



**everiToken**

# เอกสารทางเทคนิค

Version 3.1

© 2019, everiToken Public Chain

Zug, Switzerland

## คำสงวนสิทธิ์

- เอกสารทางเทคนิคของ everiToken มีวัตถุประสงค์เพื่อใช้เป็นข้อมูลเท่านั้น
- เอกสารทางเทคนิคนี้ไม่ได้แสดงถึงการรับประกันความคาดหวังของโปรเจกต์
- ข้อกำหนดทางเทคนิคหรือวิธีการทำให้เป็นจริงผ่านเทคโนโลยีที่เขียนในเอกสารนี้อาจถูกเปลี่ยนแปลงได้ตลอดเวลา
- ทีมพัฒนาอาจถูกยกเลิกหรือจัดระเบียบใหม่ได้ตลอดเวลา การสูญเสียบุคลากรหลักด้านเทคนิคอาจส่งผลให้โครงการไม่สามารถพัฒนาได้สำเร็จสมบูรณ์
- เอกสารเทคนิคนี้มีให้ชม "ตามสภาพ" ทีมงานหรือสมาชิกของโครงการขอสงวนสิทธิ์ไม่รับผิดชอบต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการใช้เนื้อหาในเอกสารนี้ในอนาคต
- โทเค็นที่ระบุไว้ในเอกสารทางเทคนิคนี้ไม่มีมูลค่าจริงและมีไว้ใช้เฉพาะในโลกเสมือนจริงเท่านั้น วัตถุประสงค์เดียวของโทเค็นคือใช้เพื่อยืนยันสิทธิ์ผู้ใช้ของโทเค็น
- เหตุการณ์ใด ๆ ที่เกิดขึ้นในบล็อกเชนหรืออนุพันธ์ของบล็อกเชนที่รันโดยใช้เทคนิคที่อธิบายไว้ในเอกสารทางเทคนิคนี้ถูกสร้างขึ้นอัตโนมัติโดยโปรแกรม ทีมงานขอสงวนสิทธิ์ไม่รับผิดชอบต่อผลที่เกิดขึ้น ผลที่เกิดขึ้นจากการใช้งานเป็นความรับผิดชอบของผู้ใช้
- เนื้อหาทั้งหมดที่มีอยู่ในเอกสารทางเทคนิคนี้อาจถูกนำไปใช้เพื่อจุดประสงค์ที่ไม่ใช่เชิงพาณิชย์ ทีมงานขอสงวนสิทธิ์ไม่รับผิดชอบต่อผลกระทบใด ๆ ที่เกิดขึ้นจากการใช้เนื้อหานี้

## สารบัญ

1. ความเป็นมาและวิสัยทัศน์.....	1
การมาถึงของเศรษฐกิจโทเคน.....	1
การวิเคราะห์การแข่งขัน.....	2
บทสรุป.....	6
2. เทคโนโลยีของ everiToken.....	7
สัญญาที่ปลอดภัย (Safe Contract).....	7
ฐานข้อมูล.....	7
โมเดลของโทเคน.....	8
ความปลอดภัย.....	18
ขั้นตอนวิธีฉันทามติ (Consensus Algorithm).....	19
การออกแบบโหนด.....	20
ฟังก์ชันล็อก (Lock Function).....	22
รายละเอียดทางเทคนิคอื่น ๆ.....	22
3. โมเดลเศรษฐกิจ.....	28
ค่าก๊าซ / เชื้อเพลิง (EVT).....	28
EVT ที่ถูกหัก.....	29
การออก EVT ใหม่.....	30
4. ระบบนิเวศ.....	31
เครื่องมือ.....	31
everiWallet.....	31
บริษัท Escrow.....	31
5. บทสรุป.....	33
ทีมผู้ก่อตั้ง.....	34

## 1. ความเป็นมาและวิสัยทัศน์

### การมาถึงของเศรษฐกิจโทเคน

กุมภาพันธ์ 2019 เทคโนโลยีบล็อกเชนมีอายุครบรอบ 10 ปี แม้จะมีวิวัฒนาการหลายรูปแบบในช่วงเวลาที่ผ่านมา คำถามสำคัญ

ที่หลายคนอยากรู้คำตอบยังคงเหมือนเดิม: เทคโนโลยีบล็อกเชนจะเป็นนวัตกรรมที่สร้างคุณค่าให้กับเศรษฐกิจโลกได้จริงหรือไม่?

ลองมาดูข้อมูลปัจจุบันกัน สินทรัพย์ที่ถูกการจัดการบนบล็อกเชนส่วนใหญ่แล้วจะเป็นเหรียญโทเคนหรือสกุลเงินดิจิทัลโดยที่มีมูลค่า

ตลาดรวมอยู่ที่ประมาณ 150 พันล้านเหรียญสหรัฐ สินทรัพย์บนบล็อกเชนเหล่านี้โดยทั่วไปมีความผันผวนสูงและมีโอกาสทั้ง

กำไรสูงซึ่งเป็นเรื่องยากที่จะเป็นประโยชน์ต่อเศรษฐกิจโลก อันที่จริงเริ่มต้นจาก ซาโตชิ นากาโมโตะ ผู้คนมักต้องการให้เหรียญโท

เคนเหล่านี้เป็นสกุลเงินทั่วไปซึ่งสามารถนำมาชำระแทนเงินได้ ณ ขณะนี้เหรียญโทเคนถูกใช้เป็นสกุลเงินดิจิทัลเป็นหลักและยังไม่

ได้ลงมาเล่นบทบาทของสกุลเงินทั่วไป สกุลเงินดิจิทัลเป็นแค่ชื่อเท่านั้นยังไม่ได้ทำหน้าที่เหมือนสกุลเงินที่แท้จริง

ในมุมมองหนึ่งสิทธิในการออกค่าเงินและอำนาจทางการเงินควรจะต้องเป็นของรัฐ ดังนั้นจึงเป็นเรื่องยากที่คริปโตเคอเรนซีจะมา

แทนที่สกุลเงินทั่วไป หากไม่มีการอนุมัติและการสนับสนุนจากรัฐ "สกุลเงินดิจิทัล" เป็นได้เพียงการแสวงหาอุดมคติ

ในอีกมุมมองหนึ่งสินทรัพย์หลักของโลกส่วนใหญ่ (จับต้องได้และจับต้องไม่ได้) ไม่ได้อยู่บนบล็อกเชนและปฏิสัมพันธ์ระหว่าง

บล็อกเชนกับสินทรัพย์ที่ไม่อยู่บนเชนมีขอบเขตจำกัด

ดังนั้นโทเคนเป็นแค่เพียงสกุลเงินดิจิทัลรูปแบบหนึ่งหรือไม่? ไม่เลย ความหมายของโทเคนคือสัญลักษณ์ แต่ควรถือเป็นใบรับรอง

แทนที่จะเป็นสกุลเงินดิจิทัล ใบรับรองเหล่านี้แสดงถึงสิทธิและประโยชน์ต่าง ๆ รวมถึงเต็มสะสม คุปอง บัตรประจำตัวประชาชน

ประกาศนียบัตร อสังหาริมทรัพย์ รหัสผ่าน และใบรับรองสิทธิและผลประโยชน์ต่าง ๆ ถ้ามองย้อนกลับไปในประวัติศาสตร์การ

พิสูจน์สิทธิและผลประโยชน์เป็นส่วนสำคัญของอารยธรรมของสังคมมนุษย์ บัญชี ความเป็นเจ้าของ คุณสมบัติ การพิสูจน์และอื่น ๆ

ล้วนเป็นตัวแทนของสิทธิและผลประโยชน์ทั้งหมด ดังที่ Yuval Noah Harari กล่าวไว้ใน Brief History of

Humankind “ข้อเท็จจริงที่เป็นทั้งเป็นเหตุผลหลักที่ทำให้คนปราชญ์โดดเด่นและสร้างอารยธรรมของมนุษย์” หากการ

พิสูจน์สิทธิและผลประโยชน์เหล่านี้เป็นแบบอิเล็กทรอนิกส์และถูกเข้ารหัสเพื่อพิสูจน์ความถูกต้องและความสมบูรณ์ อารยธรรมของมนุษย์จะมีการปฏิวัตินวัตกรรม เราเรียกปรากฏการณ์นี้ว่าเศรษฐกิจโทเคน

การเก็บใบรับรองบนบล็อกเชนนี้นสร้างรากฐานของความไว้วางใจและเพิ่มความสามารถในการตรวจสอบย้อนกลับของข้อมูลซึ่งเป็นไปไม่ได้บนโครงสร้างพื้นฐานแบบรวมศูนย์แบบดั้งเดิม ดังนั้นหากใบรับรองเป็นหน่วยเศรษฐกิจส่วนหน้าของเศรษฐกิจโทเคน บล็อกเชนนี้นเป็นเทคโนโลยีหลังบ้านของเศรษฐกิจโทเคน ทั้งสองเชื่อมโยงและพึ่งพาซึ่งกันและกัน

## การวิเคราะห์การแข่งขัน

ในฐานะที่เป็นบล็อกเชนสาธารณะที่ถูกสร้างขึ้นเพื่อเศรษฐกิจโทเคน everiToken มีคู่แข่งหลักสองรายคือ Ethereum และ EOS ความได้เปรียบทางการแข่งขันของเราจะชัดเจนขึ้นเมื่อเราวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและภัยคุกคามในตลาดของเรา

## SW (จุดแข็งและจุดอ่อน) :

everiToken เชื่อว่าเทคโนโลยีบล็อกเชนสำหรับเศรษฐกิจโทเคนควรที่จัดการพิสูจน์สิทธิและผลประโยชน์ได้อย่างมีประสิทธิภาพซึ่งโดยหลัก ๆ เกี่ยวข้องกับสามด้านต่อไปนี้:

1. ใบรับรองสิทธิและผลประโยชน์ดิจิทัล: ใบรับรองจะต้องอยู่ในรูปแบบดิจิทัลที่เชื่อถือได้และต้องมีการรับรองโดยสิ่งของที่มีมูลค่าที่แท้จริง
2. การจัดการสิทธิ์ที่ปลอดภัยและเข้ารหัส: ใบรับรองจะต้องถูกตรวจสอบได้ สามารถป้องกันจากการฉ้อโกงและ ป้องกันความเป็นส่วนตัว และถูกควบคุมดูแลได้ การจัดการสิทธิ์ของ everiToken ถูกป้องกันโดยวิทยาการเข้ารหัสลับแลใบรับรองใช้ได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
3. สภาพคล่อง: ใบรับรองสามารถถูกแลกเปลี่ยนได้อย่างสะดวกและรวดเร็ว

ตามข้อกำหนดข้างต้นเราได้เสนอชุดการแก้ปัญหาเพื่อตอบสนองความต้องการขั้นพื้นฐานของเศรษฐกิจโทเคนเพื่อส่งเสริมการไหลเวียนและการจัดการของโทเคนและวางรากฐานทางเทคนิคสำหรับเศรษฐกิจโทเคน ตามข้อกำหนดข้างต้นเราได้บรรลุคุณสมบัติหลักสามประการต่อไปนี้:

- การออกโทเคนที่สะดวกและรวดเร็ว: ผู้ใช้สามารถออกโทเคนของตนเองได้อย่างง่ายดายผ่าน API ของเราโดยที่ไม่จำเป็นต้องเขียนโค้ด (สำหรับแอป เว็บเพจ หรือแอปพลิเคชันบุคคลที่สาม)
- การถ่ายโอนโทเคนอย่างมีประสิทธิภาพ: ระบบสามารถถ่ายโอนโทเคนจำนวนนับร้อยล้านอันพร้อมกันภายในไม่กี่วินาที
- ระบบการจัดการสิทธิ์ที่ยืดหยุ่น: ระบบที่เรียบง่ายง่ายต่อการจัดการสิทธิ์ สามารถรองรับความต้องการที่ซับซ้อนเช่นการถือสิทธิ์ร่วม การกู้คืนสิทธิ์ อำนาจหลายระดับ การปฏิบัติตามกฎระเบียบของรัฐบาล โดยที่ไม่จำเป็นต้องเขียนโปรแกรมเพิ่มเติม

เราลองเอา everiToken มาเปรียบเทียบกับ Ethereum และ EOS กัน:

### Ethereum: ERC20/ERC721

วิธีหลักในการบรรลุเศรษฐกิจโทเคนด้วย Ethereum คือการพัฒนาสัญญาอัจฉริยะที่ใช้โปรโตคอล ERC20 และ

ERC721 ERC20 เป็นมาตรฐานที่ทำให้โทเคนทดแทนกันได้ (Fungible Token) และ ERC721 เป็น

มาตรฐานที่ทำให้โทเคนนั้นมีความเฉพาะตัวไม่สามารถทดแทนกันได้ (Non-Fungible Token) อย่างไรก็ตามมีปัญหาหลายประการหลายอย่างที่ไม่ควรมองข้าม:

- **TPS:** ณ ขณะนี้ Ethereum สามารถรองรับได้ประมาณ 10 กว่าธุรกรรมต่อวินาทีเท่านั้นซึ่งไม่สามารถตอบสนองความต้องการที่แท้จริงของการหมุนเวียนของโทเคนได้
- การใช้จ่าย: การดำเนินการตามสัญญาอัจฉริยะต้องมีค่าก๊าซสำหรับทุกขั้นตอน สำหรับฟังก์ชันที่มีลอจิกทางธุรกิจที่ซับซ้อน (เช่นการถือสิทธิ์หลายคน การกำกับดูแล ฯลฯ ) ค่าใช้จ่ายอาจจะสูงและไม่สามารถถูกควบคุมได้
- แพร่หลาย: การบรรลุเศรษฐกิจโทเคนด้วย Ethereum นั้นขึ้นอยู่กับสัญญาอัจฉริยะซึ่งไม่สามารถเข้าถึงได้สำหรับผู้ที่ไม่ใช่ นักพัฒนาโดยไม่ใช้แอปพลิเคชันของบุคคลที่สาม การซับซ้อนของสัญญาอัจฉริยะสร้างความกังวลด้านความปลอดภัยและกฎระเบียบซึ่งทำให้การแพร่หลายให้คนยอมรับเป็นจำนวนมากเป็นเรื่องยาก

- ไม่มีมาตรฐาน: เนื่องจากสัญญาอัจฉริยะที่แตกต่างกันอาจใช้แนวคิดการพัฒนาที่แตกต่างไปอย่างสิ้นเชิง metadata ของโทเค็นเหล่านี้จึงไม่สามารถทดแทนกันได้จึงถูกแยกออกมาไม่รวมกัน สิ่งนี้ไม่เอื้อต่อการพัฒนาระบบเศรษฐกิจโทเค็น นอกจากนี้ยังทำให้ผู้ใช้ไม่สามารถสืบหาข้อมูลจากโทเค็นประเภทต่าง ๆ ที่พวกเขาเป็นเจ้าของได้

## EOS

EOS เปิดตัว mainnet ในเดือนมิถุนายนปี 2018 เป้าหมายหลักของ EOS คือการแก้ไขปัญหของ Ethereum อย่างไรก็ดีตามปัญหาใหม่ ๆ ก็ได้เกิดตามขึ้นมา

