เครือข่ายชื่อเสียงแบบกระจายศูนย์: กรอบแนวคิดสำหรับการจัดระเบียบสังคมตามธรรมชาติ

Pavel Kudrna
Prague, Czechia
ฉบับร่าง v1 — มีนาคม 2026

Abstract

สำนึกแห่งความยุติธรรม—
ความเชื่อมั่นว่าความผิดจะได้รับการแก้ไขให้ถูกต้องและคุณความดีจะได้รับการตอบแทน—
คือแรงยึดเหนี่ยวที่ทรงพลังที่สุดของสังคม
เมื่อสถาบันการปกครองแบบรวมศูนย์ไม่สามารถมอบสำนึกนี้ได้
เพราะต้นทุนของการบังคับใช้สิทธิหนึ่งสูงเกินกว่ามูลค่าของสิทธินั้นเอง
ความเป็นน้ำหนึ่งใจเดียวกันของสังคมก็เสื่อมสลาย
โครงสร้างของสถาบันในปัจจุบันล้มเหลวในการระงับข้อพิพาทจำนวนมากอย่างเป็นระบบ
ในลักษณะเดียวกับที่การวางแผนจากส่วนกลางล้มเหลวในการจัดสรรทรัพยากร
นั่นคือ ผ่านความไม่สมมาตรของข้อมูล
การขาดวงจรป้อนกลับ
และการที่ผู้ตัดสินใจถูกตัดขาดจากผลลัพธ์ของการตัดสินใจของตน
เอกสารฉบับนี้นำเสนอเครือข่ายสังคมชื่อเสียง
(Reputation Social Network, RSN)
ซึ่งเป็นชั้นการสื่อสารแบบกระจายศูนย์
ต้านทานการทุจริต และต้านทานการเซ็นเซอร์
สร้างขึ้นบนตัวระบุแบบกระจายศูนย์ (De-
centralized Identifiers, DIDs)
ที่เปิดโอกาสให้ผู้เข้าร่วมแบบนามแฝงสามารถเผยแพร่
ตรวจสอบ และบริโภคข้อมูลชื่อเสียงเกี่ยวกับพฤติกรรมในโลกจริง
กลไกหลักตั้งอยู่บนหลักการออกแบบสามประการ
ได้แก่ (1) โครงสร้างต้นทุนแบบไม่สมมาตร
ที่การอ่านข้อมูลชื่อเสียงมีราคาถูก
แต่การเขียนต้องอาศัยความพยายามที่พิสูจน์ได้;
(2) โปรโตคอลการคัดเลือกผู้ตรวจสอบแบบไม่กำหนดตายตัว
ที่อาศัยการแฮชแบบสม่ำเสมอ
(consistent hashing)
ซึ่งตั้งราคาข้ออ้างสุดโต่งผ่านต้นทุนการทำซ้ำที่เพิ่มสูงขึ้นเรื่อยๆ
และ (3) แบบจำลองผู้มีอำนาจด้านชื่อเสียงที่ขับเคลื่อนด้วยกฎหมาย
ซึ่งผู้ตรวจสอบเอกชนเดิมพันชื่อเสียงที่สั่งสมมาไว้กับความถูกต้องของการตัดสิน
สถาปัตยกรรมที่เกิดขึ้นก่อให้เกิดระบบคุณธรรมนิยม
(meritocracy) แบบผุดขึ้นเองโดยไม่ต้องมีการประสานงานจากส่วนกลาง
และเปิดเส้นทางการโยกย้ายที่ค่อยเป็นค่อยไปและย้อนกลับได้สู่ระบบที่รัฐบริหารอยู่ในปัจจุบัน

1 บทนำ

1.1 ปัญหาของความไว้วางใจแบบรวมศูนย์

การปกครองสมัยใหม่ตั้งอยู่บนสมมติฐานพื้นฐานประการหนึ่ง
นั่นคือ สถาบันแบบรวมศูนย์สามารถเป็นตัวกลางแห่งความไว้วางใจ
ศาลตัดสินข้อพิพาท ทะเบียนรับรองกรรมสิทธิ์
องค์กรกำกับดูแลบังคับใช้มาตรฐาน
สถาบันเหล่านี้ถูกออกแบบขึ้นในยุคที่ข้อมูลหายาก
การสื่อสารเป็นไปอย่างเชื่องช้า
และกรรมอบอำนาจให้แก่หน่วยงานส่วนกลางเป็นกลไกการประสาน
อย่างไรก็ตาม การปกครองแบบรวมศูนย์ล้มเหลวด้วยเหตุผลเชิงโคร
นั่นคือ ความไม่สมมาตรของข้อมูล
การขาดวงจรป้อนกลับ
และการที่ผู้ตัดสินใจถูกตัดขาดจากผลลัพธ์ของการตัดสินใจของตน
สมมติฐานนี้ล้มเหลว ยกตัวอย่างเช่น
เมื่อต้นทุนของการไกล่เกลี่ยโดยสถาบันสูงเกินกว่ามูลค่าของข้อพิพา
ลองพิจารณาผู้เช่ารายหนึ่งที่พบว่าอพาร์ตเมนต์ที่ตนเช่าอยู่ขาดใบรับ
สภาพที่ก่อให้เกิดอันตรายต่อชีวิตในทันที
สิทธิตามกฎหมายของผู้เช่าในการถอนตัวจากสัญญานั้นชัดเจนไม่คล
แต่ต้นทุนของการบังคับใช้สิทธินั้นผ่านระบบศาลกลับสูงเกินกว่ามูลค
แม้จะรวมค่าชดเชยตามกฎหมายที่อาจได้รับไว้ด้วยแล้วก็ตาม [1]
โจทก์ไม่ต้องอย่างมีเหตุผลคือการยอมรับความสูญเสียและถอนตัว
นี่ไม่ใช่กรณีเฉพาะที่ผิดปกติ
แต่คือประสบการณ์ตามปกติสำหรับข้อพิพาทจำนวนมาก
ที่ความเสียหายเกิดขึ้นจริง
แต่มูลค่าเป็นตัวเงินต่ำกว่าเกณฑ์ที่การบังคับใช้โดยสถาบันจะคุ้มค่า
เพราะต้นทุนของการแสวงหาความยุติธรรมตกอยู่กับฝ่ายผู้เสียหาย
ตัวอย่างข้างต้นดึงมาจากสภาพแวดล้อมทางกฎหมายของผู้เขียน-
ในระบบกฎหมายแพ่งของเช็ก
ในระบบกฎหมายที่อิงบรรทัดฐาน (com-
mon law) กฎหมายจารีตประเพณี ระบบผสม—
ความยุติธรรมล้มเหลวในลักษณะที่แตกต่างกันและในระดับที่แตกต่
ขึ้นอยู่กับลักษณะเฉพาะทางวัฒนธรรมและกระบวนพิจารณาของเขตอ

ผู้อ่านมีแนวโน้มที่จะรับรู้ถึงตัวอย่างที่เทียบเคียงกันได้จากประสบการณ์ของตนเอง
สิ่งที่เป็นสากลในเชิงโครงสร้างคือรูปแบบนี้ นั่นคือ
ข้อพิพาทที่มูลค่าต่ำกว่าเกณฑ์ของการบังคับใช้ที่คุ้มค่าทางเศรษฐกิจจะจบลงด้วยการที่ฝ่ายผู้เสียหายต้องแบกรับความสูญเสีย
RSN มิได้สัญญาว่าจะมอบความยุติธรรมอันสมบูรณ์แบบ—
เพียงแต่ลดความได้เปรียบเชิงโครงสร้างที่ผู้กระทำผิดได้รับ
เมื่อการบังคับใช้โดยสถาบันไม่คุ้มค่าทางเศรษฐกิจ

1.2 เหตุใดวิธีแก้ปัญหาที่มีอยู่จึงยังไม่เพียงพอ

กรอบแนวคิดอัตลักษณ์แบบกระจายศูนย์ (DID) [2]
มอบกลไกทางวิทยาการเข้ารหัสสำหรับการจัดการอัตลักษณ์แบบอธิปไตยในตนเอง
(self-sovereign identity)
แต่มุ่งเน้นหลักไปที่การตรวจสอบอัตลักษณ์
โดยไม่ได้กล่าวถึงคำถามที่กว้างกว่าเกี่ยวกับชื่อเสียงด้านพฤติกรรม

โทเคนผูกวิญญาณ (Soulbound Tokens, SBTs) [3]
จับใจความสำคัญที่ว่าชื่อเสียงเป็นสิ่งที่โอนกันไม่ได้
แต่กลับพึ่งพาโครงสร้างพื้นฐานบล็อกเชนซึ่งมีข้อจำกัดด้านการขยายขนาด
และไม่ได้กล่าวถึงแรงจูงใจทางเศรษฐกิจที่กำกับการป้อนข้อมูลเข้าสู่ระบบ
แนวคิดที่เกี่ยวข้อง เช่น โทเคนคุณความดี (merit tokens) (เช่นของ Liberland) มีปรัชญาที่คล้ายคลึงกัน
แต่ยังคงผูกติดอยู่กับกรอบเขตอำนาจศาลเฉพาะแห่ง

