กระบวนการทำธุรกรรมทางการเงินด้วยเทคโนโลยีบล็อกเชนและการสร้างสกุลเงินดิจิทัล

FINANCIAL TRANSACTION PROCESS WITH BLOCKCHAIN TECHNOLOGY AND CREATE CRYPTOCURRENCY WITH ETHEREUM

มณฑิรา กำจร[1] และ ดร.บำรุง พ่วงเกิด[2]

[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) วิทยาการการเข้ารหัสลับทั้งกุญแจสาธารณะและกุญแจส่วนตัว

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 และเมื่อไม่กี่ปีที่ผ่านมามีนวัตกรรมเทคโนโลยีทางการเงินรูปแบบใหม่เกิดขึ้น นั่นคือ สกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซี ซึ่งเชื่อว่าสกุลเงินดิจิทัลเป็นรูปแบบของการทำธุรกรรมที่มีประสิทธิภาพ แต่เนื่องจากว่าสกุลเงินดิจิทัลไม่ถือว่าเป็นเงินตรา เป็นแค่หน่วยข้อมูลอิเล็กทรอนิกส์เท่านั้น ทำให้สกุลเงินดิจิทัลยังไม่เป็นที่ยอมรับของนานาประเทศทั่วโลก

ในปัจจุบันสกุลเงินดิจิทัลได้รับความสนใจอย่างมากทั้งในประเทศและต่างประเทศทั่วโลก ทำให้หลายๆคนอยากทราบว่าสกุลเงินดิจิทัลคืออะไร มีความหมายอย่างไร และทำไมประเทศอื่นๆต้องตื่นตัวกันอย่างมาก แม้ความต้องการสกุลเงินดิจิทัลจะเพิ่มขึ้นอย่างรวดเร็ว แต่ยังต้องเผชิญกับความท้าทายอีกหลายอย่าง ทั้งความผันผวนของอัตราแลกเปลี่ยนและมุมมองของหน่วยงานกำกับดูแลของแต่ละประเทศ ทำให้โอกาสที่คนทั่วไปจะนำมาใช้ในวงกว้างอาจไม่ง่ายนัก อย่างไรก็ดี แนวคิดของสกุลเงินดิจิทัลอย่างเทคโนโลยีบล็อกเชนที่เป็นรากฐานของบิทคอยน์นับว่ามีศักยภาพและสามารถนำไปประยุกต์ใช้กับองค์กรต่างๆเพื่อให้ขั้นตอนการทำงานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพสูงสุดโลกของฟินเทคหรือเทคโนโลยีทางการเงิน ขณะนี้ดูเหมือนให้น้ำหนักกับเทคโนโลยีบล็อกเชนเป็นเทคโนโลยีหลักที่สถาบันการเงินนำมาพัฒนาต่อยอดได้อย่างกว้างขวางไม่ใช่แค่การโอนเงินระหว่างประเทศเท่านั้น ซึ่งทั้งบรรดา Tech Startup หรือธนาคารต่างๆ ได้หันมาศึกษาและพัฒนาบล็อกเชนกันอย่างจริงจังเพื่อก้าวให้ทันกับเทคโนโลยีและพฤติกรรมของผู้บริโภคในยุคปัจจุบันที่นิยมซื้อ-ขายหรือทำธุรกรรมผ่านช่องทางออนไลน์กันมากขึ้น

ส่วนใหญ่แล้วสกุลเงินดิจิทัลถูกนำมาใช้ในการทำธุรกรรมทางการเงินภายในกลุ่มๆหนึ่ง ซึ่งโดยทั่วไปการทำธุรกรรมในด้านการเงินระหว่างบุคคลหรือองค์กรยังไม่มีประสิทธิภาพเท่าที่ควร ดังนั้นเพื่อทดสอบว่าเทคโนโลยีใหม่นี้มาช่วยให้การทำธุรกรรมมีความปลอดภัยและโปร่งใสมากยิ่งขึ้น การค้นคว้าอิสระนี้เป็นการศึกษากระบวนการทำธุรกรรมทางการเงินด้วยบล็อกเชนและวิธีการสร้างสกุลเงินดิจิทัล

2. วัตถุประสงค์การวิจัย

การวิจัยนี้มีจุดประสงค์เพื่อศึกษาเทคโนโยลีทางการเงินรูปแบบใหม่ให้ทันยุคทันสมัยตามกาลเวลา ด้วยการศึกษากระบวนการทำธุรกรรมทางการเงินด้วยบล็อกเชนของอีเทอเรียมและวิธีการสร้างสกุลเงินดิจิทัลขึ้นมาใหม่

ด้วยภาษา Solidity (ภาษาของอีเทอเรียม) 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 ซึ่งบัญชีที่สร้างครั้งแรกจะเป็น 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:

69000000000000000000
```

จำนวนที่ได้หน่วยจะเป็น Wei ถ้าจะเปลี่ยนเป็นหน่วย Ether คือ หารด้วย 10^{18}

```
Input:

>eth.getBalance('0x8f16368e3d483caf25e45fcea3c8af432239c4d5')


Output:

69000000000000000000
```

ขั้นที่ 7 ข้อมูลรหัส enode ของโหนดที่ 1

```
Input:

admin.nodeInfo.enode


Output:

enode://fa46a139f0624ee4cdbe2aab0d7a0a4665b727124956c7b0b5cbfee2
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" --rpccorsdomain "*" --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 เชื่อมต่อโหนดที่ 2 กับโหนดที่ 1 (หน้า command ของโหนดที่ 2)

```
Input:

>admin.addPeer("enode://fa46a139f0624ee4cdbe2aab0d7a0a4665b72712
4956c7b0b5cbfee21d11fa0dc11360214ab299d26cdd7eaeld7ac158921686d4
101b1b4892485e87952f5d4f@10.235.167.179:30303")

Output:

true
```

ขั้นที่ 11 การทำธุรกรรม (หน้า command ของโหนดที่ 1)

```
Input:

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

Output:

true
```

ต้องปลดล็อกรหัสผ่านของเลขบัญชีที่ต้องการส่งทุกครั้งก่อนการทำธุรกรรม

```
Input:

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

Output:

fullhash=0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33cac89186
dfd2af2f34a

recipient=0x77cc9c740edca47734144e231f1ce92c561d5169

"0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33cac89186dfd2af2f
34a"
```