- ความปลอดภัย: โทเค็นสามารถเป็นหน่วยตัวแทนของสินทรัพย์ที่มีมูลค่าสูงและไม่สามารถสร้างใหม่ได้ดังนั้นจึงเป็นสิ่งสำคัญมากที่ระบบจะไม่มีปัญหาด้านความปลอดภัย การปลอดภัยของสัญญาอัจฉริยะนั้นอยู่ที่ระดับความสามารถของนักพัฒนา การตรวจสอบให้แน่ใจว่านักพัฒนาโทเค็นตระหนักด้านความปลอดภัยเพียงพอหรือไม่เป็นเรื่องที่ยากมากสัญญาอัจฉริยะของ EOS ใช้ WebAssembly ซึ่งค่อนข้างใหม่และอยู่ในช่วงทดสอบเบต้า นอกจากนี้สัญญาอัจฉริยะของ EOS ทัวริงสมบูรณ์และมีอำนาจมากเกินไปซึ่งอาจทำให้มีช่องโหว่ด้านความปลอดภัยโดยที่นักพัฒนาไม่ได้ตั้งใจคนส่วนใหญ่ไม่สามารถเขียนสัญญาอัจฉริยะที่ปลอดภัยได้ในการสร้างและถ่ายโอนโทเค็นผู้ใช้จะต้องพึ่งพาแอปพลิเคชันของบุคคลที่สามและต้องเชื่อถือในโค้ดของบุคคลที่สามนั้น ดังนั้นการควบคุมสินทรัพย์ไม่ได้อยู่ในมือของผู้ใช้แต่อยู่ในมือของบุคคลที่สาม
- ไม่มีมาตรฐาน: เช่นเดียวกับ Ethereum สัญญาอัจฉริยะมี metadata ที่แตกต่างกันซึ่งทำให้สัญญาอัจฉริยะนั้นยากที่จะปฏิสัมพันธ์และทำงานร่วมกัน
- การควบคุมดูแล ความเชื่อใจและความถูกต้องตามกฎหมาย: การกำกับดูแลโปรแกรมบนบล็อกเชนนั้นเป็นเรื่องยากสำหรับรัฐบาลเนื่องจากต้องมีความเชี่ยวชาญด้านเทคนิคเพื่อที่จะอ่านโค้ดที่ไม่มีมาตรฐาน นอกจากนี้ผู้ที่ไม่ใช่นักพัฒนาซอฟต์แวร์ยากที่จะตัดสินใจว่าพวกเขาสามารถเชื่อถือโปรแกรมที่เกี่ยวข้องได้หรือไม่ นี่เป็นเหตุผลที่ทำให้โปรแกรมบนบล็อกเชนนั้นยากที่จะได้รับการยอมรับจากประชาชนทั่วไปและรัฐบาล

- ประสิทธิภาพในการดำเนินการ: เพื่อตอบสนองความต้องการที่หลากหลายฟังก์ชันสัญญาอัจฉริยะของ EOS นั้นซับซ้อน โมดูลระบบมีมากมายและการกำหนดเวลาและการกระจายทรัพยากรนั้นเป็นเรื่องยาก โดยรวมสิ่งเหล่านี้เพิ่มความซับซ้อนของระบบและลดความเร็วของการดำเนินการ เนื่องจากความขัดแย้งที่อาจเกิดขึ้นกับข้อมูลและฟังก์ชันต่าง ๆ การใช้ multi-thread เพื่อเพิ่มความเร็วไม่ใช่เป็นเรื่องง่ายและค่าใช้จ่ายในการจัดการเวลาที่สูง อย่างไรก็ตามสำหรับเศรษฐกิจโทเค็นฟังก์ชันที่ซับซ้อนเหล่านี้มีความสำคัญและต้องการหาทางแก้ไขปัญหาลำดับนี้ในอนาคต
- ยากที่จะแพร่หลาย: ความต้องการทางธุรกิจของเศรษฐกิจโลกมักมีความซับซ้อนและแปรปรวนขาดความมั่นคง การพัฒนาและทดสอบสัญญาอัจฉริยะต้องใช้เวลาซึ่งทำให้ยากต่อการตอบสนองความต้องการของตลาดต่าง ๆ ในช่วงเวลาสั้น ๆ สิ่งนี้จึงเป็นอุปสรรคต่อการพัฒนาเศรษฐกิจโทเค็น

ข้อแตกต่างที่สำคัญระหว่าง everiToken และบล็อกเชนอื่น ๆ คือ everiToken ใช้สัญญาที่ปลอดภัยในขณะที่อื่นใช้สัญญาอัจฉริยะ นี่หมายความว่า everiToken ไม่ทั่วถึงสมบูรณ์และอาจจะมีบางสถานการณ์ซับซ้อนของแอปพลิเคชันที่ everiToken ไม่สามารถรับรองได้ อย่างไรก็ตาม everiToken สามารถตอบสนองความต้องการของเศรษฐกิจโทเค็นได้อย่างมากถึง 99% everiToken เป็นบล็อกเชนสาธารณะที่ปลอดภัยที่สุด คู่ค้าที่สุดและใช้ง่ายสำหรับทุกคนทั่วโลก

## OT (โอกาสและภัยคุกคาม)

นอกเหนือจากจุดแข็งของ everiToken แล้วเราได้สร้างมาตรฐาน EvtLink ซึ่งใช้ในการเชื่อมต่อผู้ชำระเงินและผู้รับเงินผ่านช่องทางข้อมูลที่หลากหลายเช่น NFC, Bluetooth และ QR Code สร้างบนพื้นฐานของ EvtLink everiPay เป็นโปรโตคอล micropayment แบบ face-to-face ที่ใช้บล็อกเชนสาธารณะ everiToken เป็นโครงสร้างพื้นฐานหลักและโปรโตคอล everiPass ตรวจสอบความเป็นเจ้าของของโทเค็น

everiPay / everiPass ประกอบด้วยมาตรฐานของการสร้างรหัส QR และค่านิยมของโปรโตคอลการสื่อสาร ด้วยนวัตกรรมของเรา ระบบของเรามีจุดเด่นดังนี้:

- การชำระบัญชีทันที: การทำธุรกรรมคือการชำระบัญชี
- การกระจายอำนาจ: การชำระเงินแบบ P2P ไม่มีแพลตฟอร์มกลาง ไม่มีใครสามารถแก้ไขข้อมูลบนบล็อกเชนได้และผู้ใช้ทุกคนสามารถเข้าร่วมในการกำหนดราคาได้



- ความปลอดภัยสูง: ข้อมูลและเนื้อหาภายในบล็อกเชนไม่สามารถถูกปลอมแปลงหรือดัดแปลงได้ซึ่งเพิ่มความปลอดภัยของทรัพย์สินของผู้ใช้
- รองรับหลายรูปแบบ: รับรองโทเค็นทั้งหมดที่ได้รับการรับรองบน everiToken รวมถึงสกุลเงิน คະแนนและแม้แต่กุญแจเพื่อเปิดประตู คุณสามารถใช้งานได้เกือบทุกที่เพียงแคมีโทรศัพท์
- ความสะดวกสูง: แม้ว่า你可能ไม่สามารถเชื่อมต่ออินเทอร์เน็ตอยู่ คุณยังสามารถทำธุรกรรมได้

หัวข้อเด่นของ everiPay / everiPass ทำให้เราสามารถให้บริการระบบตรวจสอบความเป็นเจ้าของของโทเค็น

และระบบชำระเงินแบบ face-to-face ที่ใช้งานง่าย ปลอดภัยที่สุดและสะดวกที่สุด

## บทสรุป

ภัยคุกคามยังคงมีอยู่ อย่างที่กล่าวไว้ Ethereum และ EOS เป็นบล็อกเชนสาธารณะที่ยืดหยุ่นสำหรับการเฉพาะ

บางอย่างภายในเศรษฐกิจโทเค็น อย่างไรก็ตามปัญหาที่ยิ่งใหญ่ที่สุดสำหรับ Ethereum / EOS คือการเข้าถึงยากสำหรับผู้ใช้

เนื่องจากธรรมชาติของสัญญาอัจฉริยะ เราได้แก้ไขปัญหานี้ด้วยการพัฒนาสัญญาที่ปลอดภัยและในตอนนี้ everiToken พร้อมทั้ง

จะสนับสนุนเศรษฐกิจโทเค็นทั่วโลกสำหรับทุกคน

จากการวิเคราะห์ข้างต้นเราได้ออกแบบแนวคิดใหม่ที่เหมาะสมสำหรับแอปพลิเคชันส่วนใหญ่บนบล็อกเชนและได้เสนอบล็อกเชน

สาธารณะและระบบนิเวศที่มีชื่อว่า everiToken เพื่อส่งเสริมการพัฒนาเศรษฐกิจโทเค็น สินทรัพย์ ใบรับรองและบัตรกำนัลใน

โลกแห่งความเป็นจริงสามารถนำมาแปลงเป็นโทเค็นและสามารถใช้งานได้อย่างง่ายดายโดยมีความปลอดภัยและความเร็วที่สูง

## 2. เทคโนโลยีของ everiToken

### สัญญาที่ปลอดภัย (Safe Contract)

ในทางทฤษฎีแล้วสัญญาอัจฉริยะเป็นวิธีที่มีประสิทธิภาพในการอำนวยความสะดวกในการแลกเปลี่ยนสินค้าหรือบริการแบบกระจายอำนาจโดยไม่จำเป็นต้องมีตัวกลาง อย่างไรก็ตามในทางปฏิบัติ ช่องโหว่ความปลอดภัยที่หลากหลายในสัญญาอัจฉริยะสามารถนำไปสู่การรันคำสั่งที่ไม่เหมาะสมหรือข้อผิดพลาดเชิงตรรกะที่นำไปสู่การลอบขโมย การรั่วไหลของการเข้าถึง การยกเลิกบริการและอื่น ๆ ดังนั้นสัญญาอัจฉริยะมักจะล้มเหลวในการให้ความเชื่อถือที่เพียงพอกับผู้ใช้และอาจถูกมองว่ามีความน่าเชื่อถือน้อยกว่าสัญญาแบบดั้งเดิม

everiToken เสนอแนวคิดใหม่ที่เรียกว่าสัญญาที่ปลอดภัย ผู้ใช้สามารถใช้อินเตอร์เฟซของสัญญาที่ปลอดภัยเพื่ออำนวยความสะดวกในการสร้างและโอนโทเคนอย่างรวดเร็วและปลอดภัยโดยไม่จำเป็นต้องเขียนโค้ดโดยตรง สัญญาที่ปลอดภัยลดความซับซ้อนของฟังก์ชันให้เหลือแต่ตามข้อกำหนดหลัก ซึ่งทำให้มั่นใจได้ว่าธุรกรรมบนบล็อกเชนทั้งหมดปลอดภัยและไม่มีช่องโหว่เนื่องจากฟังก์ชัน API ทุกอย่างได้รับการตรวจสอบเป็นอย่างดี ถึงแม้ว่าสัญญาที่ปลอดภัยจะไม่แท้จริงสมบูรณ์ ฟังก์ชันส่วนใหญ่ที่ต้องการสามารถทำได้บนสัญญาที่ปลอดภัยโดยการเรียก API นอกจากนี้สัญญาที่ปลอดภัยยังทำให้สามารถทำธุรกรรมเกี่ยวกับโทเคนแบบออฟไลน์ได้อีกด้วย

สัญญาที่ปลอดภัยยังเพิ่มความสะดวกในการเข้าถึงและ TPS ในส่วนของการเข้าถึง API ทำให้ง่ายต่อการประสานกับเวิร์กโฟลว์ที่มีอยู่โดยไม่ต้องเขียนโค้ดใหม่ ในส่วนของ TPS การใช้ API ทำให้สามารถแยกประเภทตัวแปลได้ ซึ่งทำให้ข้อมูลชนิดต่าง ๆ ชัดเจนและระบบรู้ว่าควรดำเนินการจัดการกับข้อมูลยังใดถึงจะสามารถดำเนินการแบบขนานได้โดยที่ไม่ขัดแย้งกันเพื่อเพิ่มความเร็วของระบบ (วัดได้ 10,000 TPS ในเดือน ธันวาคม 2018)

### ฐานข้อมูล

EOS ใช้ฐานข้อมูลในหน่วยความจำแบบ Boost.MultiIndex (Chainbase) ที่รองรับการทำงานย้อนกลับ ผลลัพธ์ของการดำเนินการตามคอนแทรคทั้งหมดจะมีอยู่ในฐานข้อมูลในหน่วยความจำ เพื่อสนับสนุนการย้อนกลับเมื่อมีการ fork หรือการกู้คืนข้อมูลคอนแทรคทำงานผิดปกติ มีความจำเป็นต้องบันทึกข้อมูลเพิ่มเติมทุกการดำเนินการเพื่อรองรับการย้อนกลับ นอก

จากนี้ข้อมูลทั้งหมดจะถูกจัดเก็บและประมวลผลในฐานข้อมูลในหน่วยความจำ เมื่อเวลาผ่านไป เป็นเรื่องปกติที่ผู้ใช้และการทำธุรกรรมจะเพิ่มขึ้น เลขเป็นที่คาดการณ์ว่าความต้องการหน่วยความจำจะเพิ่มขึ้นอย่างมาก ซึ่งจะส่งผลให้ความต้องการหน่วยความจำจากผู้ผลิตบล็อกสูง นอกจากนี้หากโปรแกรมขัดข้องหรือรีสตาร์ท ข้อมูลหน่วยความจำจะมีการสูญเสีย ในการกู้คืนข้อมูลเราจะต้องทำซ้ำการดำเนินการทั้งหมดในบล็อกซึ่งต้องใช้ระยะเวลา

ในขณะที่รักษฐานข้อมูลในหน่วยความจำของ EOS เราได้พัฒนาฐานข้อมูลโทเ็นโดยใช้ RocksDB ซึ่งมีประโยชน์หลายประการดังนี้:

- RocksDB เป็นฐานข้อมูลแบบ key-value ระดับอุตสาหกรรม ซึ่งได้รับการตรวจสอบอย่างสมบูรณ์และใช้ในกลุ่มหลักของ Facebook
- RocksDB ถูกพัฒนาต่อจาก LevelDB มีประสิทธิภาพและการทำงานที่ดียิ่งขึ้น นอกจากนี้ยังช่วยเพิ่มประสิทธิภาพของการจัดเก็บข้อมูลบนอุปกรณ์ที่มีความหน่วงต่ำ เช่น Flash หรือ SSD
- หากจำเป็น RocksDB สามารถใช้เป็นฐานข้อมูลในหน่วยความจำ
- RocksDB รองรับการย้อนกลับไปเวอร์ชันเก่า ๆ และการเก็บข้อมูลแบบระยะยาว อีกทั้งยังแทบจะไม่มีผลเสียต่อประสิทธิภาพของระบบเก็บข้อมูล

ฐานข้อมูลโทเ็นของเราใช้ RocksDB เป็นเครื่องมือจัดเก็บข้อมูล เราได้เพิ่มประสิทธิภาพของการดำเนินงานโทเ็นอย่างเต็มที่เพื่อเพิ่มประสิทธิภาพของทั้งระบบ ด้วยเทคโนโลยีนี้เราสามารถย้อนกลับไปรุ่นก่อนได้ด้วยต้นทุนที่ต่ำกว่าเดิม นอกจากนี้ฐานข้อมูลโทเ็นยังรองรับฟังก์ชันเสริม เช่น การเก็บข้อมูลระยะยาว การสำรองข้อมูลเชิงปริมาณและการสำรองข้อมูลเพิ่มเติมเพื่อแก้ไข

## ปัญหาเช่น cold startup

เนื่องจากการดำเนินการใน everiToken มีระดับนามธรรมสูง โค้ดจึงสามารถอยู่ในสถานะคงที่และข้อมูลที่จำเป็นสำหรับการดำเนินการแต่ละครั้งมีเพียงเล็กน้อย ดังนั้นความซ้ำซ้อนของข้อมูลจึงต่ำมากเมื่อเทียบกับระบบทั่วไปเช่น EOS ซึ่งช่วยลดขนาดของบล็อก