องค์กรอิสระแบบกระจายศูนย์ (DAOs) [4]
ดำเนินการปกครองผ่านสัญญาอัจฉริยะ (smart contracts) แต่กลับจำลองพลวัตแบบธนาธิปไตย
(plutocratic) ที่อิทธิพลเป็นสัดส่วนกับทุน
การลงคะแนนแบบกำลังสอง (quadratic voting) [5] ช่วยบรรเทาปัญหานี้ได้บางส่วน
แต่ก็จำกัดการนำไปใช้ในทางปฏิบัติ นอกจากนี้
DAOs ยังเผชิญกับปัญหาออราเคิล (oracle problem) อันเป็นพื้นฐาน นั่นคือ
สัญญาอัจฉริยะไม่สามารถตรวจสอบสถานะในโลกจริงได้อย่างน่าเชื่อถือ ทำให้ความสามารถในการใช้งานของพวกมันถูกจำกัดอย่างมาก
และปัญหานี้ก็ไม่มีทางแก้ทั่วไปภายในสถาปัตยกรรมบล็อกเชน

ไม่มีระบบใดที่มีอยู่ในปัจจุบันที่ผสานการกระจายศูนย์
ความต้านทานการเซ็นเซอร์ ความเป็นนามแฝง
ต้นทุนการเข้าสู่ระบบที่พิสูจน์ได้
และฉันทามติแบบผุดขึ้นเองไว้ด้วยกัน

1.3 คุณูปการ

เอกสารฉบับนี้มีคุณูปการดังต่อไปนี้:

1. การนิยาม**เครือข่ายสังคมชื่อเสียง (RSN)**
   ซึ่งเป็นโปรโตคอลแบบกระจายศูนย์ที่ขยายกรอบแนวคิด
   DID เพื่อรองรับการแลกเปลี่ยนชื่อเสียงแบบสองทาง
2. **โปรโตคอลการคัดเลือกผู้ตรวจสอบแบบไม่กำหนดตายตัว**
   ที่อาศัยการแฮชแบบสม่ำเสมอ [6]
3. **หลักการความสุดโต่งราคาแพง (Expensive Radicalism Principle)**
   ที่ตั้งราคาข้ออ้างตามระยะห่างจากฉันทามติของเครือข่าย
   ผ่านช่องทางต้นทุนที่ทบต้นกันสามช่องทาง
4. **แบบจำลองผู้มีอำนาจที่น่าเชื่อถือ (Reputable Authority model)**
   ที่มีแรงจูงใจแบบไม่สมมาตร
   ซึ่งการรับรองอันเป็นเท็จมีต้นทุนสูงกว่าค่าธรรมเนียมที่ชอบด้วย
5. **เส้นทางการโยกย้ายที่ค่อยเป็นค่อยไป**
   ผ่านโครงสร้างพื้นฐานทางการคลังแบบคู่ขนาน

2 หลักการออกแบบ

สถาปัตยกรรมของ RSN
ถูกกำกับด้วยหลักการออกแบบที่ต่อรองไม่ได้ห้าประการ

ความต่อเนื่องและวิวัฒนาการ
ระบบอยู่ร่วมกับสถาบันที่มีอยู่เดิมในช่วงเปลี่ยนผ่านที่มีระยะเวลาไม่แ
การเปลี่ยนผ่านต้องย้อนกลับได้ในทุกขั้นตอน

ความสมัครใจและความรับผิดชอบ
การเข้าร่วมเป็นไปโดยสมัครใจ
แต่ความสมัครใจถูกเชื่อมโยงกับความรับผิดชอบ
นั่นคือ ผู้เข้าร่วมที่รับหน้าที่ควบคุมบทบาทของสถาบันหนึ่งย่อมรับภา

ความหลากหลายและความเป็นกลางทางวัฒนธรรม
ฉันทามติผุดขึ้นจากปฏิสัมพันธ์แบบสองทาง
มิใช่จากกฎเกณฑ์ที่ตั้งไว้ล่วงหน้าซึ่งกำหนดโดยผู้ออกแบบระบบ

ความยืดหยุ่นและความต้านทานการเซ็นเซอร์
ต้นทุนของการเซ็นเซอร์เครือข่ายต้องสูงกว่าต้นทุนของการยอมทนต่อ
มีเพียงระบอบเผด็จการเบ็ดเสร็จอย่างสมบูรณ์เท่านั้น—
ด้วยต้นทุนทางการเมืองและเศรษฐกิจอันมหันต์—
ที่จะสามารถกดขี่ระบบนี้ได้

ฉันทามติและการบังคับใช้
ระบบเชื่อมโยงโน้มของพฤติกรรมในด้านความไว้ใจได้
ความอาฆาต และความสะใจในการแก้แค้นเข้าไว้เป็นคุณลักษณะรับ
การประพฤติผิดไม่ได้ถูกห้าม แต่ถูกตั้งราคา

3 ภาพรวมของระบบ

3.1 เครือข่ายสังคมชื่อเสียง

RSN คือชั้นการสื่อสารแบบเพียร์ทูเพียร์ (peer-to-peer) ที่กระจายศูนย์
ซึ่งผู้เข้าร่วมแลกเปลี่ยนข้อมูลที่ตรวจสอบได้เกี่ยวกับพฤติกรรมในโล
คุณสมบัติที่นิยามตัวมันได้แก่
โครงสร้างพื้นฐานที่กระจายศูนย์และเซ็นเซอร์ไม่ได้;
การเข้าร่วมแบบนามแฝงผ่าน DID;
โครงสร้างต้นทุนแบบไม่สมมาตร
(การอ่านมีราคาถูก การเขียนมีราคาแพง);

ความสามารถในการตรวจสอบทางวิทยาการเข้ารหัส; และ**การรองรับมาตรฐาน**— รูปแบบที่เครื่องอ่านได้สำหรับข้อมูลที่แพร่กระจายผ่านเครือข่าย สำหรับบริการที่ผู้มีอำนาจนำเสนอ (การประกอบข้ออ้าง การรับรอง บริการเป็นพยาน) และสำหรับรูปแบบนโยบายซึ่งรวมถึงกฎเกณฑ์สำหรับการประเมินชื่อเสียงของคู่สัญญา และการประเมินความเสี่ยงของความไม่สอดคล้องของนโยบาย (ระหว่างพฤติกรรมที่ประกาศไว้กับพฤติกรรมที่แท้จริง)

3.2 องค์ประกอบทางสถาปัตยกรรม

RSN ประกอบด้วยองค์ประกอบหลักสี่ส่วน (รูปที่ 1):

1. **ชั้น DID** อัตลักษณ์ของผู้เข้าร่วมพร้อมกฎที่ประกาศไว้ ข้อมูลอภิพันธุ์ชื่อเสียง และการกำหนดเส้นทางในเครือข่าย
2. **โปรโตคอลข้ออ้าง** รูปแบบที่มีโครงสร้างสำหรับการเผยแพร่คำยืนยันเกี่ยวกับเหตุการณ์ในโลกจริง
3. **เครือข่ายการตรวจสอบ** โปรโตคอลแบบกระจายศูนย์สำหรับการมอบหมายผู้ตรวจสอบโดยใช้การแฮชแบบสม่ำเสมอ
4. **ชั้นการรวบรวมชื่อเสียง** บริการที่ผลิตบทสรุปชื่อเสียงที่มนุษย์อ่านได้

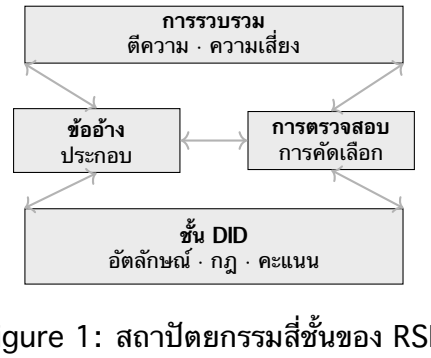

Figure 1: สถาปัตยกรรมสี่ชั้นของ RSN

3.3 บทบาทของผู้เข้าร่วม

ธุรกรรมการตรวจสอบหนึ่งเกี่ยวข้องกับบทบาท DID ที่แตกต่างกันได้มากถึงหกบทบาท (รูปที่ 2): **ผู้ออกข้ออ้าง** (DID_I สร้างและส่งข้ออ้าง), **ผู้เป็นเป้าหมายข้ออ้าง** (DID_S คือ DID ที่ข้ออ้างนั้นกล่าวถึง— อาจเป็นคนเดียวกับผู้ออกข้ออ้าง), **ผู้มีอำนาจ** (DID_A รับรองข้ออ้างโดยมีค่าธรรมเนียม; อาจเสนอบริการเป็นพยานด้วย— เป็นทางเลือก), **พยาน** ($DID_{W_{1..n}}$ ผู้เฝ้าสังเกตความซื่อสัตย์ของผู้ตรวจสอบแบบนิรนามผ่านรหัสสถานะ— เป็นทางเลือก), **ผู้ตรวจสอบ** (DID_V ถูกคัดเลือกโดยอัลกอริทึมเพื่อเผยแพร่ข้ออ้าง) และ **RSN** (เครือข่ายที่ข้ออ้างซึ่งผ่านการตรวจสอบแล้วถูกเผยแพร่) บทบาทใดๆ อาจถูกมอบหมายให้ DID อื่นได้ (หัวข้อ 7.4) ผู้มีอำนาจมักรวมการรับรองเข้ากับบริการเป็นพยาน แต่ทั้งสองหน้าที่นี้เป็นอิสระต่อกันในเชิงตรรกะ