บัญชีของโหนดที่ 1 ส่งอีเทอเรียมจำนวน 100 อีเทอร์ให้กับโหนดที่ 2

ขั้นที่ 12 ตรวจสอบยอดคงเหลือของบัญชีของโหนดที่ 2 (หน้า command ของโหนดที่ 2)

```
Input:

> eth.getBalance('0x77cc9c740edca47734144e231f1ce92c561d5169')

Output:

100000000000000000000
```

หรือเท่ากับ 100 อีเทอร์

ขั้นที่ 13 ตรวจสอบการทำธุรกรรม

```
Input:

>eth.getTransactionReceipt("0x88e88b5be9642df3e6d6abb5b341240ad0
50c3fdb8f33cac89186dfd2af2f34a")


Output:

blockHash:"0x8114f3c06778b2a2c5b9ac0ca0526d8d81b5f92f6a297029459
dec6ddfaf3f83",

blockNumber: 139,

contractAddress: null,

cumulativeGasUsed: 21000,

from: "0x8f16368e3d483caf25e45fcea3c8af432239c4d5",

gasUsed: 21000,

root:
"0xfb4bcd7e55e39c827d60ffad2c7cd074f1497fd6fa694a9b8180d10f5430c
9a9",

to: "0x77cc9c740edca47734144e231f1ce92c561d5169",

transactionHash:"0x88e88b5be9642df3e6d6abb5b341240ad050c3fdb8f33
cac89186dfd2af2f34a",
```

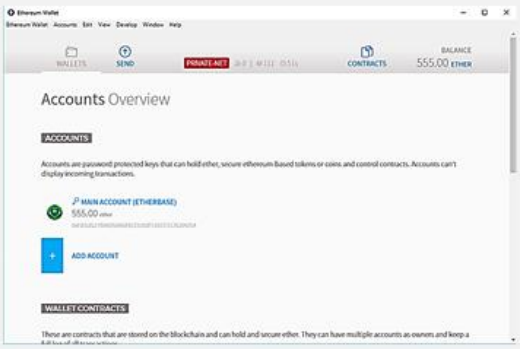
ตอนที่ 2 การสร้างสกุลเงินดิจิทัล

ขั้นที่ 1 เปิด Ethereum Wallet

```
Input:

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


Output:
```

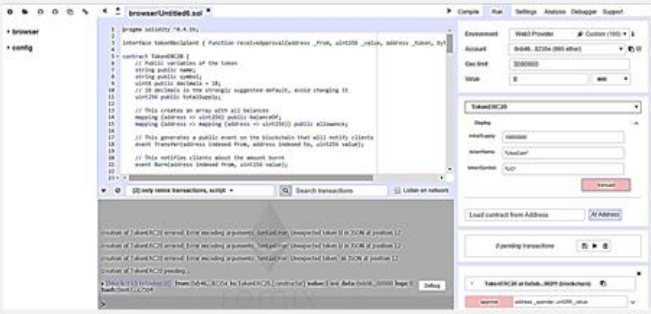


ขั้นที่ 2 เริ่มการใช้ Solidity และใส่ code การสร้างสกุลเงินดิจิทัล

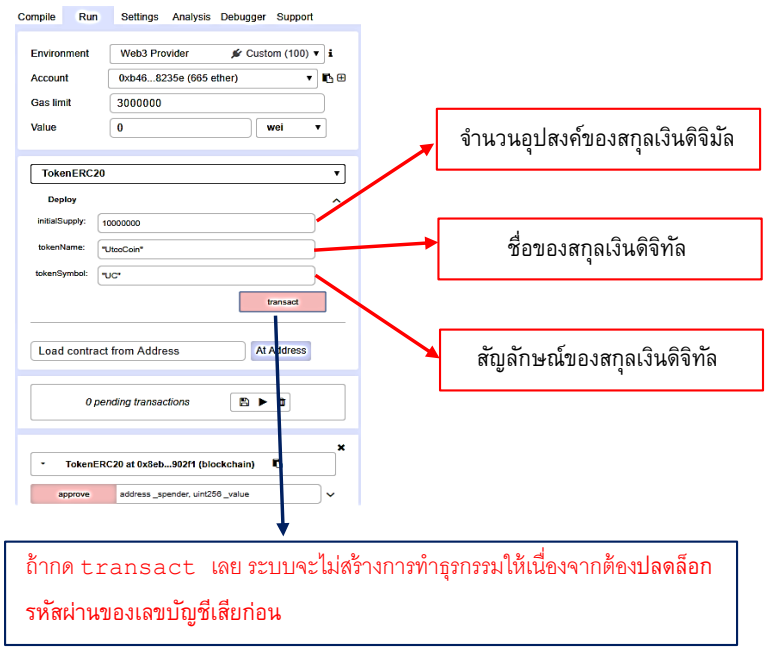
Input:

https://remix.ethereum.org

Output:



ขั้นที่ 3 ใส่พารามิเตอร์ของสกุลเงินดิจิทัลที่ต้องการสร้าง



ขั้นที่ 4 ปลดล็อกรหัสผ่านของเลขบัญชี

Input:

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

Output:

```
true
```

ต้องปลดล็อกรหัสผ่านของเลขบัญชีที่ต้องการส่งทุกครั้งก่อนการทำธุรกรรม

ขั้นที่ 5 สร้างการทำธุรกรรมของการสร้างสกุลเงินดิจิทัล

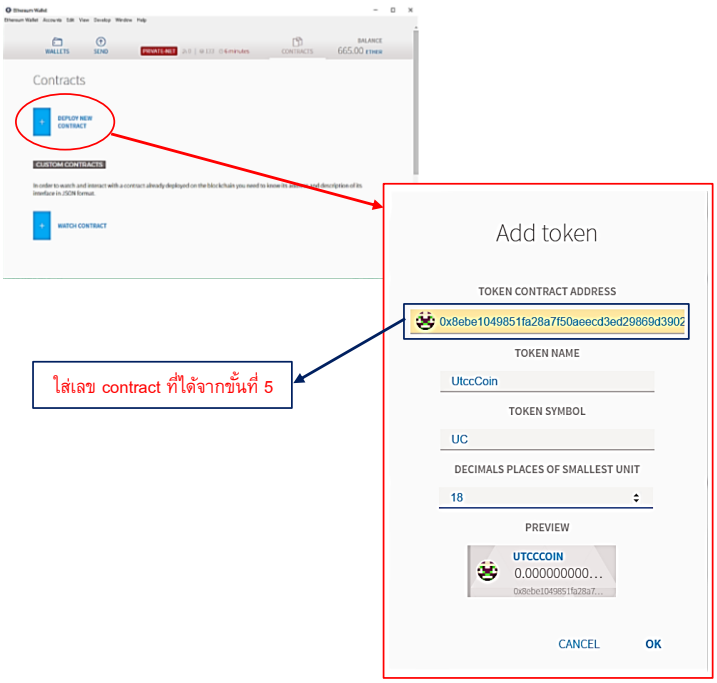
Input:

