เลือกตั้งด้วยบล็อกเชน

รวดเร็ว โปร่งใส ไร้แทรกแซง... จริงหรือ?



มกราคม 2567 วิจัยกรุงศรี

krungsri Research

เครือ MUFG หนึ่งใน สถาบันการเงินที่ใหญ่ที่สุดของโลก

สารบัญ

บทนำ	3
เทคโนโลยีบล็อกเชนกับการเลือกตั้งแบบออนไลน์	4
ตัวอย่างระบบ BVMS	6
โหวตด้วยบล็อกเชนดีกว่าจริงหรือ?	10
มุมมองวิจัยกรุงศรี: ระบบที่ดีไม่มีคำว่า “One size fits all”	15
แหล่งอ้างอิง	17

Subscribe Us

สมัครสมาชิกวิจัยกรุงศรี...

krungsri.research@krungsri.com

คำสงวนสิทธิ์

เนื้อหาและข้อมูลใดๆ ทั้งหมดที่ปรากฏในรายงานฉบับนี้ หากมิได้ระบุไว้เป็นอย่างอื่น ถือเป็นลิขสิทธิ์ของวิจัยกรุงศรี ห้ามมิให้ผู้ใดกระทำการใดๆ เกี่ยวข้องกับเนื้อหา สำเนา หรือดัดแปลงแก่บุคคลอื่นโดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากวิจัยกรุงศรี รายงานฉบับนี้จัดทำขึ้นโดยอาศัยข้อมูลจากแหล่งที่เชื่อหรือควรเชื่อว่ามีความน่าเชื่อถือ อย่างไรก็ตาม วิจัยกรุงศรีไม่อาจรับรองความครบถ้วนสมบูรณ์หรือความถูกต้องของข้อมูลดังกล่าว อีกทั้งไม่รับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งทางตรงหรือทางอ้อมจากการใช้รายงานฉบับนี้หรือเนื้อหาในรายงานฉบับนี้ ข้อมูล ความคิดเห็น และการประมาณการที่ปรากฏในรายงานนี้ถือเป็นความคิดเห็นของวิจัยกรุงศรี ไม่จำเป็นต้องสอดคล้องกับ ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) และบริษัทในเครือ ความคิดเห็นในรายงานฉบับนี้เป็นไปตามสถานการณ์ปัจจุบัน ณ วันที่มีการเผยแพร่รายงาน วิจัยกรุงศรีขอสงวนสิทธิ์ในการเปลี่ยนแปลงโดยมิต้องแจ้งให้ทราบล่วงหน้า

บทนำ

บล็อกเชน (Blockchain) เป็นเทคโนโลยีที่ได้รับการกล่าวถึงมากในปัจจุบันว่าเป็นนวัตกรรมที่มีศักยภาพสูงขนาดที่หลายคนคาดว่าจะเข้ามาเปลี่ยนโลก ในช่วงสิบกว่าปีที่ผ่านมาการพัฒนาบล็อกเชนเป็นไปอย่างไม่หยุดยั้งจากทุกภาคส่วน ไม่ว่าจะเป็นภาครัฐ ภาคเอกชน หรือสถาบันการศึกษา ซึ่งแม้ว่าเทคโนโลยีนี้จะได้รับความสนใจมาก แต่กรณีการใช้งานจริง (Use case) ยังค่อนข้างจำกัดทั้งในไทยและในต่างประเทศ โดยส่วนใหญ่มักอยู่ในแวดวงสินทรัพย์เสมือน (Virtual assets) และระบบการเงินแบบกระจายศูนย์ (DeFi)

อย่างไรก็ตาม บล็อกเชนถูกกล่าวถึงอีกครั้งภายหลังจากการเลือกตั้งสมาชิกสภาผู้แทนราษฎรไทยครั้งล่าสุดเมื่อวันที่ 14 พฤษภาคม 2566 เสร็จเรียบร้อย ซึ่งการเลือกตั้งครั้งนี้นับว่าเป็นการเลือกตั้งที่ประชาชนตื่นตัวกันมาก โดยมีผู้มาลงคะแนนถึงร้อยละ 75.71 ของผู้มีสิทธิ์ออกเสียงทั้งหมด อีกทั้งคนจำนวนไม่น้อยร่วมสังเกตการณ์การนับคะแนนพร้อมไปกับสื่อสำนักต่างๆ ที่รายงานผลการนับคะแนนแบบนาทีต่อนาที โดยต่อมาคณะกรรมการการเลือกตั้งได้ประกาศรับรองผลการเลือกตั้งอย่างเป็นทางการในวันที่ 25 พฤษภาคม 2566 หรือหลังจากการเลือกตั้ง 11 วัน **จนเริ่มมีการตั้งคำถามว่าหากมีการจัดการเลือกตั้งแบบออนไลน์** (Online voting) **จะช่วยเพิ่มความสะดวกรวดเร็วในการนับคะแนนหรือไม่ และหากยิ่งนำเทคโนโลยีที่เป็นที่กล่าวขวัญถึงในระยะหลังอย่างบล็อกเชนมาใช้ด้วยก็น่าจะยิ่งเพิ่มความโปร่งใส** เนื่องจากเทคโนโลยีบล็อกเชนใช้การประมวลผลและจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology: DLT) ที่ไม่จำเป็นต้องมีตัวกลางในการตรวจสอบความถูกต้องของการบันทึกธุรกรรมต่างๆ และเมื่อไม่ต้องพึ่งพาตัวกลางจึงเป็นเหตุให้เชื่อได้ว่าการนำบล็อกเชนมาใช้ในการเลือกตั้งแบบออนไลน์จะทำให้เกิดความโปร่งใสและปราศจากการแทรกแซง



ณธัญอร รัตนาธรรมวัฒน์

นักวิเคราะห์อาวุโส

nathanon.ratanathamwat@krungsri.com

+662 296 6389

ดร. พิมพ์นารา หิรัญกสิ

ผู้บริหารสายงานวิจัยและหัวหน้าทีมวิจัยเศรษฐกิจ

pimnara.hirankasi@krungsri.com

+662 296 6457



เทคโนโลยีบล็อกเชนกับการเลือกตั้งแบบออนไลน์

โดยหลักการแล้วการเลือกตั้งแบบออนไลน์สามารถอำนวยความสะดวกแก่ผู้จัดการเลือกตั้งและผู้มีสิทธิ์ออกเสียง อีกทั้งการรวมคะแนนเสียงแบบดิจิทัลก็สามารถกระทำได้รวดเร็ว แต่การเลือกตั้งแบบออนไลน์ต้องอาศัยองค์ประกอบอย่างน้อย 4 ประการ อันได้แก่ (1) อินเทอร์เน็ต (Internet) หรือเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเพื่อให้เกิดการสื่อสารและแลกเปลี่ยนข้อมูลระหว่างกัน (2) อุปกรณ์การลงคะแนน (Hardware) ซึ่งอาจเป็นโทรศัพท์มือถือ เครื่องคอมพิวเตอร์ หรืออุปกรณ์รับส่งข้อมูลที่เชื่อมต่อกับอินเทอร์เน็ตอื่นๆ (3) ซอฟต์แวร์ (Software) เป็นชุดคำสั่งหรือโปรแกรมที่เขียนขึ้นเพื่อสั่งและควบคุมการทำงานของระบบคอมพิวเตอร์ และ (4) การรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity) เป็นการป้องกันระบบที่เชื่อมต่อกับอินเทอร์เน็ต ไม่ว่าจะเป็นฮาร์ดแวร์ ซอฟต์แวร์ เครือข่ายและข้อมูลต่างๆ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เมื่อการเลือกตั้งมีความสำคัญมาก ไม่ว่าจะเป็นระดับท้องถิ่นหรือระดับประเทศ เพราะเกี่ยวข้องกับประชาชนจำนวนมาก ผู้จัดการเลือกตั้งออนไลน์จึงจะต้องมีความพร้อมในองค์ประกอบทั้ง 4 ประการดังกล่าวด้วยมาตรฐานที่สูง ที่ผ่านมาหลายประเทศเริ่มนำการเลือกตั้งออนไลน์มาใช้กับการลงคะแนนเสียงทางการเมืองในระดับที่แตกต่างกันไป อาทิ การเลือกตั้งท้องถิ่น การลงคะแนนเสียงในกลุ่มหรือองค์กรขนาดเล็ก เป็นต้น และเมื่อพิจารณาการนำเทคโนโลยีบล็อกเชนมาใช้ในการลงคะแนนเสียงอย่างจริงจัง พบว่าเริ่มมีการใช้งานในปี 2561 ในหลายประเทศ แม้ว่าจะจำกัดอยู่เพียงในกลุ่มองค์กรหรือพื้นที่ขนาดเล็กแต่ก็นับว่าเป็นก้าวสำคัญของการพัฒนา ซึ่งสำหรับทวีปเอเชีย การนำเทคโนโลยีบล็อกเชนมาใช้จัดการเลือกตั้งภายในองค์กรหรือท้องถิ่นของไทย ญี่ปุ่น รัสเซีย จัดเป็นประเทศแรกๆ ที่ได้รับการพูดถึงบ่อยครั้ง ส่วนในฟากตะวันตกก็มีสหรัฐฯ ที่ได้รับความสนใจจากสื่อหลายสำนัก

ตารางที่ 1

ตัวอย่างการนำบล็อกเชนมาใช้ในการลงคะแนนเสียงทางการเมืองในระยะเริ่มแรก (พ.ศ. 2561)

