



กระบวนการทำธุรกรรมทางการเงินด้วยเทคโนโลยีบล็อกเชนและการสร้างสกุลเงินดิจิทัล
FINANCIAL TRANSACTION PROCESS WITH BLOCKCHAIN TECHNOLOGY
AND CREATE CRYPTOCURRENCY WITH ETHEREUM

มณฑิรา กำจร¹ และ ดร.บำรุง พวงเกิด²

¹ สาขาวิศวกรรมการเงิน คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยหอการค้าไทย, Montira.k@outlook.co.th

² ภาควิชาวิศวกรรมเครื่องกล คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, bomroomg.pu@kmitl.ac.th

บทคัดย่อ

ในปัจจุบันการทำธุรกรรมทางการเงินได้พัฒนามาจนถึงในยุคที่เทคโนโลยีมีการเติบโตอย่างรวดเร็ว โดยทั่วไปการทำธุรกรรมในด้านการเงินระหว่างบุคคลหรือองค์กรยังไม่มีประสิทธิภาพเท่าที่ควร แต่สามารถแก้ไขปัญหาเหล่านี้ได้ด้วยเทคโนโลยีรูปแบบใหม่ที่เรียกว่าสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีและถูกนำมาใช้ในการทำธุรกรรมทางการเงิน ซึ่งเชื่อว่าสกุลเงินดิจิทัลเป็นรูปแบบของการทำธุรกรรมที่มีประสิทธิภาพ แต่เนื่องจากว่าสกุลเงินดิจิทัลไม่ถือว่าเป็นเงินตรา เป็นแค่หน่วยข้อมูลอิเล็กทรอนิกส์เท่านั้น ทำให้สกุลเงินดิจิทัลยังไม่เป็นที่ยอมรับของนานาประเทศทั่วโลก ดังนั้นเพื่อทดสอบว่าเทคโนโลยีใหม่นี้มาช่วยให้การทำธุรกรรมมีความปลอดภัยและโปร่งใสมากยิ่งขึ้น จึงได้มีการศึกษากระบวนการทำงานของบล็อกเชนและวิธีการสร้างสกุลเงินดิจิทัล โดยมีองค์ประกอบที่สำคัญได้แก่ 1) การกระจายบัญชีแบบไม่มีศูนย์กลางและการกระจายตัวของบัญชี ซึ่งหมายความว่าแต่ละคนต่างถือบัญชีของตัวเองและไม่มีใครเป็นศูนย์กลางหรือเข้ามาควบคุม 2) รายการเดินบัญชีสาธารณะในบล็อกเชนถูกออกแบบให้รายการทั้งหมดของทุกบัญชีต้องเปิดเผยสู่สาธารณะ 3) วิทยาการเข้ารหัสลับทั้งกุญแจสาธารณะและกุญแจส่วนตัว

จากการศึกษาแสดงให้เห็นว่าการนำเทคโนโลยีบล็อกเชนมาใช้ในการทำธุรกรรมทางการเงินทำให้ไม่สามารถควบคุมได้เนื่องจากไม่มีคนกลางเข้ามาเกี่ยวข้อง มีการตรวจสอบในการทำธุรกรรมได้รวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้บล็อกเชนยังสามารถนำไปใช้ในด้านอื่นๆที่นอกเหนือจากด้านการเงินได้ ตัวอย่างเช่น อุตสาหกรรมอาหาร การขนส่ง การแพทย์ การเดินทาง ซึ่งขั้นตอนการศึกษาและเทคนิคในการสร้างถูกนำเสนอในรายละเอียด
คำสำคัญ: สกุลเงินดิจิทัล, บล็อกเชน, การทำธุรกรรมทางการเงิน, เทคโนโลยีทางการเงิน

ABSTRACT

At the present, financial transactions have evolved to the times when technology is growing rapidly. In general, financial transactions between individuals or organizations are inefficient. But these problems can be solved with a new type of technology called Cryptocurrency used in financial transactions. It is believed cryptocurrency is a form of efficient transaction. Because cryptocurrency is not considered currency. It's just an electronic data unit. Cryptocurrency is not accepted by many countries around the world. To test whether this innovative technology is helping to make transactions more secure and transparent. Object of this research is the study of blockchain process and how to create cryptocurrency. The key elements are: 1) Decentralization 2) Distributed Ledger 3) Cryptography.



The study shows that the use of blockchain technology in financial transactions cannot be controlled because it is decentralization. Fast and efficient transaction detection. Blockchain can also be used in other areas besides finance. For example, the food industry, transportation, medicine and travel. The stages of the study and the techniques of creation are presented in detail.

Keywords: cryptocurrency, blockchain, financial transactions

1. บทนำ

การทำธุรกรรมเป็นกิจกรรมทางการเงินรูปแบบหนึ่งที่สำคัญ ซึ่งปัจจุบันได้พัฒนามาจนถึงในยุคที่เทคโนโลยีมีการเติบโตอย่างรวดเร็ว ตั้งแต่ในอดีตกาลที่การทำธุรกรรมนั้นยังเป็นแค่การแลกเปลี่ยนสิ่งของซึ่งกันและกัน ต่อมาได้พัฒนามาเป็นการนำโลหะต่างๆมาเป็นสื่อกลางในการแลกเปลี่ยน จนถึงในปัจจุบันที่สื่อกลางนั้นคือเหรียญกษาปณ์และธนบัตร นอกจากนี้รูปแบบการทำธุรกรรมได้พัฒนาให้อยู่ในรูปของดิจิทัลอีกด้วย แต่เนื่องจากว่าการทำธุรกรรมดังกล่าวที่ผ่านมายังมีปัญหาและข้อผิดพลาดอีกมากมาย จึงทำให้การทำธุรกรรมในปัจจุบันนั้นยังไม่มีประสิทธิภาพเท่าที่ควร และเมื่อไม่กี่ปีที่ผ่านมานวัตกรรมเทคโนโลยีทางการเงินรูปแบบใหม่เกิดขึ้น นั่นคือ สกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซี ซึ่งเชื่อว่าสกุลเงินดิจิทัลเป็นรูปแบบของการทำธุรกรรมที่มีประสิทธิภาพ แต่เนื่องจากว่าสกุลเงินดิจิทัลไม่ถือว่าเป็นเงินตรา เป็นแค่หน่วยข้อมูลอิเล็กทรอนิกส์เท่านั้น ทำให้สกุลเงินดิจิทัลยังไม่เป็นที่ยอมรับของนานาประเทศทั่วโลก

ในปัจจุบันสกุลเงินดิจิทัลได้รับความสนใจอย่างมากทั้งในประเทศและต่างประเทศทั่วโลก ทำให้หลายคนอยากทราบว่าสกุลเงินดิจิทัลคืออะไร มีความหมายอย่างไร และทำไมประเทศอื่นๆต้องตื่นตัวกันอย่างมาก แม้ความต้องการสกุลเงินดิจิทัลจะเพิ่มขึ้นอย่างรวดเร็ว แต่ยังคงเผชิญกับความท้าทายอีกหลายอย่าง ทั้งความผันผวนของอัตราแลกเปลี่ยนและมุมมองของหน่วยงานกำกับดูแลของแต่ละประเทศ ทำให้โอกาสที่คนทั่วไปจะนำมาใช้ในวงกว้างอาจไม่มากนัก อย่างไรก็ตาม แนวคิดของสกุลเงินดิจิทัลอย่างเทคโนโลยีบล็อกเชนที่เป็นรากฐานของบิตคอยน์นับว่ามีศักยภาพและสามารถนำไปประยุกต์ใช้กับองค์กรต่างๆเพื่อให้ขั้นตอนการทำงานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพสูงสุดของโลกของฟินเทคหรือเทคโนโลยีทางการเงิน ขณะนี้ดูเหมือนให้ผู้นำกับเทคโนโลยีบล็อกเชนเป็นเทคโนโลยีหลักที่สถาบันการเงินนำมาพัฒนาต่อยอดได้อย่างกว้างขวางไม่ใช่แค่การโอนเงินระหว่างประเทศเท่านั้น ซึ่งทั้งบรรดา Tech Startup หรือธนาคารต่างๆ ได้หันมาศึกษาและพัฒนาบล็อกเชนกันอย่างจริงจังเพื่อก้าวให้ทันกับเทคโนโลยีและพฤติกรรมของผู้บริโภคในยุคปัจจุบันที่นิยมซื้อ-ขายหรือทำธุรกรรมผ่านช่องทางออนไลน์กันมากขึ้น