กด transact ที่ได้บรรยายในขั้นตอนที่ 3

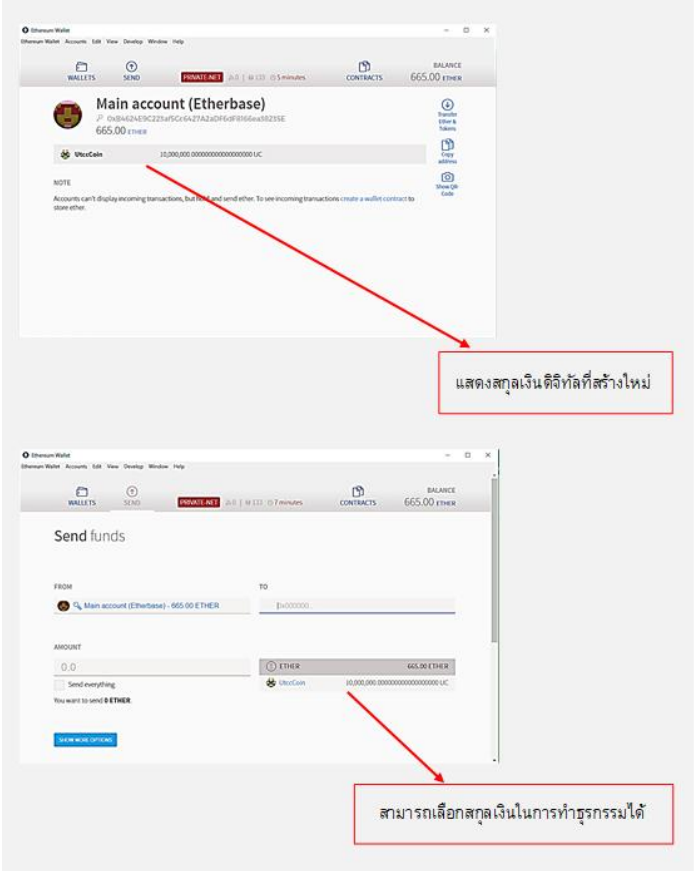
Output:

```
Submitted contract creation
fullhash=0xe871741360ae5555294fbc69c3ff7cae93e453ad136ab73351a14068b9dc7504
contract=0x8ebe1049851fa28a7f50aeecd3ed29869d3902f1
```

ขั้นที่ 6 นำเลข contract ของการทำธุรกรรมมาปรับใช้



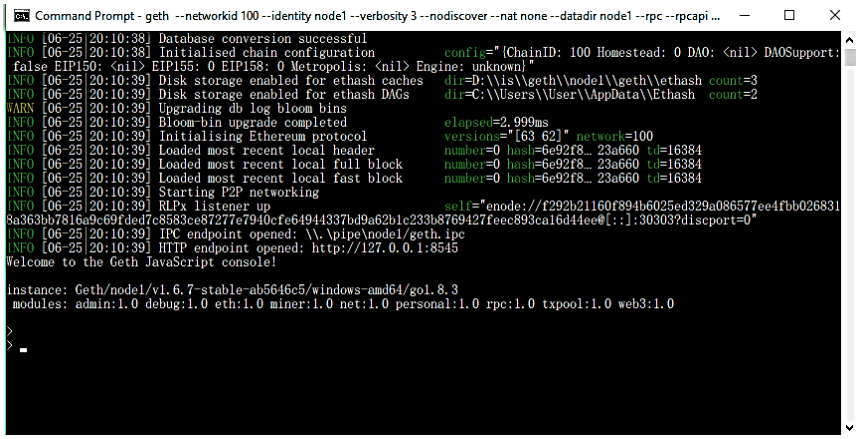
ขั้นที่ 7 หน้า Wallet แสดงสกุลเงินดิจิทัลที่เราสร้างขึ้นใหม่



