดต่อกับบล็อกเชนโหนดคอมโพเน้นต์ โดยผ่านสมาร์ทคอนแทรค (จากรูป 40 Smart Contract (1-2) ) ตามที่ได้กล่าวไว้ในบทที่ 4

ในส่วนนี้ผู้วิจัยได้กระทำการแทนผู้เล่นเป็นส่วนใหญ่ โดยแบ่งเป็นหัวข้อดังนี้

**(1) เพลเยอร์คอมโพเน้นต์ซื้อสกุลเงินดิจิทัลกับบล็อกเชนโหนดคอมโพเน้นต์**

ในงานวิทยานิพนธ์นี้ ผู้วิจัยได้รับสกุลเงินดิจิทัลมาจากการมิ้นท์ (Minted) ในการทดลอง ผู้วิจัยจึงทำหน้าที่การซื้อขายนี้แทนผู้เล่น โดยการแจกให้ฟรี เพื่อให้ผู้เล่นเอาไว้ใช้ในการจ่ายค่าแก๊สเพื่อใช้ในการทดลองและทดสอบระบบ ทั้งนี้มีความจำเป็นต้องทำเช่นนี้เพื่อหลีกเลี่ยงการทำให้ผู้เล่นที่มาร่วมทดสอบระบบต้องเสียเงินด้วยตนเอง

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**(2) เพลเยอร์คอมโพเน้นต์แลกเวลากับบล็อกเชนโหนดคอมโพเน้นต์**

ในงานวิทยานิพนธ์นี้ ผู้วิจัยได้พัฒนาส่วนที่ทำหน้าที่แลกเวลากับบล็อกเชนโหนดคอมโพเน้นต์ แต่ไม่ได้พัฒนาส่วนของอินเตอร์เฟสนี้มาให้ผู้เล่นใช้งาน เนื่องจากระบบต้นแบบที่นำเสนอมีความต้องการให้ผู้เล่นสามารถใช้งานได้โดยไม่ต้องรู้จักบล็อกเชน การแลกเปลี่ยนจึงเป็นการดำเนินการโดยผู้วิจัยเอง

แท้จริงแล้ว ผู้เล่นจะแลกเวลากับนักพัฒนาเกมคอมโพเน้นต์เลยก็ได้ หรือจะแลกกับบล็อกเชนโหนดคอมโพเน้นต์ก็ได้ถ้าผู้เล่นมีความรู้ในการจัดการกุญแจส่วนบุคคลและกระเป๋าเงินสาธารณะ

**(3) เพลเยอร์คอมโพเน้นต์แลกเปลี่ยนกุลเงินดิจิทัลกับบล็อกเชนโหนดคอมโพเน้นต์**

ในส่วนนี้ผู้วิจัยไม่ได้ทำการพัฒนาและทดลองในงานวิทยานิพนธ์นี้ เนื่องจากผู้เล่นได้สกุลเงินดิจิทัลมาฟรีและไม่ต้องแลกคืนกลับมา แต่ในระบบที่มีการใช้งานอย่างแพร่หลาย ผู้เล่นสามารถนำสกุลเงินดิจิทัลมาแลกเปลี่ยนคืนกับบล็อกเชนโหนดคอมโพเน้นต์ได้เช่นเดียวกัน

### 5.9.5 เพลเยอร์คอมโพเน้นต์กับเพลเยอร์คอมโพเน้นต์

เพลเยอร์คอมโพเน้นต์ติดต่อกับเพลเยอร์คอมโพเน้นต์นั้นอยู่นอกเหนือขอบเขตของงานวิจัย เนื่องจากเพลเยอร์คอมโพเน้นต์ด้วยกันเองนั้นสามารถแลกเปลี่ยนสกุลเงินดิจิทัลของระบบเช่น อีเธอเรี่ยม หรือ สกุลเงินดิจิทัลเข้ารหัส อีเอ็กซ์พีโทเคน ได้ด้วยตนเองอยู่แล้ว โดยเป็นมาตราฐานการแลกเปลี่ยนของบล็อกเชนสาธารณะโดยทั่วไปอยู่แล้ว เพียงแค่ขอให้ผู้ใช้งานเข้าใจหลักการการทำงานของ กระเป๋าเงินสาธารณะ กับ ชุดกุญแจส่วนบุคคล

หากแต่มีประเด็นที่นำเสนอไว้คือ หากผู้เล่นที่ยังไม่เคยอยู่ในระบบบล็อกเชน แต่ต้องการสกุลเงินดิจิทัลของระบบ หรือ ต้องการสกุลเงินเข้ารหัส ผู้เล่นที่ยังไม่เคยอยู่ในระบบบล็อกเชน อาจจะนำสิ่งของที่มีมูลค่ามาแลกเปลี่ยนกับเพลเยอร์คอมโพเน้นต์ในระบบได้

## 5.10 กระบวนการทดสอบระบบก่อนใช้งานจริง

ในบทที่ 5 นี้ เป็นการทดสอบการทำงานฟังก์ชันพื้นฐานของระบบ ซึ่งจะมีการทดสอบในส่วนที่ผู้วิจัยจัดทำขึ้น และส่วนที่อ้างอิงกับการตรวจสอบระบบบล็อกเชนที่ทำกันอย่างกว้างขวาง [19,20]

โดยผลการทดสอบนี้จะแบ่งออกเป็นหัวข้อ การทดสอบแบบแยกอิสระ (Isolation Testing) และ การทดสอบแบบบูรณาการ (Integration Testing)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

### 5.10.1 การทดสอบแบบแยกอิสระ

การทดสอบแบบอิสระ จะมุ่งเน้นการแยกส่วนระบบทดสอบ เพื่อความมั่นใจว่าระบบแต่ละระบบทำงานได้ถูกต้อง โดยแบ่งการทดสอบเป็น การทดสอบระบบเครื่องคอมพิวเตอร์แม่ข่าย การทดสอบรูปแบบกรอบอ้างอิง การทดสอบระบบบล็อกเชนสาธารณะ

#### 5.10.1.1 การทดสอบเครื่องคอมพิวเตอร์แม่ข่าย (Game Server - Isolation Testing)

ตารางที่ 3 การทดสอบเครื่องคอมพิวเตอร์แม่ข่าย

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | การได้รับชุดกุญแจ | ทดสอบการเข้าสู่ระบบโดยการเรียกขอรีเควส | แสดงการได้รับกุญแจส่วนบุคคลและกุญแจสาธารณะ ผ่าน console.log ของเว็บเบราว์เซอร์ | ผ่าน |
| 2 | การเก็บชุดกุญแจในโลคอลสโตเรจ | ทดสอบการเข้าสู่ระบบโดยการเรียกขอรีเควส | แสดงการได้รับกุญแจส่วนบุคคลและกุญแจสาธารณะ ในโลคอลสโตเรจ | ผ่าน |

#### 5.10.1.2 การทดสอบรูปแบบกรอบอ้างอิง (Framework Wrapper - Isolation Testing)

ตารางที่ 4 การทดสอบรูปแบบกรอบอ้างอิง

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | การติดต่อระหว่างเกมไคลเอนต์กับจาว่าสคริปต์ | ทดสอบโดยส่งคำสั่งคำออกจากตัวเกมไคลเอนต์ ณ.ขณะหนึ่ง ไปยังจาว่าสคริปต์ | แสดงผลของคำสั่งนั้นในทันที ผ่าน console.log ของเว็บเบราว์เซอร์ | ผ่าน |
| 2 | การติดต่อระหว่างเกมไคลเอนต์กับจาว่าสคริปต์ | ทดสอบโดยส่งคำสั่งออกจากจาว่าสคริปต์ ณ. ขณะหนึ่ง ไปยังตัวเกมไคลเอนต์ | แสดงผลของคำสั่งนั้นในทันที ผ่าน ตัวเกมไคลเอนต์ | ผ่าน |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**5.10.1.3 การทดสอบระบบบล็อกเชนสาธารณะ (Public Blockchain - Isolation Testing)**

ตารางที่ 5 การทดสอบระบบบล็อกเชนสาธารณะ

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | การสร้างกระเป๋าเงินสาธารณะและชุดกุญแจส่วนบุคคล | ทดสอบการสร้าง | ตรวจสอบสกุลเงินดิจิทัล ผ่านทาง https://exp.tch.in.th/ ต้องได้ค่าเป็น 0 | ผ่าน |
| 2 | การรับสกุลเงินดิจิทัล | ทดสอบการได้รับสกุลเงินดิจิทัลจาก จากกระเป๋าเงินสาธารณะของไทยเชน | ตรวจสอบสกุลเงินดิจิทัล ผ่านทาง https://exp.tch.in.th/ ต้องได้ค่าไม่เท่ากับ 0 | ผ่าน |
| 3 | การสร้างสมาร์ทคอนแทรค | ทดสอบโดยการสร้างสมาร์ทคอนแทรค และบรรจุลงบนบล็อกเชนผ่านทาง https://remix.ethereum.org/ | ตรวจสอบสมาร์ทคอนแทรค https://exp.tch.in.th/<br>- ต้องพบ AddressHash<br>- สกุลเงินดิจิทัลของผู้บรรจุสมาร์ทคอนแทรคต้องลดลงเนื่องจากค่าแก๊ส | ผ่าน |
| 4 | การแก้ไขค่าตัวแปรภายในสมาร์ทคอนแทรค | ทดสอบโดยการแก้ไขค่าตัวแปรบนสมาร์ทคอนแทรค ผ่านทาง https://remix.ethereum.org/ | ตรวจสอบสมาร์ทคอนแทรค ผ่านทาง https://exp.tch.in.th/<br>- ต้องพบ TransationHash<br>- สกุลเงินดิจิทัลของผู้บรรจุสมาร์ทคอนแทรคต้องลดลงเนื่องจากค่าแก๊ส | ผ่าน |
| 5 | การอ่านค่าตัวแปรภายใน | ทดสอบโดยการเรียกดูค่าตัวแปรบนสมาร์ทผ่านทาง | - แสดงผลของตัวแปรทันทีผ่านทาง https://remix.ethereum.org/<br>- สกุลเงินดิจิทัลของผู้บรรจุสมาร์ท | ผ่าน |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

| | | | | |
|---|---|---|---|---|
| | สมาร์ทคอนแทรค | https://remix.ethereum.org/ | คอนแทรคต้องไม่ลดลงเนื่องจากเป็นการเรียกดูโดยไม่ได้แก้ไข | |

