Cryptocurrency and related technologies: a concise series for lawyers

ซีรี่ส์สั้นสำหรับนักกฎหมาย เรื่อง เงินดิจิทัลและเทคโนโลยีที่เกี่ยวข้อง

ตอนที่ 1 : บล็อกเชน (Blockchain)

นายณรัณ โพธิ์พัฒนชัย*

ในชั่วโมงนี้ คงไม่มีนวัตกรรมทางการเงินใดที่จะได้รับความสนใจอย่างกว้างขวางไปมากกว่าระบบการเงินดิจิทัล หรือ Cryptocurrency ซึ่งหลายฝ่ายกำลังจับตามอง ไม่ว่าจะเป็นนักลงทุนมากประสบการณ์ ประชาชนทั่วไป หรือแม้แต่องค์กรกำกับดูแลของรัฐทั้งในประเทศและต่างประเทศ หากดูจากการเคลื่อนไหวของราคาเงินดิจิทัลสกุลบิทคอยน์ (Bitcoin) ซึ่งเป็นเงินดิจิทัลสกุลแรกและเป็นที่นิยมที่สุดในขณะนี้ จะเห็นได้ว่าราคาซื้อขายต่อหนึ่งเหรียญพุ่งทะยานกว่าสามหมื่นเปอร์เซ็นต์ในรอบห้าปีที่ผ่านมา (ถึงแม้จะเริ่มมีสัญญานแรงต้านขึ้นมาบ้างในช่วงต้นปี พ.ศ. 2561 ก็ตาม) อีกทั้งบริษัทห้างร้านต่างๆ เริ่มรับชำระค่าสินค้าและบริการด้วยเงินดิจิทัลเพิ่มมากขึ้น จนมีกระแสที่ว่า เงินดิจิทัลอาจกลายเป็นคู่แข่งกับเงินสกุลดั้งเดิมที่ออกและควบคุมโดยรัฐ ดังเช่น เงินดอลลาร์สหรัฐฯ หรือเงินบาทของไทย ก็เป็นได้ อย่างไรก็ตาม โดยที่ระบบเงินดิจิทัลยังคงเป็นเรื่องที่เข้าใจยาก เนื่องจากเป็นเรื่องที่บูรณาการศาสตร์หลายแขนง อาทิ เทคโนโลยีสารสนเทศระดับสูง การบริหารจัดการฐานข้อมูล (database management) เศรษฐศาสตร์การเงิน รวมไปถึงกฎหมายเกี่ยวกับการทำนิติกรรมและสัญญาต่างๆ ในตลาดการเงิน จึงเป็นการจุดประกายการจัดทำซีรี่ส์สั้นสำหรับนักกฎหมาย เรื่อง เงินดิจิทัลและเทคโนโลยีที่เกี่ยวข้อง โดยมีวัตถุประสงค์เพื่ออธิบายแนวคิดพื้นฐานที่เกี่ยวข้องกับระบบการเงินดิจิทัล และให้ข้อมูลเกี่ยวกับผลกระทบและความเสี่ยงของนวัตกรรมทางการเงินรูปแบบใหม่ชนิดนี้ต่อระบบเศรษฐกิจของประเทศ และแนวทางการกำกับดูแลในปัจจุบัน