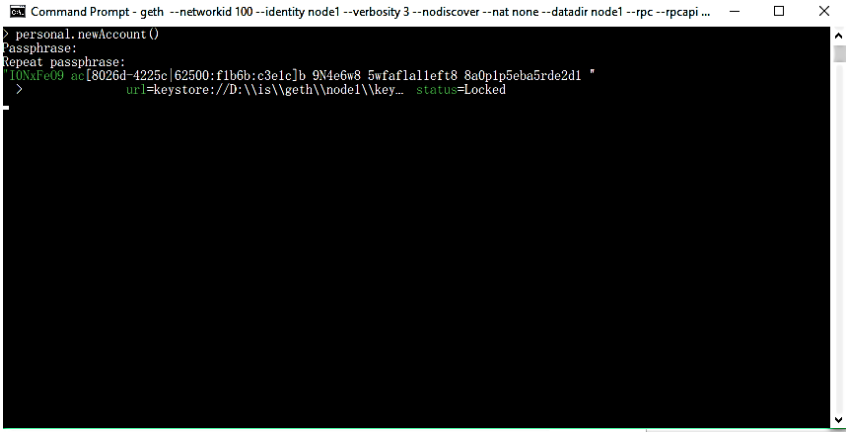
4. ผลการศึกษา

ผลการศึกษาของการทำธุรกรรมโดยการใช้แพลตฟอร์มของอีเทอเรียม

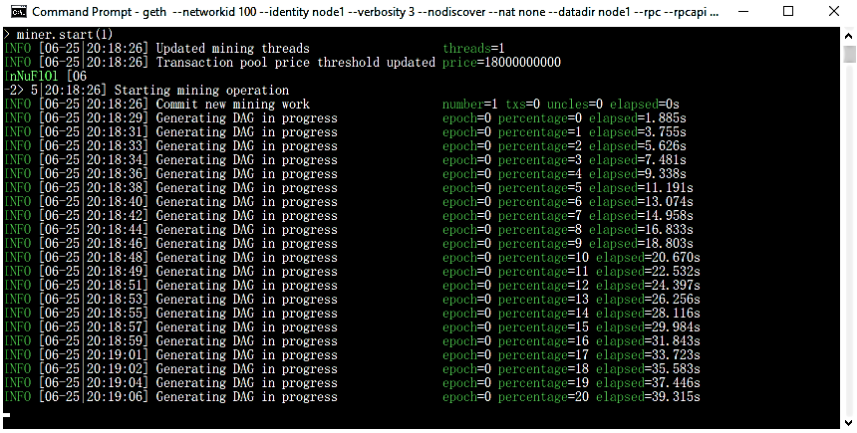
ขั้นที่ 1 สร้างโหนดและเริ่มต้นใช้โหนดที่ 1