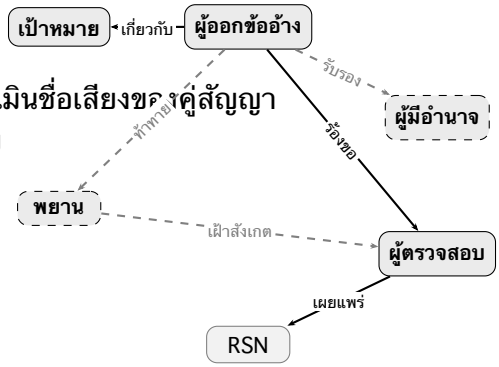

Figure 2: บทบาท DID ในธุรกรรมการตรวจสอบ เส้นประ = เป็นทางเลือก (ผู้มีอำนาจ พยาน)

3.4 ความไม่อาจทุจริตได้: สี่แรง

ความไม่อาจทุจริตได้ของ RSN มิได้เกิดจากกลไกเดียว แต่เกิดจากสี่แรงที่ทำงานพร้อมกัน ไม่มีแรงใดเพียงพอในตัวเอง มีเพียงการผสานกันของแรงเหล่านี้เท่านั้นที่ทำให้ความพยายามทุจริ

เป้าหมายที่คาดเดาไม่ได้ ผู้ตรวจสอบสำหรับแต่ละข้ออ้างถูกคัดเลือกแบบไม่กำหนดตายตัวผ่า (หัวข้อ 5.3) ผู้โจมตีไม่สามารถล็อกเป้าผู้ตรวจสอบรายใดรายหนึ่งไ เพราะอัตลักษณ์ของผู้ตรวจสอบเป็นฟังก์ชันของเนื้อหาข้ออ้างและกา มิใช่ตัวเลือกของผู้ออกข้ออ้าง

แรงเหนี่ยวนำด้านชื่อเสียง—ขึ้นช้าลงเร็ว ชื่อเสียงได้มาได้ทีละน้อยเท่านั้น ผ่านพฤติกรรมที่สม่ำเสมออย่างยั่งยืน อย่างไรก็ตาม ชื่อเสียงอาจสูญเสียไปอย่างมหันต์ด้วยการรับรองที่ฉ้อฉลเพียงครั้งเ (หัวข้อ 6.2) ความไม่สมมาตรนี้หมายความว่าชื่อเสียงที่สั่งสมมาหล กลยุทธ์ที่เหมาะสมที่สุดจึงยังคงเป็นการปฏิเสธข้ออ้างที่น่าสงสัย

คำมั่นสาธารณะ ผู้ถือ DID ทุกคนประกาศนโยบายของตนต่อสาธารณะ— ชุดกฎที่เครื่องอ่านได้ซึ่งพวกเขาให้คำมั่นว่าจะปฏิบัติตาม ความคลาดเคลื่อนระหว่างคำประกาศกับพฤติกรรมที่แท้จริงสามารถ (หัวข้อ 7.3) ความหน้าไหว้หลังหลอกจึงมีต้นทุนแพงกว่าความไม่ซื่อ

ความไม่สมมาตรของต้นทุนการโจมตีแบบตาข่าย ต้นทุนของการเซ็นเซอร์หรือการทำให้เครือข่ายไร้เสถียรภาพเติบโตเ ในขณะที่ต้นทุนของการยอมทนต่อมันคงที่ เพื่อให้การเซ็นเซอร์คุ้มค่า ผู้ปฏิบัติงานจะต้องใช้มาตรการนั้นทั่วทั้งเครือข่าย— ซึ่งต้องอาศัยมาตรการที่ไม่ได้สัดส่วนกับผลประโยชน์ใดที่นึกออก (หัวข้อ 10)

4 แบบจำลองอัตลักษณ์แบบกระจายศูนย์

4.1 DID พร้อมคุณสมบัติพิเศษ

RSN ขยายข้อกำหนด W3C DID Core [2] ด้วย: **กฎที่ประกาศไว้** (คำมั่นด้านพฤติกรรมที่เครื่องอ่านได้), **ข้อมูลอภิพันธุ์ชื่อเสียง** (คะแนนพฤติกรรมที่รวบรวมแล้ว) และ **การกำหนดเส้นทางในเครือข่าย** (เกตเวย์แบบหัวหอมที่เปลี่ยนแปลงได้ แยกออกจากตำแหน่งบนวงแหวนที่คงที่)

4.2 วงจรชีวิตของข้ออ้าง

ข้ออ้างหนึ่งดำเนินไปผ่านหกขั้นตอน (รูปที่ 3): การประกอบ การรับรองโดยผู้มีอำนาจ (ตามทางเลือก) การคัดเลือกผู้ตรวจสอบผ่านการแฮชแบบสม่ำเสมอ การตัดสินใจตรวจสอบ (ยอมรับหรือปฏิเสธพร้อมทำซ้ำ) การเผยแพร่ และการปรับปรุงชื่อเสียงสำหรับทุกฝ่าย

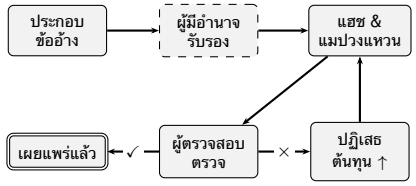

Figure 3: วงจรชีวิตของข้ออ้างพร้อมวงวนการทำซ้ำ

4.3 ความสัมพันธ์กับ W3C DID Core

แบบจำลองอัตลักษณ์ของ RSN เป็นเซตยิ่งยวด (superset) ที่ถูกต้องของข้อกำหนด W3C DID Core [2] DID ทั้งหมดของ RSN เป็น W3C DID ที่ถูกต้อง ส่วนขยายเฉพาะของ RSN ถูกเข้ารหัสเป็นคุณสมบัติของเอกสาร DID ที่นิยามไว้ในข้อกำหนดวิธีการ DID เฉพาะ ซึ่งเข้ากันได้กับโครงสร้างพื้นฐานที่มีอยู่เดิม เช่น ION [7] และ Ceramic [8]

5 การตรวจสอบและการแพร่กระจายข้อมูล

5.1 ต้นทุนของการป้อนข้อมูลเข้าสู่ระบบ

หลักการทางเศรษฐกิจแกนกลางของ RSN คือความไม่สมมาตรระหว่างการอ่านและการเขียน การอ่านข้อมูลชื่อเสียงเข้าใกล้ต้นทุนส่วนเพิ่มเป็นศูนย์สำหรับผู้เข้าร่วมที่เป็นสุจริต ในขณะที่การเขียน—การเข้าถึงตามสัดส่วนของชื่อเสียงของตน—ต้องอาศัยการลงทุนสะสมที่พิสูจน์ได้ในสามมิติ ได้แก่ **เวลา** (หลายปีของชีวิตที่ทุ่มเทให้พฤติกรรมที่สม่ำเสมอ คำมั่นที่ทำได้จริง และความสัมพันธ์ที่บ่มเพาะ), **พลังงาน** (ความพยายามที่ลงทุนไปกับการปฏิบัติต่อกันอย่างซื่อสัตย์ ความใส่ใจในหุ้นส่วน และความน่าไว้วางใจในระยะยาว) และ **เงิน** (การลงทุนในชื่อเสียงของตนเอง—การพัฒนาวิชาชีพ คุณภาพของงาน การชดใช้ความเสียหายที่ก่อขึ้น) ชื่อเสียงไม่สามารถซื้อได้ในทันที—มันคือผลลัพธ์ของการสั่งสมตลอดชีวิตซึ่งระบบเพียงทำให้มองเห็นได้ ต้นทุนทางเทคนิคครั้งเดียวของโปรโตคอล (ลายเซ็นทางวิทยาการเข้ารหัส ค่าธรรมเนียมผู้ตรวจสอบ) นั้นเล็กน้อยเมื่อเทียบกับการลงทุนพื้นฐานนี้

5.2 กราฟสังคมและความลึกของการติดต่อ

RSN โดยพื้นฐานแล้วคือเครือข่ายสังคม แต่ละ DID เพิ่มผู้ติดต่อ (DID อื่นๆ) ที่อนุญาตการเชื่อมต่อ ผู้ติดต่อเหล่านี้มีผู้ติดต่อของตนเอง และต่อเนื่องไปเช่นนี้ การค้นหาผู้ตรวจสอบด้วยอัลกอริทึมดำเนินการ h ของผู้ติดต่อที่เชื่อมโยงกันซึ่งกำหนดค่าได้ (เช่น $h = 3$: ผู้ติดต่อโดยตรงของตน ผู้ติดต่อของพวกเขา และผู้ติดต่อของผู้ติดต่อ) สถาปัตยกรรมนี้ไม่ต้องการบล็อกเชนระดับโลกเพียงหนึ่งเดียว—แต่เอื้อให้เกิดชุมชน/กลุ่มก้อนโดยธรรมชาติ ที่มีการทับซ้อนเข้าไปในชุมชนอื่นๆ ผู้เข้าร่วม DID ทุกคนต้องมี**นโยบาย**ที่เผยแพร่ไว้—ชุดกฎที่เครื่องอ่านได้ซึ่งกำกับว่าคำร้องขอที่เข้ามาจะได้รับการประเมิน การละเมิดนโยบายจะถูกบันทึกในเครือข่ายในฐานะสิ่งประดิษฐ์เชิงลบ (negative artifacts)

5.3 การคัดเลือกผู้ตรวจสอบด้วยอัลกอริทึม

โปรโตคอลการตรวจสอบใช้การแฮชแบบสม่ำเสมอ [6] (รูปที่ 4) การตรวจสอบเป็นบริการที่มีค่าใช้จ่าย ผู้ตรวจสอบดำเนินการโดยมีค่าธรรมเนียม ก่อให้เกิดตลาดที่การแข่งขันผลักดันการตั้งราคา ความเร็ว และความน่าเชื่อถือ