ส่วนใหญ่แล้วสกุลเงินดิจิทัลถูกนำมาใช้ในการทำธุรกรรมทางการเงินภายในกลุ่มๆหนึ่ง ซึ่งโดยทั่วไปการทำธุรกรรมในด้านการเงินระหว่างบุคคลหรือองค์กรยังไม่มีความมีประสิทธิภาพเท่าที่ควร ดังนั้นเพื่อทดสอบว่าเทคโนโลยีใหม่นี้มาช่วยให้การทำธุรกรรมมีความปลอดภัยและโปร่งใสมากยิ่งขึ้น การค้นคว้าอิสระนี้เป็นการศึกษากระบวนการทำธุรกรรมทางการเงินด้วยบล็อกเชนและวิธีการสร้างสกุลเงินดิจิทัล

2. วัตถุประสงค์การวิจัย

การวิจัยนี้มีจุดประสงค์เพื่อศึกษาเทคโนโลยีทางการเงินรูปแบบใหม่ให้ทันยุคทันสมัยตามกาลเวลา ด้วยการศึกษาระบบการทำธุรกรรมทางการเงินด้วยบล็อกเชนของอีเทอริยมและวิธีการสร้างสกุลเงินดิจิทัลขึ้นมาใหม่



ด้วยภาษา Solidity (ภาษาของอีเธอเรียม) และมีความเข้าใจการทำงานของเทคโนโลยีบล็อกเชนและความเสี่ยงของสกุลเงินดิจิทัล นอกจากนี้สามารถบอกได้ว่าเทคโนโลยีบล็อกเชนมีประโยชน์ต่อด้านการเงินในการทำธุรกรรมได้อย่างไร

3. การดำเนินการวิจัย

3.1. ข้อมูลที่ต้องเตรียม

1. เริ่มต้นด้วยการติดตั้ง Geth version 1.7.3. (<https://geth.ethereum.org/downloads/>)

Geth 1.7.3	4bb3c89d...	Installer	32-bit	33 MB	11/21/2017	Signature	c76fe8ff5d56c9425dbbbc275c788e3e
Geth 1.7.3	4bb3c89d...	Archive	32-bit	9.39 MB	11/21/2017	Signature	5ed32e9d12d4d0594930f1bd5e7dd610
Geth 1.7.3	4bb3c89d...	Installer	64-bit	34.69 MB	11/21/2017	Signature	6500fa0ff2c2d217ff33f9e7c3611044
Geth 1.7.3	4bb3c89d...	Archive	64-bit	9.79 MB	11/21/2017	Signature	0023f50d01cf15f175004fc2023fb998

2. บล็อกกำเนิด (Genesis.json)

```
{
  "config": {
    "chainId": 100,
    "homesteadBlock": 0,
    "eip155Block": 0,
    "eip158Block": 0
  },
  "nonce": "0x0000000000000042",
  "mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "difficulty": "0x4000",
  "coinbase": "0x0000000000000000000000000000000000000000",
  "timestamp": "0x00",
  "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "gasLimit": "0xffffffff",
  "alloc": {}
}
```

3.2. วิธีการศึกษา

ตอนที่ 1 การทำธุรกรรม

ขั้นที่ 1 สร้างโหนดและเริ่มต้นใช้โหนดที่ 1

Input:

```
geth --datadir node1 init genesis.json
```

```
geth --networkid 100 --identity node1 --verbosity 3 --nodiscover
--nat none --datadir node1 --rpc --rpcapi "web3, eth, personal,
net" --rpccorsdomain "*" --rpcport 8545 --port 30303 --ipcpath
node1/geth.ipc console
```



ขั้นที่ 2 สร้างเลขบัญชี

Input:

```
>personal.newAccount ()
```

Output:

Passphrase:

Repeat passphrase:

Address: {0x8f16368e3d483caf25e45fcea3c8af432239c4d5}

การสร้างเลขบัญชีใหม่ต้องใส่รหัสผ่านและอย่าลืมรหัสผ่านนั้น สามารถมีได้มากกว่า 1 บัญชี ซึ่งบัญชีที่
สร้างครั้งแรกจะเป็น coinbase ของโหนด

ขั้นที่ 3 การตรวจสอบการทำธุรกรรมหรือการขุด

Input:

```
>miner.start (1)
```

Output:

Starting mining operation

INFO [05-20|16:13:05] Commit new mining work
number=1 txs=0 uncles=0 elapsed=1.000ms

INFO [05-20|16:13:08] Generating DAG in progress
epoch=0 percentage=0 elapsed=1.890s

ขั้นที่ 4 หยุดการตรวจสอบหรือการขุด

Input:

```
>miner.stop ()
```

Output:

```
true
```

ขั้นที่ 5 ตรวจสอบเลขบัญชี

Input:

```
>eth.accounts
```

Output:

```
["0x8f16368e3d483caf25e45fcea3c8af432239c4d5"]
```



ขั้นที่ 6 ตรวจสอบยอดคงเหลือของบัญชี

```
Input:  
>eth.getBalance (eth.coinbase)  
  
Output:  
6900000000000000000000  
  
จำนวนที่ได้หน่วยจะเป็น Wei ถ้าจะเปลี่ยนเป็นหน่วย Ether คือ หารด้วย 1018  
  
Input:  
>eth.getBalance ('0x8f16368e3d483caf25e45fcea3c8af432239c4d5')  
  
Output:  
6900000000000000000000
```

ขั้นที่ 7 ข้อมูลรหัส enode ของโหนดที่ 1

```
Input:  
admin.nodeInfo.enode  
  
Output:  
enode://fa46al39f0624ee4cdbe2aab0d7a0a4665b727124956c7b0b5cbfee2  
1d11fa0dc11360214ab299d26cdd7eae1d7ac158921686d4101b1b4892485e87  
952f5d4f@[::]:30303?discport=0
```

ขั้นที่ 8 สร้างโหนดและเริ่มต้นใช้โหนดที่ 2 (เปิดหน้า command ใหม่)

```
Input:  
geth --datadir node2 init genesis.json  
  
geth --networkid 100 --identity node2 --verbosity 3 --nodiscover  
--nat none --datadir node2 --rpc --rpcapi "web3, eth, personal,  
net" --rpcorsdomain "*" --rpcport 8546 --port 30304 --ipcpath  
node2/geth.ipc console
```

ขั้นที่ 9 สร้างเลขบัญชีของโหนดที่ 2 (หน้า command ของโหนดที่ 2)

```
Input:  
>personal.newAccount ()  
  
Output:  
Passphrase:  
Repeat passphrase:  
Address: {0x77cc9c740edca47734144e231f1ce92c561d5169}
```