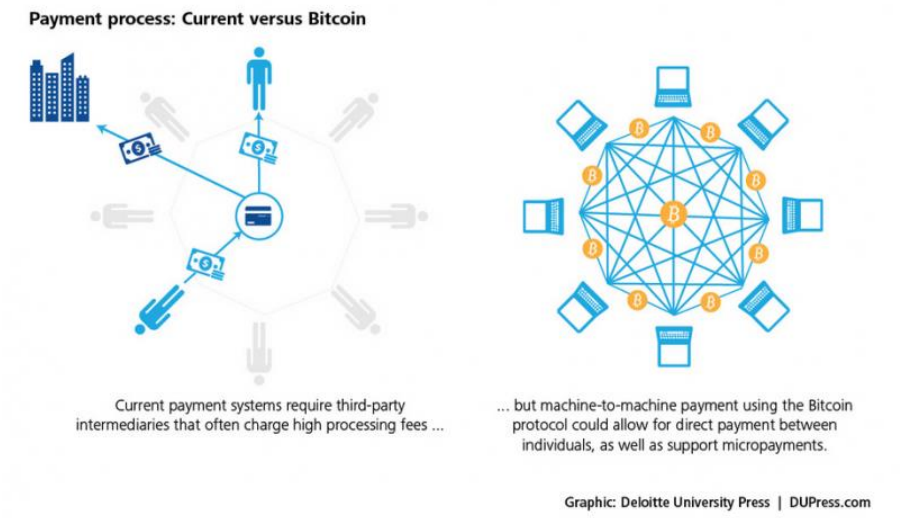
คำศัพท์ทางเทคนิคที่ควรรู้

เรามาเริ่มต้นด้วยการอธิบายคำศัพท์เบื้องต้นที่หลายคนคงเคยได้ยินกันอยู่บ่อยๆ กันก่อน คำแรกที่ควรรู้และเป็นหัวข้อของข่าวสารพัฒนากฎหมายฉบับนี้ คือคำว่า บล็อกเชน (Blockchain) ซึ่งเป็นเทคโนโลยีด้านการเข้ารหัสลับทางคอมพิวเตอร์ (cryptographic computing) ที่เป็นพื้นฐานของระบบเงินดิจิทัลและนวัตกรรมด้านการเข้ารหัสลับทางคอมพิวเตอร์อื่น ๆ คำศัพท์อีกคำที่เราคุ้นหู คือคำว่า บิทคอยน์ (Bitcoin) ตามที่ได้กล่าวมาบ้างแล้วข้างต้น ซึ่งเป็นสกุลเงินดิจิทัลสกุลแรกและยังคงเป็นสกุลเงินที่ได้รับความนิยมสูงสุดในปัจจุบัน (กล่าวคือมีสภาพคล่องสูงที่สุดและได้รับการยอมรับให้เป็นสินทรัพย์เพื่อชำระหนี้ทางกฎหมายอย่างกว้างขวางพอสมควร) และสุดท้ายคือคำว่า เงินดิจิทัล (cryptocurrency) ซึ่งเป็นตัวกลางที่ใช้ในการแลกเปลี่ยนและชำระหนี้ (medium of exchange and mean of payment) ในโลกดิจิทัล เงินดิจิทัลจึงไม่มีรูปทางกายภาพ (กล่าวคือไม่มีออกมาในรูปเหรียญหรือธนบัตร) และใช้ระบบการเข้ารหัสในการควบคุมการผลิตหน่วยการเงิน (monetary unit) และการยืนยันการถ่ายโอนเงิน

* นักกฎหมายกฤษฎีกาปฏิบัติการ กองพัฒนากฎหมาย สำนักงานคณะกรรมการกฤษฎีกา

ที่มาของเทคโนโลยีบล็อกเชน (Blockchain)