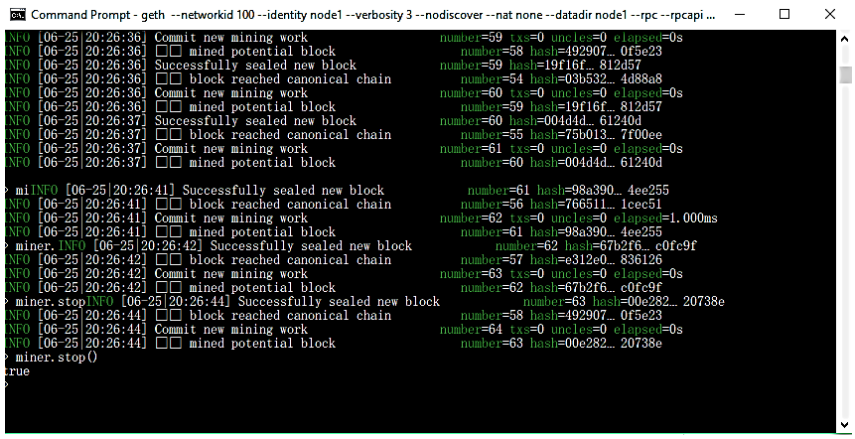
ขั้นที่ 2 สร้างเลขบัญชี



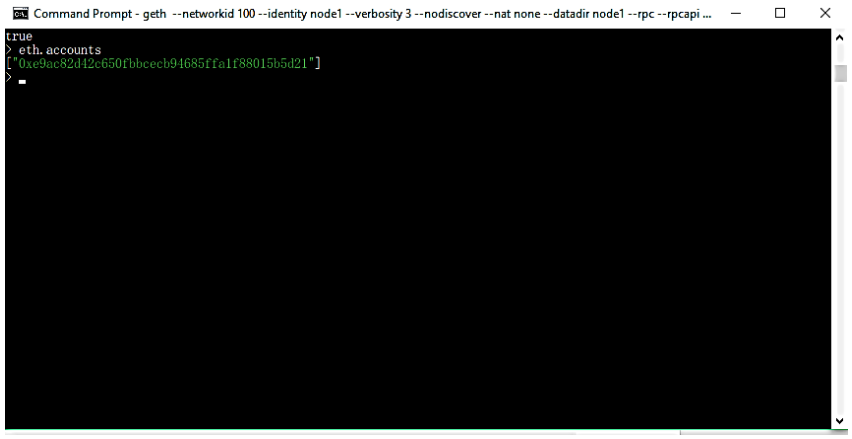
ขั้นที่ 3 การขุด



ขั้นที่ 4 หยุดการขุด

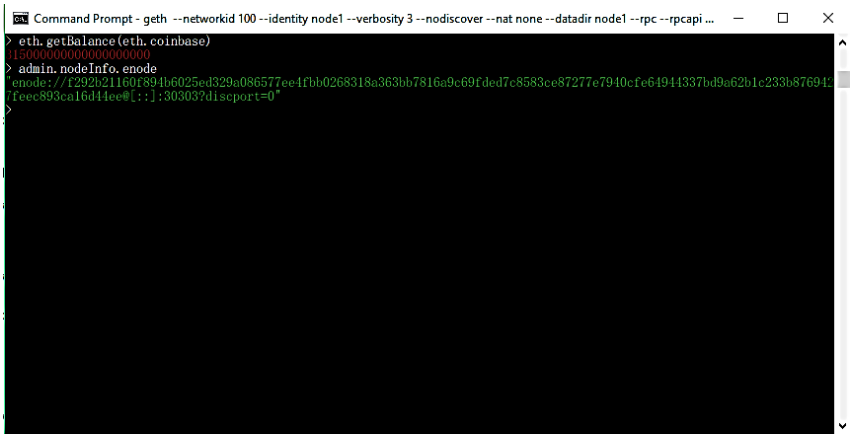


ขั้นที่ 5 ตรวจสอบเลขบัญชี

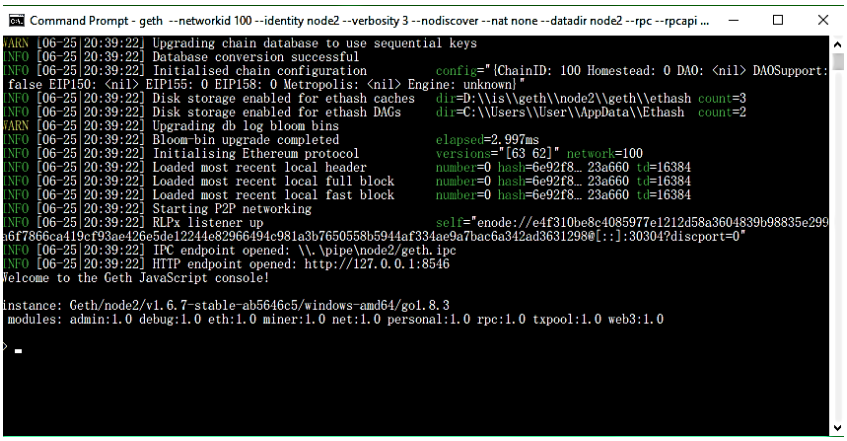


ขั้นที่ 6 ตรวจสอบยอดคงเหลือของบัญชี

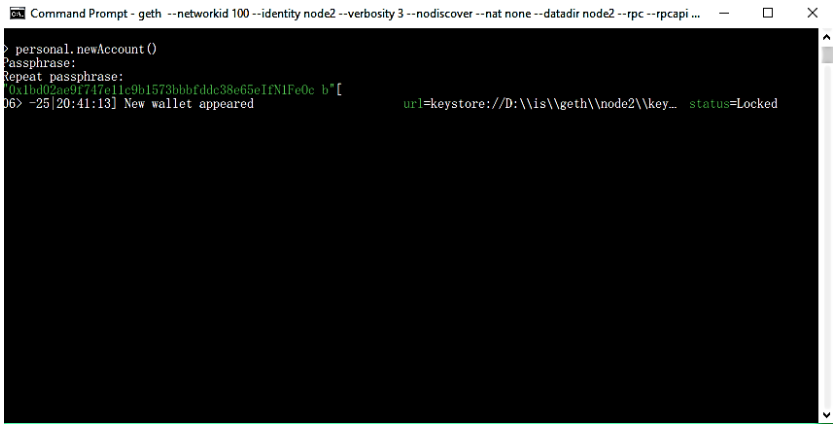
ขั้นที่ 7 ข้อมูลรหัส enode ของโหนดที่ 1



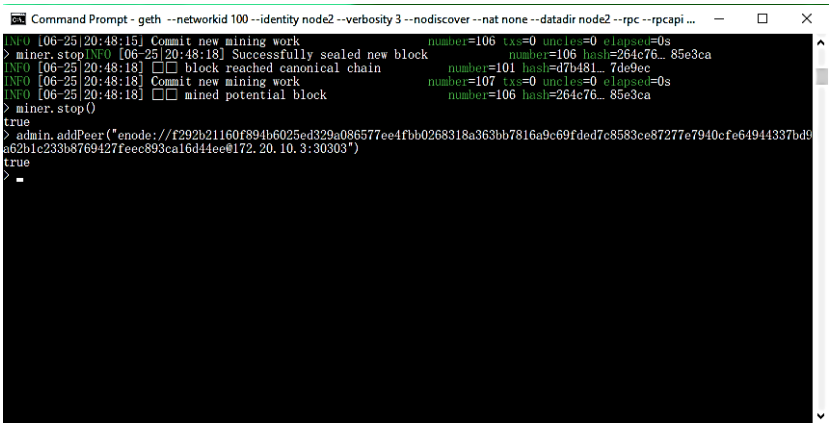
ขั้นที่ 8 สร้างโหนดและเริ่มต้นใช้โหนดที่ 2 (เปิดหน้า command ใหม่)



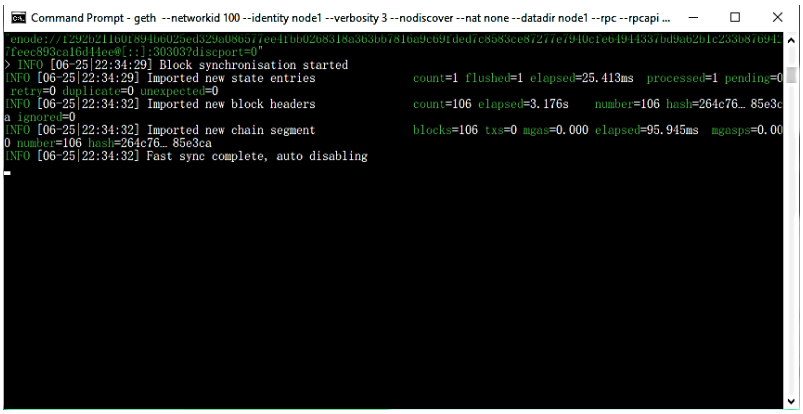
ขั้นที่ 9 สร้างเลขบัญชีของโหนดที่ 2 (หน้า command ของโหนดที่ 2)



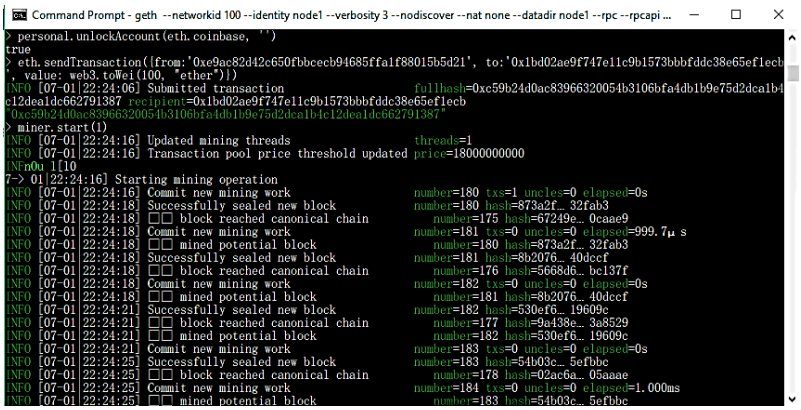
ขั้นที่ 10 เชื่อมต่อโหนดที่ 2 กับโหนดที่ 1 (หน้า command ของโหนดที่ 2)



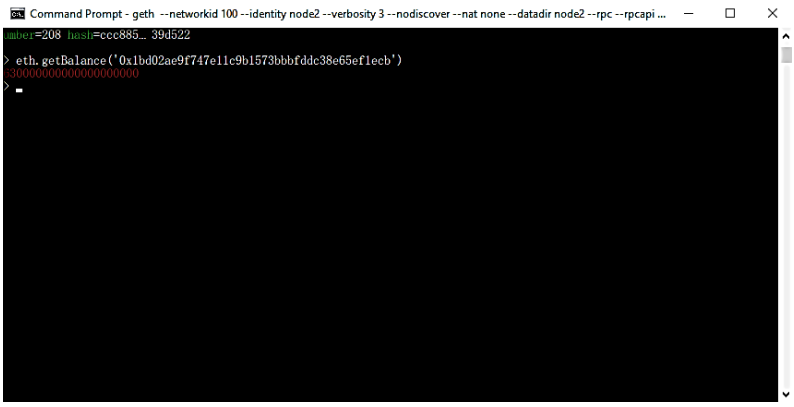
เมื่อเชื่อมต่อโหนดได้แล้ว หน้า command ของโหนดที่ 1 มีลักษณะดังด้านล่าง