ขั้นที่ 10 เชื่อมต่อ โหนดที่ 2 กับ โหนดที่ 1 (หน้า command ของ โหนดที่ 2)

Input:

```
>admin.addPeer("enode://fa46a139f0624ee4cdbe2aab0d7a0a4665b727124956c7b0b5cbfee21d11fa0dc11360214ab299d26cdd7eae1d7ac158921686d4101b1b4892485e87952f5d4f@10.235.167.179:30303")
```

Output:

```
true
```

ขั้นที่ 11 การทำธุรกรรม (หน้า command ของ โหนดที่ 1)

Input:

```
> personal.unlockAccount(eth.coinbase, 'Passphrase')
```

Output:

```
true
```

ต้องปลดล็อกกระเป๋าผ่านของเลขบัญชีที่ต้องการส่งทุกครั้งก่อนการทำธุรกรรม

Input:

```
>eth.sendTransaction({from:eth.coinbase, to:'0x77cc9c740edca47734144e231f1ce92c561d5169', value: web3.toWei(100, "ether")})
```

Output:

```
fullhash=0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33cac89186dfd2af2f34a
```

```
recipient=0x77cc9c740edca47734144e231f1ce92c561d5169
```

```
"0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33cac89186dfd2af2f34a"
```

บัญชีของโหนดที่ 1 ส่งอีเธอร์จำนวน 100 อีเธอร์ให้กับโหนดที่ 2

ขั้นที่ 12 ตรวจสอบยอดคงเหลือของบัญชีของโหนดที่ 2 (หน้า command ของ โหนดที่ 2)

Input:

```
> eth.getBalance('0x77cc9c740edca47734144e231f1ce92c561d5169')
```

Output:

```
10000000000000000000
```

หรือเท่ากับ 100 อีเธอร์



ขั้นที่ 13 ตรวจสอบการทำธุรกรรม

Input:

```
>eth.getTransactionReceipt ("0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33cac89186dfd2af2f34a")
```

Output:

```
blockHash:"0x8114f3c06778b2a2c5b9ac0ca0526d8d81b5f92f6a297029459dec6ddfaf3f83",  
blockNumber: 139,  
contractAddress: null,  
cumulativeGasUsed: 21000,  
from: "0x8f16368e3d483caf25e45fcea3c8af432239c4d5",  
gasUsed: 21000,  
root:  
"0xfb4bcd7e55e39c827d60ffad2c7cd074f1497fd6fa694a9b8180d10f5430c9a9",  
to: "0x77cc9c740edca47734144e231f1ce92c561d5169",  
transactionHash:"0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33cac89186dfd2af2f34a",
```

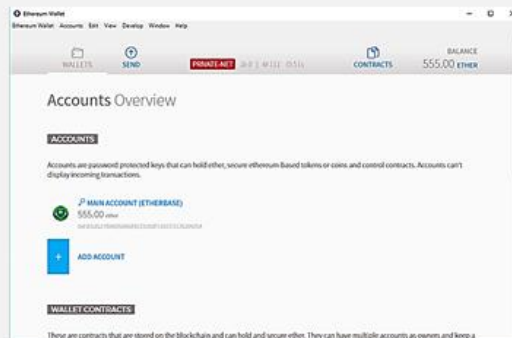
ตอนที่ 2 การสร้างสกุลเงินดิจิทัล

ขั้นที่ 1 เปิด Ethereum Wallet

Input:

```
>Ethereum Wallet.exe" --rpc http://127.0.0.1:8545
```

Output:





ขั้นที่ 2 เริ่มการใช้ Solidity และใส่ code การสร้างสกุลเงินดิจิทัล

Input:

<https://remix.ethereum.org>

Output:

ขั้นที่ 3 ใส่พารามิเตอร์ของสกุลเงินดิจิทัลที่ต้องการสร้าง

Environment: Web3 Provider | Custom (100)

Account: 0xb46...8235e (665 ether)

Gas limit: 3000000

Value: 0 wei

TokenERC20

Deploy

initialSupply: 10000000

tokenName: "UtocoCoin"

tokenSymbol: "UC"

transact

Load contract from Address: At Address

0 pending transactions

TokenERC20 at 0xb46...8235e (blockchain)

approve address_spender, uint256_value

จำนวนอุปสงค์ของสกุลเงินดิจิทัล

ชื่อของสกุลเงินดิจิทัล

สัญลักษณ์ของสกุลเงินดิจิทัล

ถ้ากด transact เลย ระบบจะไม่สร้างการทำธุรกรรมให้เนื่องจากต้องปลดล็อกรหัสผ่านของเลขบัญชีเสียก่อน

ขั้นที่ 4 ปลดล็อกรหัสผ่านของเลขบัญชี

Input:

```
> personal.unlockAccount(eth.coinbase, 'Passphrase')
```

Output:

```
true
```

ต้องปลดล็อกรหัสผ่านของเลขบัญชีที่ต้องการส่งทุกครั้งก่อนการทำธุรกรรม



ขั้นที่ 5 สร้างการทำธุรกรรมของการสร้างสกุลเงินดิจิทัล

Input:

กด transact ที่ได้บรรยายในขั้นตอนที่ 3

Output:

Submitted contract creation

fullhash=0xe871741360ae5555294fbc69c3ff7cae93e453ad136ab73351a14068b9dc7504

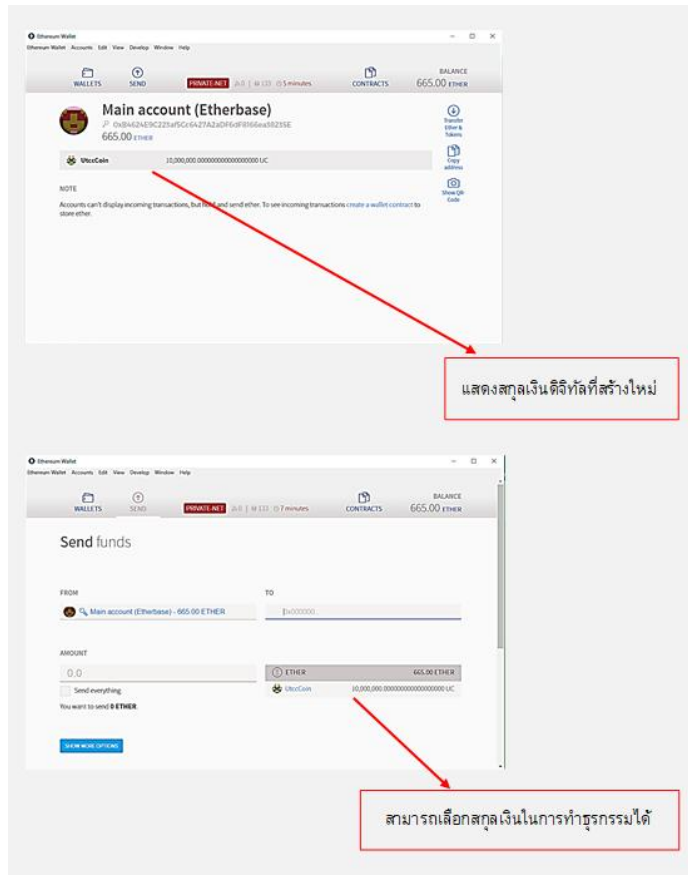
contract=0x8ebe1049851fa28a7f50aeecd3ed29869d3902f1