ขั้นที่ 1 เอกสารข้ออ้างถูกต่อเข้ากับผลลัพธ์แฮชของการทำซ้ำครั้งก่อน (หรือ $\varnothing$ ในการทำซ้ำครั้งแรก) แล้วนำไปแฮช:

$$\text{position} = H(\text{claim_id} \,\|\, \text{round_seed}) \quad (1)$$

อัลกอริทึมต้องรวมเส้นทางที่สมบูรณ์ของคำร้องขอและการตอบสนองฉบับเต็มของผู้ตรวจสอบแต่ละราย มิใช่เพียงแฮชของการทำซ้ำครั้งก่อน การตอบสนองฉบับเต็มของผู้ตรวจสอบแต่ละราย (การยอมรับ การปฏิเสธ ราคาที่เสนอ เหตุผล) ถูกต่อเข้ากับเอกสารที่เติบโตขึ้น ซึ่งตรวจสอบได้ผ่านลายเซ็นทางวิทยาการเข้ารหัสในทุกขั้นตอน

ขั้นที่ 2 แฮชถูกแมปไปยัง N ตำแหน่งบนวงแหวนแฮชแบบสม่ำเสมอ กระจายอย่างสม่ำเสมอ (เช่น สำหรับ $N = 4$: $+0°, +90°, +180°, +270°$) จากแต่ละตำแหน่ง การค้นหาตามเข็มนาฬิกาจะเลือก DID ที่ใกล้ที่สุดเป็นผู้ตรวจสอบตัวเลือก (รูปที่ 5) N เป็นพารามิเตอร์แปรผันที่อาจขึ้นอยู่กับเปอร์เซ็นต์ของ DID ที่กำลังใช้งานอยู่ในปัจจุบัน เวลาของวัน หรือการตอบสนองในอดีตของเครือข่าย

ขั้นที่ 3 ผู้ตรวจสอบยอมรับ (เผยแพร่พร้อมเดิมพันชื่อเสียง) หรือปฏิเสธ (กลับไปยังขั้นที่ 1 พร้อมแฮชของการปฏิเสธ) เมื่อโหนดหนึ่งไม่ตอบสนองทั้งที่ประกาศสถานะออนไลน์ คำร้องขอครั้งถัดไปต้องรวมการตอบสนองทั้งหมดจากผู้ตรวจสอบตัวเลือกทั้ง N รายก่อนหน้า

การต้านการเอาเปรียบ (anti-leeching) DID ที่เป็นเป้าหมายอาจตั้งค่าธรรมเนียมหรือข้อจำกัดการเข้าถึงสำหรับคำสอบถามจาก DID ใหม่ที่มีชื่อเสียงน้อย กลไกแบบเป็นลำดับขั้นนี้ (มิใช่แบบทวิภาค) บังคับให้ผู้มาใหม่ต้องสร้างชื่อเสียงผ่านกิจกรรมที่แท้จริงก่อนที่จะเข้าถึงข้อมูลของผู้อื่นได้อย่างเต็มที่

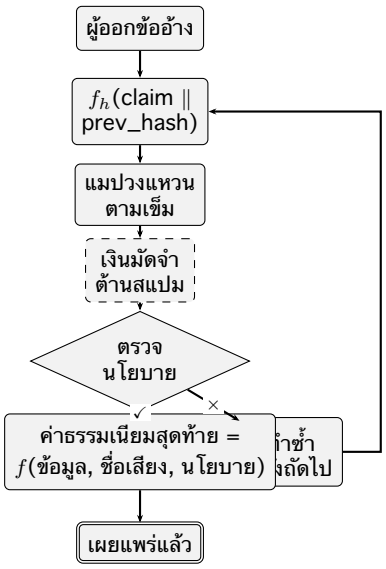

Figure 4: โปรโตคอลการคัดเลือกผู้ตรวจสอบ เงินมัดจำต้านสแปมเป็นทางเลือกและอาจคืนได้ ค่าธรรมเนียมสุดท้ายชำระเมื่อได้รับการยอมรับเท่านั้น

การปฏิเสธแต่ละครั้งจะต่อการตอบสนองฉบับเต็มของผู้ตรวจสอบ (รวมทั้งเหตุผลและเงื่อนไข) เข้ากับเอกสารข้ออ้าง ทำให้เนื้อหาขยายออก จากเอกสารที่ขยายแล้ว แฮชใหม่จะถูกคำนวณ ซึ่งไม่สามารถคาดเดาได้ล่วงหน้าโดยไม่ทราบการตอบสนองทั้งหมดก่อนหน้านี้ทั้งหมด

แมปไปยังตำแหน่งบนวงแหวนที่ต่างออกไป และคัดเลือกผู้ตรวจสอบที่ต่างออกไป การจัดทำเอกสารเส้นทางฉบับเต็มเป็นข้อบังคับ— ผู้ออกข้ออ้างไม่สามารถคาดเดาหรือมีอิทธิพลต่อผู้ตรวจสอบรายถัดไ หากผู้ตรวจสอบเพิกเฉยต่อคำร้องขอทั้งที่มีนโยบายที่ประกาศไว้เข้าก พยาน (หากมี) จะบันทึกเหตุการณ์นี้ และผู้ออกข้ออ้างอาจแนบหลักฐานจากพยานได้เมื่อเผยแพร่ครั้งสุดท้

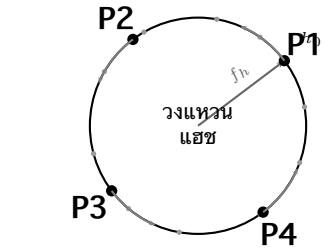

Figure 5: การคัดเลือกแบบหลายจุด (N=4) แฮช h_0 กำหนดออฟเซต; 4 จุดกระจายอย่างสม่ำเสมอจาก h_0

5.4 โปรโตคอลพยาน

บทบาท**พยาน** ให้ความรับผิดชอบแบบนิรนามต่อความซื่อสัตย์ของผู้ต ผ่านโปรโตคอลรหัสท้าทายทางวิทยาการเข้ารหัส:

ขั้น W1 ผู้ร้องขอเข้ารหัสคำร้องขอที่ได้รับการรับรองและส่งไปยังพยาน N_w ราย—ผู้ติดต่อจากเครือข่ายสังคมของผู้ร้องขอ หรือผู้ให้บริการพยานเฉพาะทางที่ดำเนินการโดยมีค่าธรรมเนียม

ขั้น W2 พยาน w_i แต่ละรายเซ็นคำร้องขอที่เซ็นแล้วทั้งฉบับ เก็บลายเซ็นต้นฉบับ σ_i ไว้ และคำนวณรหัสท้าทาย $c_i = h(\sigma_i)$ รหัสท้าทายจะถูกต่อเข้ากับคำร้องขอ

ขั้น W3 คำร้องขอซึ่งบัดนี้พกพารหัสท้าทาย N_w รหัส ถูกส่งไปยังผู้ตรวจสอบ ผู้ตรวจสอบมองเห็นรหัสเหล่านั้นแต่ไม่สามารถระบุได้ว่าใครคือพยา หรือรหัสเหล่านั้นตรงกับลายเซ็นจริงหรือไม่

ขั้น W4 (ผู้ตรวจสอบซื่อสัตย์) หากผู้ตรวจสอบตอบสนองตามนโยบายที่ประกาศไว้ รหัสท้าทายจะคงความทึบแสงไว้ พยานจะไม่ถูกเปิดเผยเลย ไม่มีการเผยแพร่ข้อมูลเพิ่มเติม

ขั้น W5 (การละเมิดนโยบาย) หากผู้ตรวจสอบละเมิดนโยบายของตน (เพิกเฉยต่อคำร้องขอ ตอบสนองอย่างไม่สอดคล้อง) ผู้ร้องขอจะถือลายเซ็นต้นฉบับ σ_i ของพยานไว้ ลายเซ็นเหล่านี้สามารถเผยแพร่เป็นข้อมูลประกอบได้ ใครก็ตามสามารถตรวจสอบ $c_i = h(\sigma_i)$ พิสูจน์ได้ว่าพยานอยู่ในเหตุการณ์

ผู้ร้องขอสามารถเผยแพร่ได้โดยอิสระ—
ผู้ตรวจสอบได้เซ็นรหัสท้าทายไว้ในการตอบสนองของตนแล้ว

คุณสมบัติการหลอกลวง (bluff property)
ผู้ร้องขออาจแทนที่รหัสท้าทายบางส่วนหรือทั้งหมดด้วยค่าสุ่ม
ผู้ตรวจสอบไม่สามารถแยกแยะรหัสของจริง
(ที่หนุนหลังโดยผู้มีอำนาจชื่อเสียงสูง)
ออกจากสัญญาณรบกวนได้
ความไม่แน่นอนนี้คือกลไกการบังคับใช้
ทุกคำร้องขอพกพาความเสี่ยงที่ว่าผู้มีอำนาจที่ได้รับการเคารพกำลังเฝ้าดูอยู่แบบนิรนาม
ต้นทุนของการรักษาแรงกดดันนี้เข้าใกล้ศูนย์
(การสุ่มตัวเลข) ในขณะที่ต้นทุนที่อาจเกิดขึ้นจากความไม่ซื่อสัตย์ของผู้ตรวจสอบนั้นไม่มีที่สิ้นสุด
พฤติกรรมซื่อสัตย์จึงถูกจูงใจแม้ในภาวะที่ไม่มีพยานอยู่จริง