**5.10.2 การทดสอบแบบบูรณาการ (Integration Testing)**

การทดสอบแบบบูรณาการ จะมุ่งเน้นการทดสอบโดยนำส่วนองค์ประกอบที่เกี่ยวข้องทั้งหมดมาทดสอบรวมกัน เพื่อการทำงานที่ถูกต้อง

**5.10.2.1 การทดสอบขณะเข้าเล่นเกม (Game Login – Intregation Testing)**

ตารางที่ 6 การทดสอบขณะเข้าเล่นเกม

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | เข้าเล่นเกม | การเข้าเล่นเกมโดยกรอกยูสเซอร์เนม และ พาสเวิร์ด | มีระบบแจ้งเตือนผู้เล่นภายในเกมเพื่อให้ผู้เล่นรับทราบว่าเข้าสู่ระบบได้แล้ว และแจ้งให้ผู้เล่นทราบ | ผ่าน |
| 2 | ไม่สามารถเข้าเล่นเกมได้ กรณีที่ 1 | เมื่อผู้เล่นเข้าเล่นภายในเกมจะทำการเข้าสู่ระบบ (ในกรณีที่ผู้เล่นต่ออินเตอร์เน็ตได้ปกติ) | มีระบบแจ้งเตือนผู้เล่นภายในเกมเพื่อให้ผู้เล่นรับทราบว่าไม่สามารถเข้าสู่ระบบได้ และอธิบายถึงสาเหตุที่ไม่สามารถเชื่อมต่อระบบได้ ดังนี้<br>- ยูสเซอร์เนม หรือ พาสเวิร์ด ไม่ถูกต้อง<br>- ระบบบล็อกเชนมีปัญหา | ผ่าน |
| 3 | ไม่สามารถเข้าเล่นเกมได้ กรณีที่ 1 | เมื่อผู้เล่นเข้าเล่นภายในเกมจะทำการเข้าสู่ระบบ (ในกรณีที่ผู้เล่นไม่ได้ต่ออินเตอร์เน็ต) | มีระบบแจ้งเตือนผู้เล่นก่อนเข้าเกมว่าไม่สามารถเข้าเล่นเกมได้เนื่องจากผู้เล่นไม่มีอินเตอร์เน็ต | ผ่าน |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**5.10.2.2 การทดสอบขณะเล่นเกม (Game Play – Intregation Testing)**

ตารางที่ 7 การทดสอบขณะเล่นเกม

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | การได้รับเวลาที่มีมูลค่า | เมื่อผู้เล่นเข้าเล่นภายในเกม เมื่อได้เข้าสู่ระบบแล้ว เมื่อเล่นเกมไปถึงจุดที่ทำการบันทึกเวลาที่ผู้เล่นใช้ในเกม ระบบจะสร้างแทรนแซคชั่น เซ็นต์แทรนแซคชั่น และส่งไปเก็บที่บล็อกเชน | สามารถตรวจสอบเวลาที่ผู้เล่นได้รับผ่านทางระบบหลังบ้าน หรือผ่านเว็บไซต์กลางที่ผู้วิจัยจัดทำขึ้น | ผ่าน |

**5.10.2.3 การทดสอบการแลกเปลี่ยนเวลาเป็นอีเอ็กซ์พีโทเคน (Time to Exptoken Exchange – Intregation Testing)**

ตารางที่ 8 การทดสอบการแลกเปลี่ยนเวลาเป็นอีเอ็กซ์พีโทเคน

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | ผู้วิจัยทำการแลกเวลาที่ผู้เล่นใช้ในเกมกับอีเอ็กซ์พีโทเคน | ทดสอบการแลกเปลี่ยนด้วยการจำลองผู้เล่นขึ้นมา โดยทดสอบหลังจากหัวข้อที่ 5.10.2.2 ลำดับที่ 1 เสร็จสมบูรณ์เพื่อให้ผู้เล่นจำลองมีเวลาที่นำมาใช้แลกเปลี่ยนเป็นอีเอ็กซ์พีโทเคนได้ | ตรวจสอบกระเป๋าเงินสาธารณะผ่านทาง ส่วนเสริม เมต้ามาร์ค<br>ต้องพบ<br>- เหรียญ อีเอ็กซ์พีโทเคน มีจำนวนเพิ่มขึ้น | ผ่าน |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**5.10.2.4 การทดสอบการแลกเปลี่ยนอีเอ็กซ์พีโทเคนเป็นไอเทมภายในเกม (Exptoken to Item Exchange – Intregation Testing)**

ตารางที่ 9 การทดสอบการแลกเปลี่ยนอีเอ็กซ์พีโทเคนเป็นไอเทมภายในเกม

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | ผู้วิจัยทำการแลกอีเอ็กซ์พีโทเคนที่ผู้เล่นมีอยู่กับไอเทมภายในเกม | ทดสอบการแลกเปลี่ยนด้วยการจำลองผู้เล่นขึ้นมา โดยทดสอบหลังจากหัวข้อที่ 5.10.2.3 ลำดับที่ 1 เสร็จสมบูรณ์เพื่อให้ผู้เล่นจำลองมีอีเอ็กซ์พีโทเคนมาใช้แลกเปลี่ยนเป็นไอเทมภายในเกมได้ | (1) สามารถตรวจสอบจำนวนไอเทมภายในเกมที่เพิ่มขึ้นผ่านทางระบบหลังบ้าน หรือผ่านเว็บไซต์กลางที่ผู้วิจัยจัดทำขึ้น<br>(2) สามารถตรวจสอบจำนวนอีเอ็กซ์พีโทเคนที่ลดลงตามอัตราที่กำหนดไว้ผ่านทางระบบหลังบ้าน หรือผ่านเว็บไซต์กลางที่ผู้วิจัยจัดทำขึ้น | ผ่าน |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

**5.10.2.5 การทดสอบการทำงานที่ผิดพลาดของระบบบล็อกเชนขณะเล่นเกม (Diagnose Blockchain Error while Play Game - Intregation Testing)**

ตารางที่ 10 การทดสอบการทำงานที่ผิดพลาดของระบบบล็อกเชนขณะเล่นเกม

| ลำดับ | การทดสอบ | คำอธิบาย | ผลลัพธ์ที่คาดหวัง | ผลการทดสอบจริง |
|---|---|---|---|---|
| 1 | ปิดระบบบล็อกเชน ณ เวลาใด ๆ | คือการไม่สามารถเชื่อมต่อบล็อกเชน ณ เวลาใด ๆ หรือเมื่อระบบที่ทำการทดสอบปิดตัวลง กล่าวคือทุกเครื่องในระบบบล็อกเชนไม่สามาถออนไลน์ได้พร้อม ๆ กัน สามารถออกแบบการทดสอบนี้ได้ด้วยบล็อกเชนระบบปิด หรือเครื่องที่เป็นโลคอลโฮสต์เท่านั้น | ไม่สามารถเข้าเกมได้ | ผ่าน |
| 2 | ระบบบล็อกเชนกลับมาทำงาน ณ เวลาใด ๆ | เมื่อระบบที่ทำการทดสอบเปิดตัวหลังจากปิดตัวลง | (1) สามารถเข้าเกมได้<br>(2) ข้อมูลเวลาของผู้เล่นยังมีอยู่เท่าเดิม<br>(3) อีเอ็กซ์พีโทเคนของผู้เล่นมีอยู่เท่าเดิม<br>(4) สกุลเงินดิจิทัลภายในระบบบล็อกเชนสาธารณะที่เลือกใช้มีอยู่เท่าเดิม | ผ่าน |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# บทที่ 6
# การทดลองและผลการทดลอง

## 6.1 การทดลอง

ในงานวิจัยฉบับนี้ ผู้วิจัยได้ออกแบบการทดลองเพื่อทดสอบความเป็นไปได้ของสถาปัตยกรรมที่ทางผู้วิจัยออกแบบในแง่ของการยอมรับจากผู้ใช้งาน โดยผู้วิจัยกำหนดกลุ่มผู้ทดลองจำนวน 120 คน ให้มาเล่นเกมในการทดลองที่ผู้วิจัยออกแบบ ซึ่งผู้วิจัยได้แบ่งผู้ทดลองออกเป็น 4 กลุ่ม กลุ่มละ 30 คน ใช้ระยะเวลาในการทดลองทั้งหมด 14 วัน โดยผู้ทดลองในแต่ละกลุ่มจะต้องเล่นเกม 2 เกม เกมละ 7 วัน ต่อเนื่องกัน ดังนี้