## โมเดลของโทเ็น

### ภาพรวม

everiToken ถือกำเนิดขึ้นเพื่อเศรษฐกิจโทเคนและมีเอกลักษณ์เฉพาะด้วยวิธีการจัดการโทเคน โทเคนในที่นี้แตกต่างจากสกุลเงินดิจิทัล (digital currency) ที่ออกโดยธนาคารกลางและสกุลเงินเข้ารหัส (cryptocurrency เช่น Bitcoin หรือ ETH) เรากำหนดให้โทเคนเป็นหลักฐานว่าคุณมีส่วนแบ่งทางเศรษฐกิจแบบเอกสิทธิ์ในสินทรัพย์ ระยะเวลา สถานที่เฉพาะหรือบริการตามเวลาที่จัดทำโดยนิติบุคคลเฉพาะ โทเคนนั้นแบ่งออกเป็นสองประเภท: โทเคนที่ทดแทนกันได้ (FTs) และโทเคนที่ไม่สามารถทดแทนกันได้ (NFT) สองประเภทนี้มีความแตกต่างบางประการในโครงสร้างและการใช้งานในแอปพลิเคชัน จากการวิเคราะห์ของเรา โทเคนที่ไม่สามารถทดแทนกันได้มีบทบาทมากกว่าในระบบเศรษฐกิจโทเคน ดังนั้นเราจะเริ่มวิเคราะห์โทเคนที่ไม่สามารถทดแทนกันได้ก่อน

## โทเคนที่ไม่สามารถทดแทนกันได้ (NFT - Non-Fungible Tokens)

ก่อนที่จะทำความเข้าใจโทเคนที่ไม่สามารถทดแทนกันได้ นั้นให้ลองนึกถึงก้อนหินจำนวนมากบนชายหาด ในโลกแห่งความเป็นจริง หินทุกก้อนบนชายหาดมีน้ำหนัก รูปร่างและประเภทที่แตกต่างกัน ไม่มีหินสองก้อนที่เหมือนกันทุกอย่าง นอกจากนี้หินพวกนี้ไม่สามารถรวมเข้าด้วยกันเป็นหนึ่งได้ ดังนั้นเราจึงบอกว่าหินทุกก้อนแบ่งแยกไม่ได้และไม่สามารถรวมเข้าด้วยกันได้ มาดูตัวอย่างในโลกของบล็อกเชนกัน CryptoKitties ครั้งหนึ่งเคยเป็นเกมยอดนิยมในโลกแห่งบล็อกเชน แมวแต่ละตัวมีหมายเลขและคุณลักษณะที่ไม่ซ้ำกัน NFT นั้นเปรียบเสมือนก้อนหินหรือแมวบน CryptoKitties มันมีความแตกต่างและเอกลักษณ์ในโลกแห่งความเป็นจริงเช่นเดียวกับ NFT ในระบบของเรา

โดยทั่วไปแล้ว NFT ถูกแบ่งออกเป็นประเภทต่าง ๆ ตามคุณลักษณะที่แตกต่างกันและถูกจัดเข้าโดเมนที่มีประเภทที่คล้ายกัน การเจาะจงที่โทเคนช่วยให้ everiToken มีคุณสมบัติมาตรฐานสูง โทเคนที่ถูกสร้างขึ้นเองทั้งหมดโดยผู้ใช้ใช้โครงสร้างเดียวกันทั้งหมด โทเคนแต่ละตัวจะมีชื่อโดเมนหนึ่งชื่อซึ่งสอดคล้องกับโดเมนเฉพาะที่โทเคนอยู่ ผู้สร้างโทเคนต้องกำหนดชื่อโทเคนซึ่งจะต้องไม่ซ้ำกันภายในโดเมนเดียวกัน ชื่อโทเคนมักจะหมายถึงความหมายพิเศษบางอย่าง ตัวอย่างเช่น บาร์โค้ดของผลิตภัณฑ์สามารถใช้เป็นกฎการตั้งชื่อ ในบาร์โค้ดมีข้อมูลเกี่ยวกับประเทศต้นทางและผู้ผลิตของผลิตภัณฑ์ ความเป็นเอกลักษณ์ของแต่ละโทเคนนั้นพิจารณาจากชื่อโดเมนพร้อมกับชื่อโทเคน นอกจากนี้ยังมีข้อมูลเกี่ยวกับความเป็นเจ้าของของโทเคนและโทเคนแต่ละตัวต้องมีเจ้าของอย่างน้อยหนึ่งราย

ดังกล่าวข้างต้น ID ของแต่ละโทเคนถูกกำหนดให้ไม่ซ้ำกันโดยใช้ชื่อโดเมนและชื่อโทเคน โครงสร้างพื้นฐานของโทเคนแสดงใน

รูปที่ 1 ด้านล่าง นอกจากโทเคน ID แล้วโครงสร้างยังแสดงถึงเจ้าของโทเคนและข้อมูลอื่น ๆ ที่จำเป็น

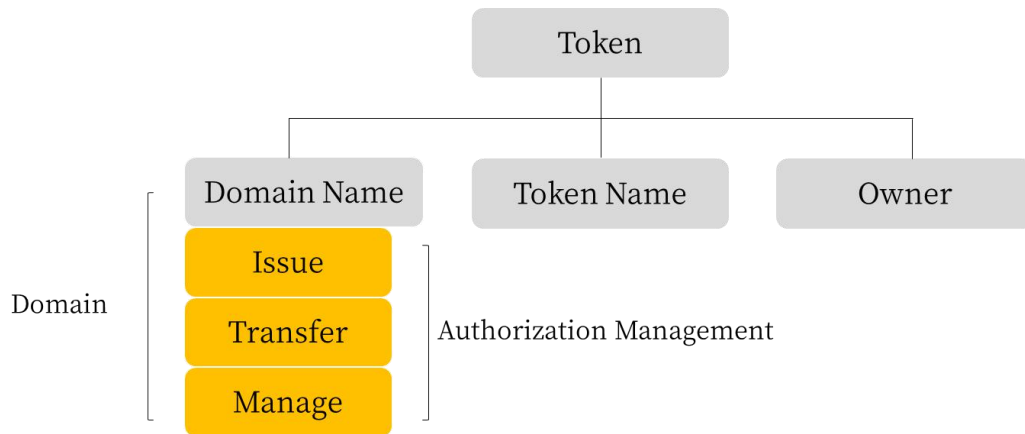


Figure 1. โครงสร้างของโทเคนใน everiToken

ผู้ใช้สามารถใช้ชื่อโดเมนในการสอบถามรายละเอียดเพิ่มเติมเกี่ยวกับโดเมนนั้น แต่ละโดเมนยังจะแสดงข้อมูลการจัดการสิทธิ์ที่เกี่ยวข้อง

ข้อด้วย

ทุกคนมีสิทธิ์ในการสร้างและออกโทเคนของตนเอง โทเคนเองนั้นไม่มีมูลค่า ผลประโยชน์ของการถือโทเคนนั้นรับรองโดยเครดิต

ของผู้สร้าง เมื่อออกโทเคนใหม่แล้วสามารถโอนไปยังผู้อื่นผ่านการทำธุรกรรม

สำหรับ NFT การถ่ายโอนโทเคนหมายถึงการเปลี่ยนเจ้าของของโทเคนนั้น โทเคนทุกตัวมีกลุ่มเจ้าของ (สามารถมีเจ้าของได้

มากกว่าหนึ่งคนขึ้นไป) เมื่อต้องการการเปลี่ยนแปลงในกลุ่มเจ้าของ สมาชิกที่เกี่ยวข้องกับการหมุนเวียนของโทเคนสามารถยืนยัน

การดำเนินการ โดยการลงนามลายเซ็นดิจิทัล กลุ่มเจ้าของโทเคนจะถูกเปลี่ยนแปลงหลังจากโหนด everiToken ยืนยันว่าการทำ

ธุรกรรมเป็นไปตามข้อกำหนดสิทธิและได้ประสานงานเช็คความถูกต้องกับโหนดอื่น ๆ เรียบร้อย

### การจัดการสิทธิ์ (Authorization Management)

ในระบบ everiToken มีสิทธิ์สามประเภทที่เกี่ยวข้องกับการจัดการสิทธิ์ได้แก่สิทธิ์การสร้าง สิทธิ์การโอน และสิทธิ์การจัดการ

(1) สิทธิ์การสร้าง หมายถึงสิทธิ์ในการสร้างและออกโทเคนในโดเมนที่ระบุ

(2) สิทธิ์การถ่ายโอน หมายถึงสิทธิ์ในการถ่ายโอนโทเคนในโดเมนที่ระบุ

### (3) สิทธิการจัดการ หมายถึงสิทธิในการแก้ไข โดเมน ประกอบด้วยการจัดการสิทธิ์และพารามิเตอร์อื่น ๆ

แต่ละสิทธิ์สามารถใช้โครงสร้างต้นไม้อธิบายได้ ดังนั้นจึงถูกเรียกว่าสิทธิ์ต้นไม้ (authorization tree) เริ่มต้นจากโหนด

ทการให้สิทธิ์แต่ละครั้งจะมีเกณฑ์ (threshold) และผู้เข้าร่วม (actor) อย่างน้อยหนึ่งรายชื่อที่เกี่ยวข้อง

### ผู้เข้าร่วม (Actor)

ผู้เข้าร่วมสามารถถูกแบ่งประเภทได้เป็นสามกลุ่ม: บัญชี กลุ่มปกติและกลุ่มเจ้าของ บัญชีคือผู้ใช้ส่วนบุคคล กลุ่มคือบัญชีที่รวมกัน

เป็นกลุ่มและกลุ่มเจ้าของเป็นรูปแบบพิเศษของกลุ่มปกติ

กลุ่มสามารถเป็นสโมสร บริษัท หน่วยงานรัฐบาล มูลนิธิหรือแม้แต่เป็นบุคคล กลุ่มจะรักษาชื่อเสียงสาธารณะ (public key) ของ

กลุ่มและชื่อเสียงสาธารณะกับน้ำหนักเสียงของสมาชิกแต่ละคน การดำเนินงานจะได้รับการอนุมัติเมื่อน้ำหนักรวมของสมาชิกที่มีสิทธิ์ทั้ง

หมดในกลุ่มที่อนุมัติเกินเกณฑ์ (threshold) ที่กำหนดของกลุ่ม

ในเวลาเดียวกันสมาชิกที่ถือชื่อเสียงสาธารณะของกลุ่มสามารถอนุมัติการแก้ไขสมาชิกกลุ่มและน้ำหนักเสียงของพวกเขาได้ กลไกนี้เรียก

ว่า group autonomy

เมื่อมีการตั้งกลุ่มระบบจะสร้าง ID กลุ่มขึ้นมาโดยอัตโนมัติ เมื่อผู้ก่อตั้งออกแบบการจัดการสิทธิ์สำหรับโดเมนสามารถอ้างอิงถึง

ID กลุ่มที่มีอยู่ได้ เนื่องจากความเป็นอิสระของกลุ่ม แต่ละกลุ่มสามารถนำกลับมาใช้ใหม่ได้อย่างสะดวกสบาย

เจ้าของโทเค็นมีชื่อกลุ่มพิเศษที่มีชื่อว่า Owner ซึ่งแสดงถึงกลุ่มของเจ้าของโทเค็น กลุ่มนี้พิเศษตรงที่สมาชิกอาจจะมีการเปลี่ยน

แปลงแต่สมาชิกของกลุ่มจะเป็นเจ้าของของโทเค็นทุกเมื่อ เงื่อนไขการอนุญาตของกลุ่มคือทุกคนภายในกลุ่มเห็นด้วย (นั่นคือน้ำหนัก

เสียงของแต่ละคนในกลุ่มคือ 1 และเกณฑ์ของกลุ่มคือจำนวนสมาชิกทั้งหมดในกลุ่ม)

### การจัดการ (Management)

การจัดการสิทธิ์ถูกกำหนดโดยผู้สร้างโทเค็น แต่ละสิทธิ์จะถูกจัดการโดยกลุ่มอย่างน้อยหนึ่งกลุ่ม เมื่อมีการสร้างโทเค็นผู้สร้างจะต้อง

ระบุน้ำหนักสัมพัทธ์ (relative weight) และกำหนดเกณฑ์ (threshold) ของแต่ละกลุ่มภายใต้แต่ละสิทธิ์ ก่อนที่จะดำเนินการ

เนินการธุรกรรมในโดเมนที่ระบุ ระบบจะต้องตรวจสอบให้แน่นอนก่อนว่ากลุ่มที่จะดำเนินการมีน้ำหนักเพียงพอหรือไม่ การดำเนินการ

การจะได้รับการอนุมัติเฉพาะในกรณีที่น้ำหนักรวมเกินเกณฑ์ที่กำหนดไว้ การออกแบบการจัดการกลุ่มนี้เหมาะสำหรับสถานการณ์ต่าง

ๆ ในโลกแห่งความเป็นจริงและการตั้งค่าน้ำหนักและเกณฑ์ที่ยืดหยุ่นสามารถตอบสนองความต้องการที่ซับซ้อนทุกชนิด สามารถชม

ตัวอย่างได้ในรูปที่ 2

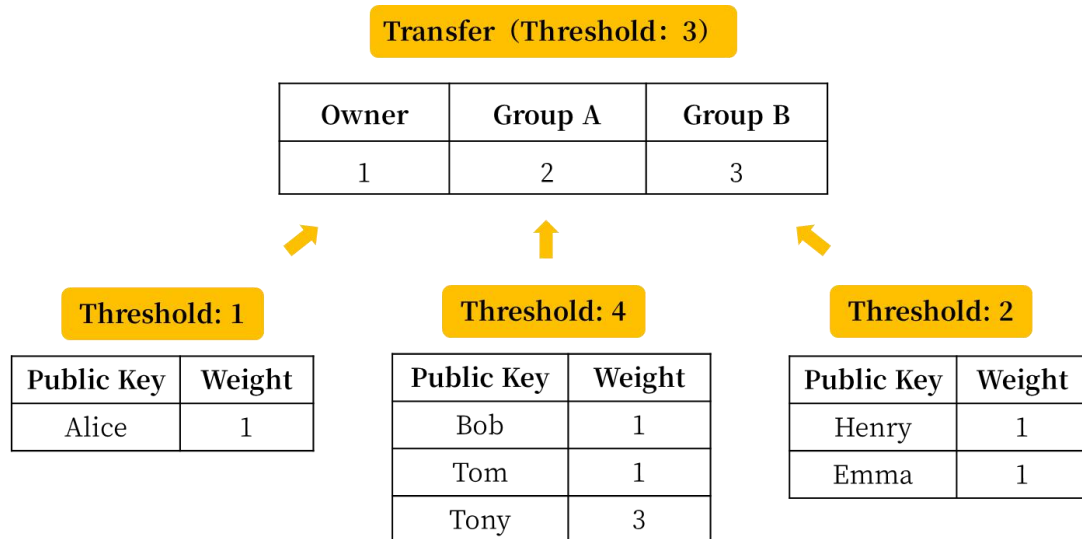


Figure 2. สิทธิ์การถ่ายโอน

รูปที่ 2 อธิบายถึงสิทธิ์การถ่ายโอนของโดเมนตัวอย่าง ในที่นี้ค่าเกณฑ์ขั้นต่ำคือ 3 และมีสามกลุ่มที่เกี่ยวข้องคือกลุ่มเจ้าของ กลุ่ม A