สมมติว่า นาย ก ต้องการซื้อสินค้าจากนาย ข หลังจากทราบว่านาย ข ได้ประกาศขายสินค้าดังกล่าวบนเว็บไซต์แห่งหนึ่ง ปัญหาและความท้าทายอย่างแรกที่นาย ก ประสบ คือ นาย ก จะรู้ได้อย่างไรว่านาย ข มีตัวตนจริงหรือไม่ และจะมีวิธีการยืนยันตัวตนได้อย่างไร นอกจากนั้น นาย ก ยังต้องแน่ใจด้วยว่าเว็บไซต์ดังกล่าวมีระบบปกป้องข้อมูลส่วนบุคคลและข้อมูลทางการเงินของตนที่รัดกุมหรือไม่ ซึ่งเทคโนโลยีที่ใช้ในการป้องกันการโจรกรรมข้อมูลในปัจจุบัน ไม่ว่าจะเป็นการตั้งรหัสลับส่วนตัว (password) การใช้เครื่องมือทางคอมพิวเตอร์เพื่อแยกระหว่างผู้ใช้อินเทอร์เน็ตที่เป็นหุ่นยนต์กับมนุษย์ (CAPTCHA) หรือการยืนยันตัวตนสองขั้นตอน (two-step verification) ยังไม่มีความสมบูรณ์ ข้อมูลต่าง ๆ จึงเสี่ยงต่อการถูกโจรกรรมโดยแฮ็กเกอร์ (hackers) ได้โดยง่าย ด้วยเหตุนี้เอง จึงมีการคิดค้นเครื่องมือใหม่เพื่อพัฒนาระบบปกป้องข้อมูลที่มีความทันสมัยและก้าวทันอาชญากรไซเบอร์ (cyber criminals) เครื่องมือดังกล่าว คือ ระบบการจัดการข้อมูลในเครือข่ายด้วยบล็อกเชน



รูปที่สอง: เปรียบเทียบระบบการชำระเงินในปัจจุบันกับระบบกระจายศูนย์ของเงินดิจิทัลสกุลบิทคอยน์

ระบบจัดการข้อมูลด้วยบล็อกเชนทำงานอย่างไร

การทำความเข้าใจระบบการเงินดิจิทัลควรเริ่มจากการทำความเข้าใจระบบการจัดการข้อมูลด้วยบล็อกเชนเป็นอันดับแรก ที่ผ่านมา วิทยาการด้านคอมพิวเตอร์ใช้ระบบจัดการข้อมูลแบบรวมศูนย์ (centralised system) กล่าวคือ มีศูนย์กลางในการจัดเก็บข้อมูลทั้งหมดในเครือข่าย (repository) เพียงแห่งเดียว หรือที่เรียกกันจนติดปากว่า เซิร์ฟเวอร์ (server) โดยมีหน่วยงานหรือเจ้าหน้าที่ผู้มีอำนาจรับผิดชอบในการบริหารจัดการข้อมูลดังกล่าว ซึ่งรวมไปถึงการเข้าถึงข้อมูล การแก้ไขและเปลี่ยนแปลงข้อมูล ตลอดจนการกำหนดรูปแบบและวิธีการจัดเก็บข้อมูล (ทั้งหมดนี้จะปรากฏอยู่ในข้อตกลงผู้ใช้ - user agreement/terms of use) ระบบรวมศูนย์ดังกล่าวนี้เองเป็นพื้นฐานของโลกยุคอินเทอร์เน็ตมาโดยตลอด ส่วนหนึ่งเป็นเพราะการรวมศูนย์ช่วยให้การบริหารจัดการข้อมูลเป็นไปอย่างรวดเร็วและสามารถเปลี่ยนแปลงได้อย่างเท่าทันความต้องการของเจ้าของข้อมูล อย่างไรก็ตาม การรวมศูนย์ในลักษณะนี้มีข้อเสีย กล่าวคือ นอกจากระบบรวมศูนย์จะใช้ทรัพยากรจำนวนมากในการดูแลรักษาและดำเนินการแล้ว ในขณะเดียวกันก็กลายเป็นการรวมศูนย์ความเสี่ยงต่าง ๆ (centralisation of risks)

ซึ่งเป็นภัยต่อความปลอดภัยของข้อมูลด้วยเช่นกัน ผลคือ เมื่อมีการโจรกรรมข้อมูลเกิดขึ้น อาชญากรจะสามารถเข้าถึงข้อมูลทั้งหมดได้ทันที ตัวอย่างของการโจรกรรมข้อมูลจากระบบศูนย์กลางที่พบเห็นได้บ่อยที่สุดก็คงหนีไม่พ้นการโจรกรรมข้อมูลบัตรเครดิต หรือข้อมูลทางการเงินอื่น ๆ จากระบบศูนย์ข้อมูลของธนาคารพาณิชย์หรือเว็บไซต์ของบริษัทห้างร้านที่มีการทำการพาณิชย์ออนไลน์ ซึ่งนอกจากปัญหาด้านความปลอดภัยของข้อมูลแล้ว ระบบรวมศูนย์ในปัจจุบันยังใช้ทรัพยากรในการดูแลรักษาและดำเนินการเป็นอย่างมากอีกด้วย