กลุ่มที่ 1 (G1) ในช่วง 7 วันแรก ผู้ทดลองจะต้องเล่นเกม Flappy Bird ก่อน ส่วนอีก 7 วันหลัง ผู้ทดลองจะต้องเล่นเกม Match-three ทั้งนี้ ผู้วิจัยได้บอกให้ผู้ทดลองทราบตั้งแต่วันแรกที่เริ่มการทดลองว่า ผู้วิจัยใช้เทคโนโลยีบล็อกเชนในการทดลอง และระยะเวลาที่ผู้ทดลองใช้ภายในเกมใน 7 วันแรก จะถูกเปลี่ยนให้กลายเป็นอีเอ็กซ์พีโทเคน ซึ่งสามารถนำไปใช้ในการแลกไอเทมหรือความสามารถพิเศษติดตัวในการเล่นเกมที่ 2 ได้

กลุ่มที่ 2 (G2) ในช่วง 7 วันแรก ผู้ทดลองจะต้องเล่นเกม Flappy Bird ก่อน ส่วนอีก 7 วันหลัง ผู้ทดลองจะต้องเล่นเกม Match-three เช่นเดียวกับกลุ่มที่ 1 แต่ในกลุ่มนี้ ผู้เล่นจะไม่ทราบข้อมูลเกี่ยวกับอีเอ็กซ์พีโทเคน และผู้ทดลองจะไม่ได้รับอีเอ็กซ์พีโทเคนเพื่อใช้ในการแลกไอเทมหรือความสามารถพิเศษเหมือนกับกลุ่มที่ 1

กลุ่มที่ 3 (G3) ในช่วง 7 วันแรก ผู้ทดลองจะได้เล่นเกม Match-three ก่อน ส่วนอีก 7 วันหลัง ผู้ทดลองจะได้เล่นเกม Flappy Bird ทั้งนี้ ผู้วิจัยได้บอกให้ผู้ทดลองทราบตั้งแต่วันแรกที่เริ่มการทดลองว่า ผู้วิจัยใช้เทคโนโลยีบล็อกเชนในการทดลอง และระยะเวลาที่ผู้ทดลองใช้ภายในเกมใน 7 วันแรก จะถูกเปลี่ยนให้กลายเป็นอีเอ็กซ์พีโทเคน ซึ่งสามารถนำไปใช้ในการแลกไอเทมหรือความสามารถพิเศษติดตัวในการเล่นเกมที่ 2 ได้

กลุ่มที่ 4 (G4) ในช่วง 7 วันแรก ผู้ทดลองจะได้เล่นเกม Match-three ก่อน ส่วนอีก 7 วันหลัง ผู้ทดลองจะได้เล่นเกม Flappy Bird เช่นเดียวกับกลุ่มที่ 3 แต่ในกลุ่มนี้ ผู้ทดลองจะไม่ทราบข้อมูลเกี่ยวกับอีเอ็กซ์พีโทเคน และผู้ทดลองจะไม่ได้รับอีเอ็กซ์พีโทเคนเพื่อใช้ในการแลกไอเทมหรือความสามารถพิเศษเหมือนกับกลุ่มที่ 3

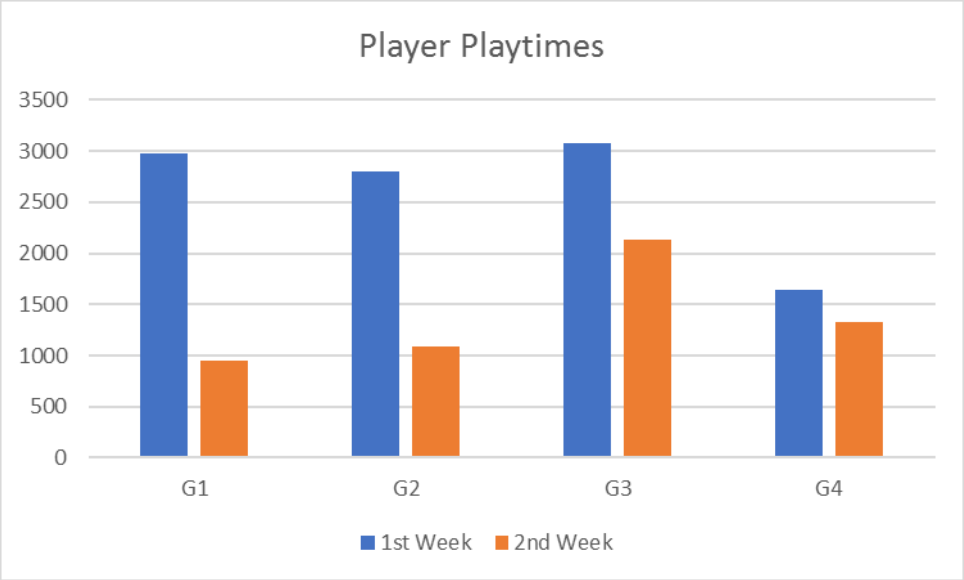
ในการวิจัยนี้ ผู้วิจัยตั้งสมมติฐานว่า ผู้ทดลองที่ทราบถึงการใช้งานบล็อกเชนและอีเอ็กซ์พีโทเคน มีแนวโน้มที่จะใช้เวลาในเกมมากกว่ากลุ่มที่ไม่ทราบ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ในการทดลองนี้ อัตราและวิธีการแลกเปลี่ยนอีเอ็กซ์พีโทเคนจะถูกควบคุมโดยผู้วิจัย เนื่องจากผู้ทดลองส่วนใหญ่ไม่ได้มีพื้นฐานความเข้าใจเกี่ยวกับเทคโนโลยีบล็อกเชน อย่างไรก็ตาม หากระบบสถาปัตยกรรมที่ทางผู้วิจัยนำเสนอถูกนำไปใช้ในวงกว้างในอนาคต ผู้เล่นจะต้องเชื่อมั่นได้ว่าบล็อกเชนโหนดคอมโพเน้นต์หรือบล็อกเชนคอมมิตตี (blockchain committee) จะทำการกำหนดอัตราและวิธีการแลกเปลี่ยนที่เป็นธรรมให้แก่ผู้เล่นภายในระบบนิเวศน์บล็อกเชนนั้น ๆ

### 6.2 ผลการทดลองและวิเคราะห์ผลการทดลอง

ในขณะทำการทดลองนี้ บล็อกเชนสาธารณะที่มีค่าเวลาการขุด (mining time) ต่ำ ๆ นั้นมีมากมาย เพราะฉะนั้นในการออกแบบสถาปัตยกรรม ผู้วิจัยจึงไม่ได้คำนึงถึงค่าเวลาการขุด โดยผู้วิจัยจะพิจารณาเฉพาะระยะเวลาที่ผู้เล่นใช้ภายในเกมเท่านั้น




รูปที่ 41 ผลการทดลอง

รูปที่ 41 แสดงค่าเฉลี่ยเวลาของการเล่นเกม (เป็นวินาที) ของผู้ทดลองในแต่ละกลุ่ม (กลุ่มที่ 1 ถึงกลุ่มที่ 4) โดยแท่งสีฟ้าซ้ายมือจะแสดงถึงระยะเวลาที่ผู้ทดลองใช้ในเกมที่ 1 และแท่งสีส้มขวามือจะแสดงถึงระยะเวลาที่ผู้ทดลองใช้ในเกมที่ 2

จากการทดลองสำหรับกลุ่มที่ 3 และ 4 พบว่าผู้ทดลองในกลุ่มที่ 3 ที่ทราบข้อมูลเกี่ยวกับอีเอ็กซ์พีโทเคน ใช้เวลาในเกมทั้งสองเกม มากกว่ากลุ่มที่ 4 ซึ่งสอดคล้องกับสมมติฐานที่ผู้วิจัยตั้งไว้ว่า ผู้ทดลองที่ทราบข้อมูลเกี่ยวกับอีเอ็กซ์พีโทเคน จะใช้เวลาในเกมมากกว่าผู้ทดลองที่ไม่ทราบ เหตุผล

ประกอบสมมติฐานก็คือ ผู้ทดลองในกลุ่มที่ 3 พยายามเล่นเกมที่หนึ่งเพื่อให้ได้อีเอ็กซ์พีโทเคนมาใช้ในเกมที่สอง และในเกมที่สองนั้น ผู้ทดลองยินดีใช้เวลากับเกมมากกว่ากลุ่มที่ 4 เพราะผู้ทดลองทราบว่าสามารถนำอีเอ็กซ์พีโทเคนไปแลกความสามารถพิเศษติดตัวในเกมที่สองได้ ส่งผลให้ผู้ทดลองในกลุ่มนี้สามารถเล่นเกมไปในจุดที่ไกลกว่า และคะแนนสูงกว่ากลุ่มผู้ทดลองที่ไม่ได้รับความสามารถพิเศษ ทำให้ผู้ทดลองในกลุ่มที่ 3 ใช้เวลาในเกมที่สองมากกว่าผู้ทดลองในกลุ่มที่ 4

