A Peer-to-Peer ecosystem for trading cash equity

Youssef RAQUI, CFA
youssef.raqui@gmail.com

ABSTRACT

This document presents a functional description of a purely peer to peer version of the financial markets. The idea being to demonstrate the feasibility of trading financial instruments using blockchain technology, we will start by exploring the case of equity like assets before extending the scope to more complex products in coming publications. More than a simple distributed system to transfer cash, assets and investments risks, the solution will focus on preserving market integrity, security and privacy. This publication is hopefully the first of a series of articles and will only deal with the case of cash equity or shares trading.

ACTUAL TRADING PROCESS

In the actual process, buying and selling shares requires to register cash and a share trading accounts with a local custodian and maintain a good relationship with some brokers who will help execute market orders. For individuals, these two services are generally proposed by the same entity (e.g., Online Brokers)

To illustrate how a cash equity trade execution works, and for simplicity's sake, we will consider two investors A and B who are respectively willing to Sell and buy the same quantity Q of a share S at price P, we will call them respectively "OrderA" and "OrderB":

⓿ A contacts his Broker and gives him his order to sell Q quantity of S at price P. The same way B informs his broker that he's willing to buy Q quantity of S at price P.

❶ The two brokers place the orders in the exchange. These sell and buy orders will match as they are sharing the same details and the trade will be executed.

❷ The central counterparty clearing house (CCP) will receive the matched trade and reconcile the orders, Then it acts as a buyer to the seller and seller to the buyer (meaning that for clearing purposes, the clearing house will buy Q of S from invertor A and sells Q of S to Investor B, this is useful when an order matches against different counterparties and there is a need to aggregate the facing orders).

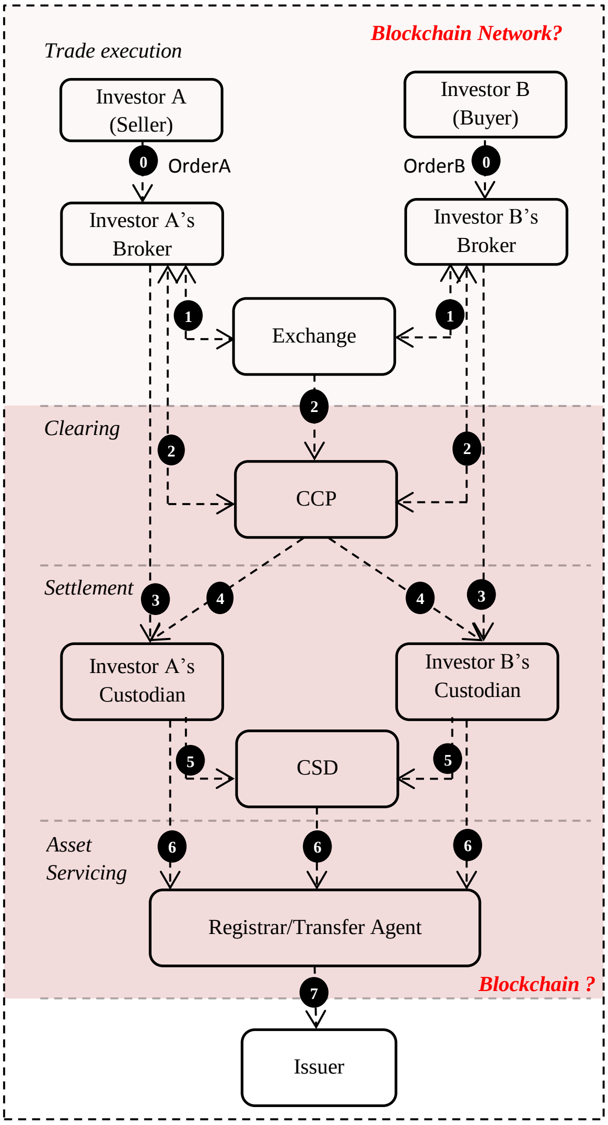


Figure 1: Actual equity trading process [1]

The local custodians, in charge of position keeping on behalf of their clients, will first ❸ be provided by trade details from investors A and B then ❹ will receive the confirmation from the CCP. The CCP will execute settlement or transfer cash and securities between custodians. Therefore, A's cash account (B's account) will be credited (debited) by an amount equal to P * Q and A's share account (B's share account) will be debited (credited) by Q.

❺Local custodians hold clients' assets in centralized custody via the Central Securities Depository (CSD). Custodian banks send trade details to the CSD which validates that trades details of both sides match and ensures that securities are correctly transferred between them.

❻Custodian banks and CSD leverage registrar's ledger to service securities for various corporate actions (e.g., dividend collections, shareholder communication, proxy voting, tax reporting)

❼Registrars (also called transfer agents) maintain up-to-date records of shareholders' information for issuers. They may also provide other services, including executing corporate actions, data analytics, and shareholders' communication/ voting/ meeting organization.

NB: for the sake of this study, we will give our definition of orders and transactions:

- *An order is issued by an investor and reflects his willingness to execute a trading strategy (e.g. investor A issues his order to sell Q of S at his target price P)*
- *A transaction happens when two orders match and are confirmed by the CCP (e.g. investor B's order will meet A's order, the CCP will verifies that the details of the two orders match. If it's the case the CCP will confirm the transaction)*

INTRODUCTION OF SOME IMPORTANT TOOLS

In this section, we will introduce two important tools to the construction of the peer-to-peer trading network: Cryptography and Blockchain.