ขั้นที่ 11 การทำธุรกรรม (หน้า command ของโหนดที่ 1)



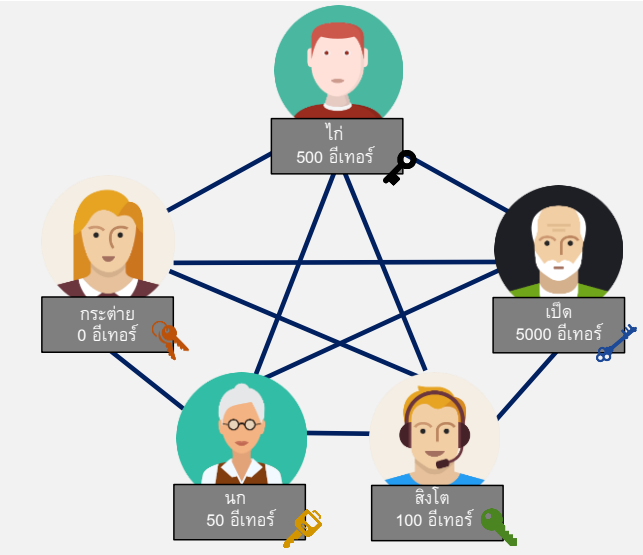
ขั้นที่ 12 ตรวจสอบยอดคงเหลือของบัญชีของโหนดที่ 2 (หน้า command ของโหนดที่ 2)



ขั้นที่ 13 ตรวจสอบการทำธุรกรรม

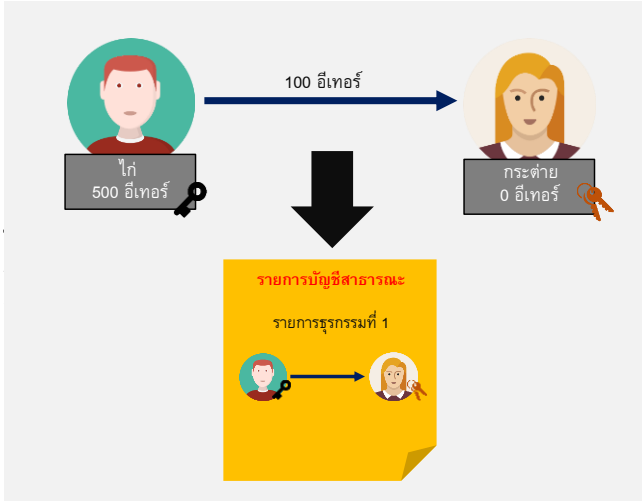
ลักษณะของการทดสอบของกระบวนการทำงานของการทำธุรกรรมเป็นลักษณะดังต่อไปนี้

1. การทดสอบโดยใช้กลุ่มตัวอย่างจำนวน 5 คน เริ่มจากทุกคนต้องมีเลขบัญชีเป็นของตัวเองที่แตกต่างกัน (แทนด้วยลูกกุญแจ หมายความว่าทุกคนมีลูกกุญแจที่แตกต่างกันออกไป) และถูกกำหนดให้มีจำนวนเหรียญดังรูปที่ 4.1 ซึ่งบัญชีของทุกคนเชื่อมต่อเข้าด้วยกันเพื่อทำการธุรกรรมซึ่งกันและกัน



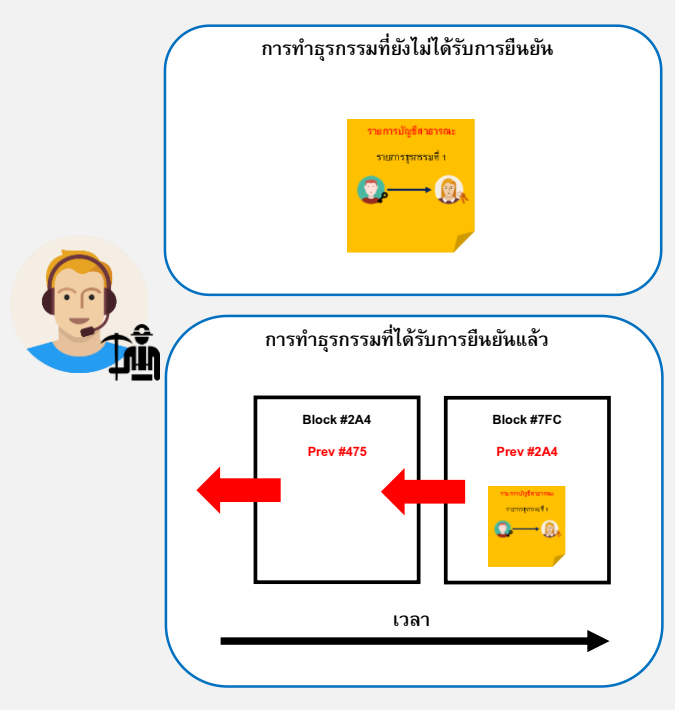
รูปที่ 4.1 รูปแบบเครือข่ายการทำธุรกรรม

2. เมื่อไก่ต้องการส่งเหรียญจำนวน 100 อีเทอร์ให้กับกระต่ายดังรูปที่ 4.2 ซึ่งไก่ได้รับเลขบัญชีของกระต่ายและต้องปลดล็อกรหัสผ่านส่วนตัวในการระบุตัวตนในการทำธุรกรรมทุกครั้งทำให้ได้รายการทำธุรกรรมมา 1 รายการเพื่อรอการยืนยันและตรวจสอบการทำธุรกรรม