ตำแหน่งที่ตั้ง (Location)	วัตถุประสงค์ของการลงคะแนน (Purpose)	ระบบการลงคะแนน (Voting System)	ผู้พัฒนาระบบ (Developer)
กรุงเทพมหานคร ประเทศไทย	การเลือกตั้งหัวหน้าพรรคประชาธิปัตย์ (Primary election)	ระบบลงคะแนนอิเล็กทรอนิกส์แบบถ่ายทอดสด โดยมีสมาชิกพรรคกว่า 120,000 คนมาใช้สิทธิผ่านอุปกรณ์ในหน่วยเลือกตั้งและแอปพลิเคชันบนโทรศัพท์มือถือ (D-Elect)	Zcoin
ซาราตอฟ ประเทศรัสเซีย	การเลือกสมาชิกรัฐสภาเยาวชนท้องถิ่น (Local youth parliament election)	ระบบลงคะแนนอิเล็กทรอนิกส์ที่เรียกว่า “Polys” ผ่านอุปกรณ์ในหน่วยเลือกตั้ง ซึ่งขณะนั้นมีผู้มาใช้สิทธิราว 40,000 คน	Kaspersky Lab
สึกูบะ ประเทศญี่ปุ่น	การลงคะแนนเสียงสนับสนุนโครงการพัฒนาสังคมของเมืองสึกุบะที่ถูกนำเสนอโดยบริษัทเอกชน ศูนย์วิจัย หรือสถาบันการศึกษา	ระบบลงคะแนนผ่านคอมพิวเตอร์ ณ ที่ทำการเมืองสึกุบะ โดยมีการติดตั้งอุปกรณ์พิเศษรวมถึงเครื่องอ่านบัตรประจำตัวผู้มีสิทธิออกเสียงเลือกตั้ง (หรือ My Number Card)	VOTE FORE
เวสต์เวอร์จิเนีย สหรัฐอเมริกา	การเลือกตั้งกลางเทอม (Midterm election) ของรัฐเวสต์เวอร์จิเนีย	ระบบลงคะแนนผ่านแอปพลิเคชันบนโทรศัพท์มือถือที่เรียกว่า “Voatz” ที่จำกัดให้ใช้เฉพาะกลุ่มเจ้าหน้าที่ทหาร(และครอบครัว)ที่ประจำการอยู่ในต่างประเทศ โดยขณะนั้นมีผู้ใช้สิทธิ 144 คน จาก 31 ประเทศ	Voatz

Source: Krungsri Research

ในปัจจุบัน แม้ว่าการนำบล็อกเชนมาใช้ในการเลือกตั้งทางการเมืองจะได้รับความสนใจมากขึ้น แต่จากการใช้งานจริงพบว่าเกิดเสียงวิพากษ์วิจารณ์ขึ้นมากโดยเฉพาะในช่วงปี 2561 อาทิเช่น ในการเลือกตั้งของรัฐเวสต์เวอร์จิเนียที่สหรัฐฯ มีข้อทักท้วงเรื่องความปลอดภัยของระบบและความแม่นยำของการนับคะแนน ซึ่งก็ยังเป็นสิ่งที่สาธารณชนไม่อาจพิสูจน์ทราบได้ว่าจริงเท็จประการใด เพราะทั้งทางการเองรวมถึงบริษัทที่เกี่ยวข้องมิได้เปิดเผยข้อมูลพื้นฐานที่จำเป็นในการประเมินความสำเร็จของการทดลองใช้บล็อกเชนในการเลือกตั้ง โดยผู้เชี่ยวชาญต่างก็ออกมาให้ความเห็นว่ามีความเป็นไปได้สูงที่จะเกิดความผิดพลาดและความเสี่ยงด้านความปลอดภัยบนอุปกรณ์มือถือ ระบบเครือข่ายการจัดการเลือกตั้ง ตลอดจนเซิร์ฟเวอร์ที่ใช้เก็บข้อมูล นอกจากนี้ Voatz ยังถูกโจมตีในประเด็นด้านความโปร่งใสในการนับคะแนน เนื่องจากบริษัทฯ ใช้วิธีพิมพ์บัตรกระดาษที่ได้รับการลงคะแนนของผู้มาใช้สิทธิ์เสมือนเป็นการสร้างบัตรลงคะแนนที่มีการทำเครื่องหมายกากบาทขึ้นมาโดยผ่านกระบวนการคือ คะแนนของผู้ใช้สิทธิที่ลงคะแนนผ่านอุปกรณ์มือถือจะถูกส่งมายังศูนย์อำนวยการจัดการเลือกตั้ง ณ ที่ทำการของรัฐในรูปแบบไฟล์ PDF เพื่อให้เจ้าหน้าที่ธุรการพิมพ์บัตรเลือกตั้งที่ลงคะแนนแล้วออกมา จากนั้นจึงนำกระดาษแผ่นดังกล่าวไปรวมกับบัตรลงคะแนนอื่นๆ ของผู้ที่มาใช้สิทธิ์โดยเดินทางมาที่คูหา แล้วจึงนับคะแนนจากบัตรกระดาษทั้งหมดพร้อมกัน ซึ่งกระบวนการนี้แม้จะช่วยเรื่องการตรวจสอบการนับคะแนนหลังการเลือกตั้ง (Post-vote tabulation audit) แต่ไม่ได้ช่วยเรื่องการตรวจสอบกระบวนการการลงคะแนน (Vote casting process) เหตุเพราะผู้ใช้สิทธิออกเสียงเลือกตั้งผ่านบล็อกเชนไม่มีโอกาสได้ตรวจสอบหรือเห็นด้วยตาตนเองว่าเครื่องหมายกากบาทที่ถูกพิมพ์ลงบนบัตรกระดาษของตนนั้นจะตรงกับช่องของผู้สมัครรับเลือกตั้งที่ตนได้เลือกจริงๆ[1/] โดยทำได้เพียงมอบความไว้วางใจทั้งหมดและหวังให้เจ้าหน้าที่รัฐและระบบการจัดการดำเนินไปอย่างถูกต้องเพื่อให้คะแนนเสียงที่ถูกนับเป็นไปตามเจตนารมณ์ของผู้มาใช้สิทธิออกเสียงเลือกตั้งโดยแท้จริง ซึ่งตัวอย่างนี้แสดงให้เห็นถึงเพียงหนึ่งในข้อกังวลที่มีต่อการลงคะแนนผ่านบล็อกเชนเท่านั้น

อย่างไรก็ดี ไม่ว่าการเลือกตั้งจะถูกจัดการแบบเข้าคูหากากบาทหรือแบบออนไลน์ **ความโปร่งใสและความปลอดภัยในการจัดการเลือกตั้งก็เป็นหัวใจสำคัญที่ผู้มีหน้าที่รับผิดชอบจะตั้งต้องคำนึงถึงอยู่เสมอ** เพราะผู้จัดการเลือกตั้งจะต้องสามารถชี้แจงแก่ผู้มาใช้สิทธิด้วยประจักษ์หลักฐานที่สามารถเชื่อถือได้ว่าการเลือกตั้งนี้ได้นำมาซึ่ง *"ผู้ชนะที่แท้จริง"*

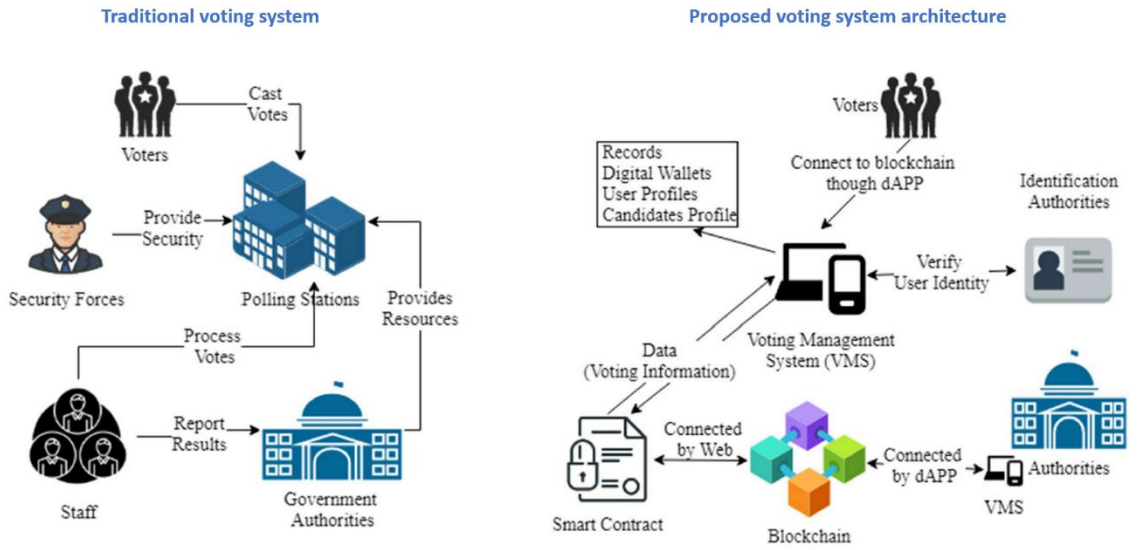
1/ https://slate.com/technology/2019/07/west-virginia-blockchain-voting-voatz.html

ตัวอย่างระบบ BVMS

ในระดับนานาชาติมีงานศึกษาอยู่มากมายที่นำเสนอกรอบแนวคิดที่จะทำให้ระบบการลงคะแนนเสียงเลือกตั้งด้วยเทคโนโลยีบล็อกเชนโปร่งใสและปลอดภัยมากที่สุด ซึ่งในบรรดาข้อเสนอต่างๆ นั้น กรอบแนวคิดระบบบริหารจัดการการลงคะแนนบนบล็อกเชน (Blockchain-based Voting Management System: BVMS) (Farooq, Ifthikhar & Khelifi, 2022) ได้เสนอให้ใช้กลไกฉันทามติแบบยืดหยุ่น (Flexible consensus algorithm) ที่ควบคุมการทำงานของระบบ ให้สามารถเปลี่ยนแปลงรูปแบบของกลไกฉันทามติได้ตามความเหมาะสมแม้ในระหว่างการลงคะแนนเพื่อให้รองรับผู้ใช้จำนวนมากได้ (Blockchain scalability) นอกจากนี้ยังมีวิธีป้องกันปัญหาการโจมตี 51% (51% Attack)[2/] ที่อาจเกิดขึ้นระหว่างการลงคะแนน ตลอดจนนำเสนอกลไกความปลอดภัยของระบบบล็อกเชน (Chain security algorithm) เพื่อพิสูจน์ความถูกต้องของเครือข่ายบล็อกเชนโดยอัตโนมัติ และยังมีกลไก UTXO[3/] และสัญญาอัจฉริยะ (Smart contracts) เพื่อป้องกันไม่ให้เกิดธุรกรรมที่ไม่สมบูรณ์หรือเป็นอันตรายในเครือข่ายบล็อกเชน ซึ่งแนวคิดที่ได้กล่าวมาทั้งหมดนี้ล้วนเป็นความพยายามในการปิดช่องโหว่ด้านต่างๆ ของการเลือกตั้งแบบใช้บล็อกเชน จึงทำให้ระบบ BVMS แตกต่างจากระบบอื่นๆ