อนึ่ง ระบบการจัดการข้อมูลด้วยบล็อกเชนเป็นการเปลี่ยนแนวความคิดดั้งเดิมไปอย่างสิ้นเชิง บล็อกเชนเปลี่ยนจากการรวมศูนย์เป็นการกระจายข้อมูลไปสู่คอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับระบบเครือข่าย การจัดเก็บข้อมูลชิ้นใหม่จะต้องได้รับความยินยอมจากคอมพิวเตอร์ทุกเครื่องที่เชื่อมโยงอยู่กับระบบ โดยเป็นไปตามกฎของระบบเครือข่ายที่ได้ตั้งค่าไว้ตั้งแต่แรก หากลองเปรียบเทียบ ชุดข้อมูลก็เปรียบเสมือนตัวต่อเลโก้ชิ้นเล็ก ๆ หลายชิ้นต่อกัน การเพิ่มเติมหรือแก้ไขข้อมูลใด ๆ ในแต่ละครั้งเปรียบเสมือนการต่อตัวต่อเลโก้ที่มีรูปร่างและขนาดเหมือนกันทุกประการอีกหนึ่งตัวเพิ่มเข้าไปในฐานข้อมูลของคอมพิวเตอร์ทุกเครื่องที่เชื่อมโยงอยู่กับระบบเครือข่าย โดยจะต้องเกิดขึ้นพร้อม ๆ กันทั้งหมดทุกเครื่อง เมื่อมีการเพิ่มเติมข้อมูลมากขึ้นเรื่อย ๆ ระบบข้อมูลก็จะมีลักษณะเป็นห่วงโซ่ของตัวต่อ จึงเป็นที่มาของชื่อ “Blockchain” ทั้งนี้ ข้อดีของบล็อกเชนก็คือ ระบบสามารถดำเนินการไปได้โดยไม่ต้องใช้เซิร์ฟเวอร์กลางในการดูแลรักษา ซึ่งสามารถประหยัดค่าใช้จ่ายได้อย่างมีนัยสำคัญ

ความไม่สามารถเปลี่ยนแปลงได้ (Immutability)

ความไม่สามารถเปลี่ยนแปลงได้ เป็นคุณสมบัติที่สำคัญที่สุดของบล็อกเชน ที่ทำให้ข้อมูลมีความปลอดภัยจากการถูกโจรกรรมมากกว่า เมื่อเทียบกับระบบการจัดเก็บข้อมูลแบบรวมศูนย์ กล่าวคือ ความสมบูรณ์และถูกต้องของฐานข้อมูลขึ้นอยู่กับความเหมือนกันของตัวต่อข้อมูลทุกชิ้นที่ได้ถูกจัดเก็บไว้แล้วก่อนหน้านี้ในคอมพิวเตอร์ทุกเครื่องที่เชื่อมโยงกันในระบบเครือข่าย ดังนั้น ความพยายามในการเปลี่ยนแปลงหรือแก้ไขข้อมูลใด ๆ จึงกระทำได้ยากมากและง่ายต่อการตรวจเจอ หากต้องการแก้ไขข้อมูล ต้องกระทำโดยการเพิ่มเติมข้อมูลใหม่ (เปรียบได้กับการวางตัวต่อเลโก้ชิ้นใหม่) ทบเข้าไปอีกในคอมพิวเตอร์ทุกเครื่องที่เชื่อมโยงกันในระบบเครือข่ายเท่านั้น ด้วยเหตุนี้เอง จึงมีการนำระบบจัดการข้อมูลด้วยบล็อกเชนไปเปรียบเทียบกับการลงบัญชีในสมุดบัญชี ต่างกันเพียงว่า คอมพิวเตอร์ทุกเครื่องในระบบของบล็อกเชน (ซึ่งทำหน้าที่เสมือนนักบัญชี) จะถือสมุดบัญชีเล่มเดียวกัน หากจะต้องมีการเพิ่มเติมข้อมูลใหม่ ก็จะต้องบันทึกข้อมูลลงในสมุดบัญชีเล่มเดียวกันไปพร้อม ๆ กัน หรือเรียกว่า สมุดบัญชีกระจายส่วน (distributed ledger)