อย่างไรก็ตาม ผลการทดลองสำหรับกลุ่มที่ 1 และ 2 กลับไม่เป็นเช่นนั้น เพราะเวลาที่ใช้ในการเล่นเกมของกลุ่มที่ 1และ 2 มีความใกล้เคียงกันมากทั้งสองเกม ผู้วิจัยจึงทำการสอบถามผู้ทดลองเพิ่มเติม พบว่าเกมแรกที่กลุ่มที่ 1 และ 2 ได้เล่นนั้นเป็นเกม flappy bird-like ผู้ทดลองทั้งสองกลุ่มสามารถเล่นได้ง่าย และเริ่มเล่นใหม่ได้เสมอ เวลาที่ใช้เล่นเกมแรกก็เลยสูง แต่สำหรับเกมที่สอง แม้ว่าผู้ทดลองในกลุ่มที่ 1 จะได้อีเอ็กซ์พีโทเคนมาเพื่อแปลงเป็นไอเทมตามเวลาที่ใช้ไป แต่ผู้ทดลองก็ใช้ไอเทมพิเศษนั้นหมดภายในครั้งเดียวที่เล่น ซึ่งทำให้ได้ High score มาอย่างสะดวก ซึ่งการที่ผู้ทดลองจะได้มาซึ่งไอเทมนี้ใหม่อีกครั้งจากการเล่นเกมที่สองนั้น ผู้ทดลองต้องใช้เวลาอย่างมากเพื่อเก็บไอเทมและนำไปใช้เพื่อให้ได้ High score ใหม่ขึ้นมา ผู้ทดลองจึงเบื่อและเลิกเล่นไปในที่สุด ส่งผลให้ใช้เวลาในเกมที่สองน้อย ส่วนกลุ่มที่ 2 ซึ่งไม่ได้ไอเทมมาจากเกมแรก แต่ในเกมมีแจกจ่ายให้เบื้องต้นจำนวนหนึ่ง ค้นพบว่าเมื่อผู้ทดลองใช้ไอเทมหมดไป ก็ต้องไปเก็บไอเทมนี้ใหม่ซึ่งใช้เวลามากเช่นกัน จึงไม่ทำให้ผู้ทดลองกลุ่มที่ 2 อยากจะไปเก็บไอเทมใหม่ และเลิกเล่นไปในที่สุด

ผู้วิจัยได้ทำการทดลองเพิ่มเติมอีก 1 กลุ่ม จำนวน 30 คน เป็นเวลา 14 วัน ลักษณะการทดลองและลำดับการเล่นเหมือนกลุ่มที่ 1 โดยผู้วิจัยทำการตั้งชื่อกลุ่มว่า G5

แต่ได้ทำการทดลองโดยจำกัดการแลกอีเอ็กซ์พีโทเคนให้น้อยลงกว่ากลุ่มที่ 1 เพื่อทดลองว่าการที่ผู้เล่นกลุ่มที่ 1 เล่นน้อยกว่าปกติ อาจจะเป็นเพราะไอเทมที่ได้มาเยอะเกินไปหรือไม่

แต่ผลปรากฏว่าผลการทดลองคล้ายเดิม คือ แม้ว่า High score จะน้อยลงจากไอเทมที่น้อยลง แต่การที่ผู้ทดลองจะกลับไปเล่นเพื่อให้ได้ไอเทมเท่าเดิมนั้น ยังคงต้องใช้เวลาและความพยายามมาก จึงส่งผลให้ผู้ทดลองไม่อยากจะกลับไปทำคะแนนเพิ่มอีก

เหตุที่ผลการทดลองจากกลุ่มที่ 3 เป็นไปตามสมมติฐานนั้น เป็นเพราะไอเทมที่ได้ในเกมที่สองเป็นความสามารถพิเศษติดตัว เพราะฉะนั้นไม่ว่าผู้เล่นจะ Game over สักกี่ครั้ง ความสามารถพิเศษนั้นก็ยังคงอยู่ ส่งผลให้ผู้เล่นมีความรู้สึกอยากเล่นต่อ เพื่อทำลายทั้งสถิติตัวเองและผู้อื่น ต่างจากกลุ่มที่ 1 ที่การได้มาซึ่งไอเทม ไม่ใช่ความสามารถพิเศษติดตัว แต่เป็นไอเทมที่ใช้แล้วหมดไป ซึ่งทำให้ผู้เล่นรู้สึกเบื่อหน่ายและไม่ได้อยากจะเล่นเกมต่อไป

### 6.3 รายละเอียดวิธีการเขียนสมาร์ทคอนแทรค

ในหัวข้อนี้จะกล่าวถึงหลักการสำคัญในการนำสมาร์ทคอนแทรคของผู้วิจัยไปประยุกต์ใช้ โดยเน้นถึงวิธีการเขียนสมาร์ทคอนแทรคของส่วนสำคัญต่าง ๆ เช่น การเก็บเวลา การแลกเวลาเป็นอีเอ็กซ์พีโทเคน การแลกอีเอ็กซ์พีโทเคนเป็นไอเทมภายในเกม การแสดงผลของไอเทม และการใช้งานไอเทมภายในเกม ซอร์สโค้ดทั้งหมด รวมถึงโปรแกรมที่ใช้งานได้จะถูกเก็บไว้ที่ กิตฮับ[41] (GITHUB) ผู้อ่านสามารถตรวจสอบ ทดสอบ และทำตามได้

#### 6.3.1 การเขียนสมาร์ทคอนแทรคของอีเอ็กซ์พีโทเคน

การเขียนสมาร์ทคอนแทรคของอีเอ็กซ์พีโทเคน เพื่อใช้ในเกมนั้นเราใช้หลักการเหมือนเขียนโทเคน ERC-20 และเพิ่มเติมฟังก์ชันที่สำคัญที่ใช้ในการให้มูลค่าเวลาแก่ผู้เล่น โดยผู้วิจัยอธิบายถึงขั้นตอนสำคัญดังนี้

```
mapping (address=>bool) owners; // KEEP TRACK OF OWNERS
```

รูปที่ 42 แสดงการประกาศตัวแปร (Private) ในสมาร์ทคอนแทรคเพื่อเก็บเจ้าของโทเคน

จากรูปที่ 42 แสดงถึงการประกาศตัวแปร owners เพื่อแสดงความเป็นเจ้าของโทเคน ใช้เพื่อจำกัดการใช้งานฟังก์ชันที่จำเป็น

จุฬาลงกรณ์มหาวิทยาลัย

```
modifier onlyOwner(){
  require(msg.sender == owner);
  _;
}
```

รูปที่ 43 แสดงเงื่อนไขการเรียกสมาร์ทคอนแทรคด้วยฟังก์ชัน onlyOwners

[41] อ้างอิงจาก https://github.com/taforyou/thesis-5970145021

จากรูปที่ 43 แสดงให้เห็นถึงการเขียนโมดิฟายเออร์ฟังก์ชัน เพื่อใช้ในการกำหนด ให้คนที่เรียกฟังก์ชันใด ๆ ต้องทำตามเงื่อนไขที่กำหนด โดยในที่นี้นำมาใช้กับฟังก์ชัน mint และ burn ที่ทุกครั้งที่เรียกจะตรวจสอบว่า ผู้ที่เรียกนั้นมีอยู่จริงภายในตัวแปรอาเรย์ของ owners หรือเปล่า

```
function addOwner(address newOwner) public onlyOwners{
  require(owners[newOwner] == false);
  require(newOwner != msg.sender);
  owners[newOwner] = true;
  emit AddOwner(newOwner,newOwnerName);
}
```

รูปที่ 44 แสดงการเพิ่มเจ้าของเหรียญโดยฟังก์ชัน addOwner

จากรูป 44 ทุกครั้งที่มีสมาร์ทคอนแทรคของเกมใหม่ ๆ เพิ่มเข้ามาภายในบล็อกเชน ผู้เป็นเจ้าของสมาร์ทคอนแทรคเหรียญ จะทำการเพิ่มสมาร์ทคอนแทรคของเกมใหม่นั้น เข้าภายในตัวแปร owners เพื่อให้สมาร์ทคอนแทรคของเกมใหม่นั้น สามารถเรียกใช้ฟังก์ชัน mint และ burn ได้

```
function mint(address _to,uint256 _value) public onlyOwners returns(bool){
    totalSupply_  += _value; // TotalSupply ของเหรียญ EXPTOKEN เพิ่มขึ้น
    balance[_to] += _value; // เหรียญของ PlayerComponent เพิ่มขึ้น
    emit Transfer(address(this),_to,_value);
    return true;
}
```

รูปที่ 45 แสดงการประกาศฟังก์ชันในโทเคนสมาร์ทคอนแทรคเพื่อเพิ่มจำนวนโทเคน

จากรูปที่ 45 มีฟังก์ชันชื่อว่ามิ้นท์ (mint) ทำหน้าที่ในการเพิ่มเหรียญอีเอ็กซ์พีโทเคนให้กับผู้เล่น โดยกระทำผ่านสมาร์ทคอนแทรคที่เป็นเจ้าของเหรียญนี้เท่านั้น โดยการส่งตัวแปร address เข้ามา ซึ่งตัวแปร address นี้ก็คือ กระเป๋าเงินสาธารณะ ส่วน _value นั้นคือจำนวนโทเคนดิจิทัลที่ผู้เล่นได้รับ เพราะฉะนั้นก่อนที่สมาร์ทคอนแทรคของนักพัฒนาเกมใด ๆ จะสามารถทำการแลกเหรียญให้ผู้เล่นได้นั้น ผู้ดูแลสมาร์ทคอนแทรคของโทเคนจะต้องทำการเพิ่มสมาร์ทคอนแทรคของนักพัฒนาเกมเข้าไปก่อน จะสังเกตเห็นได้ว่าท้ายฟังก์ชันจะมีคำว่า onlyOwners

```
function burn(address _to,uint256 _value) public onlyOwners returns(bool){
    require(balance[_to] >= _value); // จะแลกได้คนขอแลกเหรียญต้องมีเหรียญถึ
    balance[_to] -= _value; // เหรียญของ PlayerComponent ลดลง
    totalSupply_  -= _value; // TotalSupply ของเหรียญ EXPTOKEN ลดลง
    emit Transfer(address(_to),address(0),_value);
    return true;
}
```