ภาพที่ 1

การจัดการเลือกตั้งแบบดั้งเดิม (ซ้าย) และแบบ BVMS (ขวา)



Source: Farooq, Ifthikhar & Khelifi, 2022

2/ 51% Attack คือการโจมตีเพื่อปรับเปลี่ยนธุรกรรม บิดเบือนข้อมูล หรือเข้าควบคุมเครือข่ายบล็อกเชนโดยนักขุด (Miner) ที่มีพลังควบคุมเหนือง (Hash power) ของเครือข่ายหนึ่งๆ มากกว่าหรือเท่ากับร้อยละ 51 ซึ่งพลังควบคุมเหนือองที่เกินกว่ากึ่งหนึ่งนี้หมายถึงการที่นักขุดคนหนึ่งมีกำลังในการขุดเร็วกว่าและมากกว่าคนอื่นๆ ในเครือข่าย

3/ UTXO ย่อมาจาก Unspent Transaction Output หมายถึง จำนวนเหรียญที่เหลือจากการทำธุรกรรมที่สามารถนำไปใช้ทำธุรกรรมถัดไปได้ ซึ่งจะคล้ายกับการซื้อสิ่งของที่มีการจ่ายธนบัตรแล้วได้รับ "เหรียญทอน" ซึ่งเหรียญที่ได้รับทอนมานี้สามารถนำไปซื้อสิ่งอื่นเป็นลำดับถัดไปได้ หรือกล่าวได้ว่า Output (หรือเหรียญทอน) ของธุรกรรมหนึ่งสามารถใช้เป็น Input (หรือนำมาใช้จ่าย) ในการทำธุรกรรมครั้งต่อไปได้ ดังนั้น UTXO จึงเป็นทั้งจุดเริ่มต้นและจุดสิ้นสุดของการทำธุรกรรมในบล็อกเชน

ในการจัดการเลือกตั้งด้วยระบบ BVMS (ภาพที่ 1) นั้น ผู้มีสิทธิออกเสียงเลือกตั้งต้องสามารถเข้าถึงอุปกรณ์การลงคะแนนได้ ซึ่งอาจเป็นโทรศัพท์มือถือหรือเครื่องคอมพิวเตอร์ และต้องลงทะเบียนในระบบเพื่อยืนยันตัวตนก่อน โดยระบบ BVMS จะตรวจสอบผ่านสัญญาอัจฉริยะว่า (1) ผู้มาลงคะแนนคือผู้มีสิทธิออกเสียงเลือกตั้งจริงหรือไม่ และ (2) ผู้มาลงคะแนนได้ใช้สิทธิไปก่อนหน้านี้แล้วหรือยัง จึงจะอนุญาตให้ผู้มาใช้สิทธิทำการลงคะแนนได้ จากนั้นผู้เลือกตั้งจะได้รับเหรียญโหวต (Voting Coin: VC) จำนวน 1 เหรียญในวอลเล็ท เพื่อใช้ในการลงคะแนน ซึ่งในขณะที่ลงคะแนนนั้นเหรียญโหวตจะถูกใช้ไป ทำให้ผู้ลงคะแนนไม่สามารถลงคะแนนได้อีกเป็นครั้งที่สอง และหลังจากนั้นระบบจะมีกระบวนการตรวจสอบรายละเอียดต่างๆ ก่อนทำการบันทึกข้อมูลลงบนบล็อกเชน ซึ่งระบบนี้จะสามารถรองรับผู้ลงคะแนนจำนวนมากพร้อมๆ กันได้ไม่ว่าผู้มาใช้สิทธิแต่ละรายจะอยู่ที่ใดในโลก โดยรหัสอ้างอิงของธุรกรรม (Transaction hash) ของผู้ลงคะแนนทุกคน รวมถึงผลการเลือกตั้งจะถูกเก็บไว้บนบล็อกเชนและผู้ใช้งานสามารถเข้าไปดูได้จากหน้าจอหรือแดชบอร์ดแสดงผล

ตารางที่ 2

จุดเด่นของระบบการลงคะแนนเสียงเลือกตั้งแบบ BVMS

	กรอบแนวคิดการลงคะแนนเสียงเลือกตั้งแบบ BVMS
Flexible Consensus Algorithm	ออกแบบระบบให้สามารถรองรับกลไกฉันทามติได้หลายแบบเพื่อรองรับผู้มาลงคะแนนจำนวนมาก โดยค่าตั้งต้นจะเป็นกลไกฉันทามติแบบ Proof-of-Work แต่สามารถปรับเปลี่ยนเป็นกลไกอื่นได้ภายหลัง ไม่ว่าจะเป็น Proof-of-Stake Proof-of-Vote Proof-of-Trust หรือ Ripple เพื่อให้เกิดสมรรถภาพการทำงานสูงสุด (คำอธิบายกลไกฉันทามติแต่ละรูปแบบแสดงใน Box 1)
51% Attack	วางระบบเพื่อการป้องกันการโจมตี 51% ที่อาจเกิดขึ้นไว้ 2 วิธี คือ (1) บันทึก Hash rate[4/] ของนักขุด (Miner)/ผู้ทวนสอบ (Verifier) แต่ละคนไว้ในระบบล่วงหน้าเพื่อตรวจสอบ และห้ามมิให้นักขุดคนที่มี Hash rate มากกว่าร้อยละ 51 ทำการขุดในระหว่างการเลือกตั้ง และ (2) มีกระบวนการคัดเลือกนักขุดก่อนการเลือกตั้ง โดยจัดจ้างนักขุดภายใต้การควบคุมของหน่วยงานที่มีหน้าที่รับผิดชอบ ทั้งนี้ ระหว่างการลงคะแนนเสียงจะต้องสอดส่องดูแลระบบตลอดเวลา และเมื่อพบความผิดปกติ กระบวนการขุดทั้งหมดจะต้องหยุดลงทันทีโดยอัตโนมัติเพื่อตรวจสอบ จากนั้นกลุ่มนักขุดผู้ตรวจสอบที่มีบล็อกเชนขนาดใหญ่กว่า (กลุ่มผู้บริสุทธิ์) จะเข้าครอบครองเครือข่ายและสามารถทำงานต่อได้ ส่วนกลุ่มนักขุดที่ติดปัญหา (กลุ่มผู้ต้องสงสัย) จะถูกปิดกั้นจากเครือข่ายและไม่ได้รับอนุญาตให้กลับเข้ามาจนกว่าผู้มีอำนาจจัดการเลือกตั้งจะตรวจสอบความถูกต้อง
Chain Security Algorithm	สร้างกลไกอัตโนมัติเพื่อตรวจสอบความถูกต้องของบล็อกเชนเพื่อรักษาความปลอดภัย โดยกลไกนี้จะทำงานทุกครั้งที่มีการเพิ่มบล็อกใหม่ โดยตรวจสอบบล็อกใหม่ที่เกิดขึ้นว่าถูกต้องและปลอดภัยก่อนที่บล็อกใหม่นี้จะกระจายไปยังทุกคนในเครือข่าย แต่หากพบความผิดปกติกลไกจะประกาศให้ทุกคนทราบว่าบล็อกเชนนี้เป็นโมฆะ
Unspent Transaction Output (UTXO)	ระบบนี้ใช้กลไก UTXO คือเมื่อผู้มาลงคะแนนใช้ 1 เหรียญโหวต นักขุดจะได้รับเหรียญนี้เป็นรางวัลในภายหลัง โดยระบบนี้จะไม่มีค่าธรรมเนียมธุรกรรม (No transaction fee) เมื่อผู้ลงคะแนนใช้ 1 เหรียญในการลงคะแนนพร้อมลงลายมือชื่อดิจิทัล (Digital signature) แล้ว ธุรกรรมจะถูกบันทึกและนักขุดจะเริ่มทำงาน ค่าของ UTXO หลังธุรกรรมแต่ละครั้งจะถูกปรับเป็นศูนย์ทำให้ผู้ลงคะแนนไม่สามารถลงอีกคะแนนซ้ำได้อีก
Smart Contracts	สัญญาอัจฉริยะจะถูกสร้างขึ้นหลายฉบับสำหรับหลายวัตถุประสงค์ เช่น 1) ชุดสัญญาเพื่อตรวจสอบความถูกต้องว่าผู้มาลงคะแนนคนนั้นๆ มีสิทธิลงคะแนน และเมื่อถูกรับรองสิทธิ ผู้มาลงคะแนนจะถูกเชื่อมต่อกับสัญญาอีกฉบับที่จะบ่งชี้ว่าผู้มาลงคะแนนรายนั้นสามารถลงคะแนนให้แก่ผู้สมัครคนใดบ้าง 2) ชุดสัญญาที่ใช้รหัสประจำตัวประชาชนและที่อยู่ของวอลเล็ทในการตรวจสอบว่ามีเหรียญ VC ในวอลเล็ทของผู้มาลงคะแนน และลดจำนวนเหรียญให้เหลือศูนย์หลังการลงคะแนน (หนึ่งคนลงคะแนนได้หนึ่งครั้ง) รวมถึงการส่งข้อความแจ้งเตือนไปยังโทรศัพท์มือถือ 3) ชุดสัญญาที่ตรวจสอบว่าผู้มาลงคะแนนไม่ได้ลงทะเบียนซ้ำมากกว่าหนึ่งครั้ง โดยตรวจสอบอายุและรายละเอียดตามบัตรประจำตัว เป็นต้น

Source: Krungsri Research

4/ Hash rate หมายถึงความเร็วในการขุดเหรียญ จะวัดจากจำนวนครั้งของการคำนวณเพื่อคาดเดาคำตอบต่อวินาที เป็นหน่วยวัดของกำลังการประมวลผลของคอมพิวเตอร์