ผู้มีอำนาจในฐานะพยาน
ผู้มีอำนาจที่รับรองข้ออ้างหนึ่งอาจรวมบริการพยานเข้าไปด้วย:
“ข้าพเจ้ารับรองข้ออ้างของท่านและทำหน้าที่เป็นพยานนิรนามระหว่างการตรวจสอบ”
นี่คือโมเดลธุรกิจที่เป็นธรรมชาติ—
ผู้มีอำนาจมีบริบทอยู่แล้ว อย่างไรก็ตาม
บทบาททั้งสองเป็นอิสระต่อกันในเชิงตรรกะ

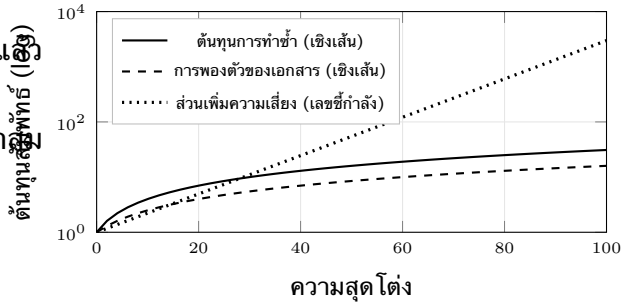

Figure 6: การทวีขึ้นของต้นทุนใน 3 ช่องทาง ส่วนเพิ่มความเสี่ยงครอบงำที่ระดับความสุดโต่งสูง

Table 1: การเปรียบเทียบต้นทุนตามประเภทข้ออ้าง

ประเภท	ทำซ้ำ	เอกสาร	ค่าธรรม.	รวม
น่าเชื่อถือ	k_{min}	B_0	P_{min}	ต่ำ
เป็นที่ถกเถียง	k_{med}	$B_0+k\Delta$	$\alpha e^{\beta d}$	ปานกลาง
สุดโต่ง	k_{max}	$\gg B_0$	$\gg P_{\text{min}}$	สูงมาก
ฉ้อฉล	$\to \infty$	—	—	เผยแพร่ไม่ได้

5.5 หลักการความสุดโต่งราคาแพง

ช่องทางต้นทุนสามช่องทางทบต้นกันพร้อมกัน
(รูปที่ 6):

ช่องทางที่ 1: ต้นทุนการทำซ้ำ
การปฏิเสธแต่ละครั้งบังคับให้เกิดการทำซ้ำใหม่ที่กินเวลาและทรัพยากร
เติบโตแบบเชิงเส้น

ช่องทางที่ 2: การพองตัวของเอกสาร
การทำซ้ำแต่ละครั้งเพิ่มการตอบสนองฉบับเต็มของผู้ตรวจสอบเข้าไปในเอกสารข้ออ้าง
การเติบโตเป็นเชิงเส้น แต่มีค่าฐานเริ่มต้น
นั่นคือ เพย์โหลดเริ่มต้น
(เนื้อหาข้ออ้าง การรับรองของผู้มีอำนาจ
ลายเซ็นทางวิทยาการเข้ารหัส)
มีขนาดที่ไม่ใช่เรื่องเล็กน้อยอยู่แล้วที่ B_0
ขนาดรวมหลังจากทำซ้ำ k ครั้ง: $S(k) = B_0 + k \cdot \Delta$
โดยที่ Δ คือขนาดเฉลี่ยของการตอบสนอง

ช่องทางที่ 3: ส่วนเพิ่มความเสี่ยงของผู้ตรวจสอบ
ความเสี่ยงเป็นเรื่องอัตวิสัย
ผู้ตรวจสอบประเมินว่านโยบายที่ประกาศไว้ของ
DID ผู้ร้องขอขัดแย้งกับผลประโยชน์ทางการค้า
สังคม หรือการเมืองของผู้ตรวจสอบเองหรือไม่
ส่วนเพิ่มอาจทวีขึ้นแบบเลขชี้กำลังตามระยะห่างที่รับรู้จาก
“อุดมคติ” ของผู้ตรวจสอบ: $P(d) = \alpha \cdot e^{\beta d}$ โดยที่
d คือมาตรระยะห่างเชิงอัตวิสัยของผู้ตรวจสอบ
เมื่อเลยเส้นแบ่งเขตห้ามเข้าส่วนตัวไปแล้ว
ผู้ตรวจสอบอาจปฏิเสธโดยสิ้นเชิง

ที่สำคัญ นี่ไม่ใช่การเซ็นเซอร์ ไม่มีข้ออ้างใดถูกห้าม
ระบบตั้งราคาความเสี่ยง (ตารางที่ 1)

6 ชื่อเสียงและการประเมินความเสี่ยง

6.1 แบบจำลองการสั่งสมชื่อเสียง

ชื่อเสียงแสดงคุณสมบัติสามประการ
ได้แก่ **การสั่งสมอย่างเชื่องช้า**
(การเติบโตทีละน้อยผ่านพฤติกรรมที่สม่ำเสมอ),
การถูกทำลายอย่างรวดเร็ว
(การฉ้อฉลเพียงครั้งเดียวสามารถลดคะแนนได้อย่างมหันต์)
และ **การประเมินเป็นรายบุคคล**
(แต่ละฝ่ายที่บริโภคข้อมูลอาจใช้ฟังก์ชันการรวบรวมของตนเอง)

6.2 ผู้มีอำนาจที่น่าเชื่อถือ

ผู้มีอำนาจที่น่าเชื่อถือทบทวนข้ออ้าง และหากพึงพอใจ
ก็ร่วมเซ็นรับรอง—โดยเดิมพันชื่อเสียงของตนเอง
(รูปที่ 7) ความไม่สมมาตรนี้เป็นไปโดยการออกแบบ
นั่นคือ การได้มาซึ่งชื่อเสียงเป็นไปอย่างเชื่องช้า
(เพิ่มขึ้น $+\delta$ ต่อการรับรองที่ซื่อสัตย์แต่ละครั้ง)
ในขณะที่การสูญเสียมันเป็นไปอย่างมหันต์
($-\Delta \gg \delta$ ต่อการรับรองอันเป็นเท็จแต่ละครั้ง;
เพื่อเป็นตัวอย่าง เช่น $+2\%$ เทียบกับ -70%)
กลยุทธ์ที่เหมาะสมที่สุดคือการปฏิเสธข้ออ้างที่น่าสงสัยเสมอ
ค่าเฉพาะของ δ และ Δ เป็นพารามิเตอร์ของระบบ

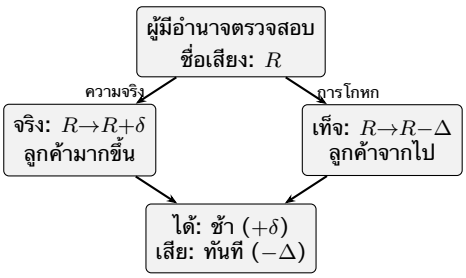

Figure 7: ผู้มีอำนาจที่น่าเชื่อถือ—แรงจูงใจแบบไม่สมมาตร

6.3 ชื่อเสียงหลายมิติ

ชื่อเสียงไม่ใช่ปริมาณสเกลาร์
แต่เป็นเวกเตอร์ที่ทอดข้ามหลายมิติ
ได้แก่ ความน่าเชื่อถือทางการเงิน
ความซื่อสัตย์ส่วนบุคคล ความสามารถทางวิชาชีพ
การมีส่วนร่วมทางพลเมือง และอื่นๆ (รูปที่ 8)
ผู้ให้บริการประเมินที่แตกต่างกันฉายเวกเตอร์นี้แตกต่างกันขึ้นอยู่กับบริบท—
ผู้ให้กู้ให้ความสำคัญกับความน่าเชื่อถือทางการเงิน
นายจ้างให้ความสำคัญกับความสามารถทางวิชาชีพ
เพื่อนบ้านให้ความสำคัญกับพฤติกรรมทางพลเมือง
ไม่มีคะแนนชื่อเสียงที่ “ถูกต้อง” เพียงหนึ่งเดียว
มีเพียงมุมมองที่ต่างกัน

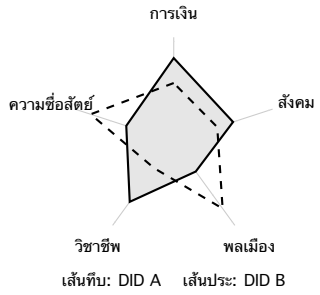

Figure 8: เวกเตอร์ชื่อเสียงหลายมิติ DID ที่ต่างกันแสดงโปรไฟล์ที่ต่างกันในแต่ละมิติ

6.4 การประเมินความเสี่ยงที่เป็นประชาธิปไตย

RSN ทำให้การประเมินความเสี่ยงอย่างเป็นระบบเป็นประชาธิปไตย—
ความสามารถที่ปัจจุบันกระจุกตัวอยู่ในสถาบันการเงิน
แต่ประยุกต์ใช้ได้ไกลเกินกว่าแวดวงการธนาคาร
กลุ่มบริษัทอุตสาหกรรมที่ประเมินความน่าเชื่อถือของซัพพลายเออร์
บริษัทประกันที่ตั้งราคาความเสี่ยงด้านพฤติกรรม
การตรวจสอบสถานะกิจการสำหรับการควบรวมและซื้อกิจการ
การประมาณอายุการใช้งานของอุปกรณ์ในภาคการผลิต—
ทุกที่ที่ความเสี่ยงของคู่สัญญาต้องได้รับการประเมิน
RSN มอบทางเลือกที่กระจายศูนย์และขับเคลื่อนด้วยตลาด
ตลาดของบริการตีความจะแปลข้อมูลชื่อเสียงหลายมิติดิบ[illegible]