รูปที่สาม: การทำงานของคุณสมบัติ Blockchain immutability โดยตัวต่อข้อมูลตัวใหม่ต้องมีการอ้างถึงข้อมูลในตัวต่อตัวก่อนหน้าเสมอเพื่อเป็นการยืนยันความถูกต้อง นอกจากนั้น ก็เพื่อเป็นการป้องกันไม่ให้มีการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตได้โดยง่าย ทั้งนี้ก็เพราะการเปลี่ยนแปลงข้อมูลเพียงหนึ่งชุดข้อมูลต้องกระทำกับตัวต่อข้อมูลทั้งหมดในสายห่วงโซ่ข้อมูลนั้น

ที่มา: เว็บไซต์ Bits on Blocks

เมื่อไม่มีผู้ควบคุมศูนย์ข้อมูลกลาง (central gatekeeper) และเมื่อการจัดเก็บข้อมูลเพิ่มเติมจะต้องได้รับการยอมรับจากคอมพิวเตอร์ในระบบทุกเครื่องตามกฎของระบบที่ได้ตั้งค่าไว้ตั้งแต่ต้นแล้ว บล็อกเชนจึงก่อให้เกิดความเชื่อมั่นในความปลอดภัยของระบบข้อมูล (trust protocol) ด้วยเหตุผลดังต่อไปนี้ ประการแรก ระบบไม่อนุญาตให้มีการแก้ไขข้อมูลที่ได้ถูกบันทึกและจัดเก็บไว้แล้วในระบบก่อนหน้านี้ไม่ว่ากรณีใด ๆ ทั้งสิ้น ประการที่สอง การเพิ่มเติมชุดหรือตัวต่อข้อมูลใหม่ต้องได้รับความยินยอมจากคอมพิวเตอร์ทุกเครื่องที่เชื่อมโยงเข้ากับระบบเครือข่ายเท่านั้น ซึ่งอาจมีจำนวนหลักพันหรือหมื่น ขึ้นอยู่กับขนาดของระบบนั้น หากแฮ็กเกอร์ต้องการใส่ข้อมูลใหม่ (เช่น คำสั่งให้โอนเงินจากบัญชีของบริษัทเข้าบัญชีส่วนตัวของตน) ก็จะต้องบันทึกข้อมูลดังกล่าวไว้ในคอมพิวเตอร์ทุกเครื่องที่เชื่อมโยงกับระบบเครือข่าย และจะต้องทำพร้อมกันทุกเครื่อง ซึ่งยากกว่าการโจรกรรมข้อมูลจากศูนย์กลางข้อมูลหรือเซิร์ฟเวอร์มาก

หลังจากที่ได้ทำความเข้าใจกับหลักการเบื้องต้นของการจัดเก็บข้อมูลด้วยบล็อกเชนแล้ว ในคราวต่อไปกองพัฒนากฎหมายขอนำเสนอวิธีการนำเทคโนโลยีนี้ไปใช้ในระบบการเงินดิจิทัล รวมถึงความแตกต่างของเงินดิจิทัลสกุลต่าง ๆ ที่กำลังได้รับความนิยมจากทั้งนักลงทุนและธุรกิจการพาณิชย์สมัยใหม่ในขณะนี้