รูปที่ 46 แสดงการประกาศฟังก์ชันในโทเคนสมาร์ทคอนแทรคเพื่อลดจำนวนโทเคน

จากรูปที่ 46 มีฟังก์ชันชื่อว่าเบิร์น (burn) ทำหน้าที่ในการลดเหรียญอีเอ็กซ์พีโทเคนให้กับผู้เล่น โดยกระทำผ่านสมาร์ทคอนแทรคที่เป็นเจ้าของเหรียญนี้เท่านั้น โดยการส่งตัวแปร address เข้ามา ซึ่งตัวแปร address นี้ก็คือ กระเป๋าเงินสาธารณะ ส่วน _value นั้นคือจำนวนโทเคนดิจิทัลที่ลดลงของผู้เล่น

ฟังก์ชันนี้มีหน้าที่ในการลดเหรียญของผู้เล่น ซึ่งจะเกิดขึ้นเมื่อผู้เล่นทำการแลกเปลี่ยนอีเอ็กซ์พีโทเคน ฟังก์ชันนี้จะนำอีเอ็กซ์พีโทเคนไปทำลายทิ้ง โดยกลไกการทำลายทิ้งคือโอนไปให้ address(0) หมายถึงกระเป๋าเงินสาธารณะที่ไม่มีอยู่จริง หรือ ไม่มีข้าวของ โทเคนดิจิทัลก็จะหายไปโดยปริยาย เช่นเดียวกันฟังก์ชันมิ้นท์ ผู้เรียกสมาร์ทคอนแทรคจำเป็นต้องเป็นเจ้าของสมาร์ทคอนแทรคเท่านั้น สังเกตเห็นได้ว่าท้ายฟังก์ชันจะมีคำว่า onlyOwners

### 6.3.2 การเขียนสมาร์ทคอนแทรคของตัวเกม

การเขียนสมาร์ทคอนแทรคของตัวเกม ทำเพื่อวัตถุประสงค์ หลักๆ คือ การเก็บเวลาของผู้เล่น การแลกเปลี่ยนเวลาเป็นอีเอ็กซ์พีโทเคน และ การแลกอีเอ็กซ์พีโทเคนเป็นไปเทมภายในเกม

```
mapping (address=>int) public userFirstGamePlayerTimes ;    // KEEP TRACK OF PLAYER TIMES
mapping (address=>int) public userFirstGameItems;           // KEEP TRACK OF PLAYER ITEMS
```

รูปที่ 47 แสดงการประกาศตัวแปรในสมาร์ทคอนแทรคเพื่อเก็บเวลาและไอเทมของผู้เล่น

จากรูปที่ 47 แสดงถึงการประกาศตัวแปร userFirstGamePlayerTimes เพื่อใช้เก็บเวลาของผู้เล่นภายในเกม และ ตัวแปร userFirstGameItems เพื่อใช้เก็บไอเทมของผู้เล่น ซึ่งในที่นี้ไอเทมอาจจะแสดงถึงเลเวลของผู้เล่นที่เพิ่มขึ้นได้ หรือ อาจจะแทนถึงไอเทมที่ใช้แล้วหมดไป ขึ้นอยู่กับจุดประสงค์ของเกมนั้น ๆ

```
function setPlayerTimes(address _address,int _gameID, int _gameStage,int _gameSeconds,uint256 _gameTimeStamp) public returns(bool) {
        userFirstGamePlayerTimes[_address] = userFirstGamePlayerTimes[_address] + _gameSeconds;
    return true;
}
```

รูปที่ 48 แสดงการประกาศฟังก์ชันในสมาร์ทคอนแทรคเพื่อเพิ่มเวลาของผู้เล่น

จากรูป 48 โดยภายในสมาร์ทคอนแทรค เวลาของผู้เล่นจะเพิ่มขึ้นทุก ๆ ครั้งที่ผู้เล่นมีการเล่นเกมและเรียกฟังก์ชัน setPlayerTimes ซึ่งจะถูกเรียกฟังก์ชันนี้จากเกมไคลเอนต์ โดยจะนำเอา ตัวแปร _address ซึ่งแสดงถึงกระเป๋าเงินสาธารณะของผู้เล่นมาใช้เป็นคีย์ เพื่อ เพิ่มเวลาที่ผู้เล่นได้รับมาจากตัวแปร _gameSeconds ตัวแปรอื่นเช่น _gameID, _gameStage หรือ _gameTimeStamp ไม่ได้สำคัญผู้อ่านอาจจะไม่เรียกใช้ก็ได้

```
contract CoinInterface {
    function mint(address _to,uint256 _value) public returns(bool);
    function burn(address _to,uint256 _value) public returns(bool);
}
```

รูปที่ 49 แสดงการประกาศอินเตอร์เฟส เพื่อเรียกการเพิ่มและลดโทเคนของอีเอ็กซ์พีโทเคน

จากรูปที่ 49 เพื่อเรียกฟังก์ชันการเพิ่มและลดโทเคนให้ผู้เล่น จำเป็นจะต้องประกาศอินเตอร์เฟสภายในสมาร์ทคอนแทรคของนักพัฒนาเกมก่อน จึงสามารถเรียกใช้ได้

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

```
contract FirstGame {
    event Registered(int score,bytes32 hash, string description, address signer);
    event ItemDeduction(int remain,address userWallet);
    CoinInterface _coinInterface;
    address owner;

    constructor() public {
        owner = msg.sender;
        _coinInterface = CoinInterface(0xF1720011f17443F733eDaBAcFe3ddF1493ACAD36);
    }
}
```

รูปที่ 50 แสดงการเชื่อมต่อระหว่างสมาร์ทคอนแทรคของนักพัฒนาเกมคอมโพเน้นต์และอีเอ็กซ์พีโทเคน

จากรูปที่ 50 จะเห็นได้ว่า CoinInterface มีการรับค่า 0xF1720011f17443F733eDaBAcFe3ddF1493ACAD36 ซึ่งในที่นี้คือสมาร์ทคอนแทรคของอีเอ็กซ์พีโทเคนเข้าไป เพื่อเป็นการระบุว่าสมาร์ทคอนแทรคนี้สามารถเรียกใช้ฟังก์ชันของอีเอ็กซ์พีโทเคนได้ ซึ่งในที่นี้คือ ฟังก์ชัน mint และ burn นั้นเอง

```
function exchangePlayerTimesToExpToken(address _address) public returns(bool) {
    require(userFirstGamePlayerTimes[_address] > 0);
    uint256 token = uint256(userFirstGamePlayerTimes[_address] * 1000000000000000000);
    _coinInterface.mint(_address,token);
    userFirstGamePlayerTimes[_address] = 0;
    return true;
}
```

รูปที่ 51 แสดงการประกาศฟังก์ชันในสมาร์ทคอนแทรคเพื่อแลกเวลาของผู้เล่นเป็นอีเอ็กซ์พีโทเคน

จากรูป 51 ผู้เล่นสามารถขอแลกเปลี่ยนเวลาที่ผู้เล่นใช้ไปภายในเกมเป็นอีเอ็กซ์พีโทเคน ได้ โดยทุกครั้งที่เรียกขอเวลาของผู้เล่นภายในเกมจะหายไปทั้งหมด และสะสมได้ใหม่ผ่านการเล่นเกม โดยเมื่อผู้เล่นทำการเรียกคำสั่ง exchangePlayerTimesToExpToken สมาร์ทคอนแทรคเกม จะไปเรียกคำสั่ง mint ของโทเคนสมาร์ทคอนแทรคเพื่อให้ผู้เล่นได้รับโทเคนดิจิทัล โดยเพื่อความง่ายต่อการอธิบายฟังก์ชัน กำหนดให้การเปลี่ยนเวลา 1 หน่วย ต่อ 1 อีเอ็กซ์พีโทเคน

```
function exchangeItemFromExpToken(address _address,int _expcoins,int _toGameID) public returns(bool) {
    require(owner == msg.sender);
    uint256 _change = uint256(_expcoins * 1000000000000000000); // Change เท่าไหร่ user คนนั้นๆ ต้องมีเหรียญด้วย
    require(_coinInterface.burn(_address,_change)); // ต้องทำการเปลี่ยนสำเร็จก่อนจึงจะทำงานบรรทัดต่อไปได้
    userFirstGameItems[_address] = userFirstGameItems[_address] + _expcoins; // ทำการเพิ่ม ITEM ให้กับผู้เล่นคนนั้น ๆ
    return true;
}
```

รูปที่ 52 แสดงการประกาศฟังก์ชันในสมาร์ทคอนแทรคเพื่อแลกอีเอ็กซ์พีโทเคนเป็นไอเทมภายในเกม

จากรูป 52 ผู้เล่นสามารถขอแลกเปลี่ยนอีเอ็กซ์พีโทเคนที่ผู้เล่นมีกับไอเทมภายในเกมได้ โดยทุกครั้งที่ผู้เล่นเรียกฟังก์ชัน exchangeItemFromExpToken จะต้องระบุจำนวนโทเคนที่จะใช้เพื่อที่จะได้รับไอเทมภายในเกมเป็นจำนวนเท่าๆ กัน โดยเพื่อความง่ายต่อการอธิบายฟังก์ชัน กำหนดให้การเปลี่ยนเวลา 1 อีเอ็กซ์พีโทเคน ต่อ 1 ไอเทมที่ผู้เล่นได้รับ หลังจากนั้นสมาร์ทคอนแทรคเกม จะไปเรียกคำสั่ง burn ของโทเคนสมาร์ทคอนแทรคเพื่อทำให้โทเคนดิจิทัลของผู้เล่นลดลง แลกกับไอเทมของผู้เล่น