ขั้นที่ 6 นำเลข contract ของการทำธุรกรรมมาปรับใช้

ใส่เลข contract ที่ได้จากขั้นที่ 5



ขั้นที่ 7 หน้า Wallet แสดงสกุลเงินดิจิทัลที่เราสร้างขึ้นใหม่



4. ผลการศึกษา

ผลการศึกษาของการทำธุรกรรมโดยการใช้แพลตฟอร์มของอีเทอริยม

ขั้นที่ 1 สร้างโหนดและเริ่มต้นใช้โหนดที่ 1

```

C:\> Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...
INFO [06-25 20:10:38] Database conversion successful
INFO [06-25 20:10:38] Initialised chain configuration
false EIP150: <nil> EIP155: 0 EIP158: 0 Metropolis: <nil> Engine: unknown"
INFO [06-25 20:10:39] Disk storage enabled for ethash caches
INFO [06-25 20:10:39] Disk storage enabled for ethash DAGs
WARN [06-25 20:10:39] Upgrading db log bloom bins
INFO [06-25 20:10:39] Bloom-bin upgrade completed
INFO [06-25 20:10:39] Initialising Ethereum protocol
INFO [06-25 20:10:39] Loaded most recent local header
INFO [06-25 20:10:39] Loaded most recent local full block
INFO [06-25 20:10:39] Loaded most recent local fast block
INFO [06-25 20:10:39] Starting P2P networking
INFO [06-25 20:10:39] RLPx listener up
8a363bb7816a0c99f0e77e85838e087277e7910cf64944337b9a62b1c233b37694277e0c893ca16d44ee61: :30303?discport=0
INFO [06-25 20:10:39] IPC endpoint opened: \\.\pipe\node1\geth_ipc
INFO [06-25 20:10:39] HTTP endpoint opened: http://127.0.0.1:8545
Welcome to the Geth JavaScript console!

Instance: Geth/node1/v1.6.7-stable-ab5646c5/windows-amd64/go1.8.3
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0
  
```



ขั้นที่ 2 สร้างเลขบัญชี

```

Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...
personal.newAccount()
Passphrase:
Repeat passphrase:
10XaFe09 ac[8026d-4225c|62500:flb6b:c3e1c|b 9N4e6w8 5wfaf1a11eft8 8a0p1p5eba5rde2d1 *
> url=keystore://D:\iss\geth\node1\key_ status=Locked
  
```

ขั้นที่ 3 การขุด

```

Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...
> miner.start(1)
INFO [06-25 20:18:26] Updated mining threads thread=1
INFO [06-25 20:18:26] Transaction pool price threshold updated price=1800000000
INFO [06-25 20:18:26] Starting mining operation
INFO [06-25 20:18:26] Commit new mining work number=1 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:18:29] Generating DAG in progress epoch=0 percentage=0 elapsed=1.885s
INFO [06-25 20:18:31] Generating DAG in progress epoch=0 percentage=1 elapsed=3.755s
INFO [06-25 20:18:33] Generating DAG in progress epoch=0 percentage=2 elapsed=5.626s
INFO [06-25 20:18:34] Generating DAG in progress epoch=0 percentage=3 elapsed=7.481s
INFO [06-25 20:18:36] Generating DAG in progress epoch=0 percentage=4 elapsed=9.338s
INFO [06-25 20:18:38] Generating DAG in progress epoch=0 percentage=5 elapsed=11.191s
INFO [06-25 20:18:40] Generating DAG in progress epoch=0 percentage=6 elapsed=13.074s
INFO [06-25 20:18:42] Generating DAG in progress epoch=0 percentage=7 elapsed=14.938s
INFO [06-25 20:18:44] Generating DAG in progress epoch=0 percentage=8 elapsed=16.833s
INFO [06-25 20:18:46] Generating DAG in progress epoch=0 percentage=9 elapsed=18.803s
INFO [06-25 20:18:48] Generating DAG in progress epoch=0 percentage=10 elapsed=20.670s
INFO [06-25 20:18:49] Generating DAG in progress epoch=0 percentage=11 elapsed=22.532s
INFO [06-25 20:18:51] Generating DAG in progress epoch=0 percentage=12 elapsed=24.397s
INFO [06-25 20:18:53] Generating DAG in progress epoch=0 percentage=13 elapsed=26.256s
INFO [06-25 20:18:55] Generating DAG in progress epoch=0 percentage=14 elapsed=28.116s
INFO [06-25 20:18:57] Generating DAG in progress epoch=0 percentage=15 elapsed=29.984s
INFO [06-25 20:18:59] Generating DAG in progress epoch=0 percentage=16 elapsed=31.843s
INFO [06-25 20:19:01] Generating DAG in progress epoch=0 percentage=17 elapsed=33.723s
INFO [06-25 20:19:02] Generating DAG in progress epoch=0 percentage=18 elapsed=35.583s
INFO [06-25 20:19:04] Generating DAG in progress epoch=0 percentage=19 elapsed=37.446s
INFO [06-25 20:19:06] Generating DAG in progress epoch=0 percentage=20 elapsed=39.315s
  
```

ขั้นที่ 4 หยุดการขุด

```

Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...
INFO [06-25 20:26:36] Commit new mining work number=59 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:26:36]  mined potential block number=58 hash=492907_0f5e23
INFO [06-25 20:26:36] Successfully sealed new block number=59 hash=19f16f_812d57
INFO [06-25 20:26:36]  block reached canonical chain number=54 hash=03b532_4d88a8
INFO [06-25 20:26:36] Commit new mining work number=60 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:26:36]  mined potential block number=59 hash=19f16f_812d57
INFO [06-25 20:26:37] Successfully sealed new block number=60 hash=004dd_61240d
INFO [06-25 20:26:37]  block reached canonical chain number=55 hash=75b013_7f00ee
INFO [06-25 20:26:37] Commit new mining work number=61 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:26:37]  mined potential block number=60 hash=004dd_61240d

> mi INFO [06-25 20:26:41] Successfully sealed new block number=61 hash=98a390_4ee255
INFO [06-25 20:26:41]  block reached canonical chain number=56 hash=766511_1ccc51
INFO [06-25 20:26:41] Commit new mining work number=62 txs=0 uncles=0 elapsed=1.000ms
INFO [06-25 20:26:41]  mined potential block number=61 hash=98a390_4ee255
> miner.INFO [06-25 20:26:42] Successfully sealed new block number=62 hash=67b2f6_c0fc9f
INFO [06-25 20:26:42]  block reached canonical chain number=57 hash=e312e0_836126
INFO [06-25 20:26:42] Commit new mining work number=63 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:26:42]  mined potential block number=62 hash=67b2f6_c0fc9f
> miner.stop INFO [06-25 20:26:44] Successfully sealed new block number=63 hash=00e282_20738e
INFO [06-25 20:26:44]  block reached canonical chain number=58 hash=492907_0f5e23
INFO [06-25 20:26:44] Commit new mining work number=64 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:26:44]  mined potential block number=63 hash=00e282_20738e
> miner.stop()
true
  
```



ขั้นที่ 5 ตรวจสอบเลขบัญชี

```
Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...  
true  
> eth.accounts  
["0xe9ac82442c650fbbceb94685ffa1f88015b5d21"]  
>
```

ขั้นที่ 6 ตรวจสอบยอดคงเหลือของบัญชี

```
Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...  
> eth.getBalance(eth.coinbase)  
1500000000000000000  
>
```

ขั้นที่ 7 ข้อมูลรหัส enode ของโหนดที่ 1

```
Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...  
> eth.getBalance(eth.coinbase)  
1500000000000000000  
> admin.nodeInfo.enode  
enode://f292b21160f894b6025ed329a086577ee4fbb0268318a363bb7816a9c69fded7c8583ce87277e7940cfe64944337bd9a62b1c233b8769147feec893ca16d44ee@[::]:30303?discport=0  
>
```