Box 1 กลไกฉันทามติแต่ละรูปแบบโดยสังเขป

- **Proof of Work (PoW)**

  PoW เป็นกลไกที่ให้นักขุด (Miner) แข่งขันแก้โจทย์หรือสมการคณิตศาสตร์ เช่น การหาว่าจำนวนสองจำนวนใดที่ไม่เท่ากับ 1 แต่คูณกันได้เท่ากับ 10,336,613 เป็นต้น เมื่อคนแรกแก้ได้ว่าตัวเลขสองจำนวนนั้นคือ 2,903 กับ 3,571 คนอื่นๆ ในระบบก็จะตรวจสอบว่าเลขสองตัวนี้คูณกันได้เท่ากับ 10,336,613 จริงหรือไม่ เมื่อผู้ใช้ในระบบมากกว่าร้อยละ 50 ตรวจสอบเสร็จ คนแรกที่แก้โจทย์ได้จะได้รับรางวัล (Reward) ซึ่งจะเห็นได้ว่าระบบ PoW ทำให้ข้อมูลที่บันทึกสามารถแก้ไขได้ยาก เนื่องจากต้องให้ผู้ใช้ในเครือข่ายมากกว่าครึ่งตรวจสอบและยืนยันการแก้ไข อย่างไรก็ตาม PoW เป็นระบบที่ก่อให้เกิดการแข่งขันระหว่างนักขุด โดยจากตัวอย่างข้างต้น การแก้โจทย์ต้องอาศัยการสุ่มคูณเลขจนเจอชุดคำตอบที่ต้องการ ซึ่งอาศัยทั้งกำลังการคำนวณและการใช้พลังงานไฟฟ้าในระดับสูง ซึ่งหากเปลี่ยนวิธีตรวจสอบเป็นว่า 2,903 กับ 3,571 คูณกันได้คำตอบที่ต้องการหรือไม่ จะทำได้ง่ายกว่ามาก[5/]

- **Proof of Stake (PoS)**

  PoS เป็นระบบที่สุ่มหาผู้ตรวจสอบ (Validator) เพื่อแก้โจทย์คณิตศาสตร์ โดยผู้ที่วางเงิน (หรือเหรียญ) ไว้ในระบบมากกว่าก็จะมีโอกาสได้รับเลือกให้แก้โจทย์สูงกว่า เมื่อคำตอบถูกตรวจสอบเรียบร้อย ผู้ตรวจสอบที่แก้โจทย์สำเร็จจะได้รับรางวัล แต่หากการแก้โจทย์นั้นผิด ผู้ตรวจสอบจะถูกหักเงินที่วางไว้ ดังนั้น PoS จึงใช้พลังงานน้อยกว่าเนื่องจากไม่มีการแข่งขันแก้โจทย์เดียวกันจากผู้ใช้หลายคนในระบบ อย่างไรก็ตาม PoS มีจุดอ่อนเพราะอาจเกิดกรณีที่มีผู้ตรวจสอบหลายคนรวมตัวกันและทำข้อตกลงบางอย่างเพื่อแบ่งรางวัลที่ได้รับ ซึ่งหากเป็นเช่นนี้จะขัดกับหลักการการกระจายศูนย์ที่สนับสนุนความโปร่งใสของเทคโนโลยีบล็อกเชน[6/]

- **Proof of Vote (PoV)**

  PoV เป็นระบบที่ทำงานบนบล็อกเชนที่เปิดใช้งานเฉพาะกลุ่ม (Consortium blockchain) และใช้กลไกการลงคะแนน (Voting mechanism) เพื่อให้เกิดฉันทามติซึ่งเป็นข้อสรุปที่สมาชิกทุกฝ่ายในกลุ่มยอมรับ ระบบนี้มีการควบคุมภายในเพื่อถ่วงดุลอำนาจระหว่างสมาชิก อีกทั้งมีความปลอดภัยสูงเพราะจะแยกสิทธิ์ในการลงคะแนน (Voting rights) ออกจากสิทธิ์ในการปฏิบัติการหรือบันทึกข้อมูล (Execution/Bookkeeping rights) ให้เป็นอิสระจากกัน กล่าวคือ ฉันทามติของสมาชิกในกลุ่มจะเป็นตัวกำหนดควบคุมการปฏิบัติการและกระบวนการตรวจสอบความถูกต้องของบล็อกโดยไม่ต้องพึ่งพาบุคคลภายนอก โดยสมาชิกในกลุ่มจะลงคะแนนเลือกทีมปฏิบัติการซึ่งผู้สมัครแต่ละรายต้องมาจากการถูกเสนอชื่อโดยสมาชิกรายใดรายหนึ่ง ซึ่งทีมปฏิบัติการจะมีหลายคนแต่จะไม่มีหัวหน้าทีมและจะทำงานตามวาระที่กำหนดเท่านั้น (หลังจากนั้นจะมีการลงคะแนนเลือกใหม่) ทีมปฏิบัติการมีหน้าที่ส่งข้อมูลธุรกรรมให้แก่สมาชิกในกลุ่มเพื่อให้สมาชิกตรวจสอบและลงคะแนน ซึ่งธุรกรรมที่ได้คะแนนสูงจะถือว่าเป็นธุรกรรมที่ถูกต้องตามฉันทามติและถูกบันทึกลงบนบล็อกเชน[7/]

- **Proof of Trust (PoT)**

  PoT เป็นกลไกฉันทามติที่คัดเลือกผู้ตรวจสอบ (Validator) จากภายในเครือข่ายซึ่งเป็นแบบกระจายศูนย์ (Decentralized network) โดยใช้คะแนนความน่าเชื่อถือ (Trust score) เป็นเกณฑ์ในการคัดเลือก ซึ่งคะแนนความน่าเชื่อถือนี้จะได้มาจากความสำเร็จในการตรวจสอบธุรกรรมครั้งก่อนๆ ที่เกิดขึ้นภายในเครือข่ายอย่าง “รวดเร็ว” และ “ถูกต้อง” ซึ่งผู้ตรวจสอบที่มีคะแนนความน่าเชื่อถือสูงก็จะมีโอกาสสูงกว่าในการถูกเลือกให้เข้าตรวจสอบธุรกรรมที่มีมูลค่าสูงขึ้น และในระยะยาวก็จะได้รับรางวัลที่มากขึ้นด้วยตามลำดับ นอกจากนี้ PoT ยังสร้างแรงจูงใจให้ผู้ตรวจสอบซื่อสัตย์ต่อเครือข่ายบล็อกเชน เพราะการฉ้อโกงจะทำให้คะแนนความน่าเชื่อถือตกลงและส่งผลลบต่อการแสวงหารางวัลหรือค่าตอบแทนในอนาคต[8/]

- **Ripple และ RPCA**

  Ripple เป็นเครือข่ายบล็อกเชนที่บริษัท Ripple พัฒนาขึ้นมา มีกลไกฉันทามติที่เรียกว่า Ripple Protocol Consensus Algorithm (RPCA) ซึ่งถูกออกแบบมาเพื่อให้สามารถจัดการกับธุรกรรมจำนวนมากได้อย่างรวดเร็วและมีต้นทุนต่ำ กล่าวโดยสรุปคือ แต่ละโหนด (Node) จะมีการสร้างกลุ่มรายชื่อโหนดที่เชื่อถือได้ขึ้นมา เรียกว่า Unique Node List (UNL) ซึ่งหากร้อยละ 80 ของ UNL ของแต่ละโหนดเห็นตรงกันว่าธุรกรรมใดถูกต้อง ข้อมูลของธุรกรรมนั้นจะถูกบันทึกและจัดเก็บ กลไกฉันทามติเช่นนี้จะดำเนินซ้ำวนไปกับทุกโหนดเป็นรอบๆ ทุก 2-3 วินาที[9/]

Source: Krungsri Research

5/ https://www.krungsri.com/th/research/research-intelligence/the-merge-of-ethereum-2023

6/ https://www.krungsri.com/th/research/research-intelligence/the-merge-of-ethereum-2023

7/ https://www.researchgate.net/publication/323209703_Proof_of_Vote_A_High-Performance_Consensus_Protocol_Based_on_Vote_Mechanism_Consortium_Blockchain

8/ https://moralismoney.com/blog/what-is-a-proof-of-trust-consensus-protocol

9/ https://reasonabledeviations.com/notes/papers/ripple_consensus_protocol

นอกจากระบบ BVMS ที่ยกตัวอย่างมานี้ ยังคงมีอีกหลายแนวคิดที่นำเสนอการใช้เทคโนโลยีบล็อกเชนในการจัดการเลือกตั้งแบบออนไลน์ ซึ่งแนวคิดทั้งหมดล้วนเป็นไปเพื่อวัตถุประสงค์ที่คล้ายคลึงกัน กล่าวคือเพื่อเพิ่มความโปร่งใส ปลอดภัย และไร้การแทรกแซง รวมถึงประหยัดงบประมาณในการจัดการเลือกตั้งด้วย อย่างไรก็ตาม การเลือกตั้งแบบออนไลน์นั้นสามารถใช้เทคโนโลยีได้หลากหลาย ไม่ว่าจะเป็นบล็อกเชนหรือเทคโนโลยีอื่นๆ จึงนำไปสู่อีกหนึ่งคำถามว่า **การจัดเลือกตั้งแบบออนไลน์โดยใช้บล็อกเชนดีกว่าแบบไม่ใช้บล็อกเชนจริงหรือ?**



โหวตด้วยบล็อกเชนดีกว่าจริงหรือ?