### 6.4 สรุปการนำสมาร์ทคอนแทรคที่พัฒนาขึ้นไปใช้งาน

ในหัวข้อนี้จะกล่าวถึงสรุปขั้นตอนการนำแนวทางการพัฒนาของผู้วิจัยไปพัฒนาระบบในส่วนของการสร้างโทเคนและการเพิ่มเกมใหม่เข้ามาในระบบ

ตารางที่ 11 สรุปการเขียนสมาร์ทคอนแทรคในการนำไปใช้งาน

| | รายละเอียดในส่วนของสมาร์ทคอนแทรค | รายละเอียด |
|---|---|---|
| 1 | ทำการสร้าง โทเคนดิจิทัล ERC-20 (สมาร์ทคอนแทรคของโทเคน) | ผู้สร้างคนแรกเป็นเจ้าของสมาร์ทคอนแทรค<br>**มีตัวแปรที่สำคัญดังนี้**<br>mapping (address=>bool) public owners |
| 2 | เพิ่มเติมฟังก์ชัน mint (สมาร์ทคอนแทรคของโทเคน) | ให้สิทธิ์เฉพาะเจ้าของสมาร์ทคอนแทรคเท่านั้นที่เรียกได้ |
| 3 | เพิ่มเติมฟังก์ชัน burn (สมาร์ทคอนแทรคของโทเคน) | ให้สิทธิ์เฉพาะเจ้าของสมาร์ทคอนแทรคเท่านั้นที่เรียกได้ |
| 4 | เกมใหม่ที่จะบรรจุลงบล็อกเชน (สมาร์ทคอนแทรคเกม) | **มีตัวแปรที่สำคัญดังนี้**<br>mapping (address=>int) public userFirstGamePlayerTimes<br>mapping (address=>int) public userFirstGameItems<br>**มีฟังก์ชันที่สำคัญดังนี้**<br>function setPlayerTimes<br>function exchangePlayerTimesToExpToken<br>function exchangeItemFromExpToken |
| 5 | นำ Address ของสมาร์ทคอนแทรค ของตัวเกม เพิ่มเป็น Owner ของ ERC-20 (สมาร์ทคอนแทรคเกม) | ทำให้สมาร์ทคอนแทรคของตัวเกมสามารถเรียกฟังก์ชัน mint และ Burn ได้ |
| 6 | เมื่อมีเกมใหม่เข้ามา ทำขั้นตอน 4,5 ซ้ำ (สมาร์ทคอนแทรคเกม) | จะทำให้สามารถมีเกมที่เป็นเจ้าของเหรียญได้ต่อไปไม่มีที่สิ้นสุด |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# บทที่ 7
# สรุปการวิจัยและแนวทางการวิจัยในขั้นถัดไป

## 7.1 สรุปการวิจัยและอภิปรายผลการวิจัย

ผู้วิจัยนำเสนอแนวคิดรูปแบบสถาปัตยกรรมผสมผสาน เพื่อความสะดวกของผู้เล่นและผู้พัฒนาเกมที่ต้องการสร้างเกมที่สามารถส่งผ่านมูลค่าทางเวลาจากตัวเกมไปเก็บไว้ในบล็อกเชน เพื่อนำไปใช้ในเกมอื่น ผู้เล่นไม่จำเป็นต้องมีความรู้เกี่ยวกับบล็อกเชนในการเล่นเกมที่พัฒนาตามสถาปัตยกรรมนี้ เนื่องจากตัวสถาปัตยกรรมทำหน้าที่จัดการกับกุญแจส่วนบุคคลและข้อมูลอื่นที่จำเป็นให้ได้ แต่เมื่อผู้เล่นมีความรู้เกี่ยวกับบล็อกเชนมากขึ้นผู้เล่นสามารถเปลี่ยนมาจัดการข้อมูลเหล่านั้นได้ด้วยตนเอง

ตัวสถาปัตยกรรมบล็อกเชนที่นำเสนอประกอบด้วย สามส่วน คือ เพลเยอร์คอมโพเน้นต์ บล็อกเชนโหนดคอมโพเน้นต์ และนักพัฒนาเกมคอมโพเน้นต์ ซึ่งทำงานร่วมกันในการให้ผู้เล่นเกมได้แลกเปลี่ยนสกุลเงินดิจิตัล เงินสด ERC-20 และไอเทม จากระบบเกม

ผู้วิจัยยังได้นำเสนอแนวคิดการจัดการคิวของบล็อกเชนแทรนแซคชั่น เพื่อให้ผู้เล่นไม่ต้องรอคอลแบ็คอีเว้นท์จากบล็อกเชนโหนดคอมโพเน้นต์

ผู้วิจัยได้พัฒนาระบบต้นแบบขึ้นมาเพื่อเป็นกรณีตัวอย่างสำหรับการพัฒนาตามแนวคิดสถาปัตยกรรมผสมผสาน และเพื่อนำระบบตัวอย่างไปทำการทดสอบการยอมรับของผู้เล่น เกมที่ใช้ในการทดสอบมีสองเกม ซึ่งเป็นเกมคนละประเภทกัน และมีวิธีการแลกมูลค่าทางเวลาไม่เหมือนกัน

ระบบต้นแบบสามารถทำงาน โดยสามารถทำฟังก์ชันที่จำเป็นได้ครบถ้วน ส่วนในการทดสอบการยอมรับจากผู้เล่นนั้น มีการทดสอบการเล่นเป็นเวลา 2 สัปดาห์ โดยแบ่งผู้ทดสอบเป็นสี่กลุ่ม สองกลุ่มให้เล่นเกมในลำดับเดียวกัน อีกสองกลุ่มให้เล่นลำดับกลับกับสองกลุ่มแรก หนึ่งในสองกลุ่มที่เล่นเกมในลำดับเดียวกันได้รับแจ้งว่า สามารถเอาเวลาที่เสียไปในการเล่นเกมไปแลกเป็นของในเกมถัดไปได้

ผลการทดสอบกลับกลุ่มผู้เล่น ได้ความว่า ระบบที่นำเสนอมีแนวโน้มที่จะถูกยอมรับได้ ผู้เล่นมีแนวโน้มใช้เวลาภายในเกมมากขึ้น แต่ทั้งนี้ ลักษณะและชนิดของตัวเกม ไอเทม ความสามารถพิเศษติดตัว หรือแม้แต่การเรียงลำดับการเล่นของเกมนั้น ก็มีผลต่อการยอมรับของผู้เล่นเช่นกัน

โดยหากมีการทดลองกับกลุ่มตัวอย่างเพิ่มเติมและเพิ่มเติมประเภทของเกมที่ใช้ทดสอบ น่าจะทำให้ได้ผลลัพธ์และข้อสรุปที่ชัดเจนขึ้น

นอกจากนี้ ระยะเวลาที่เหมาะสมในการเล่นเกมเกมหนึ่งนั้น อาจจะส่งต่อผู้เล่นเช่นกัน เช่น ผู้เล่นที่เล่นเกมบางประเภทเป็นระยะเวลานาน เช่น เป็นเดือน เป็นปี ไอเทมพิเศษ หรือความสามารถ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

พิเศษติดตัว ที่ได้มาจากอีเอ็กซ์พีโทเคน อาจจะไม่ได้มีผลต่อผู้เล่นมากนัก กล่าวคือ อาจจะช่วยผู้เล่นในช่วงแรก ๆ ของเกม ทำให้ผู้เล่นเปิดใจรับเกมใหม่ ๆ ได้มากขึ้น หากแต่ถ้าเวลาผ่านไปนาน อาจจะไม่มีผลก็เป็นได้

โดยผู้วิจัยได้จำแนกตารางตามลำดับความสำคัญ จากการสำรวจแบบสอบถามและสัมภาษณ์ผู้เล่นเพื่อให้ผู้พัฒนาสามารถใช้เป็นแนวทางในการพัฒนาต่อไปได้

ตารางที่ 12 ปัจจัยที่มีผลต่อเวลาของผู้เล่นที่ใช้ภายในเกม

| | ปัจจัยที่มีผลต่อเวลาในการเล่นเกม | 5 (มีผลมากที่สุด) | 4 (มีผลมาก) | 3 (มีผลบ้าง) | 2 (มีผลน้อย) | 1 (แทบไม่มีผลเลย) |
|---|---|---|---|---|---|---|
| 1 | ความเหมาะสมของอัตราส่วนในการเปลี่ยนเวลาเป็นไอเทม | | ■ | | | |
| 2 | ไอเทมที่ใช้แล้วหมดไป (Fungible Item) | | | | ■ | |
| 3 | ไอเทมที่ใช้แล้วไม่หมดไป (Non-Fungible Item) | ■ | | | | |
| 4 | ลำดับของการเล่นเกม | | ■ | | | |
| 5 | ระยะเวลาที่เหมาะสมในการเล่นเกม (Game Playtimes) | | | | | ■ |