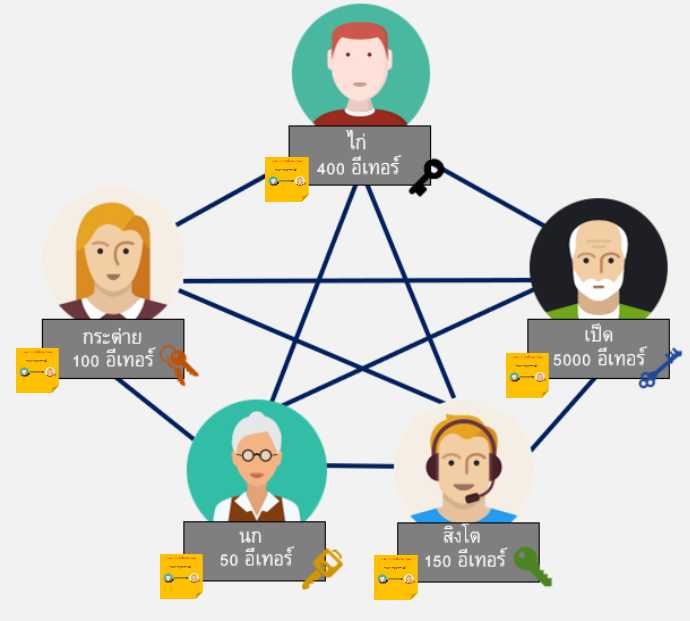
รูปที่ 4.2 การธุรกรรมระหว่าง 2 บุคคล

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



รูปที่ 4.3 การยืนยันการทำธุรกรรม

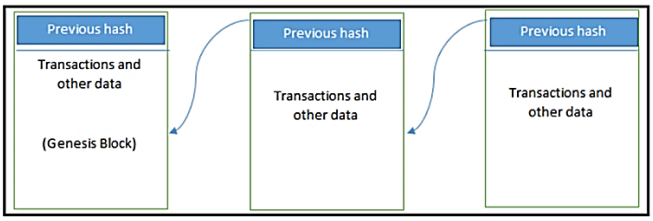
4. จากนั้นจำนวนเหรียญของกระต่ายเพิ่มขึ้นเป็น 100 อีเทอร์ จำนวนเหรียญของไก่ลดลงเหลือ 400 อีเทอร์และสิงโตได้รับรางวัลจากการทำธุรกรรมเพิ่มขึ้น 50 อีเทอร์ ดังรูปที่ 4.4 นอกจากนี้รายการทำธุรกรรมถูกส่งไปยังทุกคนในเครือข่าย ซึ่งทุกคนได้รับข้อมูลรายการเหมือนกันทุกคน



รูปที่ 4.4 ข้อมูลการทำธุรกรรมถูกส่งไปยังทุกคนในเครือข่าย

จากการกระบวนการทำธุรกรรมดังกล่าวแสดงให้เห็นว่ามีองค์ประกอบที่สำคัญดังนี้

1. บล็อกเชน จากมุมมองทางธุรกิจบล็อกเชนอาจถูกกำหนดให้เป็นแพลตฟอร์มที่สามารถแลกเปลี่ยนซึ่งกันและกันได้โดยการทำธุรกรรมที่ไม่จำเป็นต้องมีคนกลาง บล็อกเชนนั้นเป็นแนวคิดที่ทรงพลังและถ้าเข้าใจศักยภาพของเทคโนโลยีบล็อกเชนนี้จะช่วยให้การดูแลระบบฐานข้อมูลไม่ตกเป็นของใครคนใดคนหนึ่ง แต่ทุกคนสามารถรับรู้ข้อมูลที่เกิดขึ้นทั้งหมดได้ โดยโครงสร้างของบล็อกเชนทั่วๆไป แสดงได้ลักษณะดังรูปด้านล่าง



คุณสมบัติของบล็อกเชนที่นำมาใช้ในการทำธุรกรรมมีดังนี้

1) ไม่สามารถควบคุมได้เนื่องจากไม่มีคนกลางเข้ามาเกี่ยวข้อง
2) มีความโปร่งใสเนื่องจากการทำธุรกรรมสามารถตรวจสอบได้ ในการทดสอบนั้นอยู่ในขั้นตอนที่ 13
3) การทำธุรกรรมไม่สามารถเปลี่ยนรูปได้เนื่องจากทุกคนได้รับข้อมูลเหมือนกัน ถ้ามีการเปลี่ยนแปลงข้อมูลทั้งหมดของทุกคนต้องเปลี่ยนตามไปด้วยซึ่งเป็นเรื่องที่ยากมาก
4) ในกรณีที่การทำธุรกรรมไม่ถูกต้อง ในกระบวนการสามารถสร้างรายการบัญชีสาธารณะได้แต่ทำให้รายการนั้นไม่เป็นที่ยอมรับและไม่สามารถใช้งานได้

2. การกระจายข้อมูลแบบไม่มีศูนย์กลางเป็นประโยชน์หลักในการใช้เทคโนโลยีบล็อกเชน บล็อกเชนนั้นเป็นพาหนะที่ถูกออกแบบมาได้อย่างสมบูรณ์สำหรับแพลตฟอร์มที่ไม่จำเป็นต้องมีตัวกลาง ซึ่งจะทำให้ทุกคนในเครือข่ายแข่งขันกันเพื่อเป็นผู้มีอำนาจในการตัดสินใจ วิธีที่ใช้มากที่สุดคือ Proof of Work (PoW) หรือที่เรียก

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

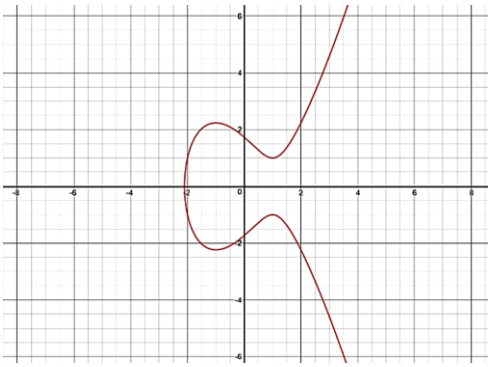
3. วิทยาการการเข้ารหัสลับเป็นการนำวิธีทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับข้อมูลตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านหรือเข้าใจได้โดยใครก็ตามที่ไม่มีกุญแจสำหรับเปิดดูข้อมูลนั้น เราเรียกกระบวนการในการแปรรูปของข้อมูลตั้งต้นว่า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

เส้นโค้งรูปไข่สามารถกำหนดเป็นสมการดังนี้ :

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

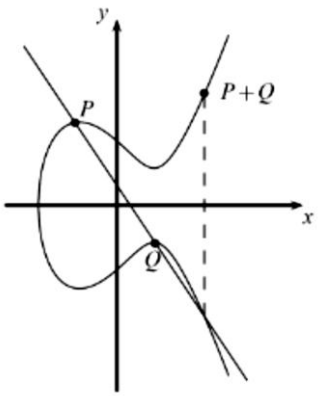
เส้นโค้งเป็นรูปไข่สามารถแสดงให้เห็นในรูปของกราฟได้ดังสมการต่อไปนี้ :