ทำให้การประเมินคู่สัญญาเข้าถึงได้สำหรับผู้เข้าร่วมทุกคนที่ต้นทุนส่

7 ฉันทามติและการระงับข้อพิพาท

7.1 แบบจำลองความยุติธรรมแบบกระจายศูนย์

RSN วางกรอบความยุติธรรมใหม่ในฐานะปัญหาการเจรจาต่อรองแ
ภัยคุกคามของความเสียหายต่อชื่อเสียงที่ถาวรและตรวจสอบได้เป็น

7.2 ฉันทามติแบบผุดขึ้นเอง

ผู้เข้าร่วมแต่ละคนรักษาเกณฑ์ความพึงพอใจส่วนบุคคลไว้
ฉันทามติโดยรวมของเครือข่ายผุดขึ้นในฐานะค่าเฉลี่ยทางสถิติของก
(รูปที่ 9) การตอบสนองที่สูงกว่าฉันทามติมาก
(ป่าเถื่อน) มีราคาแพงในการเผยแพร่
การตอบสนองที่ใกล้ฉันทามติ (ได้สัดส่วน) มีราคาถูก
ฉันทามติไม่ใช่กฎ—มันคือสัญญาณราคา

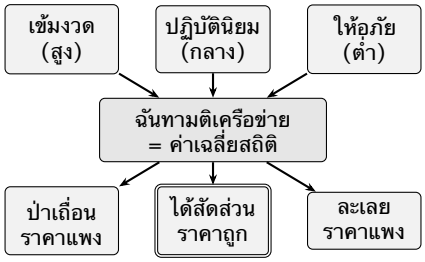

Figure 9: ฉันทามติแบบผุดขึ้นเองจากเกณฑ์ความพึงพอใจของแต่ล

7.3 การปรับเทียบบทลงโทษ

ผู้ถือ DID แต่ละคนประกาศต่อสาธารณะถึงการตอบสนองต่อประเภท
คำประกาศที่รุนแรงหรือผ่อนปรนอย่างไม่ได้สัดส่วนจะดึงดูดสัญญาณ
คำประกาศที่ได้สัดส่วนจะได้รับการยอมรับโดยไม่มีแรงเสียดทาน—
ระบบบทลงโทษที่ปรับเทียบตัวเอง

คำประกาศฉันทามติเองก็อยู่ภายใต้การตรวจจับความหน้าไหว้หล
การให้คำมั่นในเชิงประกาศต่อจุดยืนที่เป็นฉันทามติในขณะที่ประพฤ
ถือเป็นความผิดด้านชื่อเสียงที่ร้ายแรงกว่าการเบี่ยงเบนพื้นฐาน
เพราะแสดงให้เห็นถึงการหลอกลวงโดยเจตนา

7.4 การมอบหมาย

กิจกรรมทั้งหมดภายใน DID หนึ่ง—
โดยมีข้อยกเว้นหนึ่งประการ—สามารถมอบหมายให้
DID อื่นได้ **บทบาทเป้าหมาย—DID**
ที่ข้ออ้างกล่าวถึงพฤติกรรมของมัน—
ไม่สามารถมอบหมายได้;
[illegible]

บทบาทที่ทำงานอยู่อื่นๆ—ผู้ออกข้ออ้าง ผู้มีอำนาจ พยาน ผู้ตรวจสอบ— สามารถโอนย้ายให้ DID ตัวแทนที่กำหนดได้ ไม่ว่าจะเพื่อการตรวจสอบ การส่งข้ออ้าง การมีส่วนร่วมในฉันทามติ หรือการระงับข้อพิพาท การมอบหมายสามารถเพิกถอนได้ทุกเมื่อ สิ่งนี้เปิดโอกาสให้เกิดความเชี่ยวชาญเฉพาะทาง (เช่น บริการตรวจสอบระดับมืออาชีพ) ในขณะที่ผู้ถือยังคงมีการควบคุมและความรับผิดชอบสูงสุด การมอบหมายใช้ได้ทั่วทั้งระบบและจำเป็นต่อการขยายขนาด

7.5 จากศีลธรรมของปัจเจกสู่สัญญาประชาคมแบบผุดขึ้นเอง

นโยบายที่ประกาศไว้ของแต่ละ DID เป็นการทำให้ศีลธรรมของปัจเจกเป็นรูปธรรม นั่นคือ สิ่งที่ผู้ถือถือว่ายอมรับได้ วิธีที่พวกเขาตอบสนองต่อพฤติกรรมเฉพาะ สิ่งที่พวกเขาเรียกร้องจากคู่สัญญา นโยบายเหล่านี้ไม่ได้ถูกกำหนดโดยผู้ออกแบบระบบ— แต่ถูกเลือกโดยผู้เข้าร่วมแต่ละคนและแสดงออกในรูปแบบที่ตรวจสอบได้

การทำให้เป็นรูปธรรมนี้เปิดทางให้เกิดการผุดขึ้นสามขั้น ขั้นแรก ศีลธรรมของปัจเจกถูกเข้ารหัสเป็น**นโยบาย**— ชุดกฎที่ประกาศไว้ เกณฑ์ และฟังก์ชันการตอบสนองที่ DID ให้คำมั่นว่าจะปฏิบัติตาม ขั้นที่สอง ผลรวมของนโยบายทั้งหมดทั่วเครือข่ายก่อให้เกิด**จริยธรรมแบบผุดขึ้นเอง**— บรรทัดฐานที่สังเกตได้ทางสถิติซึ่งไม่มีผู้เข้าร่วมคนใดออกแบบไว้ แต่เกิดขึ้นจากปฏิสัมพันธ์ของจุดยืนทางศีลธรรมของปัจเจกนับพัน[9] ขั้นที่สาม จริยธรรมแบบผุดขึ้นเองเหล่านี้ ซึ่งแสดงออกในฐานะบรรทัดฐานพฤติกรรมร่วมที่บังคับใช้ผ่านสัญญาอัจฉริยะแบบสองทาง ประกอบกันเป็น**สัญญาประชาคมที่วัดได้**— มิใช่โครงสร้างเชิงทฤษฎีที่ไม่มีใครเซ็น [10] แต่เป็นชุดกฎที่สังเกตได้เชิงประจักษ์ซึ่งหนุนหลังด้วยพฤติกรรมจริง

กระบวนการนี้สะท้อนข้อค้นพบจากทฤษฎีรากฐานทางศีลธรรม (moral foundations theory) [11]: ศีลธรรมของมนุษย์เป็นสิ่งที่รู้ได้โดยสัญชาตญาณ มีพหุนิยม และผันแปรตามวัฒนธรรม RSN ไม่ต้องการฉันทามติทางศีลธรรมเป็นปัจจัยนำเข้า แต่ผลิตฉันทามติเชิงพฤติกรรมเป็นผลลัพธ์ สัญญาประชาคมที่เกิดขึ้นไม่ใช่สิ่งสถิต— มันวิวัฒน์ไปตามที่ผู้เข้าร่วมเข้ามา ออกไป และปรับนโยบายของตนเพื่อตอบสนองต่อการป้อนกลับของเครือข่าย ต่างจากทฤษฎีสัญญาประชาคมแบบดั้งเดิม สัญญานี้เพิกถอนได้ สังเกตได้ และบังคับใช้ได้โดยไม่ต้องมีองค์อธิปัตย์

8 แบบจำลองทางเศรษฐกิจ

หัวข้อก่อนหน้านี้ได้บรรยายถึงเครื่องมือ— กลไกการตรวจสอบ โครงสร้างต้นทุน และฉันทามติแบบผุดขึ้นเองของ RSN หัวข้อนี้บรรยายถึงระเบียบวิธีในการประยุกต์ใช้เครื่องมือนี้กับการเป เครื่องมือนี้ใช้ได้ทั่วไป ส่วนระเบียบวิธีด้านล่างเป็นการประยุกต์ใช้ที่เป็นไปได้หนึ่งอย่าง

8.1 โครงสร้างแรงจูงใจ

ชื่อเสียงในฐานะทุนสร้างแรงจูงใจโดยตรงต่อพฤติกรรมที่ซื่อสัตย์ ในการดำเนินการปกติ ผู้เข้าร่วมสร้างชื่อเสียงโดยธรรมชาติผ่านธุรกรรมประจำวันและคำมั่น ค่าใช้จ่ายหลักคือข้ออ้างเชิงลบ— การบันทึกความเสียหายที่ผู้อื่นก่อขึ้น ความไม่สมมาตรนี้จูงใจพฤติกรรมที่มีประโยชน์และน่าไว้วางใจ นั่นคือ การซื่อสัตย์ไม่มีต้นทุนเพิ่มเติม ในขณะที่การก่อความเสียหายสร้างร่องรอยที่มีการจัดทำเอกสารซึ่งผู [illegible] ค่าใช้จ่ายที่ตามมาในภายหลัง— การประกาศกฎโดยไม่ปฏิบัติตาม— เป็นรูปแบบความล้มเหลวที่แพงที่สุด เพราะแสดงให้เห็นถึงการหลอกลวงโดยเจตนา

