DVP (ชำระราคาและส่งมอบหลักทรัพย์)

* สำนักหักบัญชีเป็นคนกลางดูแลจัดการกระบวนการส่งมอบ-รับมอบเงิน ค่าซื้อ ค่าขาย ให้กับสมาชิกในฐานะตัวแทนของนักลงทุนผู้ซื้อผู้ขาย
* การส่งมอบและรับมอบหลักทรัพย์อันเกิดจากการตกลงซื้อขายในตลาดหลักทรัพย์ สมาชิกสำนักหักบัญชีตกลงให้ TSD โอน-รับโอนหลักทรัพย์ผ่านบัญชีด้วยวิธีการโอนทางบัญชี (Book Entry)
* ลดความเสี่ยงต่อระบบการชำระราคาและส่งมอบหลักทรัพย์ของสำนักหักบัญชีในฐานะที่เป็นผู้ประกันการชำระราคาและส่งมอบหลักทรัพย์
* ผู้เก็บรักษาทรัพย์สิน (Custodian) โบรกเกอร์ ธนาคารพาณิชย์และ สำนักหักบัญชี
* มีผู้เกี่ยวข้องหลายฝ่าย
* ตรวจสอบความถูกต้องทั้งในแง่ของการตรวจสอบรายการซื้อขาย
* ระยะยาวผู้ลงทุนก็จะเสียโอกาสในการนำเงินที่ได้จากการขายหุ้นไปลงทุนต่อยอด
* **Corporate Actions**
  + Information is manually extracted from the original, interpreted and re-keyed by vendors. Levels of automation are low, errors frequent, and the process highly inefficient

BlockChain

* **รูปแบบการเก็บข้อมูล (Database) แบบหนึ่งของระบบที่ไม่มีศูนย์กลางแต่เชื่อถือได้และโกงยาก**
* เป็นรูปแบบการเก็บข้อมูล (Data structure) แบบหนึ่ง ที่ทำให้ข้อมูล Digital transaction ของแต่ละคนสามารถแชร์ไปยังทุกๆ คนได้ เป็นเสมือนห่วงโซ่ (Chain) ที่ทำให้ block ของข้อมูลลิ้งก์ต่อไปยังทุกๆ คนเป็น โดยที่ทราบว่าใครที่เป็นเจ้าของและมีสิทธิในข้อมูลนั้นจริงๆ
* **Corporate Actions**
  + Block chain technology could make this process more efficient.
  + Corporate actions represent contractual information and value, which can in principle be transferred directly between payers and payees without the need for intermediaries
  + provided the parties can trust the source data and have the necessary experience to act upon the information they receive.

Blockchain ข้อจำกัด

## สิทธิในการแก้ไขข้อมูล สิทธิควรเป็นแบบเปิดกว้างหรือไม่?

## ถ้าคุณไม่ได้ต้องการให้คน/องค์กรจำนวนมากมีสิทธิแก้ไขฐานข้อมูล คุณก็ไม่จำเป็นต้องใช้ Blockchain คุณเชื่อใจคนที่มีสิทธิได้แค่ไหน? ถ้าคุณเชื่อใจ หรือมีเหตุให้ต้องเชื่อคนในระบบอยู่แล้ว คุณก็ไม่ต้องใช้ Blockchain ก็ได้ — เช่น ถ้าของที่เก็บไม่ได้มีผลประโยชน์มาเกี่ยวข้องที่จะเป็นแรงจูงใจให้คนอยากโกงระบบ เป็นต้น

ledger permanence is another key feature of blockchain ecosystems, which explicitly use cryptography to ensure that distributed records are tamper-proof. This is an essential feature of decentralised networks and one which clashes with several existing environments, including the European Union’s General Data Protection Regulation. The right to be forgotten and the right to rectification are key elements of the GDPR which conflict with the immutability of a DLT system.

1. ความรับผิดชอบต่อสิ่งที่อยู่ใน Blockchain  
   เราควรยกเลิกฐานข้อมูลตามธนาคารต่าง ๆ แล้วเปลี่ยนให้ระบบบัญชีธนาคารทั้งประเทศเก็บใน Public Blockchain หรือไม่?   
   ถ้าถามตอนนี้ ผมคนหนึ่งละที่ไม่เอา — Blockchain ยังใหม่เกินไป ช่องโหว่และปัญหาที่รอให้อุดยังมีอีกมาก อีกเหตุผลหนึ่งคือ ระบบ Blockchain อยู่บนพื้นฐานของการโหวตแบบประชาธิปไตย