การเลือกตั้งที่โปร่งใสและปลอดภัยต้องมีคุณลักษณะหลายประการ ซึ่งคุณสมบัติที่พูดถึงกันมากในวงกว้าง 3 ประการ ได้แก่ 1) การลงคะแนนของผู้ใช้สิทธิและการนับคะแนนของผู้จัดการเลือกตั้งต้องสามารถ**ตรวจสอบได้** (Verifiability/Auditability) เพื่อยืนยันเจตนารมณ์และความน่าเชื่อถือของผลการเลือกตั้ง 2) การลงคะแนนเสียงต้อง**เป็นความลับ** (Ballot secrecy) และไม่มีการระบุชื่อผู้ลงคะแนน (Voter anonymity) เพื่อป้องกันการบังคับขู่เข็ญและการซื้อสิทธิขายเสียง และ 3) ระบบจัดการหรือซอฟต์แวร์จะต้อง**เป็นอิสระ** (Software independence) กล่าวคือ ข้อผิดพลาดใดๆ ที่เกิดกับซอฟต์แวร์ของระบบจะต้องสามารถตรวจจับ แกะรอย และสืบหาสาเหตุได้ เพื่อให้ความยุติธรรมแก่ผู้ลงสมัครรับเลือกตั้ง ไม่ว่าข้อผิดพลาดที่เกิดขึ้นนั้นจะเล็กหรือใหญ่เพียงใด ผู้จัดการเลือกตั้งจะต้องสามารถอธิบายแก่สาธารณชนได้เพื่อสร้างความมั่นใจในผลการเลือกตั้ง ซึ่งหลักสำคัญพื้นฐานทั้งสามประการนี้นับว่าเป็นความท้าทายแก่ผู้ออกแบบระบบจัดการเลือกตั้งแบบออนไลน์เมื่อเทียบกับการใช้บัตรลงคะแนนแบบกระดาษ เนื่องจากข้อจำกัดตามคุณลักษณะทั้ง 3 ข้อ โดยมีรายละเอียดดังนี้

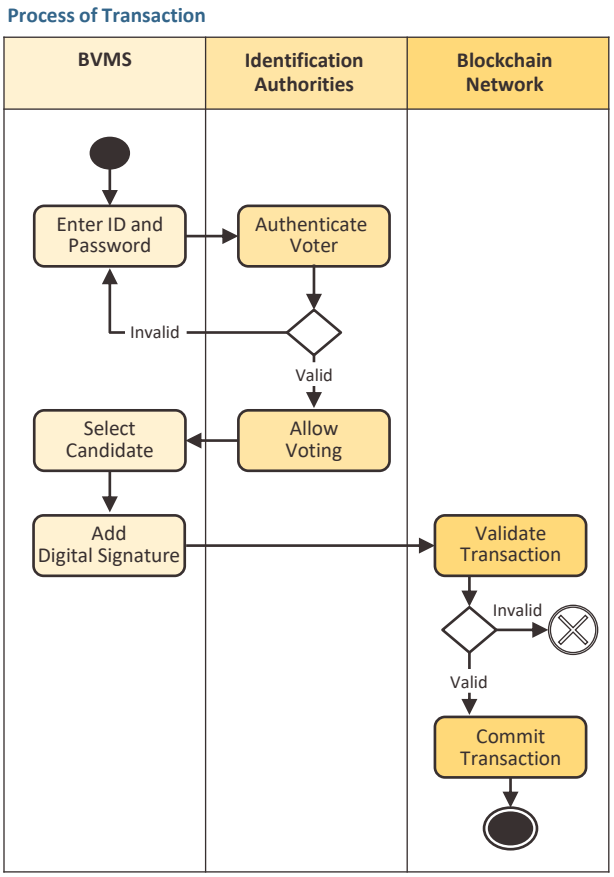
I. ตรวจสอบได้

จากกรณีการเลือกตั้งกลางเทอมของรัฐเวสต์เวอร์จิเนียในปี 2561 ที่ได้ยกตัวอย่างมานั้น ผู้ลงคะแนนไม่สามารถเห็นได้ด้วยตาของตนเองว่าบัตรเลือกตั้งกระดาษของตนที่ถูกพิมพ์ออกมาจากเครื่องเพื่อใช้นับคะแนนนั้นมีเครื่องหมายกากบาทตรงกับหมายเลขผู้สมัครที่ตนเองตั้งใจกดปุ่มเลือกผ่านแอปพลิเคชันหรือไม่ หรือหากมีข้อผิดพลาดผู้ลงคะแนนก็จะไม่สามารถทราบได้เลย ซึ่ง**ปัญหาการตรวจสอบการลงคะแนนของผู้ใช้สิทธิ** (Voter verifiability) **อาจแก้ไขได้หลายวิธีโดยนำเทคโนโลยีบล็อกเชนเข้ามาช่วย** ยกตัวอย่างเช่น ระบบ BVMS ออกแบบให้ผู้ลงคะแนนใช้ค่าแฮช (Hash value) ของธุรกรรมที่ถูกส่งเข้าไปยังโทรศัพท์มือถือเป็นกุญแจในการเข้าดูข้อมูลทั้งหมดที่ถูกบันทึกไว้ ธุรกรรมที่ถูกบันทึกจะถูกล็อคด้วยกุญแจสาธารณะ (Public key) ของผู้ลงคะแนน จากนั้นผู้ลงคะแนนจะใช้กุญแจส่วนตัว (Private key) ในการเข้าดูธุรกรรมที่ทำผ่านวอลเล็ทของตนก่อนที่จะกดปุ่มยืนยันการเลือก ซึ่งหลังจากกดยืนยันไปแล้วจะไม่สามารถเปลี่ยนแปลงแก้ไขได้อีก โดยการส่งผ่านข้อมูลขณะลงคะแนนจะถูกเข้ารหัส นอกจากนี้การเพิ่มลายเซ็นดิจิทัล (Digital signature) จะเป็นอีกส่วนหนึ่งที่ทำให้การทำธุรกรรมนั้นมีความปลอดภัย หรือสรุปได้ว่าการนำเทคโนโลยีบล็อกเชนมาใช้ตามระบบ BVMS จะทำให้ผู้ลงคะแนนเท่านั้นที่จะสามารถเข้าไปดูหรือตรวจสอบข้อมูลการลงคะแนนของตนได้ว่าเป็นไปตามความตั้งใจหรือไม่

นอกจากนี้ **อีกคุณสมบัติหนึ่งที่สำคัญคือความสามารถในการตรวจสอบระบบลงคะแนนและการนับคะแนนของผู้จัดการเลือกตั้ง** (Auditability and Auditing) เพราะผลการเลือกตั้งจะมีความน่าเชื่อถือก็ต่อเมื่อมาจากระบบที่เชื่อถือได้ ทั้งนี้ ไม่ว่าจะเป็นการเลือกตั้งออนไลน์จะผ่านระบบรวมศูนย์ (Centralized online voting system) หรือระบบกระจายศูนย์โดยใช้บล็อกเชน (Blockchain-based voting system) ที่ดูเหมือนจะมีข้อได้เปรียบในเรื่องความปลอดภัยและความโปร่งใส แต่การตรวจสอบระบบต่างๆ ของการเลือกตั้งแบบออนไลน์ยังมีความท้าทายหลายประการ อาทิ ความปลอดภัยของเครือข่าย (Network security) การรับรองความถูกต้องของผู้ใช้งาน (User authentication) ข้อกังวลด้านความเป็นส่วนตัว (Privacy concern) ความไม่สมบูรณ์พร้อมของอุปกรณ์ (Hardware vulnerabilities) หรือแม้แต่โอกาสที่โครงสร้างของระบบจะถูกโจมตี (Potential attacks on infrastructure) เป็นต้น ดังนั้นจึงอาจสรุปได้ว่า **สำหรับประเด็นนี้ การใช้บล็อกเชนในการจัดการเลือกตั้งออนไลน์ไม่ได้ทำให้การตรวจสอบระบบและการนับคะแนนง่ายขึ้นแต่อย่างใด หากแต่ความท้าทายในการตรวจสอบยังคงอยู่และอาจมีความยุ่งยากมากกว่าเดิมด้วยซ้ำตามความซับซ้อนในการออกแบบระบบ**

ภาพที่ 2

ข้อเสนอการใช้บล็อกเชนเพื่อให้ผู้ลงคะแนนเสียงสามารถตรวจสอบการลงคะแนนของตนได้



Source: Farooq, Ifthikhar & Khelifi, 2022; Krungsri Research

II. เป็นความลับและไม่ระบุชื่อหรือตัวตน

การเก็บรักษาความลับของบัตรลงคะแนน (Ballot Secrecy) **และการไม่ระบุชื่อผู้ลงคะแนน** (Voter Anonymity) **เป็นปัจจัยสำคัญของการเลือกตั้งในระบอบประชาธิปไตย** เพราะจะทำให้ผู้ลงคะแนนสามารถแสดงเจตจำนงที่แท้จริงของตนเองได้ เสมือนมีปราการป้องกันมิให้ถูกข่มขู่ คุกคาม บีบบังคับ รวมถึงป้องกันมิให้เกิดการซื้อสิทธิขายเสียงอีกด้วย ซึ่งงานศึกษาโดย Ostwald และ Riambau วิเคราะห์ผลการสำรวจจากสิงคโปร์พบว่าพฤติกรรมการลงคะแนนจะเปลี่ยนไปหากผู้ลงคะแนนสงสัยว่าอาจไม่มีการเก็บรักษาความลับของบัตรลงคะแนน แม้ว่าในความจริงแล้วการลงคะแนนเป็นแบบลับและไม่มีการให้โทษรายบุคคลในภายหลังก็ตาม (Ostwald & Riambau, 2021) โดยงานชิ้นนี้ยังสรุปว่า ในกรณีของประเทศสิงคโปร์ หากผู้มาใช้สิทธิกังวลเกี่ยวกับการรักษาความลับของบัตรลงคะแนนจะทำให้ผู้มาใช้สิทธิเลือกตั้งร้อยละ 3-5 ตัดสินใจเลือกพรรคที่คาดว่าจะได้รับชัยชนะ แม้ว่าอันที่จริงแล้วจะชื่นชอบพรรคฝั่งตรงข้ามก็ตาม[10/]