และกลุ่ม B พิจารณาจากน้ำหนักแต่ละกลุ่ม (1, 2 และ 3 ตามลำดับ) กลุ่มเจ้าของและกลุ่ม A จำเป็นต้องอนุญาตร่วมกัน แต่กลุ่ม

B สามารถอนุญาตเพียงกลุ่มเดียวเพื่อให้ผ่านเกณฑ์ขั้นต่ำของการถ่ายโอน

สำหรับแต่ละกลุ่ม กลุ่มเจ้าของต้องได้รับอนุญาตจาก Alice เท่านั้น กลุ่ม A สามารถผ่านเกณฑ์ (4) โดยการอนุญาตอย่างน้อย

Bob กับ Tony หรือ Tom กับ Tony กลุ่ม B จะต้องได้รับการอนุญาตจากทั้ง Henry และ Emma เพื่อให้ผ่าน

เกณฑ์ (2)

ผู้ใช้ทุกคนมีสิทธิ์ในการสร้างโทเคน โทเคนในแต่ละโดเมนนั้นมีจุดประสงค์ที่แตกต่างกัน ตัวอย่างเช่น การถ่ายโอนทรัพย์สินจะต้อง

ได้รับการตรวจสอบโดยหน่วยงานที่เกี่ยวข้องของรัฐบาลอย่างเข้มงวด บัณฑิตสมาชิกและอุปถัมภ์จะต้องให้เบรณด์รับรอง ตัวคอนเสิร์ตจะ

ไม่มีประโยชน์หลังคอนเสิร์ต และเจ้าของพื้นที่ที่จัดอาจเปลี่ยนแปลงได้ตลอดเวลา

เมื่อสร้างโทเคนผู้สร้างโทเคนสามารถออกแบบการจัดการสิทธิ์โดยการออกแบบสิทธิ์ต่าง ๆ ในโดเมน สถานการณ์จำลองต่อไปนี้

แสดงให้เห็นถึงความสะดวกสบายของการจัดการสิทธิ์ใน everiToken

รูปที่ 3 แสดงให้เห็นว่าปัญหาที่ซับซ้อนสามารถถูกแก้ไขได้โดยใช้กลไกการจัดการสิทธิ์ของ everiToken

บริษัท ได้สร้างอาคารสำนักงานแห่งใหม่และหวังที่จะออก 1,000 โทเคนเป็นตัวแทนของสิทธิ์เจ้าของในทรัพย์สินของอาคาร

บริษัทได้จัดตั้ง SPV (Special Purpose Vehicle) เพื่อสร้างและจัดการดูแลโทเคนเหล่านี้ ในชีวิตจริงการสร้างและ

โอนโทเคนอสังหาริมทรัพย์จะต้องได้รับการตรวจสอบและรับรองโดยสำนักงานทรัพย์สินท้องถิ่น พวกเขาจะต้องทำตามกฎเกณฑ์

ท้องถิ่นและจากนั้นจึงสามารถแสดงรายละเอียดโทเคน (จำนวน, ผู้ออก, โครงสร้างการจัดการสิทธิ์ ฯลฯ) บนแพลตฟอร์มทางการ

ได้ นอกจากนี้แผนกทรัพย์สินส่วนกลางมีอำนาจสูงสุดในการจำกัดและจัดการสำนักงานทรัพย์สินท้องถิ่นและเจ้าของโทเคน

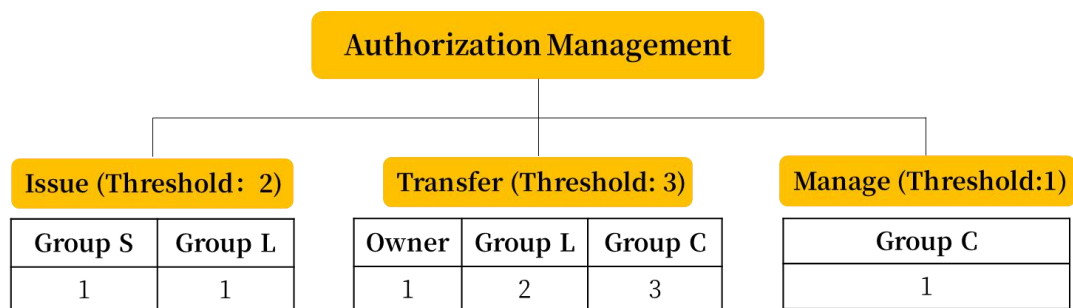


Figure 3. ตัวอย่างโครงสร้างของการจัดการสิทธิ์

กลุ่ม S เป็นตัวแทนของ SPV ซึ่งเป็นทั้งผู้สร้างและเจ้าของคนแรกของโทเคนในโดเมน กลุ่ม L เป็นตัวแทนของสำนักงาน

ทรัพย์สินท้องถิ่น กลุ่ม C เป็นตัวแทนของแผนกทรัพย์สินส่วนกลาง

ในกรณีส่วนใหญ่การถ่ายโอนโทเคนจะต้องได้รับการอนุญาตจากเจ้าของและสำนักงานทรัพย์สินท้องถิ่น (น้ำหนักรวมเกิน 3 ซึ่ง

ตามเกณฑ์ที่กำหนด) ในกระบวนการนี้การดำเนินการถ่ายโอนจะถูกตรวจสอบโดยสำนักทรัพย์สินท้องถิ่น ในกรณีที่เกิดอุบัติเหตุ

เช่น เจ้าของโทเคนเสียชีวิตหรือทำร้ายสูญหาย แผนกทรัพย์สินส่วนกลางสามารถโอนความเป็นเจ้าของของโทเคนให้กับทายาทตาม

กฎหมายหลังจากศาลหรือแผนกที่เกี่ยวข้องได้ให้คำตัดสิน



ถ้าทั้ง SPV และเจ้าของโทเคนคนอื่น ๆ ตกลงที่จะสร้างโทเคนเพิ่มพวกเขาสามารถเพิ่มโทเคนเหล่านี้ได้โดยขออนุญาตจากกลุ่ม S และกลุ่ม L นอกจากนี้โครงสร้างการจัดการการสิทธิ์ยังเหมาะสำหรับการจัดการกรณีร้ายแรง ตัวอย่างเช่น หากแผนกทรัพย์สินส่วนกลางจำเป็นต้องหยุดการแพร่กระจายของโทเคนประเภทนี้ชั่วคราวสามารถเปลี่ยนเกณฑ์ของสิทธิ์การถ่ายโอนผ่านสิทธิ์การจัดการซึ่งจะทำการแช่แข็งการหมุนเวียนของโทเคนทั้งหมดในโดเมน

## โทเคนที่สามารถทดแทนกันได้ (FT - Fungible Tokens)

### การสร้าง (Issuance)

ทุกคนสามารถสร้างโทเคนได้หลังจากลงทะเบียนด้วยสัญลักษณ์พิเศษเช่น EVT ผู้สร้างสามารถตั้งจำนวนโทเคนทั้งหมด

(total supply) และจำนวนโทเคนที่ต้องการสร้างขึ้นทันที (initial supply)

### การถ่ายโอน (Transfer)

ผู้ใช้ทุกคนที่มีคีย์ส่วนตัว (private key) ของตนเองสามารถโอนโทเคนของตนให้ผู้อื่นได้

### ข้อมูลเพิ่มเติม

แต่ละบัญชีจะบันทึกจำนวนโทเคนที่ถืออยู่พร้อมกับสัญลักษณ์ที่เกี่ยวข้อง จะมีการบันทึก key-value ต่างหากเพื่อเก็บข้อมูลพื้น

ฐานเกี่ยวกับโทเคนที่มีสัญลักษณ์แตกต่างกัน ผู้ใช้สามารถอนุญาตให้คีย์ส่วนตัวอื่นมีสิทธิ์ในการถ่ายโอนโทเคนที่ระบุตามจำนวนที่

ระบุ ฟังก์ชันนี้เรียกว่า token allowance และสามารถใช้ในแพลตฟอร์มแลกเปลี่ยนโทเคน

## โมเดลการทำธุรกรรมแบบโทเคน (Token-Based Transaction Model)

### ภาพรวม

everiToken ใช้โมเดลการทำธุรกรรมแบบโทเคน (token-based transaction model) เพื่อจัดการโทเคนทั้งหมด

ในระบบ

สำหรับแต่ละโทเคนในบัญชีแยกประเภทแบบโทเคน (token-based ledger) ทางเราสร้างพื้นที่เก็บข้อมูลต่างหากให้เพื่อ

เก็บประวัติทั้งหมดของการเป็นเจ้าของของโทเคนนั้น การเก็บข้อมูลแบบนี้ทำให้ง่ายต่อการแบ่งส่วน (sharding) และการทำ



งานขนานหลายคอร์ (multi-core paralleling) เนื่องจากพื้นที่เก็บข้อมูลของโทเคนที่กำหนดไม่มีความสัมพันธ์กันกับโท

เคนที่อื่น ๆ เป็นผลให้การดำเนินงานของโทเคนที่ต่าง ๆ สามารถทำได้ง่ายด้วยแบบคู่ขนาน โดยไม่มีความขัดแย้ง สิ่งนี้ช่วยให้

everiToken มีประสิทธิภาพสูงเป็นพิเศษและสามารถเพิ่ม TPS อย่างต่อเนื่องได้ง่ายโดยการเพิ่มคอร์ของ CPU

โมเดลธุรกรรมแบบโทเคนที่ถูกคิดค้นโดยสมาชิกในทีมหลักของ everiToken และได้รับการพิสูจน์แล้วว่าทำงานได้อย่างดีเยี่ยม

สำหรับ NFT บน EveriToken

บล็อกเชนที่ใช้โมเดลธุรกรรมแบบโทเคนที่ เช่น everiToken สามารถแบ่งฐานข้อมูลออกเป็นสองส่วน ส่วนหนึ่งคือ Token

DB อีกส่วนคือ Block DB ส่วนแรกคือที่จัดเก็บและจัดการโทเคนที่ไม่สามารถทดแทนกันได้ทั้งหมด ส่วนที่สองเป็นที่จัดเก็บ

บล็อกคั่นฉบับ

ทั้ง Token DB และ Block DB ควรเป็นฐานข้อมูลที่มีหลายรุ่น (multi-versioned database) เพื่อรองรับการ

ย้อนกลับข้อมูลอย่างรวดเร็วเมื่อบล็อกถูกย้อนกลับ ตัวอย่างเช่น everiToken ใช้ RocksDB เป็นระบบฐานข้อมูลพื้นฐาน

ของ Token DB

ทั้ง Token DB และ Block DB เป็นฐานข้อมูลที่สามารถเพิ่มได้แค่ข้อมูลเท่านั้น ดังนั้นเมื่อใดก็ตามที่มีคนอัปเดตบันทึกค่า

ใหม่ที่มีรุ่นที่เพิ่มขึ้นจะถูกเพิ่มลงในฐานข้อมูล อย่างไรก็ตามบันทึกที่รุ่นเก่าจะยังคงอยู่และไม่ถูกลบ

## Token DB

Token DB เป็นฐานข้อมูลที่มีการจัดทำดัชนี (indexed database) สำหรับการค้นหาและอัปเดตเปลี่ยนแปลงสถานะล่าสุดของ

งบล็อกเชนอย่างรวดเร็ว เช่น การเป็นเจ้าของโทเคนที่และจำนวนโทเคนที่ที่มีในบัญชี

Token DB ถือได้ว่าเป็นฐานข้อมูลแบบkey-value คีย์ระบุ ID ของโทเคนที่และค่าแสดงถึงความเป็นเจ้าของปัจจุบันของโท

เคนที่ เนื่องจากฐานข้อมูลสามารถเพิ่มได้แค่ข้อมูลเท่านั้น แต่ละคีย์จะมีหลายค่า แต่เฉพาะค่าล่าสุดเท่านั้นที่จะแสดงถึงสถานะความ

เป็นเจ้าของปัจจุบันของโทเคนที่ในขณะนี้ค่าอื่น ๆ นั้นใช้สำหรับการอ้างอิงประวัติและการย้อนกลับข้อมูลเท่านั้น สำหรับโทเคนที่แต่ละ

ตัวจะมีพื้นที่ข้อมูลส่วนตัวเหมือนกับบล็อกเชนอีกเส้นหนึ่ง ซึ่งเก็บข้อมูลเกี่ยวกับประวัติความเป็นเจ้าของทั้งหมด

ค่าแรกของเซรี่ย์ถึงการเป็นเจ้าของคนแรก ตัวอย่างเช่น เมื่อมีการทำธุรกรรมเปลี่ยนความเป็นเจ้าของ เจ้าของใหม่จะถูกเพิ่มเข้าใน

ฐานข้อมูล สามารถใช้เวอร์ชันเก่าเพื่อย้อนกลับค่าได้หากมีบล็อกที่จำเป็นต้องถูกย้อนกลับและลบออกในที่สุด

เนื่องจากโทเคนแต่ละตัวมีพื้นที่เก็บข้อมูลส่วนตัว การแบ่งส่วน (sharding) จึงกลายเป็นเรื่องง่ายมาก ตัวอย่างเช่น หากเรามี

คอมพิวเตอร์สองเครื่องสำหรับหนึ่งโหนด เราสามารถอนุญาตให้คอมพิวเตอร์แต่ละเครื่องประมวลผลโทเคนเครื่องละครึ่ง หากมี

100 โทเคนคอมพิวเตอร์เครื่องแรกจะประมวลผลโทเคน 1 - 50 และอีกอันสำหรับโทเคน 51 - 100 เนื่องจากการเปลี่ยนเจ้า

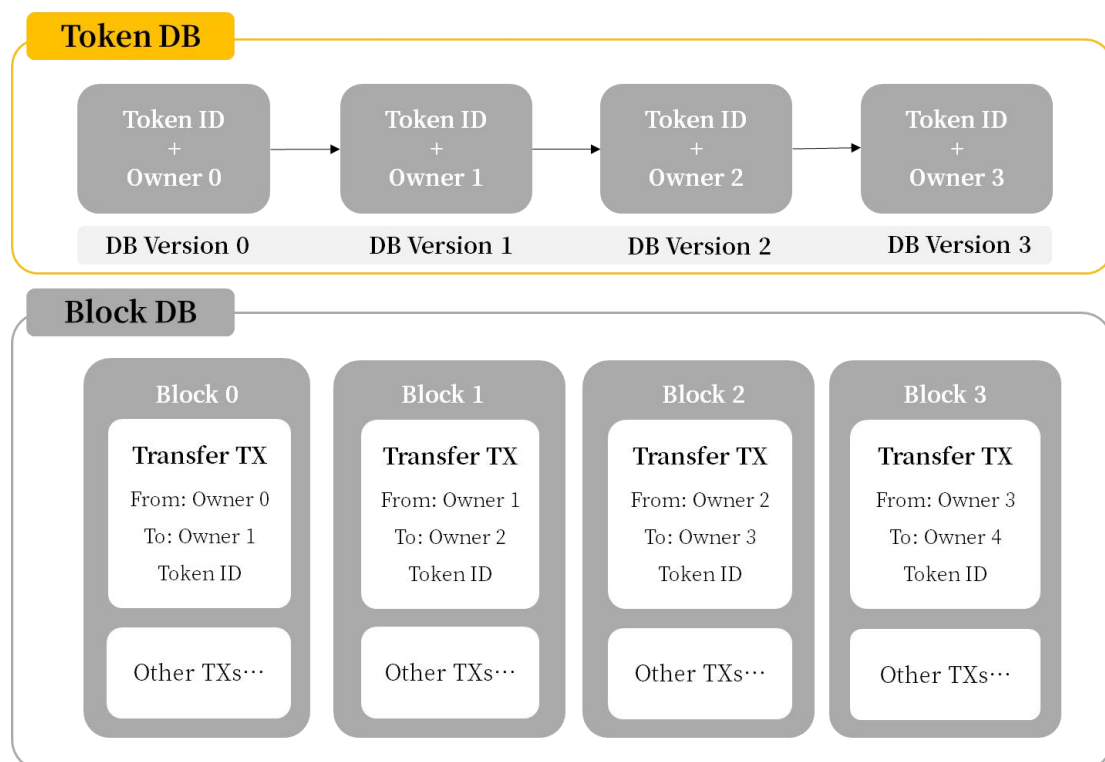
ของโทเคนหนึ่งจะไม่ส่งผลกระทบต่อโทเคนอื่น ๆ คอมพิวเตอร์ทั้งสองสามารถประมวลผลได้แบบคู่ขนาน