การเปลี่ยนแปลงที่ล่าช้า

ระบบประชาธิปไตยทำให้การแก้ไขปัญหาบางแบบล่าช้ามาก เพราะต้องรอการโหวต ต่างกับระบบ Database แบบเดิมที่รับผิดชอบโดยองค์กรใดองค์กรหนึ่ง ที่พร้อมตัดสินใจเองได้เลย

## ประชาธิปไตยที่ไม่มีการรับรองสิทธิ

ทุกวันนี้ ธนาคารแต่ละธนาคารรับผิดชอบฐานข้อมูลตัวเอง และรับผิดชอบต่อเราถ้ามีข้อผิดพลาดเกิดขึ้น อีกทั้งยังมีกฎหมายประกันเงินฝากมาคุ้มครอง   
ตอนนี้ ถ้าเราเปลี่ยนมาใช้ Blockchain แล้วเกิดข้อผิดพลาดขึ้น ใครละที่จะรับผิดชอบ?  
ในระบอบประชาธิปไตย แม้เสียงส่วนใหญ่จะกำหนดทิศทาง แต่ก็ไม่อาจละเมิดสิทธิของเสียงส่วนน้อยได้  
แต่ไม่ใช่ในระบบ Blockchain —**สมมติ**เล่น ๆ ว่าเราเปลี่ยนมาเก็บฐานข้อมูลโฉนดที่ดินด้วยระบบ Blockchain แล้วมีองค์กรหนึ่งสามารถครองคอมพิวเตอร์ได้เกินครึ่งหนึ่ง — คอมพิวเตอร์กลุ่มนี้สามารถเปลี่ยนให้คุณกลายเป็นคนไร้บ้านได้ทันที  
คุณอาจจะบอกว่า ถ้าคน crack ฐานข้อมูลกรมที่ดินก็ได้ผลเหมือนกัน และทางทฤษฎีแล้ว Blockchain ปลอดภัยกว่า  
ถ้าฐานข้อมูลกรมที่ดินโดน Crack — กรมที่ดินจะรับผิดชอบ  
กรมที่ดินอาจมีความวุ่นวายเรื่องการกู้คืนฐานข้อมูล แต่สิทธิของคุณจะไม่หายไป  
แต่ถ้าคุณปล่อยให้คนจำนวนมากกำหนดชะตาชีวิตของคุณ คุณจะทวงถามความรับผิดชอบนี้จากใคร?  
คนรับผิดชอบจำนวนมาก = ไม่มีคนรับผิดชอบ

**Consumer protection measures**If, therefore, blockchain technology and, more specifically, smart contracts (which is an increasingly common feature of use cases looking at the technology) are likely to become ubiquitous on a B2C basis, it would not be surprising if legislatures were similarly to act to implement or extend specific consumer protection measures in relation to them.

In addition, in many jurisdictions the regulatory or licensing requirements specific to the banking industry, prescribe contractual provisions that must be included in consumer contracts. It may be difficult for banks to demonstrate that an encoded smart contract includes such information, and encoding such information may not satisfy applicable transparency obligations.

Moreover, banks will need to consider whether operating a smart contracting form could, in and of itself, prevent a consumer from being able to exercise consumer rights.

Accordingly it will be necessary for banks to take appropriate legal advice on a jurisdiction-by-jurisdiction basis before deploying blockchain technology and smart contracts.

### **Prevention of crime**

It remains unclear how anti-money laundering and know-your-customer regulatory obligations (ภาระผูกพัน) may be credibly performed in the context of a pseudonymized (นามแฝง) blockchain transaction, where the ability to identify the other participants can be obscured (บดบัง). Regulatory advice on a jurisdiction-by-jurisdiction (อำนาจศาล) basis will be required to ascertain:

* whether private blockchains (within closed communities of identified counterparties) might deliver sufficient information to enable a regulated bank or financial institution to discharge its anti-money laundering and know-your-customer obligations; and
* how such obligations could be performed in the context of blockchain solutions and smart contracting more generally.

Compliance with anti-bribery and corruption legislation generally requires a business to have an understanding of (and an ability to control) its supply chain participants. That may be impossible if the counterparty is not identifiable. Legal advice will be necessary to determine whether private blockchains within closed communities of identified counterparties might enable a bank to assert control over, and have sufficient transparency in respect of, its supply chain. explores the supervision of financial markets if they evolve into DLT-based markets which may not have trusted intermediaries or central counterparties.

Ensuring finality or that transactions cannot be reversed is an essential requirement to have trust in the ledgers. Currently, that trust is often enabled by central counterparties. These institutions may be superceded by trustworthy blockchains that offer finality. This, in turn, presents a challenge in that the requirement for counterparties is enshrined in many local regulations. That would need to change.