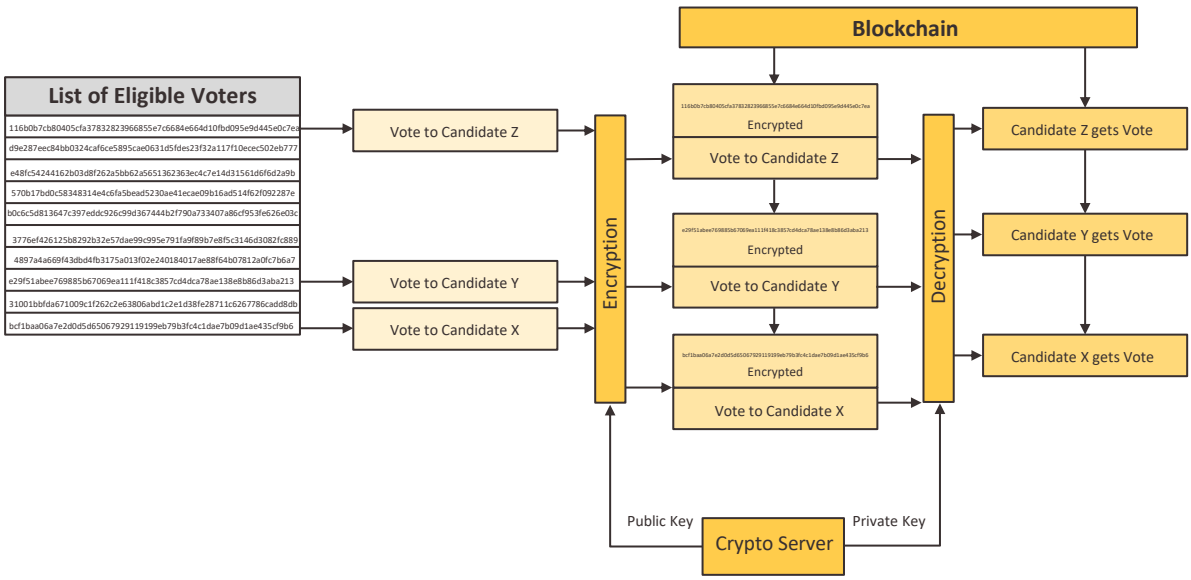
10/ สามารถอ่านรายละเอียดเพิ่มเติมได้จากการศึกษาฉบับเต็มของ Kai Ostwald and Guillem Riambau, 'Voting Behavior under Doubts of Ballot Secrecy: (Un)Intentionally Nudging Voters Towards a Dominant Party Regime', 17 May 2021

เมื่อพิจารณาการเลือกตั้งแบบออนไลน์จะพบว่า **การใช้เทคโนโลยีบล็อกเชนสามารถช่วยเรื่องการเก็บรักษาความลับของบัตรลงคะแนนแบบออนไลน์ได้ดีกว่าระบบออนไลน์อื่น ๆ** เพราะบล็อกเชนเป็นระบบเก็บข้อมูลแบบกระจายศูนย์ (Decentralization) ทำให้ปราศจากตัวกลางที่มีอำนาจควบคุมแบบเบ็ดเสร็จเด็ดขาดเพียงผู้เดียว จึงช่วยลดความเสี่ยงในการละเมิดการเข้าถึงข้อมูลการลงคะแนนที่ควรเป็นความลับได้ นอกจากนี้ยังมีคุณลักษณะที่ไม่สามารถเปลี่ยนแปลงแก้ไขข้อมูลที่เก็บไว้ในระบบได้ (Immutability) ซึ่งจะช่วยป้องกันมิให้มีการเปลี่ยนแปลงคะแนนและผลการเลือกตั้งภายหลัง และยังใช้การเข้ารหัสและความเป็นส่วนตัว (Encryption and Privacy) ที่ทำให้ผู้จัดการเลือกตั้งไปจนถึงแฮกเกอร์ไม่สามารถเข้าถึงการลงคะแนนของแต่ละบุคคล และไม่สามารถเปิดเผยผลคะแนนจนกว่าจะถึงเวลาปิดหีบเลือกตั้ง เป็นต้น

นอกจากนี้ **การใช้เทคโนโลยีบล็อกเชนโดยเก็บข้อมูลของผู้ลงคะแนนแต่ละรายในรูปแบบของค่าแฮชช่วยให้สามารถเก็บข้อมูลของผู้ลงคะแนนแต่ละรายได้โดยไม่ต้องระบุตัวตน** ซึ่งทางเลือกหนึ่งคือการจัดการเลือกตั้งโดยใช้สัญญาอัจฉริยะบนบล็อกเชนอีเธอเรียม (Alvi et al., 2022) ที่ออกแบบให้ผู้ลงคะแนนสามารถพิสูจน์สิทธิของตนได้โดยไม่จำเป็นต้องเปิดเผยข้อมูลที่ระบุตัวตนที่แท้จริง โดยในเครือข่ายบล็อกเชนจะมีการใช้กุญแจสาธารณะ ซึ่งเปรียบได้ว่าเป็น “ที่อยู่อีเมล” (E-mail address) เป็นเครื่องมือในการแสดงตัวตนบนเครือข่ายของผู้ลงคะแนน ขณะที่ค่าแฮชจะถูกใช้แทนข้อมูลของผู้ลงคะแนน ซึ่งคะแนนเสียงที่ได้รับจากผู้มีสิทธิลงคะแนนแต่ละรายจะผ่านการเข้ารหัส (Encryption) เพื่อป้องกันมิให้คะแนนเสียงเชื่อมโยงถึงกัน และภายหลังจากที่การไขรหัส (Decryption) ของคะแนนเสียงทั้งหมดสิ้นสุดลง สัญญาอัจฉริยะจะทำหน้าที่ส่งเหรียญโหวตไปยังผู้สมัครรับเลือกตั้ง (Candidate) โดยไม่เปิดเผยข้อมูลที่บ่งชี้ตัวตนของผู้ลงคะแนน เพื่อรักษากฎการไม่ระบุตัวตน ดังที่แสดงในภาพที่ 3

ภาพที่ 3

ข้อเสนอการใช้บล็อกเชนเพื่อรักษากฎแห่งการไม่ระบุตัวตน (Anonymity of Voters)



Source: Alvi et al., 2022; Krungsri Research

III. เป็นอิสระ

ดังที่กล่าวข้างต้นว่า การจัดการเลือกตั้งที่น่าเชื่อถือจะต้องมีความเป็นอิสระและสามารถตรวจสอบได้ในทุกๆ ขั้นตอน และ**สำหรับการเลือกตั้งแบบออนไลน์นั้น ความเป็นอิสระของระบบจัดการหรือซอฟต์แวร์** (Software independence) **เป็นอีกหนึ่งองค์ประกอบสำคัญ โดยระบบจัดการเลือกตั้งจะถือว่ามีคุณสมบัติด้านความเป็นอิสระของซอฟต์แวร์ หากมีการเปลี่ยนแปลงหรือข้อผิดพลาด (อันตรวจไม่พบ) เกิดขึ้นในซอฟต์แวร์นั้นๆ แล้วจะสะท้อนออกมาให้เห็นในผลการเลือกตั้งทันที ทำให้สามารถทราบถึงความผิดปกติได้ชัดเจน** (Rivest, 2008) ในทางกลับกัน หากการจัดการเลือกตั้งขาดความเป็นอิสระของซอฟต์แวร์อาจก่อให้เกิดความผิดพลาดขนาดใหญ่ (Large-scale errors) หรือการโจมตีทางไซเบอร์ได้ เช่น หากโปรแกรมเมอร์ซึ่งทำงานจากพื้นที่อื่นๆ ที่ห่างไกลได้เข้าไปเปลี่ยนโค้ดแม้เพียงหนึ่งบรรทัด ไม่ว่าจะด้วยเจตนาดีหรือร้ายก็ตาม อาจทำให้บัตรเลือกตั้งอิเล็กทรอนิกส์ (Electronic ballots) จำนวนหลายล้านใบเปลี่ยนแปลงได้ในเสี้ยววินาที ซึ่งต่างจากการจัดการเลือกตั้งแบบปัจจุบัน เพราะหากมีคนต้องการเปลี่ยนแปลงบัตรเลือกตั้งกระดาษ (Paper ballots) ผู้ลงมือกระทำจะต้องเข้าถึงสถานที่เก็บบัตรเลือกตั้งและทำการเปลี่ยนแปลงบัตรทีละใบ (Park et al., 2020) ซึ่งจะเห็นได้ว่าขนาดของความเสียหายในการเลือกตั้งแบบออนไลน์และแบบแอนะล็อกนั้นแตกต่างกันมาก

ในเชิงหลักการแล้ว การตรวจสอบว่าระบบจัดการเลือกตั้งมีซอฟต์แวร์ที่เป็นอิสระหรือไม่นั้น ไม่ควรอยู่บนพื้นฐานของการใช้ซอฟต์แวร์เพื่อตรวจสอบซอฟต์แวร์ ซึ่งทำได้ยากในทางปฏิบัติ และอาจต้องรอให้เทคโนโลยีถูกพัฒนาจนถึงวันที่เราสามารถสร้างโค้ดที่สมบูรณ์แบบหรือไร้ข้อผิดพลาด (Error-free code) มาใช้งานได้ อย่างไรก็ดี ในปัจจุบันการใช้ซอฟต์แวร์ยังเป็นสิ่งจำเป็นสำหรับการจัดการเลือกตั้งออนไลน์ เพียงแต่ผู้วางระบบควรออกแบบวิธีการตรวจสอบที่พึ่งพาการใช้ซอฟต์แวร์ให้น้อยที่สุด หรือไม่พึ่งพาซอฟต์แวร์เลย (Non-software-based means) อาทิเช่น การออกแบบขั้นตอนให้คนทั่วไปเข้าตรวจสอบได้โดยไม่พึ่งพาเทคโนโลยี หรือเปิดให้สาธารณชนนำซอฟต์แวร์ของตนเองมาใช้ในการตรวจสอบระบบได้ ซึ่งการออกแบบระบบลักษณะนี้จะมีความท้าทายมากในทางปฏิบัติไม่ว่าระบบจัดการนั้นจะใช้บล็อกเชนหรือไม่ก็ตาม

> *Democracy — and the consent of the governed — cannot be contingent on whether some uncheckable software correctly recorded voters' choices.*
>
> *Park, Specter, Narula & Rivest (2020)*