## Block DB

Block DB รับผิดชอบการจัดเก็บบล็อกดัชนีฉบับทั้งหมดที่ไม่สามารถย้อนกลับได้ของบล็อกเชน แต่ละบล็อกจะเก็บข้อมูลราย

ละเอียดหลายอย่างประกอบด้วยชื่อการค้าเงินและการพารามิเตอร์ ลายเซ็นบนบล็อกและข้อมูลเพิ่มเติมอื่น ๆ

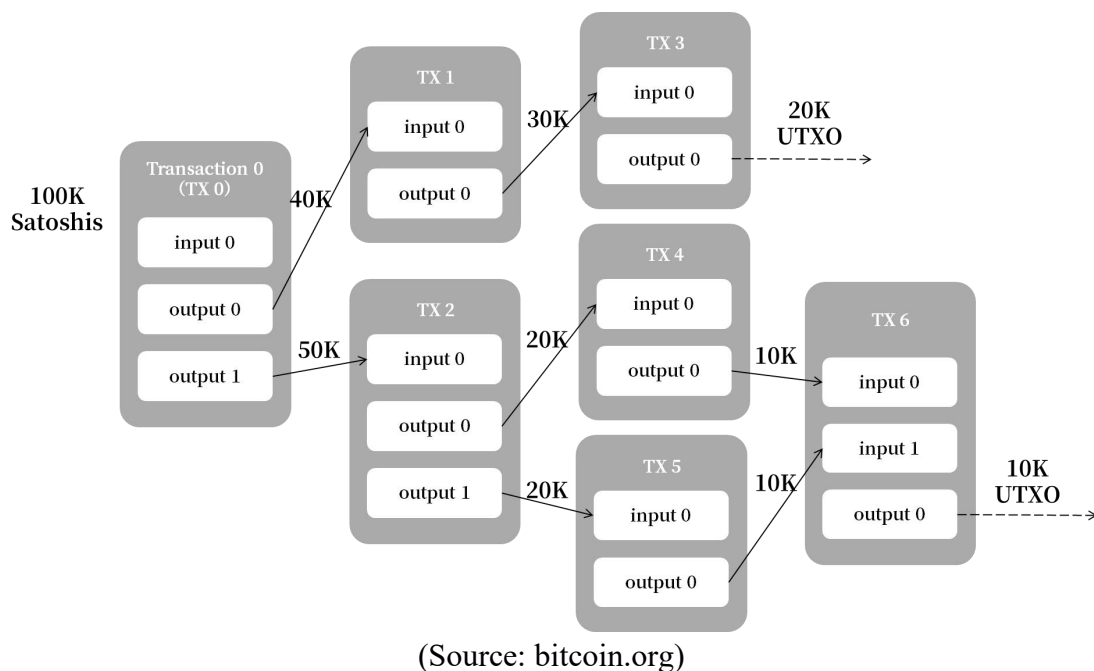
รูปด้านล่างแสดงถึงวิธีการทำงานร่วมกันของฐานข้อมูลทั้งสองชนิดสำหรับ NFT:



การเปรียบเทียบโมเดลการทำธุรกรรม

### a) UTXO (Unspent Transaction Output)

ในโมเดลการทำธุรกรรมแบบ UTXO เจ้าของโทเคนแต่ละคนจะโอนเหรียญที่พวกเขาเป็นเจ้าของด้วยการเซ็นแฮชของธุรกรรมก่อนหน้านี้ ลำดับของ input ในธุรกรรมก่อนหน้านี้ และคีย์สาธารณะหรือแอดเดรสของเจ้าของรายต่อไปและเพิ่มรายชื่อนี้ตรงที่ส่วนท้ายของธุรกรรมการโอนเหรียญ กลไกหลักคือการมอบอำนาจเจ้าของผ่าน input และ output เจ้าของโทเคนไม่ได้เป็นเจ้าของโทเคนโดยตรงแต่เป็นเจ้าของ output ซึ่งสามารถมอบอำนาจให้เจ้าของคนใหม่โดยการสร้าง output ใหม่ด้วยกันเซ็น



อย่างที่เห็น โมเดลแบบ UTXO นั้นเหมาะสำหรับการหลีกเลี่ยงการถ่ายโอนซ้ำ (double-spending) เนื่องจากเห็นได้ชัดว่า

input ทุกอันสามารถใช้ได้เพียงครั้งเดียว แต่ก็มีข้อเสียบางประการเช่นกัน:

- โมเดลนี้ถูกใช้ใน Bitcoin เนื่องจาก BTC ไม่ใช่ NFT แต่เป็น FT มันไม่มีประโยชน์เลขที่ UTXO ทุกตัวนั้นต้องมีเอกลักษณ์ (everiToken รองรับทั้ง NFT และ FT)
- UTXO สามารถใช้ได้เพียงครั้งเดียว การจัดเก็บ UTXO จำนวนมากเป็นการสิ้นเปลืองทรัพยากรในการประมวลผลและพื้นที่ฮาร์ดดิสก์

### b) Account-based

โมเดลการทำธุรกรรมแบบบัญชีคล้ายกับโมเดลของธนาคาร คุณสร้างบัญชีที่ธนาคารแล้วบันทึกเงินลงในบัญชีเพื่ออัปเดตยอดคง

เหลือ โมเดลนี้แตกต่างจากวิธีการทำงานของ UTXO อย่างสิ้นเชิงและมีประสิทธิภาพมากกว่าเพียงเพราะแค่ต้องอัปเดตยอดคง

เหลือในฐานข้อมูลไม่ต้องสร้าง UTXO ใหม่ นี่เป็นเหตุผลว่าทำไม UTXO ไม่เหมาะสำหรับ NFT

โมเดลการทำธุรกรรมแบบบัญชีไม่เหมาะต่อการแบ่งส่วน (sharding) เพราะว่าเมื่อต้องการทำการถ่ายโอนบางสิ่งไปยังบุคคลอื่นมันต้องใช้สองขั้นตอน ขั้นแรกคือการแก้ไขบัญชีของผู้ถือเก่า ขั้นที่สองคือการปรับเปลี่ยนบัญชีของผู้ถือใหม่ ด้วยเหตุผลด้านความปลอดภัยจำเป็นต้องทำสองขั้นตอนนี้ในขั้นตอนเดียว ในสภาพแวดล้อมที่ถูกแบ่งส่วนนั้นสิ่งนี้เป็นไปได้ยากและประสิทธิภาพจะไม่ดี อย่างไรก็ตามในโมเดลธุรกรรมแบบโทเค็นนั้นมีเพียงขั้นตอนเดียวเท่านั้นคือการเพิ่มชื่อเจ้าของของโทเค็นใหม่

## ความปลอดภัย

การเจาะจงไปที่ฟังก์ชันที่เกี่ยวข้องกับโทเค็นของ everiToken ช่วยลดนามธรรมที่ไม่จำเป็นซึ่งไม่เพียงแต่เพิ่มประสิทธิภาพของระบบอย่างมาก แต่ยังให้ความปลอดภัยที่ดีขึ้นมากอีกด้วย แม้ว่าประเภทของโทเค็นบน everiToken นั้นมีมากมายและไม่ได้จำกัดตามทฤษฎี โครงสร้างโทเค็นที่เหมือนกันทำให้ระบบหรือองค์กรบุคคลที่สามารถตรวจสอบโทเค็นเหล่านี้ได้โดยใช้หลักการเดียวกัน ผู้ใช้สามารถมองได้ว่าระบบ everiToken นั้นมีเพียงสัญญาอัจฉริยะแบบเดียว ซึ่งทำให้การตรวจสอบง่ายขึ้นและความปลอดภัยดีขึ้น

## everiToken Core Codebase

จนถึงฤดูใบไม้ผลิปี 2019 everiToken ได้เรียกองค์กร เช่น Hacken Proof และ Chaitin มาตรวจสอบฐานโค้ดหลักทั้งหมดของบล็อกเชนสาธารณะ everiToken การวิเคราะห์รวมไปถึงการวิเคราะห์แบบคงที่ (static analysis) และแบบไดนามิก (dynamic analysis) เนื่องจาก everiToken ใช้สัญญาที่ปลอดภัย เมื่อได้รับการพิสูจน์แล้วว่าฐานโค้ดหลักของเรานั้นปลอดภัย สัญญาทั้งหมดบน everiToken จึงจะได้รับการพิสูจน์ว่าปลอดภัยเช่นกัน

## Script (everiSigner)

everiSigner เป็นปลั๊กอินเอาไว้เซ็นออฟไลน์สำหรับเบราวเซอร์ กระบวนการเซ็นทั้งหมดดำเนินการภายในปลั๊กอินเพื่อไม่ให้มีการเปิดเผยคีย์ส่วนตัว เว็บไซต์ทำการสื่อสารกับ everiSigner โดยการสร้างช่องทางใหม่ขึ้นมาเพื่อความปลอดภัย เว็บไซต์จะส่งข้อมูลที่จะต้องเซ็นเข้าในช่องทาง หลังจากนั้น everiSigner จะส่งคืนข้อมูลที่เซ็นแล้วกลับไป

## คีย์ส่วนตัวสูญหาย

ผ่านการจัดการสิทธิ์บุคคลที่สามารถให้บริการได้หลายอย่าง ตัวอย่างเช่น บริษัท C มีความเชี่ยวชาญในการให้บริการระบบ

ป้องกันคีย์ และ Alice กล่าวว่าเธอจะลืมหรือสูญเสียคีย์ส่วนตัวของโทเคนของเธอ Alice สามารถโอนสิทธิ์การถ่ายโอนของโค

เมนไปยังกลุ่มเจ้าของ (1) และกลุ่ม C (1) และตั้งค่าค่าเกณฑ์ขั้นต่ำเป็น 1 ในกรณีนี้ถ้า Alice ลืมคีย์ส่วนตัวของเธอ เธอ

สามารถพิสูจน์ตัวเองว่าเป็น Alice กับกลุ่ม C (ผ่านบัตรประชาชนหรือลายนิ้วมือ) เพื่อรับอนุญาตในการถ่ายโอนโทเคนของเธอ

ด้วยวิธีนี้ Alice สามารถกู้คืนโทเคนได้โดยการโอนไปยังบัญชีใหม่หลังจากการตรวจสอบ

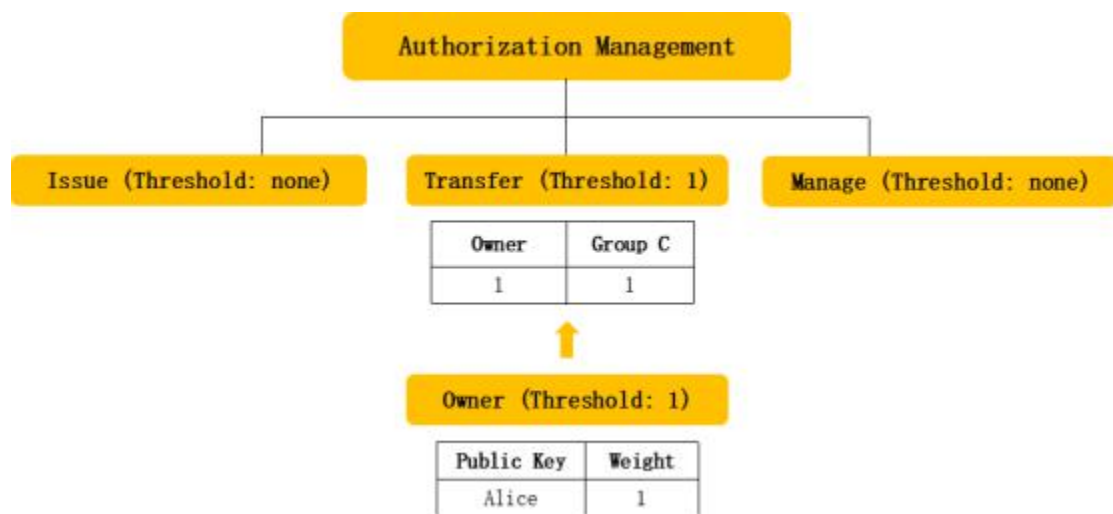


Figure 4. บริษัท C ให้บริการกู้คืนคีย์

แน่นอนว่ากลุ่ม C สามารถขโมยโทเคนของอลิซได้ทุกเมื่อ แต่การดำเนินการทั้งหมดจะถูกบันทึกไว้บนบล็อกเชนซึ่งจะทำให้ความ

น่าเชื่อถือของกลุ่ม C

## ขั้นตอนวิธีฉันทามติ (Consensus Algorithm)

ขั้นตอนวิธีฉันทามติที่ everiToken ใช้คือ BFT-DPOS DPOS ได้รับการพิสูจน์แล้วว่าสามารถตอบสนองความต้องการ

การด้านประสิทธิภาพของแอปพลิเคชันบนบล็อกเชนได้ ภายใต้อัลกอริทึมนี้ผู้ที่ถือ EVT สามารถเลือกผู้ผลิตบล็อกผ่านระบบการ

ลงคะแนนอย่างต่อเนื่อง ทุกคนสามารถเลือกที่จะมีส่วนร่วมในการผลิตบล็อกและจะได้รับโอกาสในการผลิตบล็อกถ้าหากสามารถ

เรียกให้ผู้ถือโทเคนลงคะแนนให้พวกเขาได้

บล็อกใน everiToken ถูกสร้างขึ้นทุก ๆ 0.5 วินาทีและมีแค่ผู้ผลิตหนึ่งรายที่จะได้รับอนุญาตในการสร้างบล็อกในทุก ๆ ช่วงเวลา หากไม่มีการสร้างบล็อกในเวลาที่กำหนดบล็อกสำหรับช่วงเวลานั้นจะถูกข้ามไป เมื่อมีการข้ามบล็อกเกิดขึ้นบล็อกเชนจะมีช่องว่างตั้งแต่ 0.5 วินาทีขึ้นไป

จำนวนผู้ผลิตบล็อกสำหรับบล็อกเชนสาธารณะ everiToken นั้นเป็นแบบไดนามิก สำหรับปีแรกมีการกำหนดผู้ผลิตทั้งหมด 15 ราย หลังจากนั้นจะมีการตัดสินใจจำนวนโดยคณะกรรมการดูแลบล็อกเชนแบบกระจายอำนาจ เพื่อความสะดวกเราจะใช้ 15 ในกระดาษขาวนี้

ใน everiToken บล็อกจะถูกสร้างขึ้นในรอบละ 180 บล็อก (ผู้ผลิต 15 ราย แต่ละผู้ผลิตผลิต 12 บล็อก) ในช่วงแรกของแต่ละรอบผู้ผลิตบล็อกที่ไม่ซ้ำกัน 15 คนจะถูกเลือกจากการโหวตจากผู้ถือ EVT ผู้ผลิตที่ถูกเลือกจะถูกกำหนดเวลาตามข้อตกลงที่ตกลงกันโดยผู้ผลิต 11 รายขึ้นไป