8.2 ระบบการคลังแบบคู่ขนาน

องค์ประกอบสามส่วนเปิดทางให้เกิดแรงกดดันจากการแข่งขัน: (1) **ภาษีอย่างง่าย (Simple Tax)**— อัตราตามสัดส่วนเดียวโดยไม่มีข้อยกเว้น เริ่มแรกอยู่ต่ำกว่าอัตราที่แท้จริงที่มีอยู่เพียงเล็กน้อย; (2) **การลงทะเบียนรายจ่ายอิเล็กทรอนิกส์ (Electronic Spending Registration, ESR)**—การกลับด้านโมเดล EET ของเช็ก เพื่อให้พลเมืองสอดส่องรายจ่ายของรัฐ; (3) **การจัดสรรภาษีที่พลเมืองกำกับ**— เริ่มต้นที่ไม่กี่เปอร์เซ็นต์ในปีแรก และไปถึง หลังจากหนึ่งทศวรรษ ที่ระดับตั้งแต่เลขสองหลักช่วงต้นไปจนถึงการโยกย้ายเต็มรูปแบบสู่ร ขึ้นอยู่กับอัตราการยอมรับ จังหวะที่แท้จริงขึ้นอยู่กับความเร็วที่ทางเลือกตลาดเสรีต่อบริการของ และความเต็มใจของรัฐในการร่วมมือกับการเปลี่ยนผ่าน ฟังก์ชันของเวลาไม่จำเป็นต้องเป็นเชิงเส้น และไม่มีเหตุผลใดที่จะตั้งขอบเขตบนว่าการยอมรับจะไปถึงระดับใด

9 เส้นทางการโยกย้าย

การโยกย้ายดำเนินไปผ่านสามระยะ (รูปที่ 10): **ระยะที่ 1: การซ้อนทับ** (RSN ในฐานะชั้นข้อมูล รัฐเป็นผู้ให้บริการเพียงรายเดียว), **ระยะที่ 2: การแข่งขัน** (RSN มอบทางเลือกที่ใช้งานได้จริง มีการใช้งานระบบคู่) และ **ระยะที่ 3: การเปลี่ยนผ่าน** (RSN ทำได้ดีกว่าสิ่งเทียบเท่าของรัฐ การโยกย้ายโดยสมัครใจ)
การเปลี่ยนผ่านย้อนกลับได้ในทุกขั้นตอน

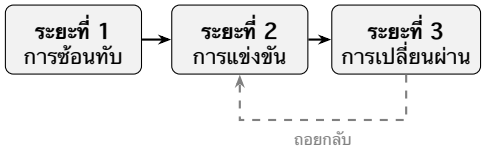

Figure 10: การโยกย้ายสามระยะ—ย้อนกลับได้ในทุกขั้นตอน

กลไกแรงกดดันหลักคือด้านการคลัง เมื่อผู้เสียภาษีแบบมีเงื่อนไขไปถึง “ชนกลุ่มน้อยที่มีนัยสำคัญทางเศรษฐกิจ X”—กลุ่มที่ใหญ่พอที่การปราบปรามต่อกลุ่มนี้จะก่อความเสียหายทางเศรษฐกิจที่ไม่ใช่เรื่องเล็กน้อย และการดื้อแพ่งกลายเป็นภัยคุกคามที่น่าเชื่อถือ—รัฐก็เข้าสู่การเจรจา เพื่อเป็นตัวอย่าง เราใช้ $X \approx 15\%$ ของ GDP แต่เกณฑ์ที่แท้จริงขึ้นอยู่กับเศรษฐกิจเฉพาะแห่ง

10 การวิเคราะห์ความมั่นคง

เราพิจารณาปฏิปักษ์ห้าประเภท ได้แก่ ผู้กระทำผิดรายบุคคล กลุ่มที่จัดตั้ง ปฏิปักษ์ระดับองค์กร ปฏิปักษ์ระดับรัฐ และปฏิปักษ์ระดับโปรโตคอล

ความต้านทานซิบิล (Sybil resistance) [12] การสร้างชื่อเสียงต้องอาศัยปฏิสัมพันธ์ที่ต่อเนื่องและตรวจสอบได้ ต้นทุนของการโจมตีซิบิลที่สำเร็จเพิ่มขึ้นแบบเชิงเส้นตามจำนวนอัตลักษณ์ และแบบกำลังสองตามระดับชื่อเสียงเป้าหมาย การดำเนินการหลาย DID พร้อมกันเป็นไปได้แต่แพงโดยการออกแบบ—แต่ละอัตลักษณ์ต้องสั่งสมชื่อเสียงด้วยตนเองอย่างอิสระผ่านการมีส่วนร่วมที่แท้จริง ในสังคมเสรี ต้นทุนนี้ยับยั้งการใช้ในทางที่ผิดแบบไม่จริงจัง ในระบอบเผด็จการ DID แบบคู่ขนานกลายเป็นเครื่องมือเอาชีวิตรอด ที่เปิดทางให้เกิดการต่อต้านแบบแยกส่วน การประสานงานใต้ดิน และการเดินทางในตลาดมืดที่ปลอดภัยยิ่งขึ้น

การป้องกันการสมรู้ร่วมคิด รูปแบบของการรับรองซึ่งกันและกันในหมู่กลุ่มปิดสามารถตรวจจับได้ผ่านการวิเคราะห์กราฟ ฟังก์ชันการรวบรวมชื่อเสียงจะลดทอนน้ำหนักข้ออ้างจากแหล่งที่รวม

ปฏิปักษ์ระดับรัฐ การกำหนดเส้นทางแบบหัวหอม การไร้ซึ่งโครงสร้างพื้นฐานแบบรวมศูนย์ และการกระจายบทบาทผู้ตรวจสอบไปทั่วฐานผู้เข้าร่วม ทำให้มั่นใจได้ว่าการกดขี่ต้องอาศัยมาตรการที่ไม่ได้สัดส่วนกับผลป

ความเป็นส่วนตัวเทียบกับความรับผิดชอบ ความเป็นนามแฝง—จุดกึ่งกลางระหว่างความนิรนามกับการเปิดเผย เปิดโอกาสให้ DID สั่งสมชื่อเสียงที่มีความหมายได้โดยไม่ต้องเปิดเผ

11 ข้อพิจารณาด้านความเป็นส่วนตัว

แบบจำลองความเป็นส่วนตัวของ RSN สร้างขึ้นบนความเป็นนามแฝง ผู้ถือควบคุมการเปิดเผยอัตลักษณ์: ขั้นต่ำ (นามแฝงล้วน) เลือกเฉพาะส่วน (เชื่อมโยงหนังสือรับรองเฉพาะ) หรือเต็มรูปแบบ (ผูกอัตลักษณ์ตามกฎหมาย) ข้ออ้างที่เผยแพร่แล้วเป็นสิ่งถาวร—ระบบรองรับการแก้ไขตามบริบทแต่ไม่รองรับการลบทิ้ง ผู้ถืออาจละทิ้ง DID ที่ถูกละเมิดและเริ่มต้นใหม่ โดยยอมสละชื่อเสียงที่สั่งสมมา

12 งานที่เกี่ยวข้อง

ข้อกำหนด W3C DID Core [2] และเครือข่าย Ceramic [8] มอบรากฐานด้านอัตลักษณ์ EigenTrust [13] ได้สาธิตการรวบรวมชื่อเสียงแบบกระจายศูนย์โดยไม่มีผู้มีอำนาจส่ว SBTs [3] ได้นำเสนอโทเคนสังคมที่โอนกันไม่ได้ RSN แตกต่างในการเน้นต้นทุนทางเศรษฐกิจในฐานะตัวกรองคุณภาพ และในกลไกการตั้งราคาความสุดโต่ง

DAOs [4] และการลงคะแนนแบบกำลังสอง [5] ได้สาธิตความเป็นไปได้ของการปกครองแบบกระจายศูนย์ RSN ได้ฉันทามติจากการเจรจาต่อรองราคาแบบสองทางแทนที่จะเป็ ข้อเสนอนี้อยู่ในกรอบปรัชญาอนาธิปไตยทุนนิยม (anarcho-capitalist) [14, 15] สำหรับการจัดหาบริการแบบเอกชน แต่แตกต่างในสองประเด็นสำคัญ นั่นคือ มันออกแบบเพื่อรับมือกับความอาฆาตและแรงกระตุ้นในการแก้แค้น มันไม่ได้สันนิษฐานที่จะสมมติความมีเหตุผล และมันเสนอการเปลี่ยนผ่านที่ค่อยเป็นค่อยไปแทนการปฏิวัติ แนวคิดสัญญาประชาคมแบบผุดขึ้นเองมีที่มาจากทฤษฎีระเบียบที่เกิ (spontaneous order) ของ Hayek [16]

อนาธิปไตยแบบอะกอริสม์ (Anarcho-agorism) RSN มีจุดร่วมสำคัญกับเศรษฐศาสตร์ตอบโต้แบบอะกอริสม์ (agorism) [17]—