ขั้นที่ 8 สร้างโหนดและเริ่มต้นใช้โหนดที่ 2 (เปิดหน้า command ใหม่)



```

Command Prompt - geth --networkid 100 --identity node2 --verbosity 3 --nodiscover --nat none --datadir node2 --rpc --rpcapi ...
WARN [06-25 20:39:22] Upgrading chain database to use sequential keys
INFO [06-25 20:39:22] Database conversion successful
INFO [06-25 20:39:22] Initialised chain configuration      config="{ChainID: 100 Homestead: 0 DAO: <nil> DAOSupport:
false EIP150: <nil> EIP155: 0 EIP158: 0 Metropolis: <nil> Engine: unknown}"
INFO [06-25 20:39:22] Disk storage enabled for ethash caches   dir=D:\is\geth\node2\geth\ethash count=3
INFO [06-25 20:39:22] Disk storage enabled for ethash DAGs             dir=C:\Users\User\AppData\Local\geth\ethash count=2
WARN [06-25 20:39:22] Upgrading db log bloom bins
INFO [06-25 20:39:22] Bloom-bin upgrade completed
INFO [06-25 20:39:22] Initialising Ethereum protocol
INFO [06-25 20:39:22] Loaded most recent local header                 number=0 hash=6e92f8...23a660 td=16384
INFO [06-25 20:39:22] Loaded most recent local full block            number=0 hash=6e92f8...23a660 td=16384
INFO [06-25 20:39:22] Loaded most recent local fast block           number=0 hash=6e92f8...23a660 td=16384
INFO [06-25 20:39:22] Starting P2P networking
INFO [06-25 20:39:22] RLPx listener up                               self="enode://ef310be8c4085977e1212d58a3604839b98835e299
a6f7866ca19ef93ae42650e1224f68296f94e981a3b7650558b5944af334aa9a7bac6a342ad363129801::j:30304?discport=0"
INFO [06-25 20:39:22] IPC endpoint opened: \\.\pipe\geth\ipc
INFO [06-25 20:39:22] HTTP endpoint opened: http://127.0.0.1:8546
Welcome to the Geth JavaScript console!

instance: Geth/node2/v1.6.7-stable-ab5646c5/windows-amd64/go1.8.3
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0
>

```

ขั้นที่ 9 สร้างเลขบัญชีของโหนดที่ 2 (หน้า command ของโหนดที่ 2)

```

Command Prompt - geth --networkid 100 --identity node2 --verbosity 3 --nodiscover --nat none --datadir node2 --rpc --rpcapi ...
> personal.newAccount()
Passphrase:
Repeat passphrase:
[0x1bd02ae9f7f7e11e9b1573bbbfdde38e65ef1f1fe0c b"]
[06-25 20:41:13] New wallet appeared                               url=keystore://D:\is\geth\node2\key... status=Locked

```

ขั้นที่ 10 เชื่อมต่อโหนดที่ 2 กับโหนดที่ 1 (หน้า command ของโหนดที่ 2)

```

Command Prompt - geth --networkid 100 --identity node2 --verbosity 3 --nodiscover --nat none --datadir node2 --rpc --rpcapi ...
INFO [06-25 20:48:15] Commit new mining work                               number=106 txs=0 uncles=0 elapsed=0s
> miner.stop
INFO [06-25 20:48:18] Successfully sealed new block                       number=106 hash=264c76...85e3ca
INFO [06-25 20:48:18] block reached canonical chain                     number=101 hash=d7b481...7de9ec
INFO [06-25 20:48:18] Commit new mining work                               number=107 txs=0 uncles=0 elapsed=0s
INFO [06-25 20:48:18] mined potential block                             number=106 hash=264c76...85e3ca
> miner.stop()
true
> admin.addPeer("enode://f292b21160f894b6025ed329a086577ee4fbb0268318a363bb7816a9c69fded7c8583ce87277e7940cfe64944337bd9
a62b1c233b8769427feec893ca16d4ee@172.20.10.3:30303")
true
>

```



เมื่อเชื่อมต่อ โหนด ได้แล้ว หน้า command ของ โหนดที่ 1 มีลักษณะดังด้านล่าง

```

Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...
mnode://1292211601894b6d2e6d329a096677ee41b0b268318a363b6781b69c691ded7c883ce87277e940c1eb1944357bd9ab2b1c233b876914...
f6ec890ca16a14ca1...:1:306037discport=0"
> INFO [06-25] [22:34:29] Block synchronisation started
INFO [06-25] [22:34:29] Imported new state entries count=1 flushed=1 elapsed=25.413ms processon=1 pending=0
  > INFO [06-25] [22:34:29] Imported new block headers count=106 elapsed=3.176s number=106 hash=264c76... 85e3c...
  > INFO [06-25] [22:34:32] Ignored empty blocks
  > INFO [06-25] [22:34:32] Imported new chain segment blocks=106 txs=0 mgas=0.000 elapsed=95.945ms mgasps=0.000
  > INFO [06-25] [22:34:32] Fast sync complete, auto disabling
  >
  > personal.unlockAccount(eth.coinbase, "")
  > eth.sendTransaction({from: '0xe9ac82d42c650fbbecb94685ffaf88015b5d21', to: '0x1bd02ae9f747e11c9b1573bbfddc38e65ef1ecb...
  > INFO [07-01] [22:24:06] Submitted transaction fullhash=0xc59b24d0ac83966320054b3106bfa4db1b9e75d2ca1b4c12dea1dc662791387
  > miner.start(1)
  > INFO [07-01] [22:24:16] Updated mining threads threads=1
  > INFO [07-01] [22:24:16] Transaction pool price threshold updated price=1800000000
  > INFO [07-01] [22:24:16] Starting mining operation
  > INFO [07-01] [22:24:16] Commit new mining work number=180 txs=1 uncles=0 elapsed=0s
  > INFO [07-01] [22:24:18] Successfully sealed new block number=180 hash=873a2f... 32fab3
  > INFO [07-01] [22:24:18] block reached canonical chain number=175 hash=87249c... 0caae9
  > INFO [07-01] [22:24:18] Commit new mining work number=181 txs=0 uncles=0 elapsed=999.7µ s
  > INFO [07-01] [22:24:18] mined potential block number=180 hash=873a2f... 32fab3
  > INFO [07-01] [22:24:18] Successfully sealed new block number=181 hash=8b2076... 40dcef
  > INFO [07-01] [22:24:18] block reached canonical chain number=176 hash=5668d6... bc137f
  > INFO [07-01] [22:24:18] mined potential block number=182 txs=0 uncles=0 elapsed=0s
  > INFO [07-01] [22:24:18] Commit new mining work number=181 hash=8b2076... 40dcef
  > INFO [07-01] [22:24:21] Successfully sealed new block number=182 hash=530ef6... 19609c
  > INFO [07-01] [22:24:21] block reached canonical chain number=177 hash=9e438e... 3a8529
  > INFO [07-01] [22:24:21] mined potential block number=182 hash=530ef6... 19609c
  > INFO [07-01] [22:24:21] Commit new mining work number=183 txs=0 uncles=0 elapsed=0s
  > INFO [07-01] [22:24:25] Successfully sealed new block number=183 hash=54b03c... 5efb6c
  > INFO [07-01] [22:24:25] block reached canonical chain number=178 hash=02ac6a... 05aaae
  > INFO [07-01] [22:24:25] Commit new mining work number=184 txs=0 uncles=0 elapsed=1.000ms
  > INFO [07-01] [22:24:25] mined potential block number=183 hash=54b03c... 5efb6c
  >