ความเป็นอิสระของซอฟต์แวร์เป็นเรื่องที่สำคัญมาก และนำมาซึ่งประเด็นคำถามอื่นๆ ที่เกี่ยวข้องอีกมากมาย เช่น (1) เมื่อมีผู้พบข้อผิดพลาดของซอฟต์แวร์แล้ว สาธารณชนจะมั่นใจได้อย่างไรว่าความผิดพลาดนั้นเกิดขึ้นจริงตามที่ผู้พบชี้แจง มิใช่เพียงกล่าวอ้างเพื่อผลประโยชน์อื่น เพราะต้องไม่ลืมว่ากระบวนการตรวจสอบข้อผิดพลาดในบางขั้นตอนอาจกระทำโดยเปิดเผยได้ แต่ในบางขั้นตอนอาจต้องให้ผู้ลงคะแนนแต่ละรายเป็นคนตรวจสอบเท่านั้น ซึ่งไม่ว่าจะอยู่ในขั้นตอนใดการประกาศให้ทุกฝ่ายรับทราบถึงข้อผิดพลาดของซอฟต์แวร์จะต้องอาศัยหลักฐานที่สามารถเปิดเผยชี้แจงต่อสาธารณชนได้เสมอ (2) เมื่อตรวจพบข้อผิดพลาดขึ้น ระบบจะสามารถแก้ไขให้ถูกต้องได้ทันทีเลยหรือไม่ หรือหากยังแก้ไขไม่ได้จะต้องดำเนินการอย่างไรต่อไป เพราะหากวางระบบไว้ดีและมีซอฟท์แวร์ที่เป็นอิสระสูง ในกรณีที่เกิดข้อผิดพลาดผู้ใช้งานจะสามารถเรียกกู้คืนผลลัพธ์ที่ถูกต้องกลับมาได้จากร่องรอยหลักฐานทางดิจิทัล (Digital footprint) ที่ปรากฏระหว่างการเลือกตั้ง แต่เราไม่อาจมั่นใจได้ว่าซอฟต์แวร์ที่ใช้อยู่นั้นจะถูกออกแบบมาดีมากพอและมีคุณสมบัติในลักษณะดังกล่าว

Box 2 การจัดการเลือกตั้งในไนจีเรีย กับบทบาทที่ไม่ธรรมดาของธนาคารกลาง

ไนจีเรียเป็นประเทศที่มีขนาดทางเศรษฐกิจใหญ่ที่สุดในทวีปแอฟริกา โดยในปี 2565 มีขนาดเศรษฐกิจถึง 477.38 พันล้านดอลลาร์สหรัฐ[11/] หรือประมาณร้อยละ 94 ของขนาดเศรษฐกิจไทยในปีเดียวกัน และยังมีการเติบโตเป็นลำดับต้นๆ ในด้านการพัฒนาเทคโนโลยีทางการเงินในภูมิภาคนี้โดยเฉพาะบล็อกเชน โดยรัฐบาลไนจีเรียมุ่งมั่นให้เทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญในการพัฒนาเศรษฐกิจควบคู่ไปกับอุตสาหกรรมด้านพลังงาน จึงได้จัดทำนโยบายและยุทธศาสตร์เศรษฐกิจดิจิทัลแห่งชาติ 2563-2573 ซึ่งมียุทธศาสตร์การปรับใช้เทคโนโลยีบล็อกเชนแห่งชาติ (National Blockchain Adoption Strategy) ที่ถูกขับเคลื่อนโดยรัฐบาลเป็นหนึ่งในองค์ประกอบสำคัญ



Picture credit: Naija247news

สำหรับการเลือกตั้งในประเทศไนจีเรียนั้น ในช่วงหลายปีที่ผ่านมา คณะกรรมการการเลือกตั้งแห่งชาติอิสระ (Independent National Electoral Commission: INEC) ได้เผชิญกับปัญหาหลายรูปแบบของการจัดการเลือกตั้งทั่วไปในประเทศ จึงเป็นเหตุให้ภาครัฐและนักวิชาการหันมาให้ความสนใจและทำการศึกษาเกี่ยวกับการนำบล็อกเชนมาใช้ในการจัดการเลือกตั้ง ด้วยเล็งเห็นว่าประเทศมีความพร้อมในระดับหนึ่งแล้ว ซึ่งเมื่อต้นปี 2566 ที่ผ่านมา มีการตีพิมพ์งานศึกษาเกี่ยวกับการเลือกตั้งในประเทศไนจีเรียที่ระบุถึงความสัมพันธ์ของภาคธนาคารกับการเลือกตั้งโดยใช้บล็อกเชน (Eghe-Ikhurhe et al., 2023) โดยระบุว่าหนึ่งในขั้นตอนสำคัญคือขั้นตอนการลงทะเบียนของประชาชนผู้มีสิทธิ์เลือกตั้ง ที่ต้องลงทะเบียนกับหน่วยจัดการเลือกตั้งก่อนเพื่อแสดงสิทธิ์ โดยต้องใช้สิ่งที่สามารถระบุตัวตนได้แบบเฉพาะบุคคล (Unique identifier) ที่หน่วยงานราชการเป็นผู้ออก อาทิเช่น หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวไบโอเมตริกซ์ในฐานข้อมูลของธนาคารกลางของไนจีเรีย (Bank Verification Number: BVN) เพื่อควบคุมมิให้มีประชากรที่มิได้ลงทะเบียนแฝงตัวมาลงคะแนนและป้องกันการลงคะแนนซ้ำซ้อนของผู้ใช้สิทธิรายเดียว **ซึ่งจะเห็นได้ว่าธนาคารกลางไนจีเรียเป็นหน่วยงานที่มีความน่าเชื่อถือสูง จนได้รับความไว้วางใจให้เป็นส่วนหนึ่งของกระบวนการยืนยันตัวตนของการจัดการเลือกตั้งทั่วไปแบบใช้บล็อกเชน** อันเป็นบทบาทของธนาคารกลางที่ *"ไม่ธรรมดา"*

ไม่เพียงแต่ธนาคารกลางเท่านั้น หากแต่อุตสาหกรรมการเงินการธนาคารโดยทั่วไปยังได้รับการยอมรับในวงกว้างว่าเป็นอุตสาหกรรมแถวหน้าในการพัฒนาและปรับใช้นวัตกรรมทางเทคโนโลยีในการทำธุรกรรมต่างๆ ให้เกิดประสิทธิภาพและความโปร่งใสเพิ่มขึ้นด้วย จนอาจมีคำถามว่า ธนาคารพาณิชย์จะสามารถมีบทบาทในการประยุกต์ใช้บล็อกเชนในวงกว้างสำหรับกิจกรรมที่ไม่เกี่ยวข้องโดยตรงกับภาคการเงินอย่างการเลือกตั้งทั่วไปได้หรือไม่

Source: Krungsri Research

11/ https://www.statista.com/statistics/1120999/gdp-of-african-countries-by-country/

มุมมองวิจัยกรุงศรี: ไม่มีคำว่า “One size fits all”

การเปลี่ยนแปลงระบบการเลือกตั้งย่อมนำมาซึ่งความท้าทายไปจนถึงปัญหาใหม่ๆ ในรูปแบบต่างๆ ดังนั้น หากเราย้อนกลับไปที่จุดตั้งต้นแล้วตั้งคำถามว่า **การจัดการเลือกตั้งแบบใช้บล็อกเชนนั้นดีกว่าแบบปัจจุบันจริงหรือไม่** คำตอบที่สามารถให้ได้ ณ ขณะนี้คือ **“ดีกว่าเพียงบางด้าน”** เพราะหากพิจารณาบนพื้นฐานของความก้าวหน้าทางเทคโนโลยีแล้ว แม้การใช้บล็อกเชนจะมีส่วนดีอยู่มากแต่ก็ยังไม่สามารถอุดช่องโหว่ของปัญหา (Pain points) จากการจัดเลือกตั้งแบบปกติได้ครบทุกมิติ แม้การเลือกตั้งแบบออนไลน์โดยใช้บล็อกเชนจะมีจุดแข็งด้านความสะดวกรวดเร็วในการลงคะแนนและการประมวลข้อมูล รวมไปถึงความน่าเชื่อถือของระบบเพราะหลังจากที่มีการบันทึกผลเรียบร้อยแล้วมีโอกาสน้อยมากที่ข้อมูลการลงคะแนนจะถูกลบ แก้ไข หรือเปลี่ยนแปลงในภายหลังได้

การใช้บล็อกเชนในการเลือกตั้งยังอาจสร้างปัญหาใหม่ เนื่องจากหลักการทำงานแบบกระจายศูนย์ของบล็อกเชนมาพร้อมกับผู้เกี่ยวข้องหลายฝ่ายและหลายราย และนำมาซึ่งปัญหาใหม่ในเรื่องของระบบการจัดการ (Governance) และการประสานงาน (Coordination) เพราะจะต้องมีระบบจัดการและซอฟท์แวร์ที่ถูกออกแบบมาอย่างรัดกุมและซับซ้อนมากกว่าระบบที่มีการควบคุมจากศูนย์กลางเพียงแห่งเดียว โดยความซับซ้อนที่เพิ่มขึ้นนี้อาจมาในรูปของการแก้ไขข้อบกพร่อง (Bug fix) และการติดตั้งซอฟต์แวร์ใหม่ (New software deployment) เช่น เมื่อมีการพบช่องโหว่หรือข้อผิดพลาดด้านความปลอดภัย การแก้ไขปัญหาให้กับระบบที่ใช้บล็อกเชนอาจต้องการเวลาและต้องใช้ความพยายามมากกว่าการแก้ปัญหาเดียวกันสำหรับระบบออนไลน์แบบรวมศูนย์