โดยเฉพาะการเน้นการสร้างสถาบันคู่ขนานและการแลกเปลี่ยนโดยสมัครใจ
อย่างไรก็ตาม อะกอริสม์มีแนวโน้มที่จะสมมติว่าผลประโยชน์ส่วนตัวเป็นแรงจูงใจ
และมักขาดเส้นทางการโยกย้ายที่เป็นรูปธรรมจากโครงสร้างที่มีอยู่
RSN ผนวกแนวโน้มพฤติกรรมที่ไม่มีเหตุผลเข้าไว้อย่างชัดแจ้ง
และมอบกลไกแรงกดดันทางการคลังสำหรับการเปลี่ยนผ่านที่ค่อยเป็นค่อยไป

คุณธรรมนิยม (Meritocracy) RSN อาจเป็นคำอธิบายที่ใช้งานได้จริงครั้งแรกว่าคุณธรรมนิยม [18] สามารถผุดขึ้นในฐานะคุณสมบัติเชิงระบบได้อย่างไร แทนที่จะเป็นเพียงคำขวัญ ระบบคุณธรรมนิยมแบบดั้งเดิมล้มเหลวเพราะต้องอาศัยผู้มีอำนาจส่วนกลางในการนิยามและบังคับใช้ “คุณความดี” ใน RSN คุณความดีผุดขึ้นจากการประเมินแบบสองทาง นั่นคือ ผู้ที่มอบคุณค่าจะสั่งสมชื่อเสียง; ไม่มีคณะกรรมการใดตัดสินว่าใครมีคุณความดี

ทรัพย์สินในฐานะอภิสิทธิ์ RSN แตกต่างอย่างมีนัยสำคัญจากการปฏิบัติต่อสิทธิในทรัพย์สินของสำนักอนาธิปไตยทุนนิยมและสำนักออสเตรียนที่มองว่าเป็นสิ ในกรอบแนวคิดของ RSN ทรัพย์สินเป็นอภิสิทธิ์— การยอมรับทางสังคมที่ในกรณีสุดขั้ว สามารถถูกเพิกถอนโดยชุมชนได้เมื่อผู้เข้าร่วมละเมิดบรรทัดฐานร่วมอย่างรุนแรง (การทรยศ การปฏิเสธที่จะปกป้องชุมชนในยามวิกฤตที่คุกคามความอยู่รอด การเอารัดเอาเปรียบอย่างเป็นระบบ) นี่ไม่ใช่การยึดทรัพย์โดยรัฐ แต่เป็นการถอนการยอมรับทางสังคมโดยเครือข่ายของความสัมพันธ์แบบสองทาง

13 อภิปรายและข้อจำกัด

การเริ่มต้นที่เย็นชา (Cold start) คุณค่าของ RSN ขึ้นอยู่กับผลกระทบเครือข่าย ผู้รับเอาไปใช้ในระยะแรกเผชิญกับคุณค่าที่จำกัดจนกว่าการยอมรับจะแพร่หลาย อย่างไรก็ตาม แม้ในระยะแรกๆ เครือข่าย DID ก็ทำหน้าที่เป็นแหล่งข้อมูลเสริมที่มีประโยชน์ คาดว่าการประเมินชื่อเสียงในระยะแรกและการประเมินผู้มีอำนาจจะพัฒนาขึ้นทีละน้อยพร้อมกับความซับซ้อนที่เพิ่มขึ้น

การต้านการเอาเปรียบและการควบคุมการเข้าถึง DID ที่เป็นเป้าหมายอาจกำหนดค่าธรรมเนียมแบบเป็นลำดับขั้นและข้อจำกัดการเข้าถึงต่อคำสอบถามจาก DID ที่มีชื่อเสียงต่ำ นี่ไม่ใช่แบบทวิภาค แต่เป็นสเกลต่อเนื่อง นั่นคือ ยิ่ง DID ผู้สอบถามมีชื่อเสียงน้อยเท่าใด ก็ยิ่งได้รับข้อมูลน้อยลง รอนานขึ้น และจ่ายมากขึ้น กลไกนี้จูงใจการมีส่วนร่วมที่แท้จริงเหนือการบริโภคแบบเฉื่อยชา

ความไม่เท่าเทียมในการเข้าถึง ต้นทุนของการเผยแพร่ข้ออ้างอาจกรองข้อร้องเรียนที่ชอบธรรมออกจากผู้เข้าร่วมที่ด้อยโอกาสทางเศรษฐกิจ การบรรเทา: ผู้เข้าร่วมทุกคนทำหน้าที่เป็นผู้ตรวจสอบที่มีศักยภาพไปพร้อมกัน (หรือมอบหมายบทบาทนี้) และได้รับค่าธรรมเนียมการตรวจสอบ ในกรอบเวลาที่ยาวนานเพียงพอ ผู้เข้าร่วมที่ไม่สุดโต่งควรเข้าใกล้ความเป็นกลางทางการเงิน รายได้จากการตรวจสอบชดเชยต้นทุนการเผยแพร่โดยประมาณ

ความไม่เท่าเทียมแต่เริ่มแรกของชื่อเสียง ชื่อเสียงที่ได้มาโดยไม่ต้องลงทุนจะมีค่าน้อยกว่าชื่อเสียงที่ได้มาจากการประสานงานที่เพียงพอ สิ่งนี้อาจใช้ในระยะแรกสั่งสมข้อได้เปรียบที่อาจสร้างกำแพงกั้นสำ อย่างไรก็ตาม การประเมินชื่อเสียงดำเนินการโดยผู้ให้บริการภายนอ การเข้าถึงครั้งแรกที่มีชื่อเสียงดีเป็นข้อได้เปรียบเชิงเปรียบเทียบทางเศร และนั่นเป็นไปโดยการออกแบบ

คำถามที่เปิดกว้าง ฟังก์ชันต้นทุนที่เหมาะสมที่สุด มาตรฐานการรวบรวม การกำกับดูแลโปรโตคอล และปฏิสัมพันธ์กับข้อมูลชื่อเสียงสังเคราะห์ที่สร้างโดย AI ยังคงเป็นประเด็นสำหรับงานในอนาคต

เอกสารฉบับนี้มิได้อ้างว่า RSN จะให้ผลลัพธ์ที่เหมาะสมที่สุดในทุกสถานการณ์ แต่อ้างว่า RSN เป็นตัวแทนของทางเลือกที่เป็นไปได้— นำไปปฏิบัติได้ในทางเทคนิค ยั่งยืนด้วยตัวเองในทางเศรษฐกิจ และเข้ากันได้ในทางสังคมกับแนวโน้มพฤติกรรมของมนุษย์ตามที่มัน

14 บทสรุป

เอกสารฉบับนี้ได้นำเสนอเครือข่ายสังคมชื่อเสียง ซึ่งเป็นโปรโตคอลแบบกระจายศูนย์ที่เปิดโอกาสให้เกิดการแลกเปลี่ หลักการความสุดโต่งราคาแพงรับประกันว่าข้ออ้างที่ฉ้อฉลจะถูกตั้งร เส้นทางการโยกย้ายที่นำเสนอเปิดทางให้เกิดการเปลี่ยนผ่านที่ค่อยเ การออกแบบผนวกธรรมชาติของมนุษย์ตามที่มันเป็น— รวมทั้งความใจแคบ ความอาฆาต และความปรารถนาในความสะใจจากการแก้แค้น— แทนที่จะเรียกร้องการเปลี่ยนแปลงทางอุดมการณ์ ผลลัพธ์ไม่ใช่ยูโทเปีย แต่เป็นระบบที่ความยุติธรรมเข้าถึงได้ ซึ่งเป็นไปได้ด้วยเทคโนโลยีที่มีอยู่ และต้นทุนของการประพฤติผิดถูกแบกรับโดยฝ่ายที่ก่อมันขึ้น

References

[1] Czech Republic, “Act no. 549/1991 coll., on court fees, as amended,” 1991, fee schedule for court proceedings; cost rules per Act No. 99/1963 Coll. (Code of Civil Procedure) and Decree No. 177/1996 Coll. (Attorney Tariff).

[2] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, “Decentralized identifiers (DIDs) v1.0,” W3C Recommendation, Jul. 2022.

[3] E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized society: Finding

Web3's soul," SSRN Electronic Journal, May 2022.

[4] V. Buterin, "DAOs, DACs, DAs and more: An incomplete terminology guide," Ethereum Blog, May 2014.

[5] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," Management Science, vol. 65, no. 11, pp. 5171–5187, 2019.

[6] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, "Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web," in Proc. 29th ACM STOC, 1997, pp. 654–663.

[7] D. Buchner, "ION — a scalable DID method based on Bitcoin," Microsoft, 2021.

[8] Ceramic Network, "Ceramic protocol specification," GitHub, 2023. [Online]. Available: https://github.com/ceramicnetwork

[9] É. Durkheim, The Division of Labor in Society. Free Press, 1893, english translation 1984.

[10] J. Rawls, A Theory of Justice. Harvard University Press, 1971.

[11] J. Haidt, The Righteous Mind: Why Good People Are Divided by Politics and Religion. Vintage Books, 2012.

[12] J. R. Douceur, "The Sybil attack," in Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS), 2002, pp. 251–260.

[13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in Proc. 12th International Conference on World Wide Web, 2003, pp. 640–651.

[14] M. N. Rothbard, For a New Liberty: The Libertarian Manifesto. Macmillan, 1973.

[15] H.-H. Hoppe, Democracy: The God That Failed. Transaction Publishers, 2001.

[16] F. A. Hayek, Law, Legislation and Liberty. University of Chicago Press, 1973.

[17] S. E. I. Konkin, An Agorist Primer. KoPubCo, 2006.

[18] M. Young, The Rise of the Meritocracy. Thames and Hudson, 1958.