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

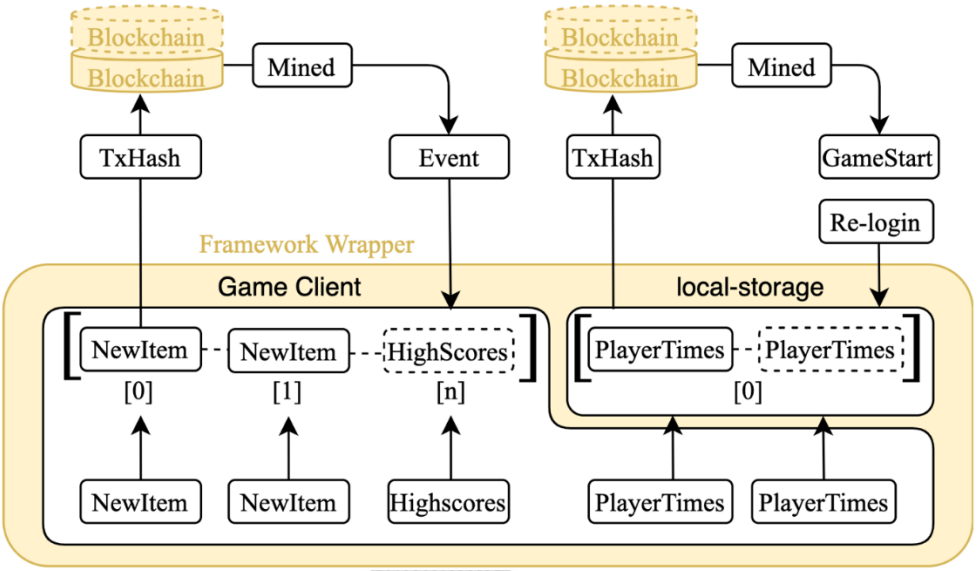
ในเรื่องความสะดวกในการสร้างและการจัดการ กระเป๋าเงินสาธารณะ และ กุญแจส่วนบุคคล นั้น การเปลี่ยนสกุลเงินจากเงิน เป็นคริปโตเคอเรนซี่ เพื่อใช้จ่ายค่าแก๊สในการยืนยันแทรนแซคชั่น และการติดต่อกับบล็อกเชนขณะเล่นเกมก็เป็นสิ่งที่น่าศึกษาต่อไป อย่างไรก็ตาม การจะประเมินทุกองค์ประกอบของระบบนิเวศน์ จำเป็นจะต้องมีจำนวนเกมและระบบต่าง ๆ รองรับให้มากพอ

### 7.2 ข้อจำกัดและข้อเสนอแนะ

กลไกที่เพลเยอร์คอมโพเน้นต์กระทำกับบล็อกเชนโหนดคอมโพเน้นต์ หากสังเกตดูจะพบว่าขณะที่ผู้เล่นเล่นเกมอยู่นั้นอาจจะมีอีเว้นต์ต่าง ๆ เกิดขึ้นมากหรือน้อยสลับกันไปขึ้นกับลักษณะของเกมนั้นๆ แต่ปัญหาจะเกิดขึ้นหากเกมนั้นๆ มีอีเว้นท์ระหว่างเล่นเกมมาก จะทำให้จำนวนอ็อบเจ็คต์ใน

อาร์เรย์มีจำนวนมาก ส่งผลให้ผู้เล่นต้องรอนาน เพราะต้องรอคอลแบคอีเว้นท์จากบล็อกเชนก่อนอ็อบเจ็คต์ใหม่จึงจะถูกส่งขึ้นไปได้

หากจะแก้ด้วยการรออ็อบเจ็คต์จำนวนมาก ๆ ก่อนแล้วค่อยส่งขึ้นไปทีเดียว ก็อาจจะมีปัญหาตามมาเนื่องจากหากจังหวะที่ส่งอ็อบเจ็คต์หลาย ๆ ตัวขึ้นไปทีเดียว หากเครือข่ายอินเตอร์เน็ตไม่เสถียร ก็จะทำให้ข้อมูลของผู้เล่นหายไปเป็นจำนวนมาก เนื่องจากไม่ได้ส่งอ็อบเจ็คต์ขึ้นไปถี่ ๆ




รูปที่ 53 แสดงการแก้ไข Queueing Process

จากรูปที่ 53 ผู้วิจัยขอเสนอแนวทางพัฒนาเพิ่มเติม โดยเอาอีเว้นท์ที่ไม่สำคัญมาก เช่น PlayerTimes (ระยะเวลาการเล่นของผู้เล่นที่ใช้ในเกม) บรรจุไว้ใน Window.localStorage[42] ของเว็บบราวเซอร์ จะทำให้ผู้เล่นไม่ต้องรอแทรนแซคชั่นที่ไม่สำคัญ ทำให้ผู้เล่นไม่ได้รู้สึกว่าต้องรอให้แทรนแซคชั่นเสร็จทั้งหมด โดยจะรอเฉพาะแทรนแซคชั่นที่สำคัญ ๆ เท่านั้น เช่น High Score หรือ New Item เป็นต้น ภายหลังเมื่อผู้เล่นเข้าเกมใหม่อีกครั้ง ก็ให้เอาแทรนแซคชั่นที่เหลือรวมกันแล้ว จัดการขึ้นไปทีเดียว

อย่างไรก็ดี แนวทางนี้อาจจะมีข้อเสียคือ ในครั้งแรกที่เล่นเกม ผู้เล่นก็จะไม่ได้บันทึกเวลาในการเล่นลงบล็อกเชน เวลาถูกบันทึกต่อเมื่อผู้เล่นเข้ามาเล่นเกมครั้งต่อไป (Re-login) ซึ่งอาจจะทำให้เวลาของผู้เล่นครั้งแรกหายไปถ้าผู้เล่นไม่ได้กลับเข้ามาเล่นเกมใหม่ ซึ่งก็เป็นผลดีในแง่หนึ่งเช่นกันที่ว่า

[42] อ้างอิงจาก https://developer.mozilla.org/en-US/docs/Web/API/Window/localStorage

หากผู้เล่นไม่กลับมาเล่น ผู้เล่นก็ไม่ควรได้เวลาของการเล่นไป อีกสิ่งหนึ่งที่ต้องระวังคือ จะต้องมีการระบุเวลาไทม์สแตมป์ (Timestamp) ที่ชัดเจนเพื่อป้องกันการโกงเกม

ในงานวิจัยฉบับนี้ มีประเด็นที่ละไว้ในเรื่องของระบบความปลอดภัย เช่น การเก็บกุญแจส่วนบุคคลไว้ในรูปแบบกรอบอ้างอิง ซึ่งจริง ๆ แล้วอันตรายอย่างมาก เพราะ กุญแจส่วนบุคคลอาจถูกโจรกรรมและอาจหลุดออกไป ส่งผลให้คริปโตเคอเรนซี่ทั้งหมดภายในกระเป๋าเงินสาธารณะถูกขโมยไป และยังรวมถึง ERC20 หรือ อีเอ็กซ์พีโทเคน ก็สามารถถูกขโมยออกไปได้ด้วยเช่นกัน

ซึ่งแนวทางการแก้ไขในปัจจุบัน นิยมใช้กระเป๋าเงินที่ได้รับการยอมรับจาก บล็อกเชนสาธารณะนั้น ๆ หรือ ทำการแยกกระเป๋า เป็นกระเป๋าหลัก และกระเป๋ารอง เพื่อลดความเสี่ยงในการถูกขโมย[43] เป็นต้น

งานวิจัยนี้ยังไม่ได้คำนึงถึงคณะกรรมการเพื่อกำกับดูแลบล็อกเชนโหนด หรือบล็อกเชนโหนดคอมมิตตี ที่เป็นผู้กำกับดูแลกฎต่าง ๆ ภายในระบบนิเวศน์บล็อกเชน ซึ่งเรื่องนี้ต้องคำนึงถึงหลาย ๆ ปัจจัย เช่น หากมีการควบคุมมาก ก็จะขัดกับนิยามของระบบกระจายศูนย์กลางที่ไม่มีใครสามารถควบคุมได้ ประเด็นนี้จึงต้องให้เป็นอำนาจของคณะกรรมการซึ่งมาจากโหนดในระบบ และจะต้องควบคุมระบบเศรษฐศาสตร์ภายในระบบนิเวศน์ให้เหมาะสมอีกด้วย

### 7.3 บทวิเคราะห์การใช้บล็อกเชนสาธารณะกับเกม

จากแนวทางในการนำไปใช้ในข้อ 6.3 ในส่วนนี้พูดถึงการนำบล็อกเชนไปใช้ในเกมของตนเองและในฐานะผู้สร้างระบบนิเวศน์ ที่จะนำเกมใหม่ ๆ เข้ามาสามารถทำได้โดยง่าย เพียงแค่บรรจุสมาร์ทคอนแทรค ของนักพัฒนาเกมคอมโพเน้นต์ ก็สามารถทำให้ผู้เล่นสามารถได้รับอีเอ็กซ์พีโทเคนได้

เพียงแต่การนำไปใช้สำหรับอุตสาหกรรมที่มีผู้เล่นมากแล้วนั้น จำเป็นจะต้องมีการป้องกันผู้เล่นที่ตั้งใจจะใช้ช่องโหว่ของสมาร์ทคอนแทรคในการทำให้ตัวเองได้เปรียบ เช่น การเรียกคำสั่งเพิ่มเวลา สามารถเรียกโดยไม่ผ่านตัวเกมได้เลย ซึ่งทางแก้ไขก็มีอยู่หลายทาง ซึ่งในงานวิทยานิพนธ์ฉบับนี้ไม่ได้ทำในส่วนของการการป้องกันการโกงเกมในลักษณะนี้เอาไว้ หากแต่ให้พึงระวังหากจะนำไปใช้โดยเปิดเผย จะต้องแก้ไขปัญหาในเรื่องนี้ก่อน