หากผู้ผลิตลืมผลิตบล็อกและไม่ได้ผลิตบล็อกใด ๆ ภายใน 24 ชั่วโมงที่ผ่านมาพวกเขาจะถูกไล่ออกจากกลุ่มผลิตบล็อกจนกว่าพวกเขาจะแจ้งให้คนอื่น ๆ ทราบถึงความตั้งใจที่จะเริ่มผลิตบล็อกอีกครั้ง สิ่งนี้ทำให้มั่นใจได้ว่าเครือข่าย everiToken จะทำงานได้อย่างราบรื่นโดยลดจำนวนบล็อกที่ถูกทิ้งโดยไม่ได้กำหนดเวลาผลิตบล็อกแก่ผู้ผลิตที่ไม่มีความน่าเชื่อถือ

BFT ถูกใช้เพื่อเพิ่มความปลอดภัยของระบบและผู้ใช้โดยกำหนดให้ผู้ผลิตทุกคนเซ็นยืนยัน ผู้ผลิตไม่สามารถเซ็นสองบล็อกที่มีการประทับเวลาหรือความสูงของบล็อกเหมือนกัน เมื่อผู้ผลิต 11 รายได้เซ็นบล็อก บล็อกนั้นก็ถือว่าได้รับการยืนยันและไม่สามารถถูกย้อนกลับได้ สองบล็อกที่ถูกเซ็นโดยผู้ผลิตไบแซนไทน์ใด ๆ ที่มีเวลาประทับหรือความสูงบล็อกเหมือนกันจะถูกนำไปเป็นหลักฐานการเข้ารหัสของการทรยศ ภายใต้โมเดลนี้ระบบสามารถเข้าสู่ฉันทามติที่ไม่สามารถย้อนกลับได้ภายใน 1 วินาที

## การออกแบบโบนัส

โบนัสถูกเพิ่มเข้ามาใน everiToken 3.0 ในเดือนกุมภาพันธ์ 2019 โบนัสเป็นองค์ประกอบที่ทรงพลัง ยืดหยุ่นและสะดวกสบายที่สามารถร่วมเข้ากับฟังก์ชันที่มีอยู่ วัตถุประสงค์ของโบนัสคือการกระจายผลกำไรให้กับผู้มีส่วนได้เสียหรือผู้ถือหุ้นตามกฎหมาย

เกณฑ์ ณ ตอนนี้โบนัสมีอยู่สองประเภท: โบนัสแบบพาสซีฟและโบนัสแบบแอคทีฟ โบนัสสองประเภทนี้มีจุดแตกต่างอยู่ตรงที่วิธีการเก็บผลกำไร

สำหรับโบนัสแบบพาสซีฟกำไรจะถูกรวบรวมในทุก ๆ การทำธุรกรรมที่เกี่ยวข้องกับ FT หนึ่ง ดังนั้นหากผู้จัดการของ FT หนึ่งตัดสินใจที่จะตั้งโบนัส ทุกธุรกรรมที่เกี่ยวข้องกับ FT นี้ไม่เพียงแต่จะต้องจ่าย EVT เป็นค่าเชื้อเพลิงและยังต้องจ่ายค่าธรรมเนียมเพิ่มเติมของ FT ด้วย

มีหลายตัวเลือกในการควบคุมค่าธรรมเนียมในการทำธุรกรรมแต่ละครั้ง ตัวเลือกหลักคืออัตราการทำธุรกรรม ค่าธรรมเนียมสามารถคิดได้จากการเอาอัตราการทำธุรกรรมคูณด้วยจำนวนธุรกรรม นอกจากนี้ยังสามารถตั้งค่าเกณฑ์เพื่อจำกัดขอบเขตบนและล่างของค่าธรรมเนียมสุดท้าย วิธีดังกล่าวนี้ช่วยป้องกันไม่ให้ค่าใช้จ่ายของการทำธุรกรรมมีมูลค่าสูงเกินไป

ผู้จัดการ FT สามารถตัดสินใจได้ว่าจะมีการเรียกเก็บค่าธรรมเนียมอย่างไร เช่น ฝ่ายใดจะเป็นผู้รับผิดชอบค่าธรรมเนียมและวิธีการแบบค่าธรรมเนียม วิธีแรกเหมือนบัตรเครดิตโดยผู้จ่ายเงินจ่าย  $n$  จำนวน และผู้รับจะได้รับน้อยกว่า  $n$  เนื่องจากค่าธรรมเนียมถูกหักออกจากจำนวนเงินเริ่มต้น วิธีที่สองนั้นเหมือนกับธุรกรรมธนาคารทั่วไป หากคุณต้องการโอนเงินจำนวน  $n$  ไปยังอีกท่านหนึ่งคุณจะต้องชำระค่าธรรมเนียมเพิ่มเติมจากจำนวนเงินดั้งเดิม

โบนัสแบบแอคทีฟมีความคล้ายกับเงินปันผลของหุ้น ผู้จัดการ FT เป็นคนตัดสินใจว่าควรแบ่งโบนัสยังไงและเมื่อไร

ไม่ว่าโบนัสจะเป็นแบบแอคทีฟหรือพาสซีฟก็มีกฎการกระจาย ณ ปัจจุบันมีกฎอยู่สามประเภท: กฎแบบ **fixed** กฎแบบ **percent** และกฎแบบ **remaining percent** กฎแบบ **fixed** คือจำนวนโบนัสที่ผู้รับจะได้รับจะคงที่ ในขณะที่กฎแบบ **percent** จำนวนโบนัสที่จะได้รับจะถูกคำนวณโดยการคูณจำนวนโบนัสทั้งหมดด้วยเปอร์เซ็นต์ กฎ **remaining percent** จะต่างจากกฎ **fixed** และกฎ **percent** และประกอบด้วยจำนวนโบนัสที่เหลือคูณกับค่าเปอร์เซ็นต์

สำหรับกฎแต่ละข้อจำเป็นต้องกำหนดผู้รับ ผู้รับไม่ได้ถูกจำกัดให้เป็นผู้ใช้ท่านหนึ่ง แต่สามารถเป็นเจ้าของ FT ชนิดหนึ่งและผู้ถือแต่ละคนสามารถได้รับส่วนแบ่งกำไรตามจำนวนโทเค็นที่ถือ นอกจากนี้โบนัสไม่จำเป็นต้องเป็น FT ชนิดนี้ แต่สามารถเป็น FT



ชนิดไหนก็ได้ที่ได้ลงทะเบียนบน everiToken ดังนั้นจึงเป็นไปได้ที่จะออกโทเคนโบนัสเพื่อเอาไว้แบ่งผลกำไรโดยเฉพาะ โทเค็นนี้จะได้รับประโยชน์จากความโปร่งใส ยุติธรรมและสภาพคล่องที่มอบให้โดย everiToken

เมื่อฝั่งรับมี address มากกว่าหนึ่งจำเป็นต้องทำการถ่าย snapshot ของยอดคงเหลือของ address ของผู้ถือหุ้นทั้งหมด การทำเช่นนี้จะใช้พื้นที่เก็บข้อมูลเพิ่มขึ้นเนื่องจาก address ผู้ถือหุ้นแต่ละรายต้องมีขนาด 34 ไบต์ แต่เราได้ทำการปรับขั้นตอนนี้ให้มีประสิทธิภาพมากขึ้นในกรณีส่วนใหญ่ให้เหลือเพียง 4 ไบต์เท่านั้นต่อราย สมมติว่ามีผู้ถือหุ้น 1 ล้านคนขึ้นไปพื้นที่จะอยู่ที่ประมาณ 4 เมกะไบต์แทนที่จะเป็น 34 เมกะไบต์ ด้วยฐานข้อมูลของเรามีประสิทธิภาพสูง ระบบสามารถอ่านและอัปเดตยอดคงเหลือของผู้ถือหุ้นได้ในต้นทุนที่ต่ำเป็นพิเศษ

## ฟังก์ชันล็อก (Lock Function)

everiToken รองรับฟังก์ชันล็อกซึ่งทำให้สามารถล็อกทั้ง FT และ NFT เป็นระยะเวลาหนึ่งได้ ระยะเวลาที่ถูกล็อกขึ้นอยู่กับเงื่อนไขที่กำหนดไว้ในข้อเสนอการล็อก ไม่ว่าจะเป็นไปตามเงื่อนไขหรือไม่ก็ตามในช่วงเวลาที่ถูกล็อก หลังจากช่วงเวลาที่กำหนดสินทรัพย์จะถูกปลดล็อกและถูกโอนไปยัง address อื่นที่ถูกลงทะเบียน ปัจจุบันเงื่อนไขการล็อกสามารถถูกแก้ไขได้ด้วยคีย์สาธารณะเท่านั้นซึ่งหมายความว่าในช่วงเวลาที่ถูกล็อกนั้นมิได้มีส่วนตัวที่ได้รับการอนุมัติในข้อเสนอการล็อกเท่านั้นที่สามารถใช้งานได้

## รายละเอียดทางเทคนิคอื่น ๆ

### บล็อกเชนพื้นฐาน

เราไม่ต้องการที่จะสร้างทุกอย่างใหม่ ดังนั้นเราได้ดูซ้ำส่วนที่ดีของระบบบล็อกเชนสาธารณะที่มีอยู่และปรับปรุงจุดอ่อนของมันให้ดีขึ้น เราได้นำ Graphene (DPOS + PBFT) มาใช้เป็นขั้นตอนวิธีฉันทามติ โค้ดของขั้นตอนวิธีฉันทามติถูกเขียนขึ้นจาก DPOS 3.0 (จากโค้ดของ EOS) และถูกปรับแต่งโดยทีมงานของเรา เราขอรับว่า EOS มีโครงสร้างโค้ดที่ยอดเยี่ยม ดังนั้นทางเราจึงได้ใช้โครงสร้างโค้ดเดิม แต่นอกเหนือจากส่วนนี้บล็อกเชนสาธารณะทั้งหมดได้ถูกพัฒนาขึ้นมาใหม่

ในการพัฒนาเราได้สร้างสัญญาที่ปลอดภัย (แทนสัญญาอัจฉริยะ) โมเดลฐานข้อมูลแบบใหม่ (ใช้ RocksDB เพื่อประสิทธิภาพที่ดีกว่า) และโปรโตคอลการชำระเงินโทเคน everiPay

มีข้อดีหลายประการสำหรับการทำเช่นนี้:

- Graphene ได้รับการตรวจสอบเป็นเวลานาน DPOS และกลไกหลักอื่น ๆ ได้รับการทดสอบอย่างเต็มที่ในโปรเจกต์เช่น BitShares และ EOS
- การนำขั้นตอนวิธีฉันทามติกลับมาใช้ใหม่สามารถลดปริมาณงานบางส่วนทำให้เราสามารถมุ่งเน้นไปที่การเพิ่มประสิทธิภาพในการพัฒนาฟังก์ชันหลักของ everiToken

## การดำเนินการให้สิทธิ์ Authorization Operation

การดำเนินการให้สิทธิ์ของ everiToken ส่วนใหญ่รวมถึงการเซ็นชื่อแบบหลายคน (multi-signing) การคำนวณน้ำหนักการตั้งค่าเกณฑ์และอื่น ๆ เนื่องจากการถ่ายโอนโทเคนแต่ละตัวนั้นไม่ขึ้นอยู่กับผู้อื่น ดังนั้นการดำเนินการถ่ายโอนโทเคนที่แตกต่างกันจึงสามารถถูกดำเนินการแบบขนานกันได้ นอกจากนี้เนื่องจากสถานะสิทธิ์ของแต่ละกลุ่มไม่เกี่ยวข้องกัน การดำเนินการการสร้าง (issuance operation) และการจัดการ (management operation) จึงสามารถถูกดำเนินการขนานกันระหว่างกลุ่มต่าง ๆ ได้

แต่ละธุรกรรมประกอบด้วยแฟล็กเก็ตข้อมูลและรายการลายเซ็น ในกรณีของการตรวจสอบสิทธิ์เราแค่ต้องตรวจสอบลายเซ็นแต่ละอันเนื่องจากไม่มีความสัมพันธ์ระหว่างลายเซ็น ดังนั้นการดำเนินการให้สิทธิ์สามารถดำเนินการแบบขนานได้

## Execution Engine

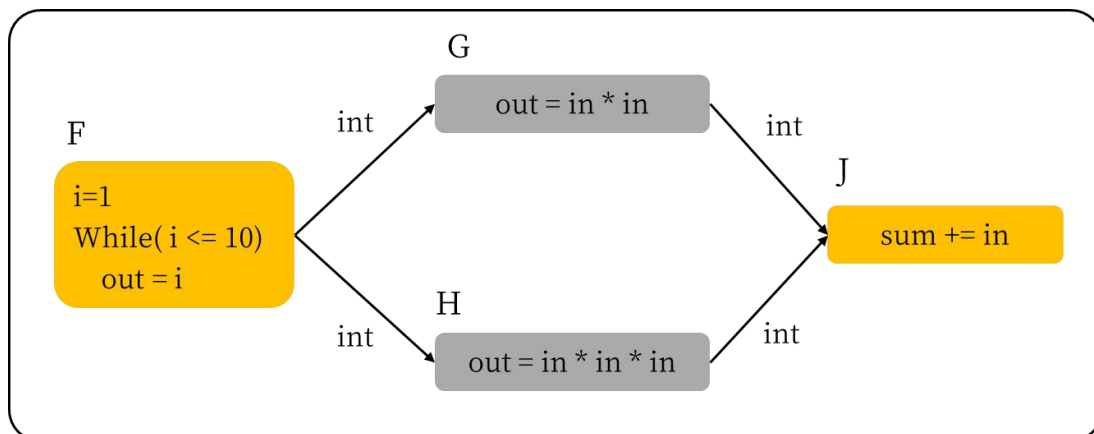
ในระบบของ everiToken เนื่องจากการดำเนินการของแต่ละโทเคนไม่เกี่ยวข้องกันเลย กระบวนการแบบขนานจึงไม่มีภาระต่อการแบ่งส่วนพาร์ติชันเพิ่มเติม นอกจากนี้เนื่องจากชนิดของการดำเนินการโทเคนมีจำนวนจำกัดและได้ดำเนินการถูกเขียนไว้บนบล็อกเชนตั้งแต่เริ่ม トラバースที่มีการทดสอบแต่ละชนิดของการดำเนินการซ้ำหลายครั้ง ระบบจะมีความเสถียรที่ดี

การดำเนินการของธุรกรรมหนึ่งสามารถแบ่งออกเป็นหลายขั้นตอน เช่น การกู้คืนลายเซ็น การตรวจสอบสิทธิ์ การคำนวณ การเขียนลงฐานข้อมูล ฯลฯ ทุกขั้นตอนควรถูกดำเนินการตามลำดับ แต่บางขั้นตอนไม่มีความเกี่ยวข้องกันในธุรกรรมที่แตกต่างกัน หนึ่งในขั้นตอนเหล่านี้คือการกู้คืนลายเซ็นแต่ละลายเซ็นของธุรกรรมไม่มีการพึ่งพาตรรกะและไม่มีการเกี่ยวข้องกัน ดังนั้นจึงสามารถกู้คืน

ลายเซ็นแบบคู่ขนานได้ อีกหนึ่งขั้นตอนคือการตรวจสอบสิทธิ์ ตอนแรกอาจจะดูเหมือนว่าการตรวจสอบสิทธิ์จะคล้ายกับการกู้คืนลายเซ็น แต่ถ้าวางจินตนาการถึงการตรวจสอบสิทธิ์ของสองธุรกรรมที่ทำการถ่ายโอนโทเคน แม้ว่าโทเคนแต่ละตัวไม่มีความเกี่ยวข้องกัน แต่หากมีธุรกรรมสองรายการที่โอนโทเคนอันเดียวกันระบบจะพบกับพฤติกรรมที่ไม่คาดคิดหากยังดำเนินการแบบขนานอยู่

เนื่องจากเจ้าของโทเคนจะถูกเปลี่ยนในธุรกรรมแรก ดังนั้นขั้นตอนนี้จึงไม่สามารถถูกดำเนินการแบบขนานได้

บทสรุปคือบางขั้นตอนไม่สามารถถูกดำเนินการแบบคู่ขนานได้ อย่างไรก็ตามเราสามารถเพิ่มประสิทธิภาพในสถานการณ์เหล่านี้ได้โดยการวางแผนให้รอบคอบ วิธีที่ทางเราใช้ถูกแสดงไว้ในกราฟการพึ่งพาด้านล่าง ระบบของเราใช้ graph parallelism เพื่อประมวลผลข้อมูลในแบบคู่ขนาน การคำนวณถูกแสดงโดยโหนดและช่องทางการสื่อสารระหว่างการคำนวณเหล่านี้ถูกแสดงด้วยขอบ



กราฟด้านบนเป็นตัวอย่างของวิธีการวิธีการคำนวณผลรวมของอนุกรมกำลังสองและกำลังสาม จาก 1 ถึง 10 ในการดำเนินการของเราแต่ละโหนดคือหนึ่งขั้นตอนของการทำธุรกรรมและมี scheduler หนึ่งคนที่จะรับธุรกรรมและแยกพวกมันออกเพื่อสร้างกราฟทั้งหมด

## ธุรกรรมที่ถูกกระงับ (Suspended Transaction)

ธุรกรรมที่ถูกกระงับคือธุรกรรมที่จะเสร็จสมบูรณ์หลังจากผ่านไประยะเวลาหนึ่ง การทำธุรกรรมทั่วไปที่ไม่ได้ถูกระงับจะถูกดำเนินการแค่ครั้งเดียวและจะต้องปฏิบัติตามเงื่อนไขทั้งหมดเมื่อธุรกรรมถูกส่งเข้าเน็ตเวิร์คบล็อกเชน ตัวอย่างเช่น ผู้ลงนามทั้งหมดต้องเซ็นร่วมกันพร้อมกัน อย่างไรก็ตามในความเป็นจริงการทำธุรกรรมจำนวนมากต้องผ่านกระบวนการหลายขั้นตอนกว่าจะเสร็จสิ้น ผู้เข้า

ร่วมการทำธุรกรรมอาจไม่สามารถรอกลายเซ็นได้ในเวลาเดียวกัน การทำธุรกรรมที่ถูกระงับอนุญาตให้ผู้เข้าร่วมสามารถลงลายเซ็นที่ละคนจนกว่าจะครบ เมื่อครบการทำธุรกรรมจึงจะถือว่าเสร็จสมบูรณ์

## everiPay / everiPass / EvtLink

### everiPay / everiPass

everiPay / everiPass เป็นวิธีการชำระเงินที่ถูกสร้างมาเพื่อ micropayment แบบ face-to-face โดยใช้บล็อกเชนสาธารณะ everiToken

EvtLink ประกอบด้วยมาตรฐานการสร้าง QR Code และคำนิยามของโปรโตคอลการสื่อสาร

จุดเด่นของ everiPay / everiPass / EvtLink มีดังนี้:

- **การชำระเงินทันที:** การทำธุรกรรมคือการชำระเงินทันที
- **การกระจายอำนาจ:** การชำระเงินแบบ P2P ไม่มีแพลตฟอร์มกลาง ไม่มีใครสามารถแก้ไขข้อมูลบนบล็อกเชนได้และผู้ใช้ทุกคนสามารถเข้าร่วมในการกำหนดราคาได้
- **ความปลอดภัยสูง:** ข้อมูลและเนื้อหาภายในบล็อกเชนไม่สามารถถูกปลอมแปลงหรือดัดแปลงได้ซึ่งเพิ่มความปลอดภัยของทรัพย์สินของผู้ใช้
- **รองรับหลายรูปแบบ:** รับรองโทเคนทั้งหมดที่ได้รับการรับรองบน everiToken รวมถึงสกุลเงิน คะแนนและแม้แต่กุญแจเพื่อเปิดประตู คุณสามารถใช้งานได้เกือบทุกที่เพียงแคมีโทรศัพท์
- **ความสะดวกสูง:** แม้ว่า คุณจะไม่สามารถเชื่อมต่ออินเทอร์เน็ตอยู่ คุณยังสามารถทำธุรกรรมได้
- **ความเร็วสูง:** everiToken มี TPS ที่สูงมาก การทำธุรกรรมสามารถทำได้ภายใน 1 - 3 วินาทีขึ้นอยู่กับคุณภาพของอุปกรณ์และเครือข่าย
- **การวางมาตรฐาน:** ไม่เหมือนกับเทคโนโลยีด้านกระเป๋าเงิน EvtLink เป็นมาตรฐานที่ cross-wallet, cross-chain และ cross-app ที่ถูกสร้างขึ้นโดยตรงสำหรับระบบนิเวศทั้งหมด ผู้ใช้สามารถใช้แอปใดก็ได้เพื่อสร้างหรือแจกส่วนมัน

เจ็ดจุดเด่นข้างต้นทำให้ everiPay / everiPass สามารถให้บริการที่ปลอดภัยที่สุด สะดวก และใช้งานง่ายในอุตสาหกรรม

การชำระเงินแบบ face-to-face

สำหรับการใช้งาน everiPay / everiPass ผู้รับเงินต้องใช้แอปพลิเคชันที่สามารถเข้าใจ EvtLink และรองรับการส่งธุรกรรม

รวมถึง everiToken โค้ดตัวอย่างและ API ที่ใช้งานง่ายของเราทำให้กระบวนการนี้้ง่ายมาก วิธีใช้คล้ายกับการเพิ่มการ

สนับสนุน AliPay / WeChat สำหรับร้านค้าของคุณแต่ยังดีกว่า

### รหัส QR ของผู้รับเงิน

รหัส QR ของผู้รับเงินไม่รองรับฟีเจอร์หลายอย่างที่ everiPay มี ตัวอย่างเช่น ผู้ชำระเงินต้องเชื่อมต่ออินเทอร์เน็ตเพื่อทำธุรกรรม

ผ่านรหัส QR ของผู้รับเงิน และ ผู้ชำระเงินและผู้รับเงินต้องป้อนจำนวนเงินของธุรกรรมด้วยตนเอง นอกจากนี้พวกเขาจะไม่สามารถ

สามารถรับการแจ้งเตือนอัตโนมัติเมื่อการชำระเงินเสร็จสิ้น

อย่างไรก็ตามผู้รับเงินไม่จำเป็นต้องใช้แอปที่รับรองวิธีการชำระเงินแบบนี้ ในความเป็นจริงผู้รับเงินเพียงแต่ต้องใช้กระเป๋าเงินที่รองรับ

everiToken บนโทรศัพท์ของพวกเขาเพื่อตรวจสอบว่าพวกเขาได้รับเงินจากผู้จ่ายหรือไม่ วิธีนี้เหมาะสำหรับร้านค้าทุก

ประเภทและทุกขนาดรวมทั้งการแลกเปลี่ยนระหว่างบุคคล

ทางเราแนะนำให้ใช้ everiPay แทนรหัส QR ของผู้รับเงินเพราะมีความโปร่งใส ปลอดภัย และใช้งานง่ายกว่า

### EvtLink ทำงานอย่างไร?

EvtLink เป็นมาตรฐานของฟอร์แมตไบนารีของ everiPay / everiPass บล็อกเชนสาธารณะ everiToken ใช้การ

ดำเนินการ (operation) ของ everiPay และ everiPass เพื่อทำธุรกรรมที่เป็นไปตามมาตรฐานของ EvtLink

ด้านล่างคือกระบวนการชำระเงินผ่าน everiPay / everiPass จากมุมมองทางเทคนิค:

1. ผู้ชำระเลือกโทเค็นที่ต้องการใช้ กระเป๋าเงินของผู้จ่ายจะแสดงชุดรหัส QR แบบไดนามิกที่ประกอบด้วย LinkId

ขนาด 128 บิตที่ไม่ซ้ำกัน ลายเซ็นของผู้ชำระเงินและสัญลักษณ์ของโทเค็นที่ใช้สำหรับการชำระเงิน โปรดทราบว่า

LinkId ไม่ควรถูกเปลี่ยนแปลงระหว่างการแลกเปลี่ยนรหัส QR ยกเว้นหากการทำธุรกรรมที่เกี่ยวข้องได้เกิดขึ้นแล้ว

วิธีนี้ช่วยป้องกันความเสี่ยงของการชำระเงินซ้ำซ้อนเนื่องจากบล็อกเชนไม่อนุญาตให้ดำเนินการสองรายการบน

EvtLink ที่มี LinkId เดียวกัน

2. แอปพลิเคชันกระเป๋าดังของผู้ชำระเงินควรเช็กระบุธุรกรรมที่เกี่ยวข้องกับ LinkId อย่างต่อเนื่องโดยการเรียก API ที่ชื่อ

‘get\_trx\_id\_for\_link\_id’ จนกว่า API จะส่งคืน ID ธุรกรรมที่ถูกต้องกลับมา กระเป๋าดังควรเปลี่ยน

LinkId ในครั้งต่อไปที่แสดงรหัส QR นอกจากนี้กระเป๋าดังควรแสดงผลการทำธุรกรรมโดยการค้นหาข้อมูลเกี่ยว

กับ ID ธุรกรรม กระเป๋าดังของผู้ชำระเงินไม่จำเป็นต้องส่งธุรกรรมโดยตรง

3. ในขณะที่ผู้รับเงินจะสแกนรหัส QR โดยใช้โทรศัพท์ สแกนเนอร์ หรือสมาร์ตเควดเวย์ หลังจาก EvtLink

ถูกสแกนและแจ้งส่วนแล้วมันจะถูกห่อเข้าธุรกรรม จากนั้นจะถูกส่งไปยังบล็อกเชน หลังจากนั้นโหนดบล็อกเชนทั้งหมด

จะทำการซิงโครไนซ์ข้อมูลและการเรียก ‘get\_trx\_id\_for\_link\_id’ จะส่งคืน ID ของธุรกรรม

## การเข้ารหัส Base42

Base42 เป็นอัลกอริทึมการเข้ารหัสสำหรับการแปลงไบนารีเป็นสตริง มันคล้ายกับการเข้ารหัสเลขฐานสิบหก แต่ใช้ 42 เป็นฐาน

แทน ตัวอักษรในสตริง Base42 นั้นเหมือนกับตัวอักษรในการเข้ารหัสโหมดตัวอักษรและตัวเลขของ QR Code ดังนั้นมันจึง

ง่ายที่จะแปลสตริง Base42 เป็น QR Code อย่างมีประสิทธิภาพ นอกจากนี้ยังส่งผลให้รหัส QR มีขนาดเล็กซึ่งช่วยให้

การสแกนสะดวกยิ่งขึ้นอีกด้วย

everiToken ใช้ Base42 ในการเข้ารหัสเนื้อหาของ EvtLink

### 3. โมเดลเศรษฐกิจ

#### ค่าก๊าซ / เชื้อเพลิง (EVT)

เพื่อหลีกเลี่ยงการโจมตีของระบบ เช่น DDoS เพื่อให้มีหลักฐานการถือหุ้นสำหรับกลไกฉันทามติ DPOS และเพื่อให้รางวัล

แก่ผู้ผลิตบล็อก ทางเราได้สร้างโทเคน EVT ขึ้นมาเพื่อทำงานเป็นเชื้อเพลิงของเรา ทุกการดำเนินการจะต้องใช้ EVT เป็นค่า

บริการซึ่งจะถูกนำไปเป็นรางวัลแก่ผู้ผลิตบล็อก จำนวน EVT ที่เรียกเก็บจะถูกเพิ่มหรือลดตามอุปสงค์และอุปทานของตลาด การ

เก็บค่าธรรมเนียมไว้เพื่อป้องกันการโจมตีที่เป็นอันตรายและจะไม่ส่งผลกระทบต่อการใช้งานปกติของผู้ใช้ส่วนใหญ่

วิธีการสร้างและถ่ายโอน EVT เหมือนกับสกุลเงินเข้ารหัสของบล็อกเชนทั่วไป EVT ใช้เพื่อเป็นรางวัลให้แก่ผู้ผลิตบล็อก

สำหรับการแบ่งทรัพยากรและป้องกันพฤติกรรมที่เป็นอันตราย

150 ล้าน EVT (รวม 15%) จะมอบให้กับทีมหลักของ everiToken (14% สำหรับผู้ร่วมก่อตั้งห้ารายของ

everiToken และอีก 1% สำหรับผู้สนับสนุนหลัก)

400 ล้าน EVT (รวม 40%) จะมอบให้กับสมาชิกชุมชนที่สร้างแอปบน everiToken และมีส่วนสำคัญอย่างยิ่งต่อระบบ

นิเวศของ EveriToken โดยการช่วยในด้านเทคโนโลยี ทรัพยากร การระดมทุน การส่งเสริม การขาย และอื่น ๆ

450 ล้าน EVT (รวม 45%) สำหรับนักลงทุน

เซอร์วิสทั้งหมดบน everiToken คิดค่าบริการตามสูตรต่อไปนี้:

$$ServiceFuelCost = FuelUsed \times R$$

ในสูตรนี้ FuelUsed คือราคาของการดำเนินการเฉพาะ (specific operation) หน่วยของราคาคือ EVT R แสดงถึง

อัตราการปรับ (adjusting rate) โหนด BP สามารถตัดสินใจได้อย่างอิสระตลอดเวลาเพื่อปรับอัตรา R ขึ้นเมื่อบล็อกเชนทำ

งานหนักหรือถูกโจมตี และสามารถลดอัตรา R ลงหากราคาของ EVT สูงเกินไป ค่าของ R คำนวณโดยการหาค่าเฉลี่ยของค่า R

ที่แต่ละ BP 15 รายคิดว่าควรจะเป็น

ผู้ใช้งานของบล็อกเชนสามารถสันนิษฐานได้ว่าค่าของ R เป็น 1 สำหรับครั้งแรกที่พวกเขาเรียก API ถ้าค่า R ไม่ได้รับการ

เปลี่ยนแปลงโดย BP การเรียก API จะเสร็จสมบูรณ์ หากมีการเปลี่ยนแปลงการเรียกจะล้มเหลวและจะมีการส่งค่า R ใหม่ให้ผู้

ใช้งานผ่าน response จาก BP ผู้ใช้จะต้องดำเนินการการเรียก API อีกครั้งโดยใช้ค่า R ใหม่

ตัวอย่างเช่น เมื่อราคาของ createAccount API เป็น 2 EVT

โดยปกติผู้ใช้จะสามารถเรียกใช้ createAccount API ด้วย 2 EVT

ถ้า BP ปรับอัตรา R ขึ้นเป็น 1.1 ราคาจะเปลี่ยนเป็น 2.2 EVT

ทางเราใช้ค่าเฉลี่ยของค่า R ที่แต่ละ BP คิดว่าควรจะเป็นในการคำนวณค่าของ R หาก 3 ผู้ผลิตแนะนำให้ R เป็น 1.15, 5 ผู้

ผลิตให้เป็น 1.2, 2 คนให้เป็น 1.1, อีก 2 ให้เป็น 1.3 , อีก 1 เป็น 1.1, อีก 1 เป็น 1.4 และ อีก 1 เป็น 1.45 ค่า R สุดท้าย

ท้าย หรือค่าเฉลี่ยของ R ทั้งหมดจะเท่ากับ 1.2

## EVT ที่ถูกปิดกั้น

EVT ที่ถูกปิดกั้นคล้ายกับ EVT แต่จะไม่สามารถถูกถ่ายโอนได้และสามารถใช้ได้เป็นค่าเชื้อเพลิงเท่านั้น ระบบอนุญาตให้ทำ

การแปลง EVT ธรรมดาเป็น EVT ที่ถูกปิดกั้น อัตราแลกเปลี่ยนของ EVT เทียบกับ EVT ที่ถูกปิดกั้นจะคงที่อยู่ที่ 1

เนื่องจาก EVT ที่ถูกปิดกั้นไม่ใช่สกุลเงินจึงปลอดภัยที่จะให้ EVT ที่ถูกปิดกั้นไว้กับคนอื่น

โดยหลักแล้วไม่ควรแปลง EVT ธรรมดาเป็น EVT ที่ถูกปิดกั้นเนื่องจากสามารถใช้ EVT ธรรมดาเพื่อชำระค่าธรรมเนียม

เชื้อเพลิงได้ หากตัดสินใจที่จะแปลง EVT ธรรมดาเป็น EVT ที่ถูกปิดกั้น EVT ที่ถูกปิดกั้นจะถูกผูกเข้ากับผู้รับโดย

อัตโนมัติ

EVT ที่ถูกปิดกั้นไว้เป็นของบัญชีหนึ่งและไม่สามารถโอนให้ผู้อื่นได้ ดังนั้นจึงสะดวกและปลอดภัยที่จะทำการปล่อย EVT

แก่ผู้ใช้ บริษัทและองค์กรสามารถแปลง EVT ธรรมดาเป็น EVT ที่ถูกปิดกั้นและเชื่อบัญชีผู้รับตามต้องการได้



ผู้ชำระเงินเป็นบัญชีที่ง่ายสำหรับการทำธุรกรรมที่กำหนด everiToken อนุญาตให้ผู้ชำระและผู้ชำระเงินในการทำธุรกรรม ฟังก์ชัน

นี้มีประโยชน์มากสำหรับการสร้างบัญชี เพื่อความปลอดภัยผู้ชำระเงินต้องมีการเซ็นธุรกรรมนั้น

แต่ละ โดเมนมีบัญชีพิเศษเพื่อเอาไว้เก็บ EVT ที่ถูกปิดกั้น

everiToken ชอบที่จะใช้ยอด EVT ที่ถูกปิดกั้นของโดเมนก่อน (หากไม่เป็นศูนย์) ในการดำเนินการต่าง ๆ เช่นการถ่ายโอน

หรือการทำลายโทเคนในโดเมน

ผู้ใช้สามารถชำระเงินล่วงหน้าสำหรับ EVT ที่ถูกปิดกั้นของโดเมนผ่าน EVT ธรรมดา

## การออก EVT เพิ่ม

ปริมาณเริ่มต้นของ EVT คือ 1 พันล้าน everiToken อาจสร้าง EVT เพิ่มเป็นประจำทุกปี การออกเพิ่มจะต้องผ่านการ

ตัดสินใจของคณะกรรมการดูแลบล็อกเชนแบบกระจายอำนาจของ everiToken ทางเราจะไม่สร้าง EVT เพิ่มจนหลังวันที่ 1

มกราคม 2020

## ผู้ผลิตบล็อก (BPs – Block Producers)

จำนวนของ BP: โดนามิก (เปลี่ยนแปลงได้ตลอดเวลา)

เราให้สิทธิ์เล็กน้อยกับ BP ดังนั้นจึงยากมากที่ BP จะทำสิ่งเลวร้าย สิ่งชั่วร้ายที่ BP สามารถทำได้คือ DoS (Denial of

Service) เพื่อความสมดุลของรายได้ของ BP และสร้างความมั่นใจในการกระจายอำนาจเรากำหนดให้จำนวนของ BP เป็นค่า

โດนามิก ซึ่งจะเท่ากับหรือมากกว่า 15 ในปี 2019 เราจะใช้ 15 BPs ในปีต่อ ๆ ไปคณะกรรมการดูแลบล็อกเชนแบบกระจาย

อำนาจจะเป็นผู้ตัดสินใจ

## 4. ระบบนิเวศ

### เครื่องมือ

#### everiWallet

everiWallet เป็นกระเป๋าตั้งของ everiToken ที่รองรับทั้งเว็บเบราว์เซอร์และโทรศัพท์มือถือ สำหรับข้อมูลเพิ่มเติมกรุณา

เยี่ยมชมเว็บไซต์ของเรา <https://www.everiwallet.com/>

#### EVTJS

EVTJS เป็น API ไลบรารีของ everiToken สำหรับ JavaScript ซึ่งรองรับทั้ง NodeJS และเบราว์เซอร์ นอกจากนี้

นี้ยังรองรับ everiSigner ดังนั้นคุณสามารถใช้ไลบรารีนี้พัฒนาเว็บแอปพลิเคชันบน everiToken ได้อย่างง่ายดาย สำหรับ

ข้อมูลเพิ่มเติมกรุณาเยี่ยมชม <https://www.github.com/everitoken/evtjs>

#### evtScan

evtScan เป็นบล็อกเชนเบราว์เซอร์ของ everiToken ที่ผู้ใช้สามารถค้นหาข้อมูลเกี่ยวกับบล็อกทั้งหมดที่ถูกสร้างขึ้นโดย

โหนดใน mainnet ของ everiToken ได้ ข้อมูลที่สามารถค้นหาได้รวมถึงรายละเอียดของธุรกรรม บัญชี กลุ่มและโดเมน

นอกจากนี้ผู้ใช้ยังสามารถดูสถิติและทำการวิเคราะห์ได้ด้วย สำหรับนักพัฒนาซอฟต์แวร์ evtScan เป็นเครื่องมือที่มีประสิทธิภาพ

ในการยืนยันว่าข้อมูลนั้นเชื่อมโยงกับบล็อกเชนอย่างถูกต้องหรือไม่ สำหรับผู้ใช้ธรรมดา evtScan สามารถช่วยในการตรวจ

สอบความถูกต้องของการทำธุรกรรม สำหรับข้อมูลเพิ่มเติมกรุณาเยี่ยมชม <https://evtscan.io/>

#### คณะกรรมการดูแลบล็อกเชนแบบกระจายอำนาจ

บล็อกเชน everiToken จะมีคณะกรรมการแบบกระจายอำนาจเพื่อกำหนดสิ่งสำคัญ เช่น จำนวนโหนดที่สร้างบล็อก กฎเกณฑ์

ในการออก EVT เพิ่มและอื่น ๆ คณะกรรมการอยู่ในระหว่างการเตรียมการและคาดว่าจะออนไลน์ได้ก่อนวันที่ 1 มกราคม

2020

#### บริษัท Escrow



everiToken รู้เพียงโทเคน ID ไม่มีการเกี่ยวข้องกับสินทรัพย์และโทเคนของผู้ใช้ มูลค่าของโทเคนถูกรับรองโดยบริษัท

Escrow ซึ่งสามารถลงลายเซ็นดิจิทัลเพิ่มเติมในระหว่างกระบวนการออกโทเคนเพื่อเพิ่มความน่าเชื่อถือให้ผู้ซื้อ หากผู้ซื้อเชื่อ

ถือในตัวบริษัทที่ลงลายเซ็นดิจิทัลผู้ซื้อจะมีความเชื่อถือในตัวโทเคนมากขึ้น หลักการนี้คล้าย ๆ กับ SSL

## 5. บทสรุป

เศรษฐกิจโทเคนกำลังเคลื่อนไหวไปยังทุกมุมของโลก สัญญาอัจฉริยะของ **Ethereum** และ **EOS** เป็นการเริ่มต้นที่ดี แต่ไม่เหมาะสำหรับการพัฒนาเศรษฐกิจโทเคนที่ทุกคนในโลกสามารถใช้ประโยชน์ได้

**everiToken** เกิดมาพร้อมกับเป้าหมายในการสร้างเทคโนโลยีบล็อกเชนที่ใช้โทเคนซึ่งให้ประโยชน์กับทุกคนทุกที่ ทางเราได้สร้างระบบที่ทำให้ต้นทุนต่ำและใช้ง่ายสำหรับนักพัฒนา ธุรกิจและผู้ใช้ปลายทางในการสร้าง ถ่ายโอน และตรวจสอบการใช้โทเคนภายในระบบของเรา สัญญาที่ปลอดภัยของเราไม่ทั่วถึงสมบูรณ์แต่ผลลัพธ์ที่ได้คือระดับนามธรรมและความซับซ้อนในระบบลดลงอย่างมาก แทนที่จะสร้างโมเดลที่สามารถกำหนดได้เองอย่างต่อเนื่องเราได้สร้างโมเดลขนาดเดียวที่เหมาะสมกับทุกคน ซึ่งเป็นโซลูชันที่เหมาะสมสำหรับคนทั่วไปมากกว่า 99% ทางเราได้ปรับปรุงความเร็ว ความปลอดภัย ความสามารถในการใช้งาน ความเสถียร และการควบคุมดูแลที่จำเป็นต่อการสร้างเศรษฐกิจโทเคนที่มีประสิทธิภาพและเจริญรุ่งเรือง ขณะเดียวกันทางเราต้องการที่จะเป็นแพลตฟอร์มที่มีการกระจายอำนาจสำหรับทุกคนในโลก ให้พวกเขามาเรียนรู้ สร้าง ได้ตอบ และแลกเปลี่ยนมูลค่าแบบดิจิทัลอย่างแท้จริง เข้าร่วมการปฏิบัติเศรษฐกิจโทเคนและเยี่ยมชมเว็บไซต์ของเราที่ [www.everitoken.io](http://www.everitoken.io)

## ทีมผู้ก่อตั้ง

### Hengjin Cai, หัวหน้านักวิทยาศาสตร์

ศาสตราจารย์และอาจารย์พิเศษที่มหาวิทยาลัยหวู่ฮั่น ตีพิมพ์บทความทางวิชาการมากกว่า 80 เรื่อง หนังสือเรื่อง *Before the Rise of Machines - The Beginning of the Consciousness and the Human Intelligence* ของอาจารย์ได้รับรางวัล 2017 Wu Wenjun Artificial Intelligence Science and Technology Award ในปี 2005 อาจารย์ได้รับเชิญจากมหาวิทยาลัยหวู่ฮั่นให้เดินทางกลับประเทศจีนมาเป็นอาจารย์สอนพิเศษระดับปริญญาเอกของคณะซอฟต์แวร์นานาชาติ งานหลักทำวิจัยและสอนเกี่ยวกับวิทยาศาสตร์การบริการ ปัญญาประดิษฐ์และวิศวกรรมข้อมูลทางการเงิน ในปี 2011 ได้รับเลือกให้เป็นหนึ่งในสมาชิกชุดแรกของโครงการ Huanghe Yingcai ของหวู่ฮั่น ในปี 2012 ได้รับรางวัลผลการสอนดีเด่นจากครูใหญ่ของมหาวิทยาลัยหวู่ฮั่น

### Brady Luo, CEO



Brady-everiToken

Brady เป็นผู้เชื่อที่แท้จริงในเศรษฐกิจโทเท็นระดับโลกโดยใช้เทคโนโลยีบล็อกเชน เขาได้รับปริญญาตรีจากมหาวิทยาลัยการบินและอวกาศแห่งกรุงปักกิ่งในสาขาวิศวกรรมไฟฟ้า ปริญญาโทสาขาการเงินจากมหาวิทยาลัยแบรนไดซ์ในสหรัฐอเมริกาและศึกษาหลักสูตรกลยุทธ์การใช้บล็อกเชนที่ Said Business School ที่มหาวิทยาลัยออกซ์ฟอร์ด เขาเป็นผู้ประกอบการต่อเนื่อง เขาได้รับเลือกเข้าเป็นชุดที่สามของโปรแกรม 1,000 Talents Plan ในเมืองเซี่ยงไฮ้ เขาทำงานเป็นนักวิเคราะห์เป็นเวลาเกือบสี่ปีที่กลุ่มการลงทุนในสินทรัพย์ทางเลือกของ OppenheimerFunds ซึ่งเป็นผู้จัดการกองทุน 10 อันดับแรกของสหรัฐอเมริกา และกลุ่มการเงินที่ใหญ่ที่สุดของญี่ปุ่นหลักทรัพย์มีดซุบิชิยูเอฟเอ (สำนักงานใหญ่โตเกียว ส่องกงและเซี่ยงไฮ้)

### Bozhen Chen, COO

Bozhen มีประสบการณ์มากมายในการดำเนินงานโครงการของรัฐบาลและความเชี่ยวชาญด้านการสื่อสารและการประชาสัมพันธ์ เขาจบการศึกษาปริญญาตรีจากมหาวิทยาลัย Aston ด้านวิทยาศาสตร์สาขาบริหารธุรกิจ Bozheng มีประสบการณ์ทำงานกับผู้ให้บริการไอทีอเมริกัน ใช้อุปทานเครื่องแต่งกาย บริการ B2B และหน่วยงานภาครัฐ ตลอดเวลาที่ทำงานเขาได้พัฒนา

ทักษะการปฏิบัติงานการสื่อสารและการประชาสัมพันธ์ที่แข็งแกร่งในหลากหลายอุตสาหกรรม เขาเป็นโฮสต์ของการประชุมทางอินเทอร์เน็ต เป็นผู้นำของศูนย์บริการสาธารณะพาณิชย์อิเล็กทรอนิกส์ของตงเฉิงและเป็นผู้อำนวยความสะดวกศูนย์บริการผู้ประกอบการอินเทอร์เน็ตสำหรับเยาวชน เขาได้รับรางวัลมากมายในฐานะหนึ่งในผู้นำเยาวชนของจีนรวมถึงรางวัลเยาวชนดีเด่นในเจียงและรางวัลเยาวชนที่มีความตั้งใจและจิตใจที่ดีในปี 2018 จากลีกเยาวชนคอมมิวนิสต์ของจีน

### **Ceeji Cheng, CPO**

Ceeji เป็นนักพัฒนาโปรแกรม Full Stack และ System Architect ที่มีประสบการณ์ทำงานมากกว่า 10 ปี เขามีประสบการณ์มากมายในด้านพัฒนาซอฟต์แวร์และการจัดการ เขาเป็นผู้ชนะรางวัลชนะเลิศ National Informatics Olympiad และก่อนหน้านี้ทำงานที่สตาร์ทอัพของตัวเองในฐานะ CTO และผู้ร่วมก่อตั้ง

### **Harry Wang, CTO**

Harry เป็น System Architect และวิศวกรระบบที่มีประสบการณ์กว่า 10 ปีในอุตสาหกรรมการเงินและอินเทอร์เน็ต ก่อนหน้านี้เขาเคยทำงานที่หลักทรัพย์ Tianfeng ในเซี่ยงไฮ้และเคยเข้าร่วมในการก่อตั้งบริษัท Quantitative Hedge Fund ที่หนึ่งในฐานะหุ้นส่วนทางเทคนิค เขายังพัฒนาระบบการซื้อขายเชิงปริมาณที่มีประสิทธิภาพสูงซึ่งดำเนินงานถึงทุกวันนี้ในหลายตลาดทั่วโลก