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



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 :

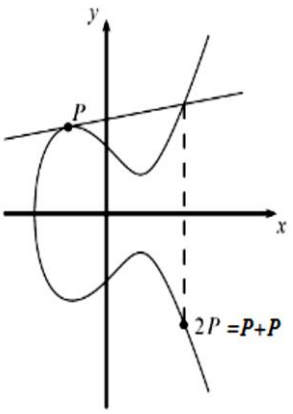
$$x_3 = s^2 - x_1 - x^2 \bmod p$$

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

เป็นผลให้ :

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

2) จุดเสเสร้งหรือจุดสองเท่า (Point doubling)



สมการเป็นดังต่อไปนี้

$$P + Q = R$$

หมายความว่าพิกัดถูกเพิ่มตามที่แสดงในสมการต่อไปนี้:

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

สมการของจุดบวกมีดังนี้ :

$$x_3 = s^2 - x_1 - x^2 \bmod p$$

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

เป็นผลให้ :

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

5. บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการศึกษา

จากการศึกษาพบว่ากระบวนการทำธุรกรรมของสกุลเงินดิจิทัลมีเทคโนโลยีที่อยู่เบื้องหลังคือ บล็อกเชน ซึ่งบล็อกเชนคือ รูปแบบการเก็บข้อมูลที่ให้ทุกคนถือข้อมูลชุดเดียวกัน เมื่อมีการเปลี่ยนแปลง ข้อมูลที่ทุกคนถืออยู่ก็เปลี่ยนแปลงตามไปด้วย โดยข้อมูลการทำธุรกรรมทั้งหมดจะถูกใส่ไว้ในบล็อกและมีการเชื่อมโยงเป็นสายต่อไปเรื่อยๆ มีองค์ประกอบที่สำคัญดังนี้

1) การกระจายบัญชีแบบไม่มีศูนย์กลางและการกระจายตัวของบัญชี ซึ่งหมายความว่าแต่ละคนต่างถือบัญชีของตัวเองและไม่มีใครเป็นศูนย์กลางหรือเข้ามาควบคุม
2) รายการเดินบัญชีสาธารณะในบล็อกเชนถูกออกแบบให้รายการทั้งหมดของทุกบัญชีต้องเปิดเผยสู่สาธารณะ
3) วิทยาการการเข้ารหัสลับทั้งกุญแจสาธารณะและกุญแจส่วนตัว

ทั้งหมดนี้แสดงให้เห็นว่าเทคโนโลยีนี้มีประสิทธิภาพ, มีความโปร่งใส, เชื่อถือได้และไม่สามารถปลอมแปลงได้ สกุลเงินดิจิทัลแรกที่ใช้เทคโนโลยีที่เรียกว่าบล็อกเชนคือ บิทคอยน์ในปี 2008 เทคโนโลยีบล็อกเชนนอกจากเป็นสกุลเงินดิจิทัลแล้ว สามารถนำไปประยุกต์ในด้านอื่นๆได้อีกมากมาย ถือได้ว่าเป็นเทคโนโลยีที่ทำให้อุตสาหกรรมต่างๆเกิดความปั่นป่วนอย่างมากมาย แต่เนื่องจากว่าสกุลเงินดิจิทัลไม่ใช่เงินตรา จึงไม่สามารถนำมาใช้กับนานาประเทศทั่วโลกได้ ซึ่งเป็นแค่หน่วยข้อมูลอิเล็กทรอนิกส์ที่สามารถนำไปประยุกต์ใช้กับกลุ่มๆหนึ่งหรือองค์กรๆหนึ่งเท่านั้น เช่นเดียวกับคูปองในโรงอาหาร นอกจากนี้ยังมีพระราชกำหนดที่ได้ตราขึ้นเพื่อการจัดเก็บภาษีเงินได้บุคคลธรรมดาจากเงินได้พึงประเมินที่ได้จากการถือหรือครอบครองโทเคนดิจิทัล (digital token) หรือการโอนคริปโทเคอร์เรนซี (cryptocurrecy) หรือโทเคนดิจิทัล

5.2 ข้อเสนอแนะ

ในการศึกษาครั้งนี้เห็นได้ว่าวิวัฒนาการของการธุรกรรมทางการเงินถูกพัฒนามาจนถึงยุคของการใช้ธนบัตรเป็นเงินตราและมีรูปแบบของการทำธุรกรรมออนไลน์ ไม่ว่าจะเป็นนวัตกรรมตู้ ATM ที่ช่วยให้คนกดเงินสดได้สะดวกเพียงแค่มีบัตร, บัตรเครดิต, การโอนเงินออนไลน์ เป็นต้น แต่การทำธุรกรรมดังกล่าวนั้นยังไม่มีประสิทธิภาพเท่าที่ควร

และมีปัญหาหลายๆอย่างเกิดขึ้น ยกตัวอย่างเช่นการปลอมแปลงธนบัตรหรือการแอบอ้างข้อมูล ซึ่งเทคโนโลยีบล็อกเชนในปัจจุบันยังอยู่ในช่วงเริ่มต้นเท่านั้น แต่ก็แสดงให้เห็นว่าบล็อกเชนเป็นเครื่องมือที่สามารถแก้ไขปัญหาเหล่านั้นได้ โดยเฉพาะองค์กรทางการเงินจะได้รับอิทธิพลจากบล็อกเชนเป็นอย่างมาก ในอนาคตสกุลเงินดิจิทัลอาจเป็นมากกว่าหน่วยข้อมูลอิเล็กทรอนิกส์ก็ได้และเส้นทางของเทคโนโลยีบล็อกเชนจะไปในทิศทางไหนนั้นจึงต้องติดตามกันต่อไป

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระเรื่องนี้สำเร็จรุล่วงได้ด้วยความกรุณาจาก ดร.บำรุง พ่วงเกิด ที่ให้คำปรึกษาแนะนำในการศึกษาค้นคว้าอิสระ การตรวจทานเนื้อหาการค้นคว้า และ ให้แนะนำในการแก้ไขปัญหาที่เกิดขึ้น ในระหว่างการศึกษาค้นคว้า จนสำเร็จลุล่วงไปด้วยดี 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..