ในส่วนของฉันทามติ ฉันทามติปรู๊ฟออฟออธอริทิ ที่ผู้วิจัยเลือกมาใช้ในงานวิจัยฉบับนี้ อาจจะไม่เหมาะสมในการนำไปใช้งานอย่างเปิดเผยมากนัก เนื่องด้วยมีการระบุผู้ที่สามารถยืนยันแทรนแซคชั่น ได้เลย ทำให้เหมือนเป็นการกีดกันกลุ่มผู้ที่ประสงค์จะเข้ามาภายในระบบนิเวศน์บล็อกเชน ซึ่งหากทำเช่นนี้ปัญหาที่เกิดขึ้นก็อาจจะตามมาอีกได้ เช่น การที่กลุ่มบล็อกเชนโหนดร่วมมือกันไม่เปิดโหนด พร้อมๆ กันก็จะสามารถทำได้

---

[43] อ้างอิงจาก https://ethereum.org/en/wallets/

แต่สิ่งที่จำเป็นอย่างยิ่งในการเลือกใช้บล็อกเชนสาธารณะเพื่อมาใช้กับเกม คือ ความเร็วของแทรนแซคชั่นต่อวินาที ซึ่งจำเป็นเป็นอย่างมาก เพราะถึงแม้ว่าจะมีการปรับให้ตัวเกมส่งข้อมูลมาที่บล็อกเชนทีละมาก ๆ แต่ไม่ถี่ หรือ ส่งน้อยครั้ง สุดท้ายแล้ว ผู้เล่นก็จะต้องรอเป็นระยะเวลาหนึ่งอยู่ดี

BLOCKCHAIN COMPARISON

| Network | Speed | Capacity | Fees |
|---|---|---|---|
| ThaiChain | 5 sec | 1300 tps | $0.000002 |
| Bitcoin | 10-60 min | 6 tps | $0.07-$3.50 |
| Ethereum | 1-14 min | 13 tps | $0.01-$0.50 |

รูปที่ 54 แสดงความเร็วโดยเฉลี่ยของแทรนแซคชั่นต่อวินาที และ ค่าใช้จ่ายโดยประมาณสำหรับแต่ละบล็อกเชน[44]

นอกจากความเร็วของแทรนแซคชั่นต่อวินาที แล้ว ยังต้องคำนึงถึงค่าใช้จ่ายที่เกิดขึ้นของผู้เล่นด้วย เพราะผู้เล่นยังเคยชินกับระบบการเล่นแบบไม่เสียค่าเงินใดๆ อยู่ เพราะฉะนั้นเรื่องนี้จำเป็นอย่างยิ่งที่จะต้องคิดให้ละเอียดถี่ถ้วน ซึ่งเหตุผลของการจ่ายค่าแก๊สก็จะสมเหตุสมผลหากผู้เล่นตระหนักและรับรู้ว่าค่าแก๊สที่ตัวเองจ่ายไป เพื่อสิทธิ์ที่จะได้ข้อมูลเป็นของผู้เล่นเอง

อีกทางเลือกหนึ่งที่นิยมใช้กันในบล็อกเชนสาธารณะเพื่อใช้ในเกม และ มีแทรนแซคชั่นต่อวินาที สูงมากคือ บล็อกเชนข้างเคียง (Sidechain) ซึ่งหลักการนี้ผู้วิจัยมองว่าเป็นการแก้ปัญหา แต่นำมาซึ่งอีกปัญหาหนึ่งเพราะหากบล็อกเชนข้างเคียงปิดตัวลงไปก็จะเป็นปัญหาอีกเช่นเดิม

สุดท้ายนี้ผู้วิจัยแนะนำให้เลือกใช้บล็อกเชนสาธารณะที่ใช้ฉันทามติดีลีเกตปรู๊ฟออฟสเตค ด้วยการที่ฉันทามตินี้ตอบโจทย์ในเรื่องของความเร็วและสามารถป้องกันการครอบครองสิทธิ์ในการยืนยันทั้งระบบเพียงแต่ต้องพิจารณาถึงค่าแก๊สและความน่าเชื่อถือของบล็อกเชนสาธารณะนั้น ๆ ที่เลือกใช้ด้วย

[44] อ้างอิงจาก https://exp.tch.in.th/home

**7.4 แนวทางวิจัยในขั้นถัดไป**

ขั้นตอนต่อไปของงานวิจัยที่สามารถทำได้คือ การทดสอบอัตราการแลกเปลี่ยนอีเอ็กซ์พีโทเคนของเกมหลาย ๆ ประเภท เพื่อค้นหาการใช้อีเอ็กซ์พีโทเคนที่ไม่ทำให้สมดุลของเกมเสียไป และยังคงสามารถเพิ่มเวลาในการเล่นของผู้เล่นได้

เนื่องด้วยงานวิทยานิพนธ์ฉบับนี้ ผู้วิจัยเป็นคนกำหนดความเหมาะสมด้วยตนเอง จึงควรทำสมาร์ทคอนแทรคกลางเพื่อมากั้นอีกชั้นหนึ่งระหว่าง สมาร์ทคอนแทรคของผู้พัฒนาเกม และ สมาร์ทคอนแทรคของโทเคนดิจิทัล เพื่อให้ง่ายต่อการจัดการ โดยสมาร์ทคอนแทรคกลางเท่านั้นที่มีหน้าที่ mint และ burn เหรียญ และยังสามารถเป็นสมาร์ทคอนแทรคที่ใช้กำหนดอัตราการแลกเปลี่ยนที่เหมาะสมภายในเกมหนึ่งๆ ด้วย

นอกจากนี้การให้ผู้เล่นสามารถครอบครองไอเทมเข้ารหัส ERC-721 ที่มาจากการเล่นเกม รวมถึงการทดสอบการจัดตั้งตลาดรอง เพื่อรองรับการแลกเปลี่ยนอีเอ็กซ์พีโทเคน หรือไอเทมพิเศษ ERC-721 สำหรับผู้เล่นด้วยกันเอง ก็เป็นสิ่งที่ควรทำการทดสอบเพิ่มเติม

อีกประเด็นหนึ่งที่น่าสนใจ คือ เรื่องของการโกงเกม ตอนนี้สมมติฐานของผู้วิจัยคือ ผู้เล่นจะไม่ทำการโกงเกม ซึ่งในความเป็นจริงนั้นเป็นไปได้ยาก เพราะตัวเกมอยู่ที่ฝั่ง ไคลเอนต์ และการเรียกคำสั่งการได้รับมูลค่าเวลา สามารถสั่งได้จากผู้เล่นโดยตรง แนวทางที่ผู้วิจัยคิดไว้คือ การทำระบบการต่ออายุกุญแจสาธารณะ (Public Key Rolling) ที่ฝังไว้ที่เกมไคลเอนต์ กล่าวคือ ทุก ๆ ครั้งที่ผู้เล่นเล่นเกม จะมีการเซ็นต์แทรนแซคชั่น ด้วยกุญแจสาธารณะ ของ นักพัฒนาเกมคอมโพเน้นต์ ที่ซึ่งอาจจะเปลี่ยนแปลงไปตามเวลา เพราะฉะนั้นหากผู้เล่นทำการโกงและส่งแทรนแซคชั่น ผู้เล่นจะสามารถทำได้แค่เพียงช่วงเวลาหนึ่ง เพราะกุญแจสาธารณะ ที่ใช้ในการเซ็นต์แทรนแซคชั่นนั้นเปลี่ยนไปเรื่อย ๆ ซึ่งแนวคิดนี้ทำให้การพัฒนาปลอดภัยขึ้น แต่ก็แลกมากับความซับซ้อนขึ้นของการพัฒนาระบบ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

# บรรณานุกรม


1. Johnson, D., A. Menezes, and S.J.I.j.o.i.s. Vanstone, *The elliptic curve digital signature algorithm (ECDSA).* 2001. **1**(1): p. 36-63.
2. Preneel, B. *The first 30 years of cryptographic hash functions and the NIST SHA-3 competition*. in *Cryptographers' track at the RSA conference*. 2010. Springer.
3. Rogaway, P. and T. Shrimpton. *Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance*. in *International workshop on fast software encryption*. 2004. Springer.
4. Buterin, V.J.w.p., *A next-generation smart contract and decentralized application platform.* 2014. **3**(37).
5. De Angelis, S., et al., *Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain.* 2018.
6. Zyskind, G. and O. Nathan. *Decentralizing privacy: Using blockchain to protect personal data*. in *2015 IEEE Security and Privacy Workshops*. 2015. IEEE.
7. Maymounkov, P. and D. Mazieres. *Kademlia: A peer-to-peer information system based on the xor metric*. in *International Workshop on Peer-to-Peer Systems*. 2002. Springer.
8. Delmolino, K., et al. *Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab*. in *International conference on financial cryptography and data security*. 2016. Springer.
9. Luu, L., et al. *Making smart contracts smarter*. in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.
10. Min, T., et al. *Blockchain games: A survey*. in *2019 IEEE Conference on Games (CoG)*. 2019. IEEE.
11. Besançon, L., C.F. Da Silva, and P. Ghodous. *Towards Blockchain Interoperability: Improving Video Games Data Exchange*. in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2019. IEEE.


จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

# ประวัติผู้เขียน

| | |
|---|---|
| **ชื่อ-สกุล** | Chanon Yaklai |
| **วัน เดือน ปี เกิด** | 13 July 1985 |
| **สถานที่เกิด** | Bangkok, THAILAND |
| **วุฒิการศึกษา** | Chulalongkorn University |
| **ที่อยู่ปัจจุบัน** | 18 Soi Charansanitwong 52 |



จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY