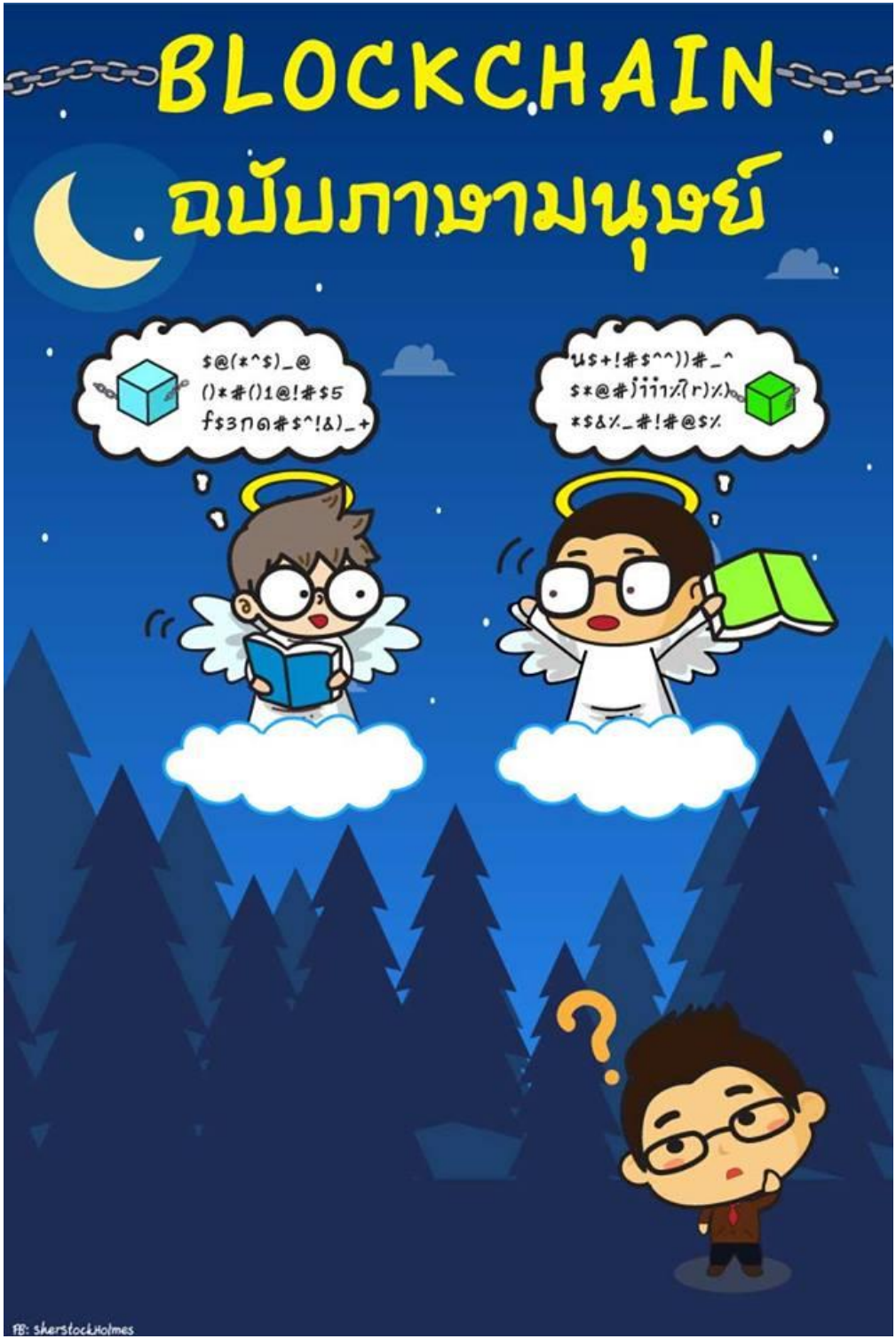
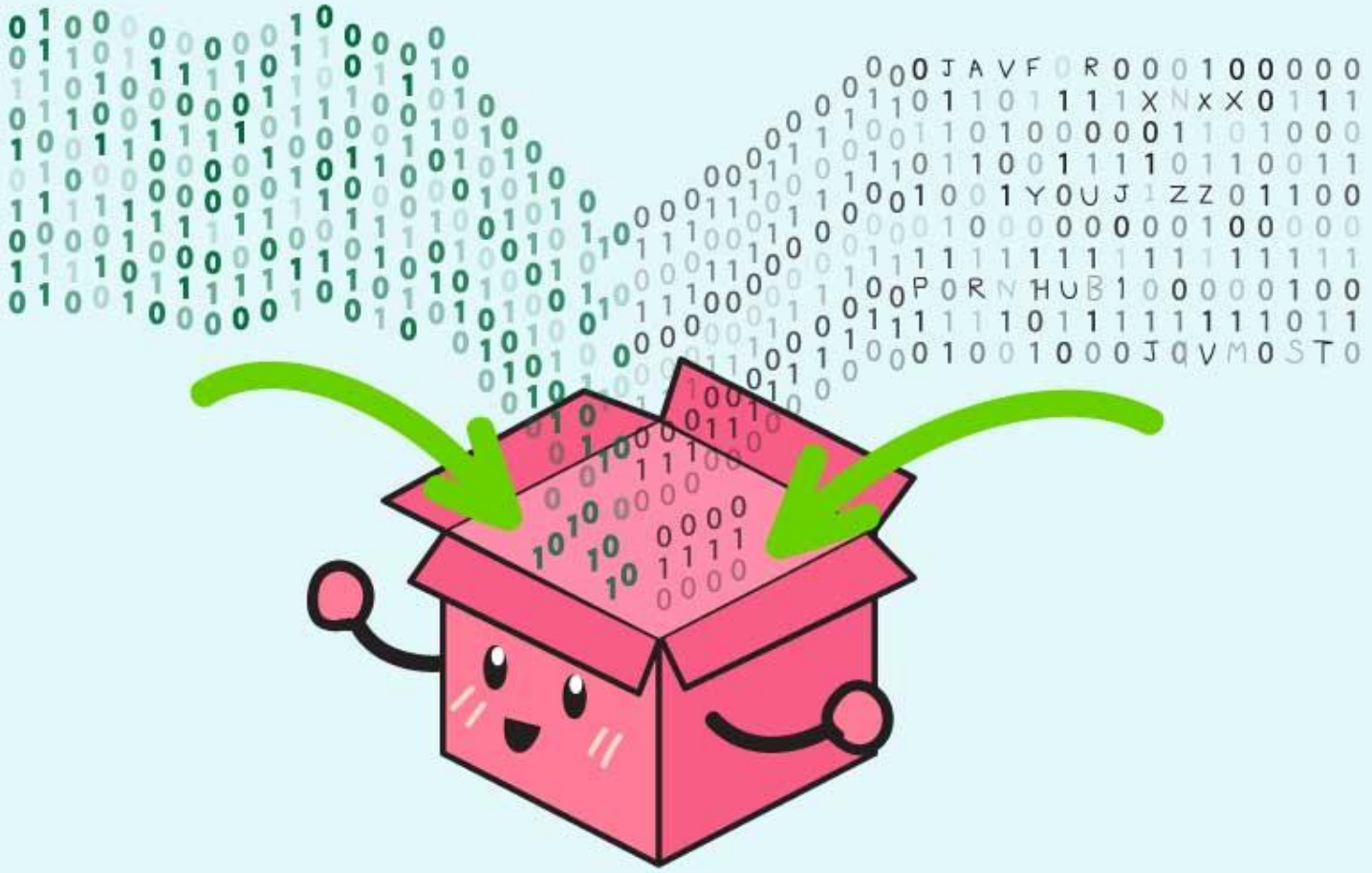

BLOCKCHAIN
ฉบับภาษามนุษย์
$@(*^$)_@
()*#()1@!#$5
f$3ก๑#$^!&)_+
u$+!#$^^))#_^
$*@#)ๅๅๅา%(r)%)
*$&%_#!#@$%
FB: sherstockHolmes

Blockchain คืออะไร?

ความหมายง่ายๆก็คือ การเก็บข้อมูลรูปแบบหนึ่งที่ไม่ต้องมีตัวกลาง แต่เชื่อถือได้ และโกงได้ยาก(มาก)



FB: sherstockHolmes

ก่อนอื่นต้องอธิบายก่อนครับว่า **Blockchain ไม่ใช่ Bitcoin**

Blockchain คือ ระบบ ส่วน **Bitcoin คือ ผลิตภัณฑ์ที่ใช้งานบนระบบนั้น**

เปรียบง่ายๆ

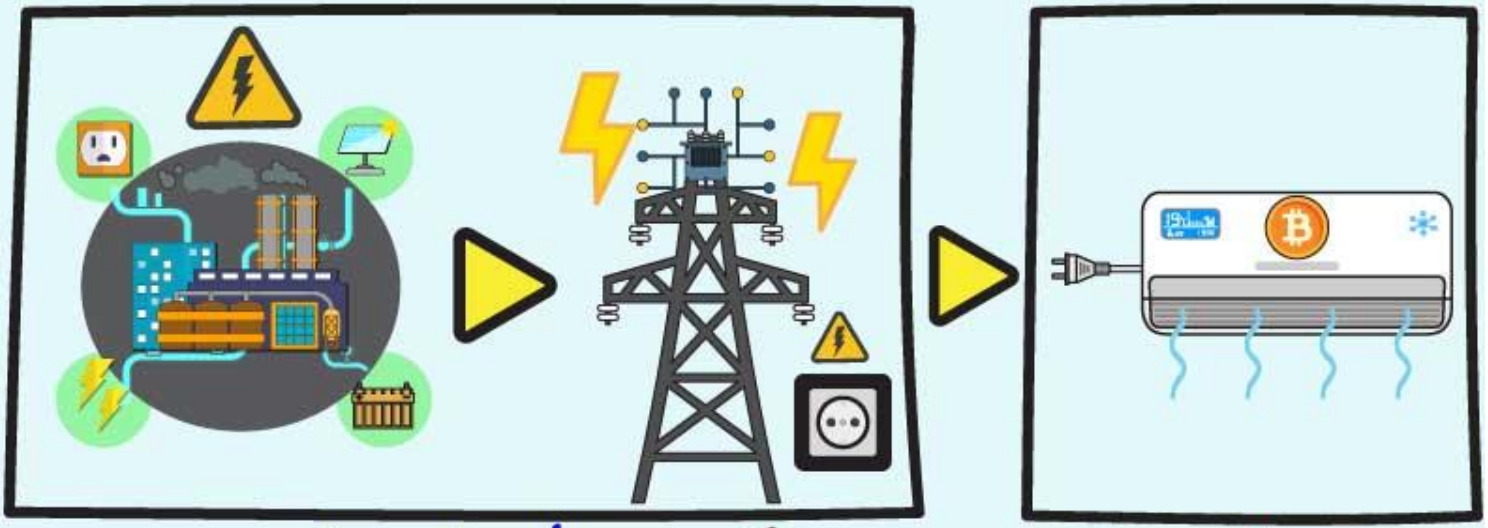
Blockchain คือ ระบบไฟฟ้า โรงไฟฟ้า สายไฟ เต้าเสียบ ฯลฯ

Bitcoin ก็คือ เครื่องใช้ไฟฟ้าชนิดหนึ่ง สมมติว่าเป็น แอร์

เงินดิจิตัลตัวอื่นๆก็อาจจะเป็นแอร์ยี่ห้ออื่น

เพราะฉะนั้นในอนาคตอาจจะมีเครื่องใช้ไฟฟ้าอื่นๆ

ที่มาใช้ระบบ Blockchain ได้อีกมากมายเต็มไปหมดนั่นเอง

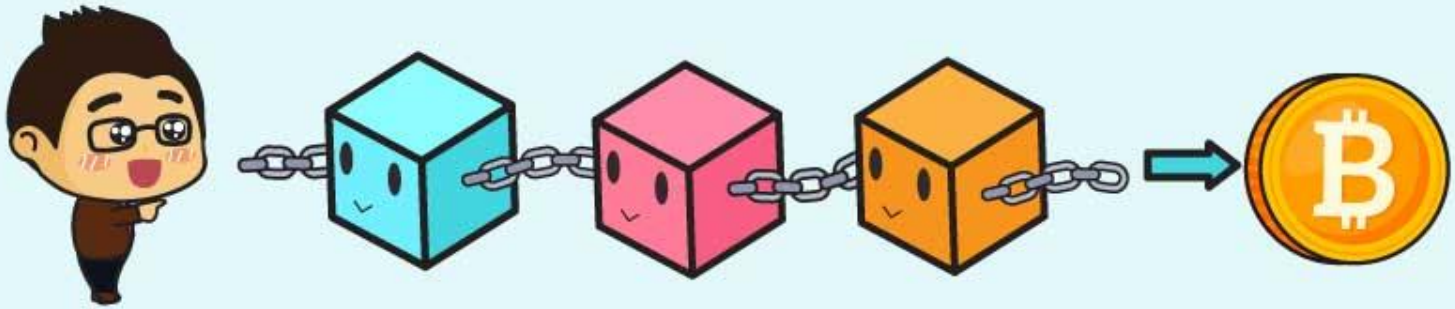


Blockchain

Bitcoin

FB: sherstockHolmes

และเพื่อให้เข้าใจกันได้ง่ายๆ วันนี้ผมจะขอยกตัวอย่างเป็นเรื่องของการเงิน
และ Bitcoin ในการอธิบายละกันนะครับ



ในปัจจุบันนี้ถ้าเราจะโอนเงินให้ใครซักคนเราต้องทำยังไงครับ?
ธุรกรรมการเงินในสมัยปัจจุบันเราใช้ระบบที่เรียกว่า
ระบบแบบมีศูนย์กลาง

FB: sherstockHolmes

ตัวอย่างเช่น

ถ้า นาย งง จะโอนเงินให้ นาย หาย

นาย งง สามารถทำรายการโอนให้ นาย หาย

โดยตรงเลยได้มั้ยครับ?

คำตอบคือ "ไม่ได้" ครับ

นาย งง ต้องทำรายการผ่านตัวกลางก็คือ ธนาคาร ชิบ

แล้วให้ ธนาคาร ชิบ ตรวจสอบข้อมูล

แล้วจึงโอนให้ นาย หาย อีกทอดนึง

รูปแบบธุรกรรมจะเป็นแบบนี้ครับ งง >> ชิบ >> หาย

นั่นล่ะครับ งงชิบหาย...

FB: sherstockHolmes

ในปัจจุบันข้อมูลทุกอย่างของระบบจะอยู่ที่ “ศูนย์กลาง”

ซึ่งระบบแบบนี้มีข้อเสียหลักๆอยู่ 3 ข้อด้วยกันครับ

1. มีต้นทุนสูง

2. เราต้อง
ไว้ใจตัวกลางมากๆ

3. การโจมตีข้อมูล
ทำได้ง่าย

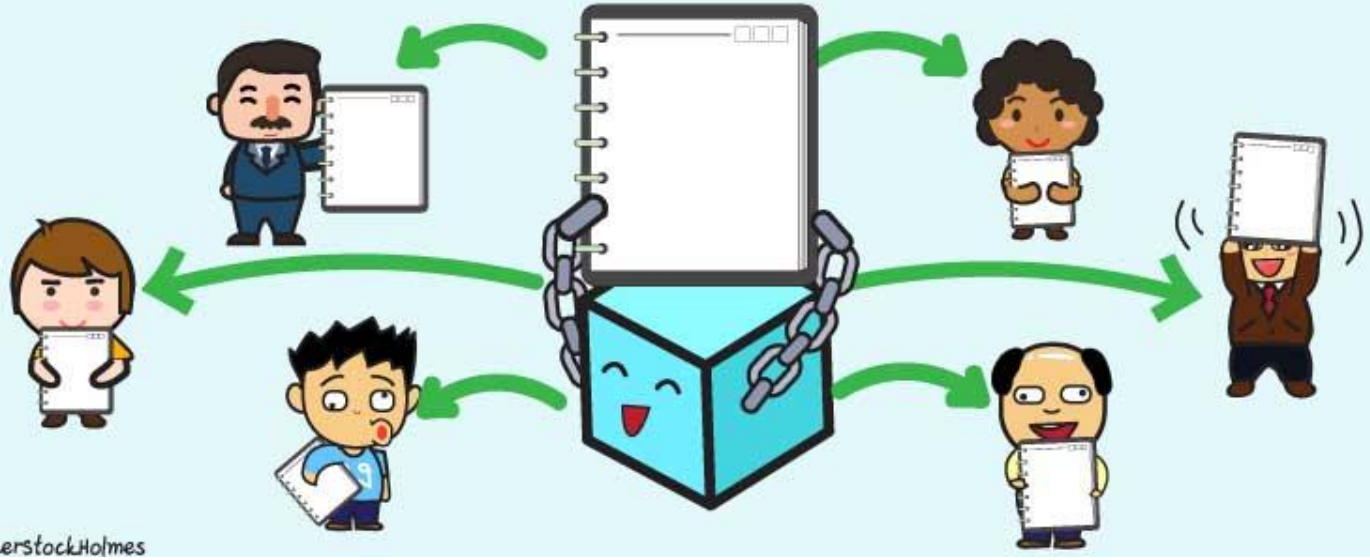
ซึ่งระบบ Blockchain สามารถมาแก้ปัญหาเหล่านี้ได้นั่นเอง

FB: sherstockHolmes

แล้ว Blockchain มันทำงานยังไง?

เปรียบง่ายๆก็คือ แทนที่ “สมุดข้อมูล” ของทุกคนจะไปรวมไว้ที่ “ศูนย์กลาง”

ก็เอา “สมุดข้อมูล” นั้น แจกให้ “ทุกคน” ไปเลย (โอ้ว ฉลาดจุง)

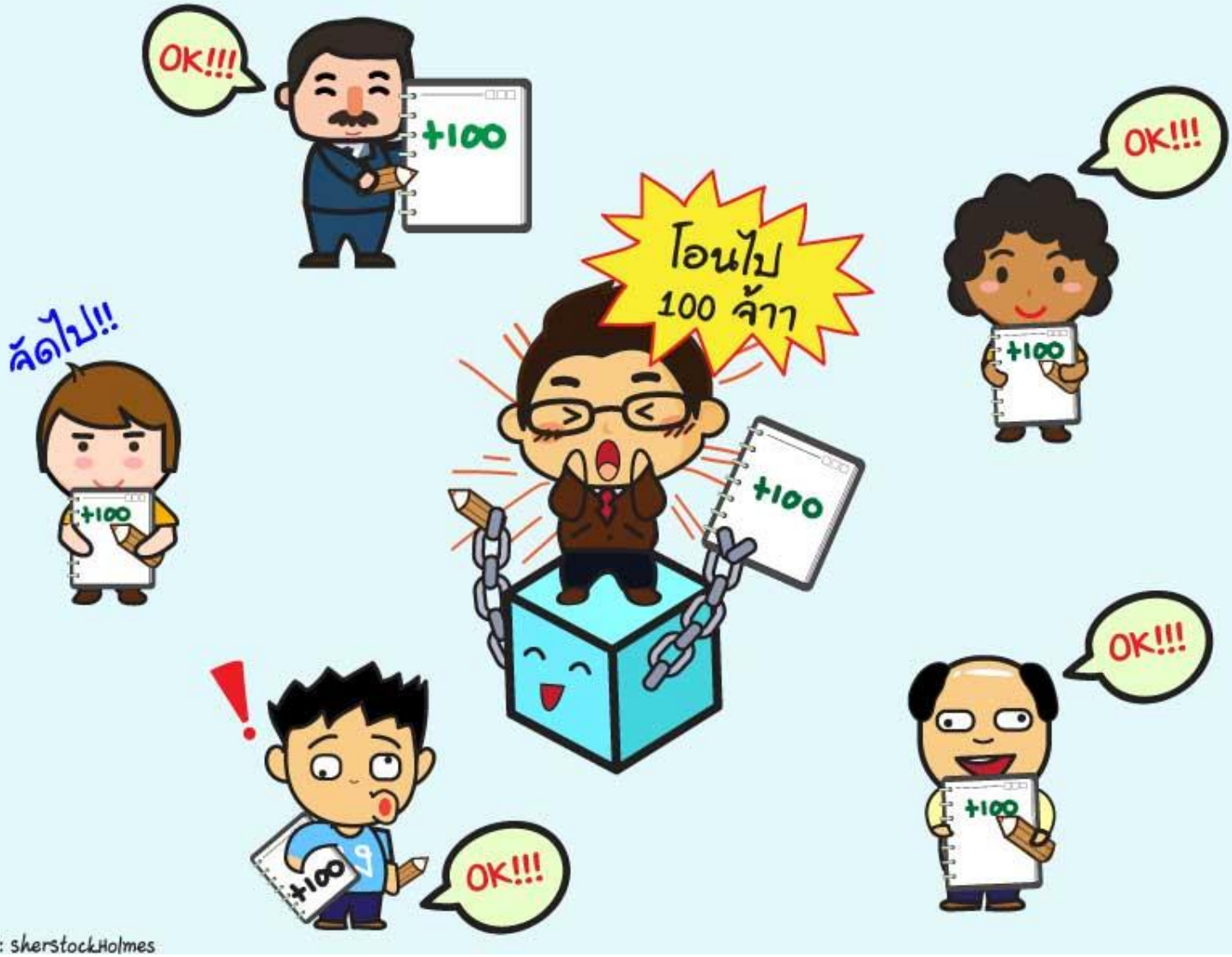


FB: sherstockHolmes

เวลามีการโอนเงิน เราก็ไปยืนกลางวง

แล้วป่าวประกาศบอกทุกคนว่า “ฉันโอนเงินให้นายเอ 100 บาทนะ”

ทุกคนก็ “จดบันทึก” ในสมุดตัวเองให้ “เหมือนกันหมด”



FB: sherstockHolmes

อ้าวแล้วถ้าเราโกงอะ
แอบจดว่าตัวเองมีเงินเยอะขึ้นได้มะ?

ไม่ได้ครับ เพราะ “สมุดข้อมูล” ของเราจะไม่เหมือนคนอื่นไง
คนอื่นก็จะรู้ว่าเรากำลังโกง

FB: sherstockHolmes

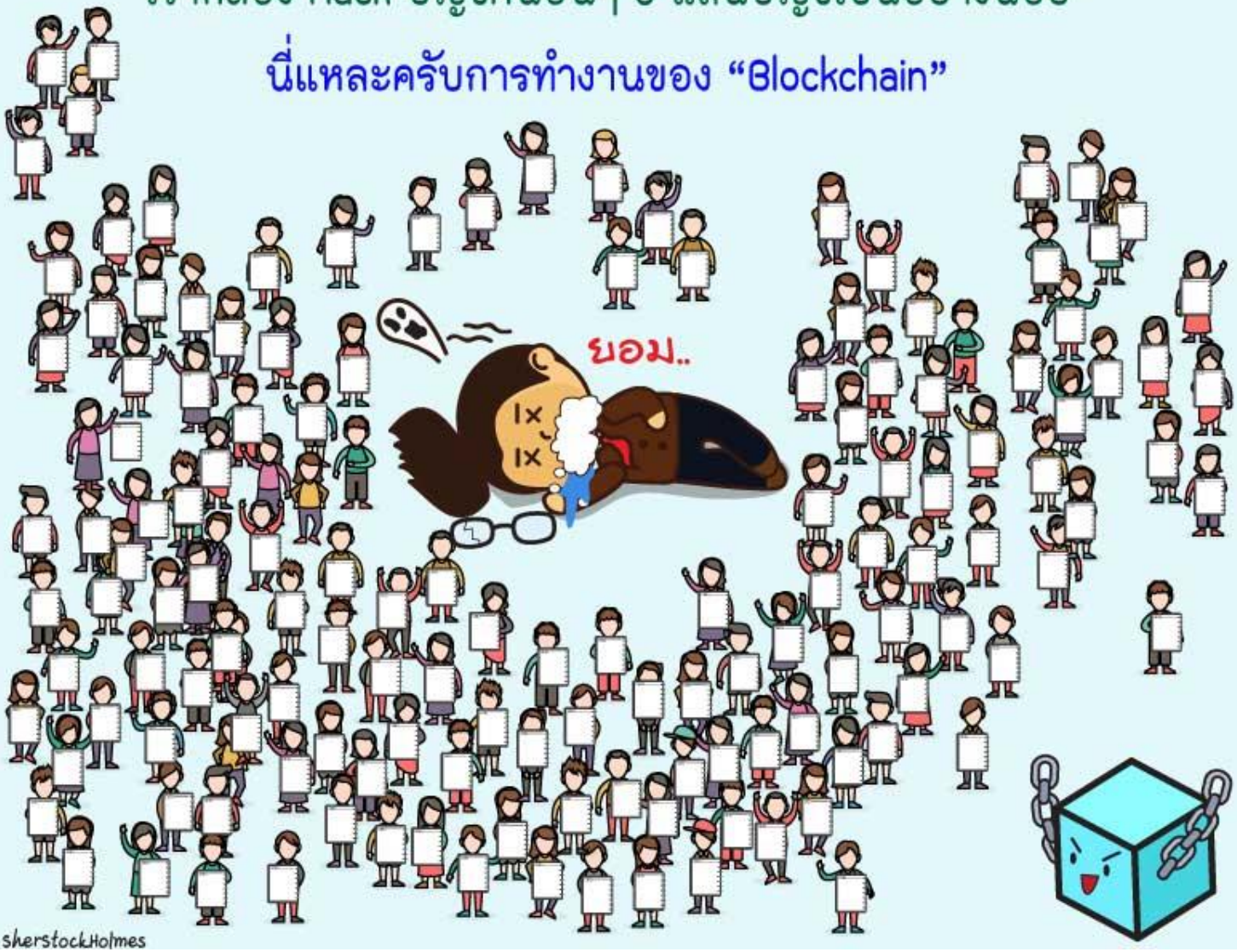
เพราะฉะนั้น ถ้าเราจะโกง

เราต้องไปแอบเปลี่ยนข้อมูลใน สมุดข้อมูล ของ “คนอื่นๆ”

ให้เกิน 50% ถ้ามีคนอยู่ในระบบนี้ 1 ล้านคน

เราก็ต้อง Hack บัญชีคนอื่นๆ 5 แสนบัญชีเป็นอย่างน้อย

นี่แหละครับการทำงานของ “Blockchain”



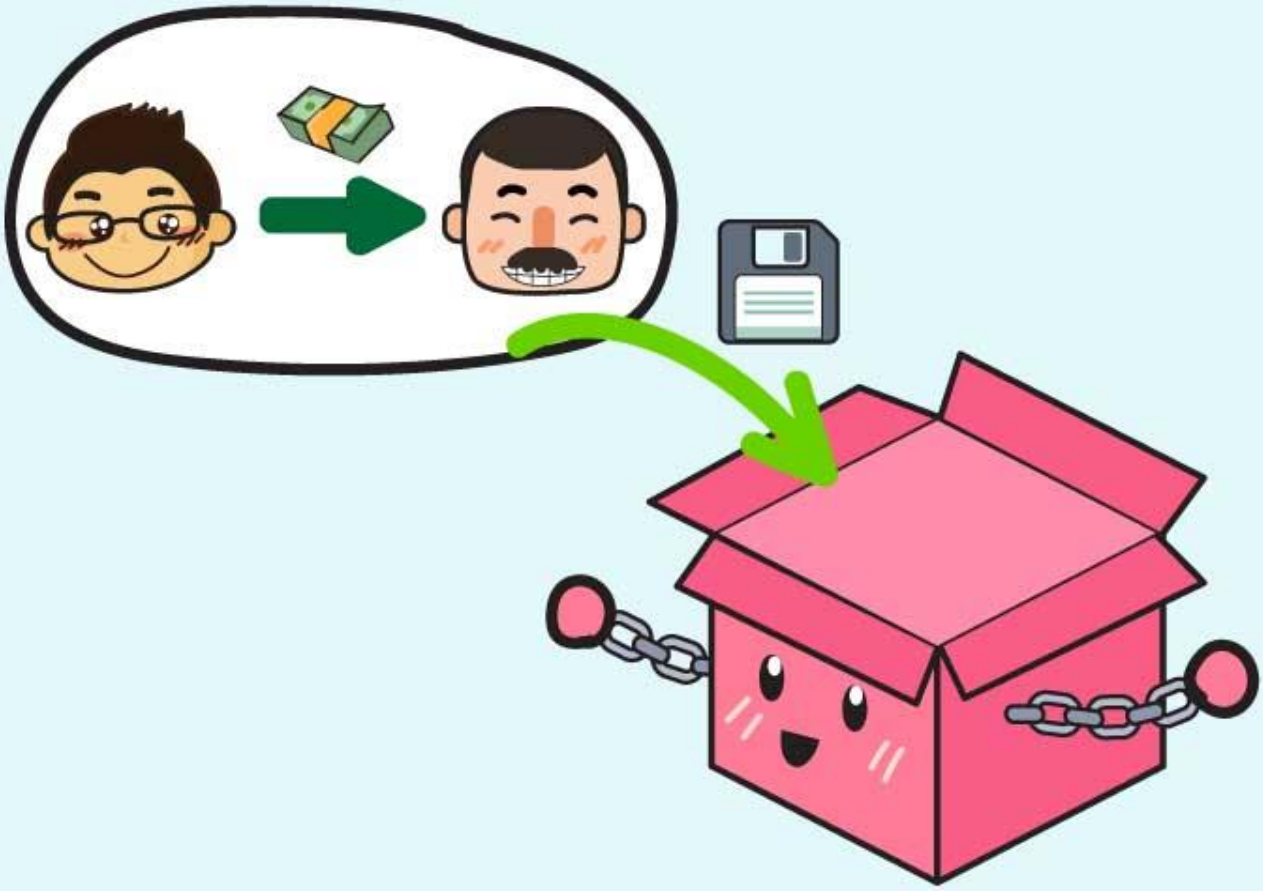
FB: sherstockHolmes

แล้วทำไมถึงต้องเรียกว่า Blockchain ด้วย?

คืองี้ครับ การทำงานของมันเนี่ย เมื่อทุกคนมีบัญชีแล้ว

และเกิด Transaction หรือมีการโอนเงิน มีการเปลี่ยนแปลงข้อมูล

ระบบจะทำการบันทึกข้อมูลนั้นเก็บไว้เหมือนกับเป็น Block



FB: sherstockHolmes

แล้วใน Block นี้มันมีอะไรบ้าง?

Block เหล่านี้จะประกอบไปด้วย 3 ส่วนด้วยกัน

1. ข้อมูล (Data) ซึ่งจะเป็นอะไรก็ได้

แต่ยกตัวอย่างในส่วนของ Bitcoin ก็จะเป็นแบบนี้ครับ

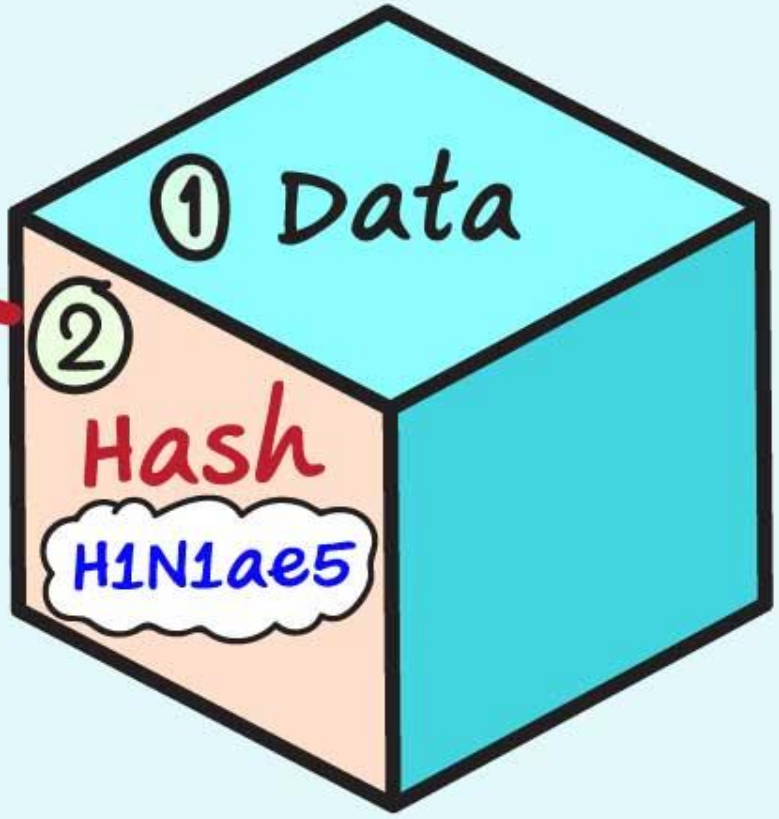
แล้วใน Block นี้มันมีอะไรบ้าง?

Block เหล่านี้จะประกอบไปด้วย 3 ส่วนด้วยกัน

2. รหัสข้อมูล (Hash) มันเหมือนรหัสลับประจำกล่องอะครับ

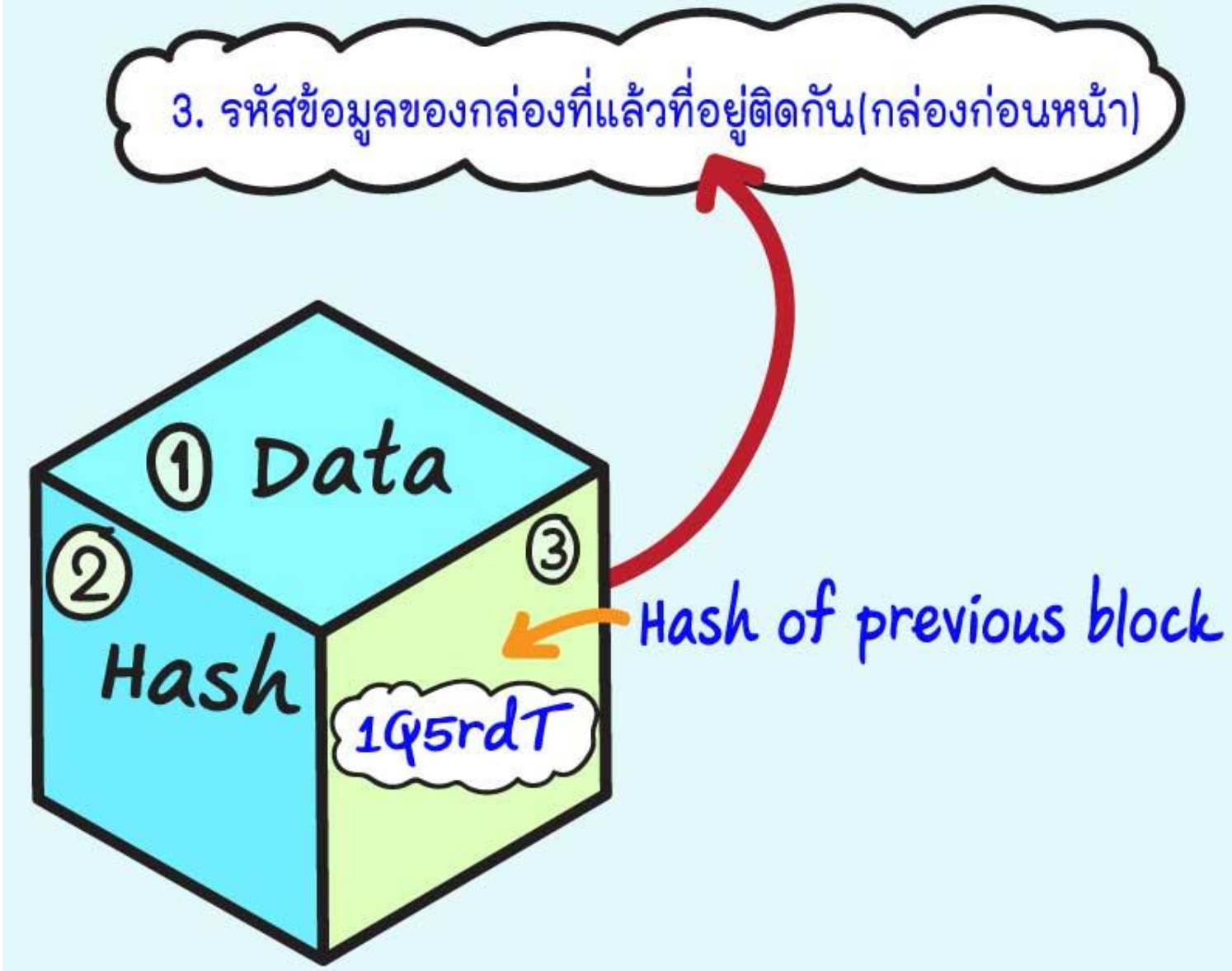
"แต่ละกล่องจะไม่มีทางซ้ำกันเลย"

ถ้าข้อมูลข้างในถูกเปลี่ยน Hash ก็จะเปลี่ยนทันที



แล้วใน Block นี้มันมีอะไรบ้าง?

Block เหล่านี้จะประกอบไปด้วย 3 ส่วนด้วยกัน



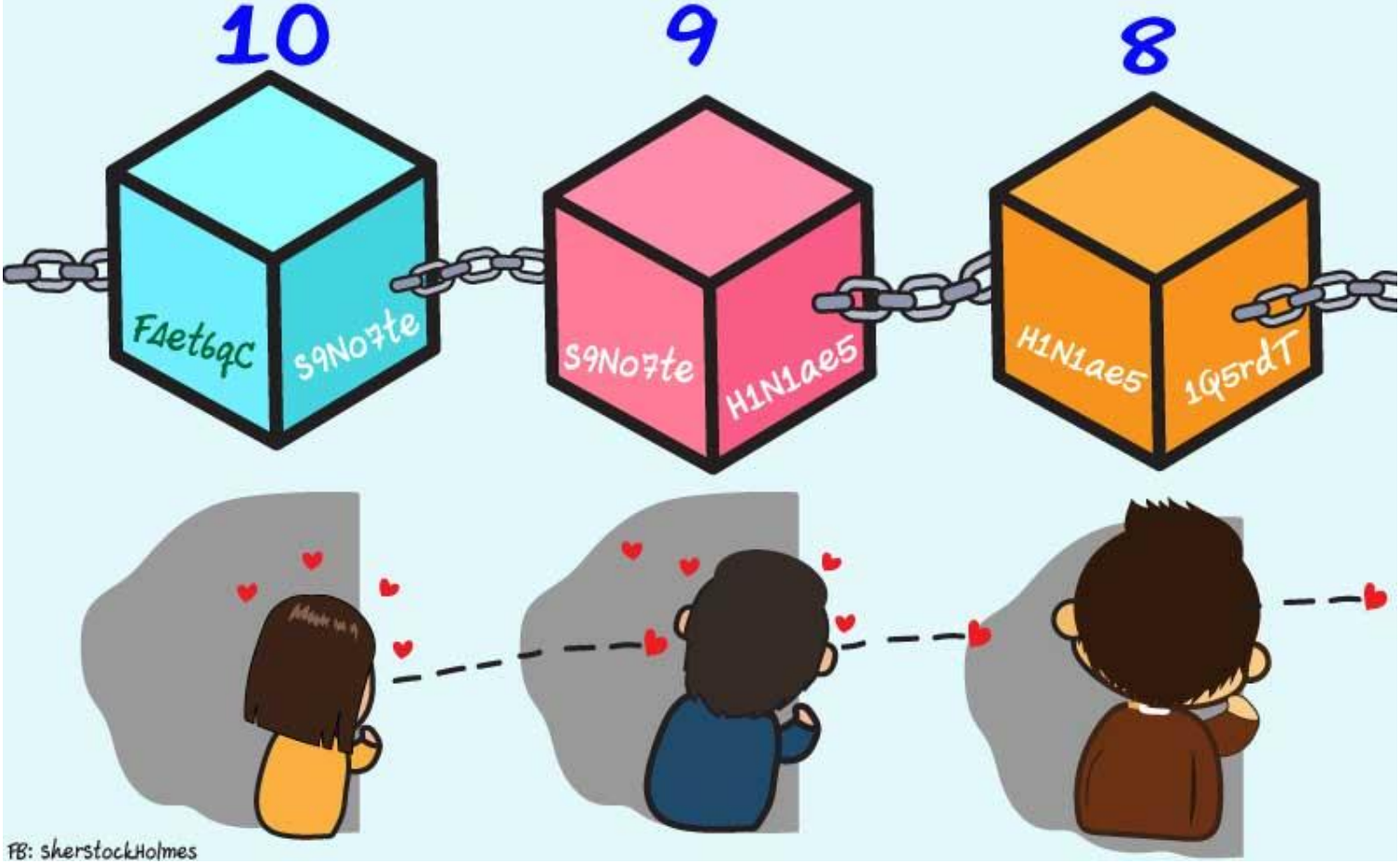
หน้าตาก็เป็นแบบนี้ครับ

กล่องที่ 10 ก็จะมีรหัสของกล่องที่ 9 แปะอยู่ด้วย

กล่องที่ 9 ก็จะมีรหัสของกล่องที่ 8 แปะอยู่ด้วย

อารมณ์แบบ...แอบมองเธออยู่นะแจ๊ะ แต่มุงไม่สนใจตูเลย

เหมือนความรักอันซับซ้อน ยากแท้จะหยั่งถึง



FB: sherstockHolmes

ระบบแบบนี้จะทำให้ปลอดภัยเพิ่มอีกขั้นหนึ่ง

ถ้ามีคนพยายามจะแก้ข้อมูลในกล่องใดกล่องหนึ่ง

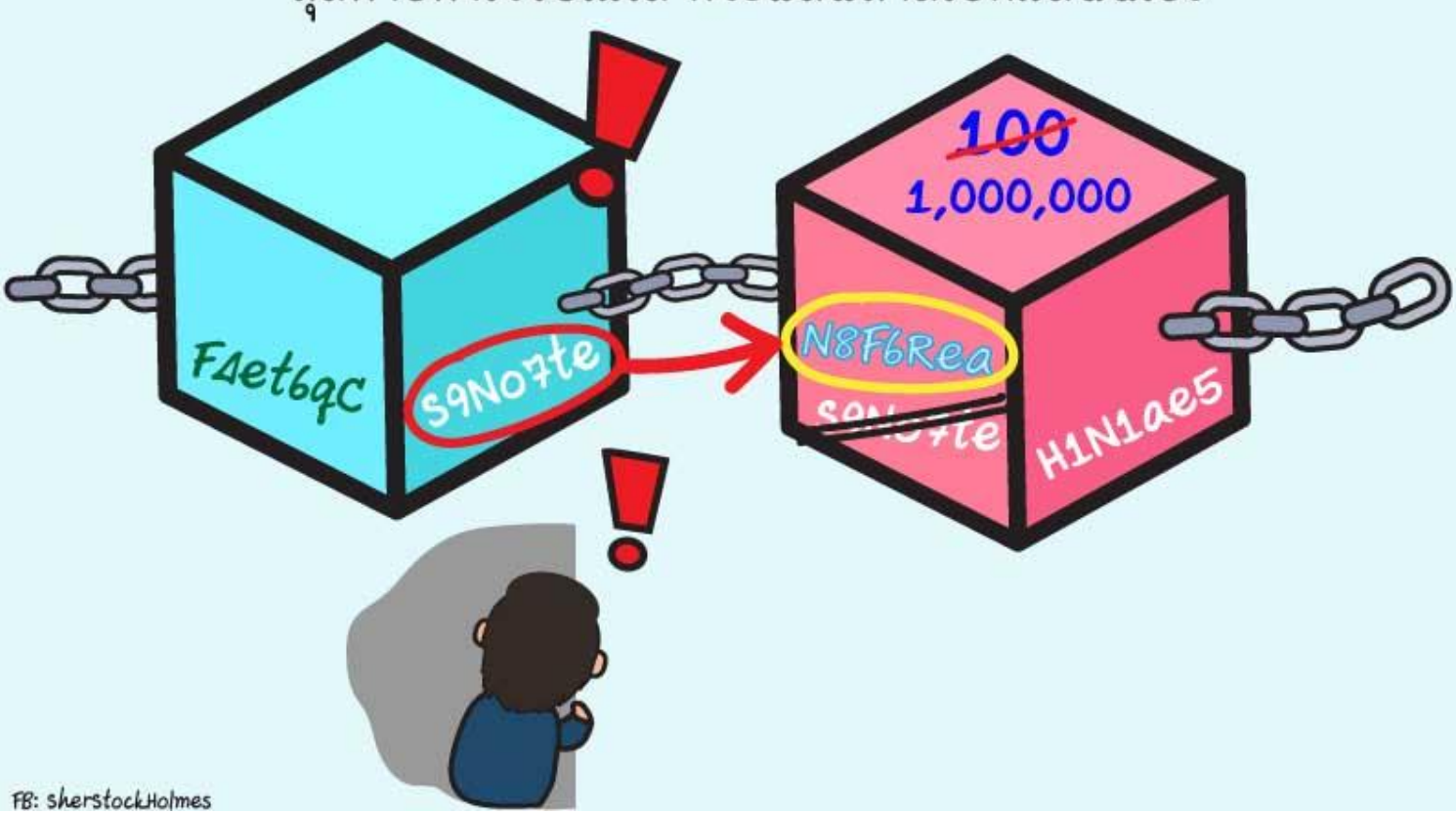
(แก้ไข Transaction) เช่นมีคนโอนมา 100 แต่ไปแก้ไขว่า โอนมา 1 ล้าน

Hash ของกล่องก็จะเปลี่ยนทันที

พอ Hash เปลี่ยน ไอ่กล่องหลังจากนั้นที่แอบมองอยู่

ก็จะตกใจ ทำไมเธอเปลี่ยนไป

สุดท้ายทำใจรับไม่ได้ ก็จะผิดพลาดไปหมดนั่นเอง



FB: sherstockHolmes

ยังไม่จบแค่นั้นครับ(ทำไมมันเยอะจังฟะ)

ถึงระบบจะป้องกันอย่างดีแล้ว

ถ้าจะ Hack ต้องแก้ทุกกล่องในระบบ Blockchain

และต้องแก้ “สมุดข้อมูล” ของคนในระบบมากกว่าครึ่ง

แต่ก็ยังอาจจะ Hack ได้นะเออ

เพราะคอมพิวเตอร์สมัยนี้ประมวลผลเร็วมาก

ระบบจึงต้องป้องกันอีกชั้น เราเรียกกันว่า “Proof of work”

FB: sherstockHolmes

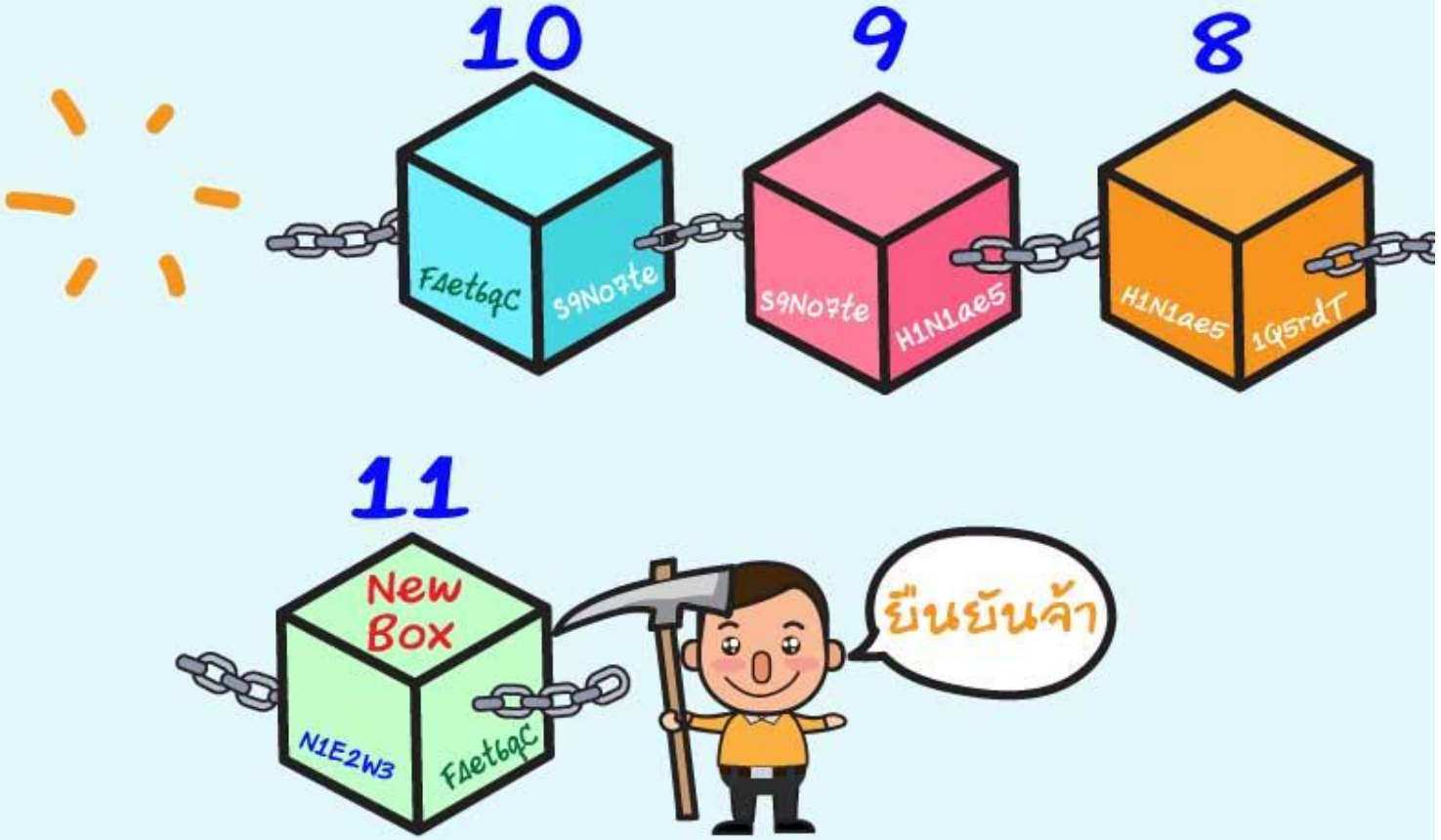
การแก้ไข Transaction มันใช้คอมพิวเตอร์ทำได้เร็ว