นอกจากนี้ การใช้บล็อกเชนในการเลือกตั้งยังไม่สามารถแก้ไขปัญหาเรื่องความปลอดภัยขั้นพื้นฐานทั้งหมดได้ แม้ว่าระบบจะถูกออกแบบให้ป้องกันปัญหาเรื่องการโจมตี 51% หรือวางกลไกอัตโนมัติเพื่อตรวจสอบความถูกต้องและปลอดภัยของบล็อกเชน แต่ปัญหาการโจมตีทางไซเบอร์ก็ยังคงมีอยู่และไม่สามารถถูกขจัดให้หมดไปได้ เพราะการเลือกตั้งโดยใช้บล็อกเชนยังคงตั้งอยู่บนพื้นฐานของระบบออนไลน์ ซึ่งยังมีช่องโหว่ที่จะทำให้เกิดความล้มเหลวขั้นรุนแรงได้ เช่น ระบบล่ม โดยเฉพาะเมื่อเทียบกับการเลือกตั้งด้วยบัตรกระดาษแบบดั้งเดิม ยกตัวอย่างเช่น ช่องโหว่ ‘INVDoS’ รหัส CVE-2018-17145 ที่ถูกพบโดย Braydon Fuller ในปี 2561[12/] ที่เปิดทางให้ผู้โจมตีระบบสามารถสร้างธุรกรรมที่ผิดรูปแบบเข้าไป และเมื่อธุรกรรมนั้นถูกนำไปประมวลผลภายในเครือข่ายจะทำให้มีการใช้หน่วยความจำ (Memory) ในลักษณะที่ผิดปกติบนเซิร์ฟเวอร์ ทำให้ระบบล่มและเกิดความเสียหายในที่สุด ซึ่งในเวลาต่อมา มีรายงานจากระบบตรวจติดตามซอฟต์แวร์ (Software tracker) ของเหรียญชื่อดัง ที่ระบุว่า ในปี 2563 เครือข่ายเหรียญดังกล่าวร้อยละ 27 ยังคงเผชิญกับช่องโหว่ที่ว่านี้ (Park et al., 2020) แม้กระทั่งในปัจจุบัน การตรวจพบช่องโหว่และข้อผิดพลาดของซอฟต์แวร์ถือเป็นเรื่องปกติในแวดวงนักพัฒนาและการตรวจติดตามระบบบล็อกเชน

12/ https://www.zdnet.com/article/researcher-kept-a-major-b itcoin-bug-secret-for-two-years-to-prevent-attacks/

ในกรณีของการจัดการเลือกตั้งใหญ่ที่มีผู้มีส่วนได้ส่วนเสียจำนวนมาก หากเกิดข้อผิดพลาดขึ้นมา นอกจากที่หน่วยงานที่ดูแลการเลือกตั้งจะต้องแก้ไขปัญหาเฉพาะหน้าแล้ว ยังจะต้องชี้แจงให้สาธารณชนได้รับทราบด้วยหลักฐานเชิงประจักษ์ที่ได้จากการสืบพิสูจน์ ซึ่งข้อผิดพลาดที่เกิดขึ้นกับซอฟต์แวร์หรือการขัดข้องของระบบออนไลน์อาจไม่สามารถแสดงให้เห็นหรืออธิบายให้สาธารณชนเข้าใจได้โดยง่าย ไม่เหมือนการเลือกตั้งที่ใช้บัตรกระดาษที่สามารถเทหีบที่ใส่บัตรเลือกตั้งแล้วนับใหม่ให้ดูต่อหน้าเพื่อให้สาธารณะชนสิ้นข้อสงสัยได้

สำหรับการจัดการเลือกตั้งระดับประเทศที่มีเดิมพันสูงแล้ว **การนำระบบหรือเทคโนโลยีใหม่ใดๆ เข้ามาใช้ควรจะต้องมีการทดสอบที่รัดกุมก่อน โดยอาจทดลองระบบนำร่องกับการเลือกตั้งขนาดเล็กในระดับท้องถิ่นและ/หรือทดลองใช้ระบบกับการเลือกตั้งล่วงหน้านอกเขตหรือในการลงคะแนนในพื้นที่ห่างไกลก่อนหลายๆ ครั้ง จนกระทั่งมั่นใจว่าระบบการจัดการเลือกตั้งแบบออนไลน์มีความพร้อมในทุกด้านสำหรับการเลือกตั้งใหญ่ระดับประเทศ** ซึ่งก็มีความเป็นไปได้ว่าอาจใช้เวลาร่วมทศวรรษในการศึกษาทดลองเพื่ออุดช่องโหว่ของระบบ โดยขึ้นอยู่กับการพัฒนาเทคโนโลยีว่าจะมีความก้าวหน้าและดำเนินไปอย่างรวดเร็วมากเพียงใด

อย่างไรก็ตาม แม้ระบบการเลือกตั้งออนไลน์แบบใช้บล็อกเชนอาจจะยังไม่เหมาะสมกับการนำมาใช้เลือกตั้งทั่วไปในระดับประเทศด้วยปัจจัยความพร้อมด้านเทคโนโลยีในขณะนี้ แต่ระบบดังกล่าวก็เป็นทางเลือกหนึ่งที่น่าสนใจสำหรับการเลือกตั้งบางประเภทที่มีขนาดเล็กกว่าหรือมีงบประมาณที่จำกัด หรือแม้กระทั่งสามารถนำมาปรับใช้กับการเลือกตั้งในพื้นที่ที่มีความยากลำบากในการเดินทางมาลงคะแนน เช่นสำหรับผู้ที่อยู่ในต่างประเทศหรืออยู่ในพื้นที่ห่างไกล เพราะท้ายที่สุดแล้วเทคโนโลยีจะเกิดประโยชน์สูงสุดได้ก็ขึ้นอยู่กับการนำมาประยุกต์ใช้เช่นกัน เพราะไม่มีระบบสำเร็จรูปแบบใดเพียงแบบเดียวที่จะเหมาะสมที่สุดกับทุกบริบทการเลือกตั้ง



References

Alvi et al. (2022) DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. Retrieved May 16, 2023 from https://www.sciencedirect.com/science/article/pii/S1319157822002221/pdf

Catalin Cimpanu (2020) Researcher kept a major B itcoin bug secret for two years to prevent attacks [Blog post]. Retrieved August 10, 2023 from https://www.zdnet.com/article/researcher-kept-a-major-b itcoin-bug-secret-for-two-years-to-prevent-attacks/

Eghe-Ikhurhe et al. (2023) The Relevance of Blockchain Based Voting Adoption in Governance Structure. Evidence from Nigeria. International Journal of Economics, Commerce & Management, United Kingdom. Retrieved August 20, 2023 from https://ijecm.co.uk/wp-content/uploads/2023/01/1111.pdf

Farooq, Ifthikhar and Khelifi (2022) A framework to make voting system transparent using blockchain technology. IEEE Access. Retrieved May 16, 2023 from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9787540

Kai Ostwald and Guillem Riambau (2021) Voting Behavior under Doubts of Ballot Secrecy: (Un)Intentionally Nudging Voters Towards a Dominant Party Regime. Retrieved August 13, 2023 from http://guillemriambau.com/Ostwald%20Riambau%20Voting%20under%20doubts%20of%20ballot%20secrecy.pdf

Li et al. (2017) Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain [Conference paper]. Retrieved September 13, 2023 from https://www.researchgate.net/publication/323209703_Proof_of_Vote_A_High-Performance_Consensus_Protocol_Based_on_Vote_Mechanism_Consortium_Blockchain

Park et al. (2020) Going from Bad to Worse: From Internet Voting to Blockchain Voting. [Draft November 6, 2020] Retrieved May 17, 2023 from https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf

Ronald L. Rivest (2008) On the notion of 'software independence' in voting systems. Philosophical Transactions of the Royal Society. Retrieved August 10, 2023 from https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2008.0149

Yael Grauer (2019) What Really Happened With West Virginia's Blockchain Voting Experiment? [Blog post] Retrieved July 22, 2023 from https://slate.com/technology/2019/07/west-virginia-blockchain-voting-voatz.html

วิจัยกรุงศรี

ดร.พิมพ์นารา หิรัญกสิ

ผู้บริหารสายงานวิจัยและหัวหน้าทีมวิจัยเศรษฐกิจ

ทีมวิจัยเศรษฐกิจ

สุจิต ชัยวิชญชาติ

ผู้บริหารทีมวิจัยเศรษฐกิจมหภาค

วนิชา ดิเรกอุดมศักดิ์

เศรษฐกรอาวุโส

จุไรลักษณ์ พลศรี

เศรษฐกรอาวุโส (พยากรณ์ตัวเลขเศรษฐกิจ)

ทรรศิน กลิ่นถนอม

เศรษฐกร

กฤตพร ศิริใจชิงกุล

เศรษฐกร

ศุภสิน อิทธิพัทธ์วงศ์

เศรษฐกร

ทีมวิเคราะห์และพัฒนางานวิจัย

ดร.พิมพ์นารา หิรัญกสิ

รักษาการผู้บริหารทีมวิเคราะห์และพัฒนางานวิจัย

ณธัญอร รัตนาธรรมวัฒน์

นักวิเคราะห์อาวุโส

นฤชยา สาตแฟง

นักวิเคราะห์

ปริญญา มิ่งสกุล

นักวิเคราะห์

ชณัฐฐา ธาระรส

นักวิเคราะห์

ทีมบริหารระบบข้อมูลวิจัย

ธมณ เสริญสุขสกุล

เจ้าหน้าที่บริหารงานทั่วไป

เชิดศักดิ์ ศรีชัยตัน

เจ้าหน้าที่ระบบข้อมูลวิจัย

วงศกร แก้วอุดทัง

เจ้าหน้าที่ระบบข้อมูลวิจัย

ทีมวิจัยอุตสาหกรรม

ดร.พิมพ์นารา หิรัญกสิ

รักษาการผู้บริหารทีมวิจัยอุตสาหกรรม

ธเนศ มหัทธนาลัย

นักวิเคราะห์อาวุโส (Digital)

พูลสุข นิลกิจศรานนท์

นักวิเคราะห์อาวุโส (Healthcare, Mobile Operators)

ปิยะนุช สถาพงศ์ภักดี

นักวิเคราะห์อาวุโส (Transport & Logistics)

นรินทร์ ตันไพบูลย์

นักวิเคราะห์อาวุโส (Power Generation, Modern Trade, Chemicals, Medical Devices)

เตียร เทียมศักดิ์

นักวิเคราะห์อาวุโส (Energy, Petrochemicals)

พุทธชาด ลุนคำ

นักวิเคราะห์อาวุโส (Construction Contractors, Construction Materials, Hotels, Industrial Estate)

พัชรา กลิ่นชวนชื่น

นักวิเคราะห์อาวุโส (Real Estate)

ชัยวัช โชวเจริญสุข

นักวิเคราะห์อาวุโส (Agriculture)

ประพันธ์ ลีน้อย

นักวิเคราะห์ (ESG)

ศุภวัฒน์ โชคสวัสดิ์ไพศาล

นักวิเคราะห์ (Automobile, Electronics & Electrical Appliances)

ศุภกร กรบุญไตรทศ

นักวิเคราะห์ (Agriculture, Food & Beverages)