```

ขั้นที่ 11 การทำธุรกรรม (หน้า command ของ โหนดที่ 1)

```

Command Prompt - geth --networkid 100 --identity node1 --verbosity 3 --nodiscover --nat none --datadir node1 --rpc --rpcapi ...
> personal.unlockAccount(eth.coinbase, "")
true
> eth.sendTransaction({from: '0xe9ac82d42c650fbbecb94685ffaf88015b5d21', to: '0x1bd02ae9f747e11c9b1573bbfddc38e65ef1ecb...
, values web3.toWei(100, 'ether')})
> INFO [07-01] [22:24:06] Submitted transaction fullhash=0xc59b24d0ac83966320054b3106bfa4db1b9e75d2ca1b4c12dea1dc662791387
  > INFO [07-01] [22:24:06] Submitted transaction fullhash=0xc59b24d0ac83966320054b3106bfa4db1b9e75d2ca1b4c12dea1dc662791387
  > miner.start(1)
  > INFO [07-01] [22:24:16] Updated mining threads threads=1
  > INFO [07-01] [22:24:16] Transaction pool price threshold updated price=1800000000
  > INFO [07-01] [22:24:16] Starting mining operation
  > INFO [07-01] [22:24:16] Commit new mining work number=180 txs=1 uncles=0 elapsed=0s
  > INFO [07-01] [22:24:18] Successfully sealed new block number=180 hash=873a2f... 32fab3
  > INFO [07-01] [22:24:18] block reached canonical chain number=175 hash=87249c... 0caae9
  > INFO [07-01] [22:24:18] Commit new mining work number=181 txs=0 uncles=0 elapsed=999.7µ s
  > INFO [07-01] [22:24:18] mined potential block number=180 hash=873a2f... 32fab3
  > INFO [07-01] [22:24:18] Successfully sealed new block number=181 hash=8b2076... 40dcef
  > INFO [07-01] [22:24:18] block reached canonical chain number=176 hash=5668d6... bc137f
  > INFO [07-01] [22:24:18] mined potential block number=182 txs=0 uncles=0 elapsed=0s
  > INFO [07-01] [22:24:18] Commit new mining work number=181 hash=8b2076... 40dcef
  > INFO [07-01] [22:24:21] Successfully sealed new block number=182 hash=530ef6... 19609c
  > INFO [07-01] [22:24:21] block reached canonical chain number=177 hash=9e438e... 3a8529
  > INFO [07-01] [22:24:21] mined potential block number=182 hash=530ef6... 19609c
  > INFO [07-01] [22:24:21] Commit new mining work number=183 txs=0 uncles=0 elapsed=0s
  > INFO [07-01] [22:24:25] Successfully sealed new block number=183 hash=54b03c... 5efb6c
  > INFO [07-01] [22:24:25] block reached canonical chain number=178 hash=02ac6a... 05aaae
  > INFO [07-01] [22:24:25] Commit new mining work number=184 txs=0 uncles=0 elapsed=1.000ms
  > INFO [07-01] [22:24:25] mined potential block number=183 hash=54b03c... 5efb6c
  >

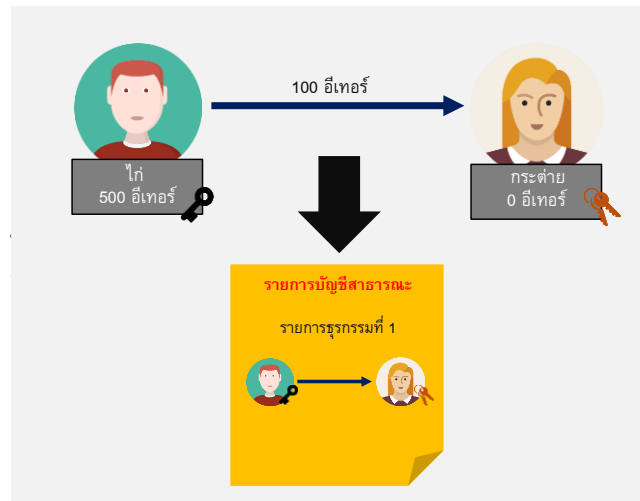
```

ขั้นที่ 12 ตรวจสอบยอดคงเหลือของบัญชีของ โหนดที่ 2 (หน้า command ของ โหนดที่ 2)

```

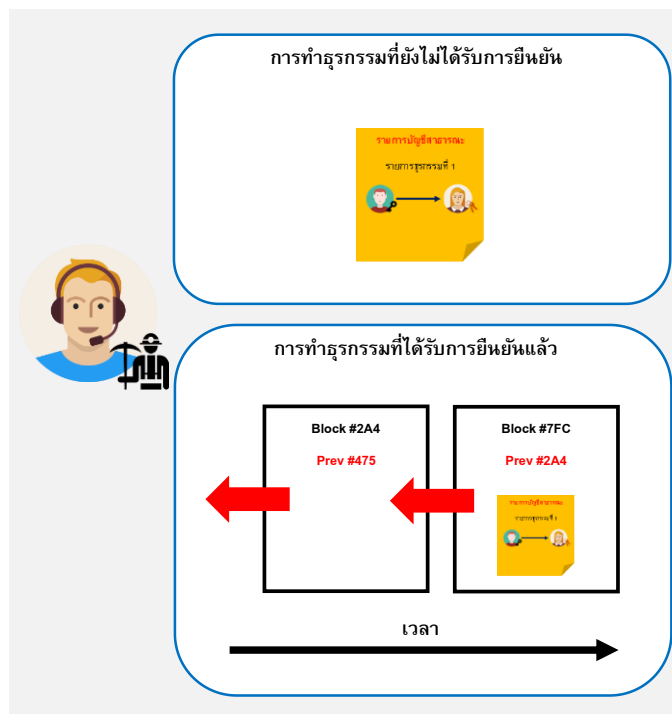
Command Prompt - geth --networkid 100 --identity node2 --verbosity 3 --nodiscover --nat none --datadir node2 --rpc --rpcapi ...
mnode://208 hash=ccc883... 39d522
> eth.getBalance('0x1bd02ae9f747e11c9b1573bbfddc38e65ef1ecb')
3000000000000000000
>

```

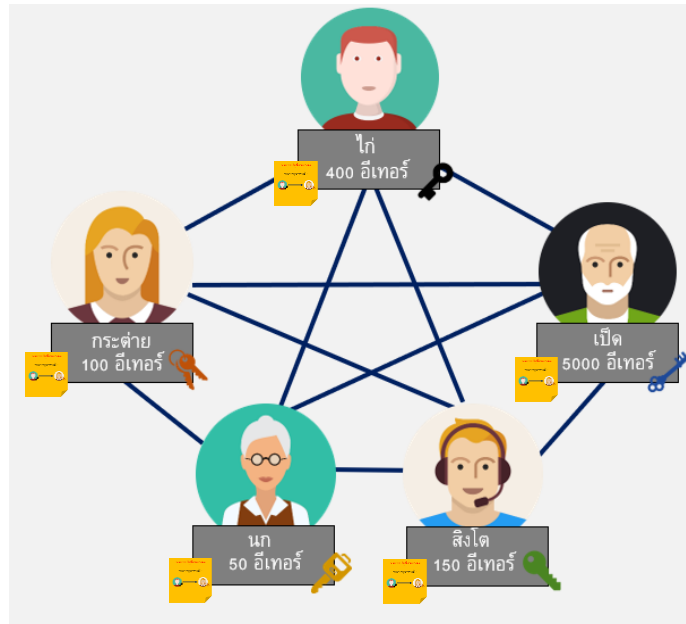
รูปที่ 4.2 การธุรกรรมระหว่าง 2 บุคคล

3. รายการการทำธุรกรรมนั้นยังไม่ถูกส่งต่อให้ทุกคนในเครือข่ายได้จนกว่า "miner" ทำการตรวจสอบและยืนยันการทำธุรกรรม เมื่อรายการถูกยืนยันแล้ว รายการนั้นถูกใส่ลงในบล็อกที่เกิดขึ้นใหม่และถูกนำไปเชื่อมต่อกับบล็อกก่อนหน้าดังรูปที่ 4.3 กำหนดให้สิงโตเป็นผู้ยืนยันการทำธุรกรรม (miner)



รูปที่ 4.3 การยืนยันการทำธุรกรรม

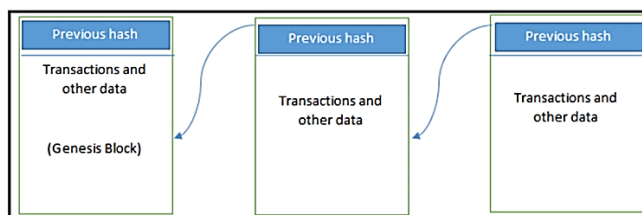
4. จากนั้นจำนวนเหรียญของกระต่ายเพิ่มขึ้นเป็น 100 อีเทอร์ จำนวนเหรียญของไท่ลดลงเหลือ 400 อีเทอร์และสิงโตได้รับรางวัลจากการทำธุรกรรมเพิ่มขึ้น 50 อีเทอร์ ดังรูปที่ 4.4 นอกจากนี้รายการทำธุรกรรมถูกส่งไปยังทุกคนในเครือข่าย ซึ่งทุกคนได้รับข้อมูลรายการเหมือนกันทุกคน



รูปที่ 4.4 ข้อมูลการทำธุรกรรมถูกส่งไปยังทุกคนในเครือข่าย

จากการกระบวนการทำธุรกรรมดังกล่าวแสดงให้เห็นว่าม็อดประกอบที่สำคัญดังนี้

1. บล็อกเชน จากมุมมองทางธุรกิจบล็อกเชนอาจถูกกำหนดให้เป็นแพลตฟอร์มที่สามารถแลกเปลี่ยนซึ่งกันและกันได้โดยการทำธุรกรรมที่ไม่จำเป็นต้องมีคนกลาง บล็อกเชนนั้นเป็นแนวคิดที่ทรงพลังและถ้าเข้าใจศักยภาพของเทคโนโลยีบล็อกเชนนี้จะช่วยให้การดูแลระบบฐานข้อมูลไม่ตกเป็นของใครคนใดคนหนึ่ง แต่ทุกคนสามารถรับรู้ข้อมูลที่เกิดขึ้นทั้งหมดได้ โดยโครงสร้างของบล็อกเชนต่างๆ ไป แสดงได้ลักษณะดังรูปด้านล่าง



คุณสมบัติของบล็อกเชนที่นำมาใช้ในการทำธุรกรรมมีดังนี้

- 1) ไม่สามารถควบคุมได้เนื่องจากไม่มีคนกลางเข้ามาเกี่ยวข้อง
 - 2) มีความโปร่งใสเนื่องจากการทำธุรกรรมสามารถตรวจสอบได้ ในการทดสอบนั้นอยู่ในขั้นตอนที่ 13
 - 3) การทำธุรกรรมไม่สามารถเปลี่ยนรูปได้เนื่องจากทุกคนได้รับข้อมูลเหมือนกัน ถ้ามีการเปลี่ยนแปลงข้อมูลทั้งหมดของทุกคนต้องเปลี่ยนตามไปด้วยซึ่งเป็นเรื่องที่ยากมาก
 - 4) ในกรณีที่การทำธุรกรรมไม่ถูกต้อง ในกระบวนการสามารถสร้างรายการบัญชีสาธารณะได้แต่ทำให้รายการนั้นไม่เป็นที่ยอมรับและไม่สามารถใช้งานได้
2. การกระจายข้อมูลแบบไม่มีศูนย์กลางเป็นประโยชน์หลักในการใช้เทคโนโลยีบล็อกเชน บล็อกเชนนั้นเป็นพาหนะที่ถูกออกแบบมาได้อย่างสมบูรณ์สำหรับแพลตฟอร์มที่ไม่จำเป็นต้องมีตัวกลาง ซึ่งจะช่วยให้ทุกคนในเครือข่ายแข่งขันกันเพื่อเป็นผู้มีอำนาจในการตัดสินใจ วิธีที่ใช่มากที่สุดคือ Proof of Work (PoW) หรือที่เรียก



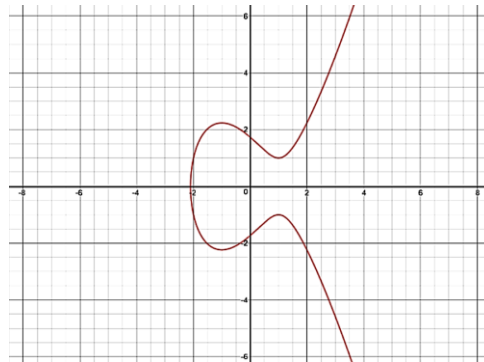
ว่า การขุด นั่นเอง แต่ในส่วนของอีเทอร์เรียมนั้นถูกเรียกว่า Proof of Stake (PoS) ในการทดสอบนั้นอยู่ในขั้นตอนที่ 3

3. วิทยาการเข้ารหัสลับเป็นการนำวิธีทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับข้อมูลตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านหรือเข้าใจได้โดยใครก็ตามที่ไม่มีกุญแจสำหรับเปิดดูข้อมูลนั้น เราเรียกกระบวนการในการแปรรูปของข้อมูลตั้งต้นว่า "การเข้ารหัสข้อมูล" (Encryption) และกระบวนการในการแปลงข้อความที่ไม่สามารถอ่านและทำความเข้าใจให้กลับไปสู่ข้อความดั้งเดิม ว่าการถอดรหัสข้อมูล (Decryption) โดยวิธีการที่ถูกใช้เรียกว่า การเข้ารหัสแบบเส้นโค้งรูปไข่ (Elliptic curve cryptography : ECC)
เส้นโค้งรูปไข่สามารถกำหนดเป็นสมการดังนี้ :

$$y^2 = x^3 + Ax + B \pmod p$$

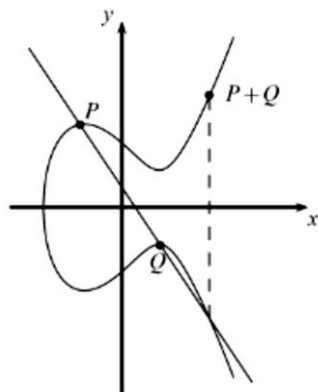
เส้นโค้งเป็นรูปไข่สามารถแสดงให้เห็นในรูปของกราฟได้ดังสมการต่อไปนี้ :

$$y^2 = x^3 + ax + b$$



การเข้ารหัสแบบเส้นโค้งรูปไข่มี 2 แบบดังนี้

- 1) การเพิ่มจุด (Point addition)



สมการเป็นดังต่อไปนี้

$$P + Q = R$$

หมายความว่าพิกัดถูกเพิ่มตามที่แสดงในสมการต่อไปนี้:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

สมการของจุดบวกมีดังนี้ :

$$x_3 = s^2 - x_1 - x_2 \pmod p$$

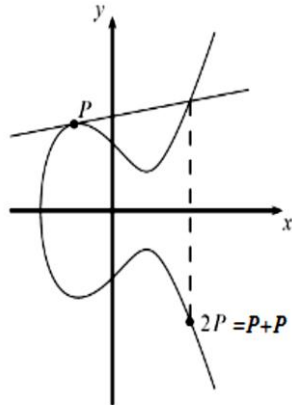
$$y_3 = s(x_1 - x_3) - y_1 \pmod p$$

เป็นผลให้ :

$$s = \frac{(y_2 - y_1)}{(x_2 - x_1)} \pmod p$$



2) จุดเสี้ยวหรือจุดสองเท่า (Point doubling)



สมการเป็นดังต่อไปนี้

$$P + Q = R$$

หมายความว่าพิกัดถูกเพิ่มตามที่แสดงในสมการต่อไปนี้:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

สมการของจุดบวกมีดังนี้ :

$$x_3 = s^2 - x_1 - x_2 \pmod p$$

$$y_3 = s(x_1 - x_3) - y_1 \pmod p$$

เป็นผลให้ :

$$s = \frac{(y_2 - y_1)}{(x_2 - x_1)} \pmod p$$

5. บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการศึกษา

จากการศึกษาพบว่ากระบวนการทำธุรกรรมของสกุลเงินดิจิทัลมีเทคโนโลยีที่อยู่เบื้องหลังคือ บล็อกเชน ซึ่งบล็อกเชนคือ รูปแบบการเก็บข้อมูลที่ให้ทุกคนถือข้อมูลชุดเดียวกัน เมื่อมีการเปลี่ยนแปลง ข้อมูลที่ทุกคนถืออยู่ก็เปลี่ยนแปลงตามไปด้วย โดยข้อมูลการทำธุรกรรมทั้งหมดจะถูกใส่ไว้ในบล็อกและมีการเชื่อมโยงเป็นสายต่อไปเรื่อยๆ มีองค์ประกอบที่สำคัญดังนี้

- 1) การกระจายบัญชีแบบไม่มีศูนย์กลางและการกระจายตัวของบัญชี ซึ่งหมายความว่าแต่ละคนต่างถือบัญชีของตัวเองและไม่มีใครเป็นศูนย์กลางหรือเข้ามาควบคุม
- 2) รายการเดินบัญชีสาธารณะในบล็อกเชนถูกออกแบบให้รายการทั้งหมดของทุกบัญชีต้องเปิดเผยสู่สาธารณะ
- 3) วิทยาการเข้ารหัสลับทั้งกุญแจสาธารณะและกุญแจส่วนตัว

ทั้งหมดนี้แสดงให้เห็นว่าเทคโนโลยีนี้มีประสิทธิภาพ, มีความโปร่งใส, เชื่อถือได้และไม่สามารถปลอมแปลงได้ สกุลเงินดิจิทัลแรกที่ใช้เทคโนโลยีที่เรียกว่าบล็อกเชนคือ บิทคอยน์ในปี 2008 เทคโนโลยีบล็อกเชนนอกจากเป็นสกุลเงินดิจิทัลแล้ว สามารถนำไปประยุกต์ในด้านอื่นๆ ได้อีกมากมาย ถือได้ว่าเป็นเทคโนโลยีที่ทำให้อุตสาหกรรมต่างๆ เกิดความปั่นป่วนอย่างมาก แต่เนื่องจากว่าสกุลเงินดิจิทัล ไม่ใช่เงินตรา จึงไม่สามารถนำมาใช้กับนานาประเทศทั่วโลกได้ ซึ่งเป็นแค่หน่วยข้อมูลอิเล็กทรอนิกส์ที่สามารถนำไปประยุกต์ใช้กับกลุ่มๆ หนึ่งหรือองค์กรๆ หนึ่งเท่านั้น เช่นเดียวกับคูปองในร้านอาหาร นอกจากนี้ยังมีพระราชกำหนดที่ได้ตราขึ้นเพื่อการจัดเก็บภาษีเงินได้บุคคลธรรมดาจากเงินได้พึงประเมินที่ได้จากการถือหรือครอบครองโทเคนดิจิทัล (digital token) หรือการโอนคริปโทเคอร์เรนซี (cryptocurrency) หรือโทเคนดิจิทัล

5.2 ข้อเสนอแนะ

ในการศึกษาค้นคว้าครั้งนี้เห็นได้ว่าวิวัฒนาการของการธุรกรรมทางการเงินถูกพัฒนามาจนถึงยุคของการใช้ธนบัตรเป็นเงินตราและมีรูปแบบของการทำธุรกรรมออนไลน์ ไม่ว่าจะเป็นนวัตกรรมตู้ ATM ที่ช่วยให้คนกดเงินสดได้สะดวกเพียงแค่มีบัตร, บัตรเครดิต, การโอนเงินออนไลน์ เป็นต้น แต่การทำธุรกรรมดังกล่าวนี้ยังไม่มีความปลอดภัยเท่าที่ควร



และมีปัญหาหลายอย่างเกิดขึ้น ยกตัวอย่างเช่นการปลอมแปลงธนบัตรหรือการแอบอ้างข้อมูล ซึ่งเทคโนโลยีบล็อกเชนในปัจจุบันยังอยู่ในช่วงเริ่มต้นเท่านั้น แต่ก็แสดงให้เห็นว่าบล็อกเชนเป็นเครื่องมือที่สามารถแก้ไขปัญหาเหล่านั้นได้ โดยเฉพาะองค์กรทางการเงินจะได้รับอิทธิพลจากบล็อกเชนเป็นอย่างมาก ในอนาคตสกุลเงินดิจิทัลอาจเป็นมากกว่าหน่วยข้อมูลอิเล็กทรอนิกส์ก็ได้และเส้นทางของเทคโนโลยีบล็อกเชนจะไปในทิศทางไหนนั้นจึงต้องติดตามกันต่อไป

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระเรื่องนี้สำเร็จรูกลงได้ด้วยความกรุณาจาก ดร.บำรุง พ่วงเกิด ที่ให้คำปรึกษาแนะนำในการศึกษาค้นคว้าอิสระ การตรวจทานเนื้อหาการค้นคว้า และ ให้แนะนำในการแก้ไขปัญหาที่เกิดขึ้น ในระหว่างการศึกษาค้นคว้า จนสำเร็จรูกลงไปด้วยดี รวมถึงคณาจารย์ผู้สอนทุกท่านที่ได้ประศาสตร์วิชาความรู้ตลอดหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมการเงิน มหาวิทยาลัยหอการค้าไทย

เอกสารอ้างอิง

- David Lee Kuo Chuen. (2015). Chapter 1 Introduction to Bitcoin. Handbook of Digital Currency. (5-29).: Packt Publishing Ltd..
- David Lee Kuo Chuen. (2015). Chapter 5 Evaluating the Potential of Alternative Cryptocurrencies. Handbook of Digital Currency. (81-135). : Packt Publishing Ltd..
- Imran Bashir. (2017). Mastering Blockchain. : Elsevier Inc..
- Gerald P. Dwyer. (2014). The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability. : Elsevier B.V.
- Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo. (2017). A Blockchain Future to Internet of Things Security: A position paper.
- Nigel Smart. (2017). Cryptography: An Introduction. 3rd Edition.
- James Altucher. (3 February 2018). Everything You Need to Know About Bitcoin. Sqwawqs, (5-17).
- Andreas M. Antonopoulos. (2014). Mastering Bitcoin. : O'Reilly Media, Inc..