เพราะงั้นต้อง “ถ่วงเวลา” มันซะ

โดยบังคับให้ทุก “การแก้ไข” และ “การเพิ่มกล่อง” ใหม่ๆ

ต้องมีคนมา “ยืนยัน” ซะก่อนครับ

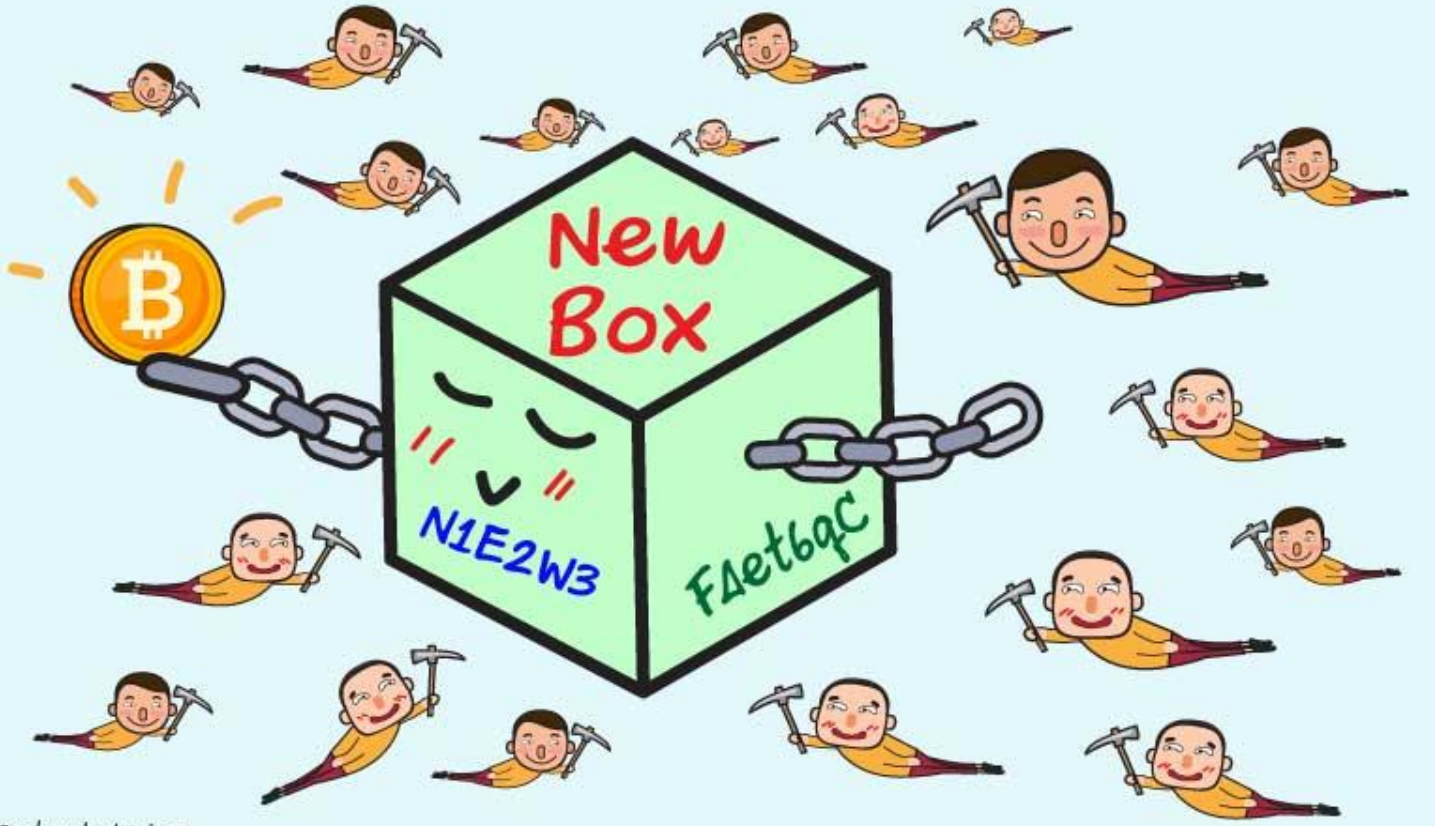
ซึ่งบุคคลเหล่านั้นเราเรียกกันว่า “นักขุดเหมือง(Miner)” นั่นเอง



FB: sherstockHolmes

วิธีการยืนยันทำยังไง? ระบบจะสร้างโจทย์ขึ้นมาครับ
และเครื่องคอมพิวเตอร์ที่ประมวลผล จะต้องใช้เวลาหาคำตอบราวๆ 10 นาที
(ไม่อธิบายละกันเนอะ เดี๋ยวยาวไป)

ซึ่ง Miner ทั่วโลกจะ "แย่งกันยืนยัน" ใครยืนยันได้ก่อน
ก็จะได้ "รางวัล" เป็นเหรียญ Bitcoin นั่นเอง



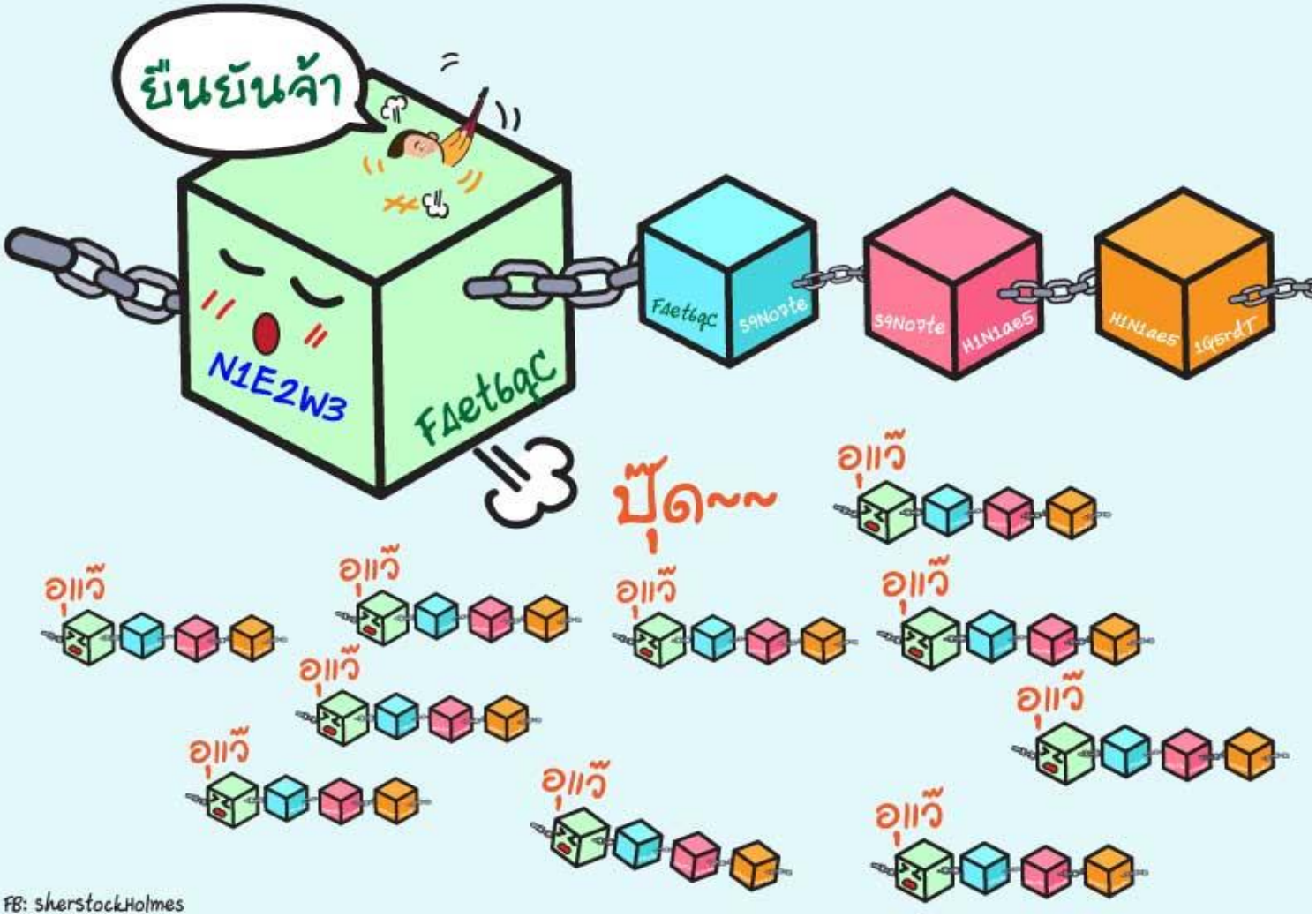
FB: sherstockHolmes

หลังจาก Block นั้นถูกปฏิสนธิ เอ้ย!!! ยืนยันเสร็จแล้ว

จึงจะถูกส่งลูกหลาน ... ไม่ใช่ๆ

ส่ง “สำเนา” ไปให้ทุกคนในระบบ

และเอาไปต่อกับกล่องที่อยู่ก่อนหน้านั้น เรียงต่อกันยาวไปไม่จบสิ้น



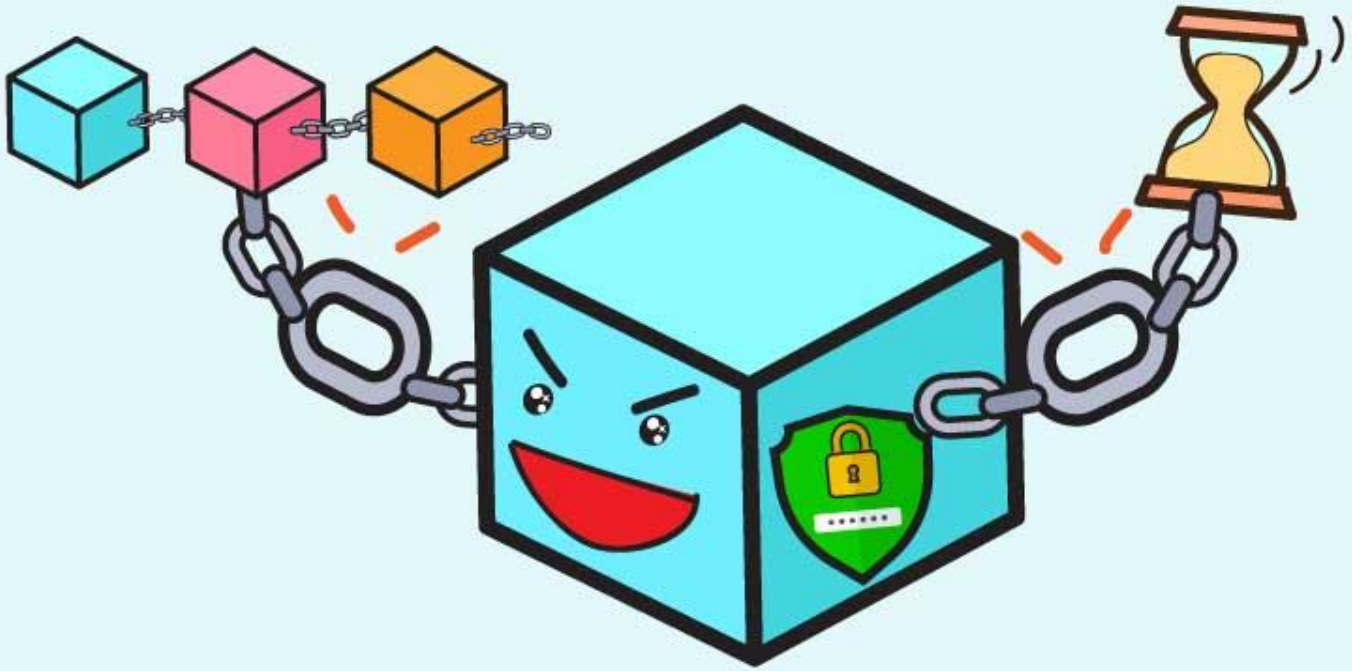
FB: sherstockHolmes

สรุปจึงกลายเป็นว่า ถ้าจะ Hack ระบบ Blockchainได้

เราต้องเปลี่ยนแปลงข้อมูลของทุกกล่อง และของคนมากกว่าครึ่ง

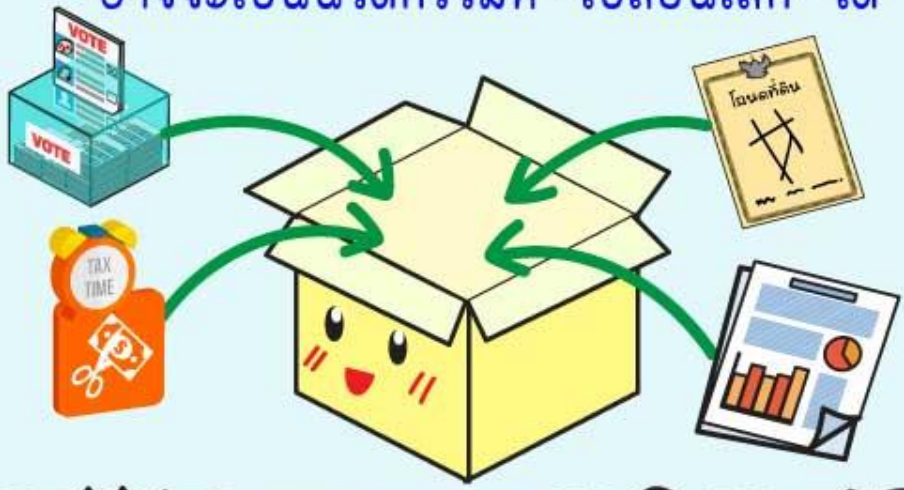
ในขณะที่จะเปลี่ยน 1 กล่อง ต้องใช้เวลา 10 นาที

ระบบนี้จึงเรียกได้ว่า “โคตรจะปลอดภัย” นั่นเองครับ



FB: sherstockHolmes

ระบบ Blockchain สามารถนำไปปรับใช้ได้อีกมากมายเลยครับ
ไม่ใช่แค่เรื่องของการเงิน ในอนาคต เราอาจจะเห็นระบบของ Blockchain
ถูกใช้ในการค้าขายในธุรกิจ และอุตสาหกรรมต่างๆมากมาย
หรือแม้แต่ในการเลือกตั้ง เรียกได้ว่า “Blockchain”
อาจจะเป็นนวัตกรรมที่ “เปลี่ยนโลก” ได้



แต่หนังสือ “วัดมูลค่าหุ้น เล่มนี้ง่ายฝุดๆ”
อาจจะ “เปลี่ยนฐานะ” เราได้เลยน๊า

FB: sherstockHolmes