Introduction to Cryptography

Cryptography is a very power tool to preserve privacy and security; hence it will be widely used in this solution.

Wikipedia definition [2]: "Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography"

To pictorialize, we will consider the classic example of two individuals Alice and Bob who are using internet network to exchange information and a third person Oscar (the intruder) who's trying to listen to their conversation. Alice would like to send her credit card credentials to Bob and fears that Oscar intercepts her message (this is what happens for example when you purchase goods online using your credit card). Therefore, Alice will use cryptography.

Let's consider the following notations:

- X : Plain message (Alice's credit card credentials)
- Enc : Encryption function
- Dec : Decryption function
- Ke: key used by Alice to encrypt the plain message X
- Kd: key used by Bob to decrypt the cipher (encrypted) message Y
- $Y = Enc_{Ke}(X)$: encryption of message X
⇨ $X = Dec_{Kd}(Y)$

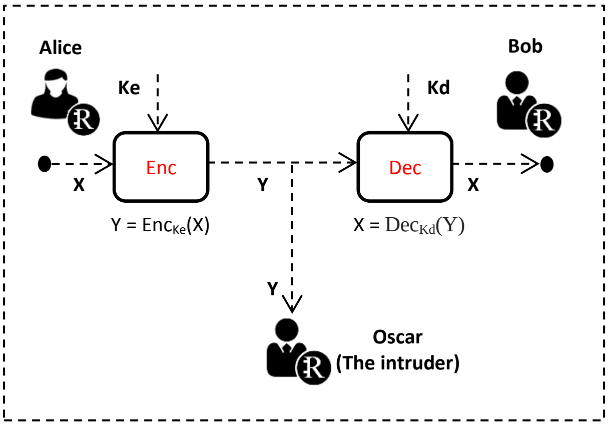


Figure 2: Encryption/Decryption scheme

Alice takes the plain message X = "Credit card credentials", encrypts it using the key Ke and send the cipher message $Y = Enc_{Ke}(X)$ to Bob. Y will look like a random message and will be very different from the plain message. All persons listening to the conversation like Oscar can see the cipher message Y, but only Bob have the right key Kd to decrypt it, hence only Bob can convert Y to $X = Dec_{Kd}(Y)$ = "Credit card credentials".

There are two major families of cryptography:

- Symmetric : When Ke = Kd
- Asymmetric: When Ke != Kd

NB: != means different from.

In this document we will only be interested in the asymmetric family or what is called public key encryption. In this case we say that Ke is the public key of Bob and Kd is the private key of Bob.

When Bob joins the network, he has to create two keys, a private key Kd that should be kept secret (only Bob will know it) and a public key Ke that will be visible by all other network participants, this way, if Alice wants to send a private message to Bob, she will get his public key Ke and encrypt the plain text before sending it.

Another important application of the public key cryptography is proving authenticity. Suppose that Bob is willing to transfer an amount of money to Alice, so he sends a message to Souka his banking agent asking her to perform the transaction. Souka has a doubt; she already faced the case where Oscar tried to initiate a money transfer on behalf of another client and wants to make sure that the transfer order comes from Bob. The solution is to use a digital signature:

- Bob creates a message X = ”Bob wants to transfer M amount to Alice”
- He encrypts his message X using Souka public key to create a cipher text Y.
- He then sign his message using his private key and sends “Y+Bob signature” to Souka
- Souka uses her private key to decrypt Y and gets X = ”Bob wants to transfer M amount to Alice”
- Then she uses Bob’s public key to check the validity of his signature. Note that if the message was from Oscar, he cannot sign it using Bob’s private key and the verification will fail

NB: You will notice the importance of keeping the private key secret. If Oscar finds out Bob’s private key, he can send and sign messages on his behalf.

In addition to encryption and digital signatures, this solution necessitates the use of two other powerful concepts: Homomorphic Encryption and Zero Knowledge Proof (ZKP).

Homomorphic Encryption [3]: is a form of encryption that allows computation on cipher texts (encrypted values), generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on plain values.

To illustrate the part we will use, consider the following:

- ***P*** the group of plain values on which we define some operation ^
- ***Q*** the group of encrypted values on which we define some operation ¤
- EncH/DecH : is an encryption system
- $(X_1, X_2) \in \boldsymbol{P}^2$ and $(Y_1, Y_2) \in \boldsymbol{Q}^2$ such that $(Y_1, Y_2) = (\mathrm{EncH}(X_1), \mathrm{EncH}(X_2))$
  ⇨ $(X_1, X_2) = (\mathrm{DecH}(Y_1), \mathrm{DecH}(Y_2))$

EncH is called homomorphic encryption if X_1 ^ X_2 is equal to DecH(Y_1 ¤ Y_2).

Example of homomorphic encryptions: El Gamal, Paillier, Goldwasser–Mical... [4].

Zero Knowledge Proof [5]: or Zero Knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a statement is true without revealing any information apart from the fact that the statement is true (e.g. Alice may want to prove to bob that an integer n_1 is superior than n_2 without conveying the values (n_1, n_2) [6]).

NB: If you don’t get Homomorphic Encryption and Zero Knowledge Proof you can still follow the lecture.

Introduction to Blockchain

Blockchain is a consensus-based secure distributed database (existing on various computers at the same time) which stores information immutably in the form of transactions over a peer-to-peer network. Its main characteristics are [7]:

⇨ *Data structure*: information is stores in the form of transactions which, when validated, are add to a block then to the blockchain

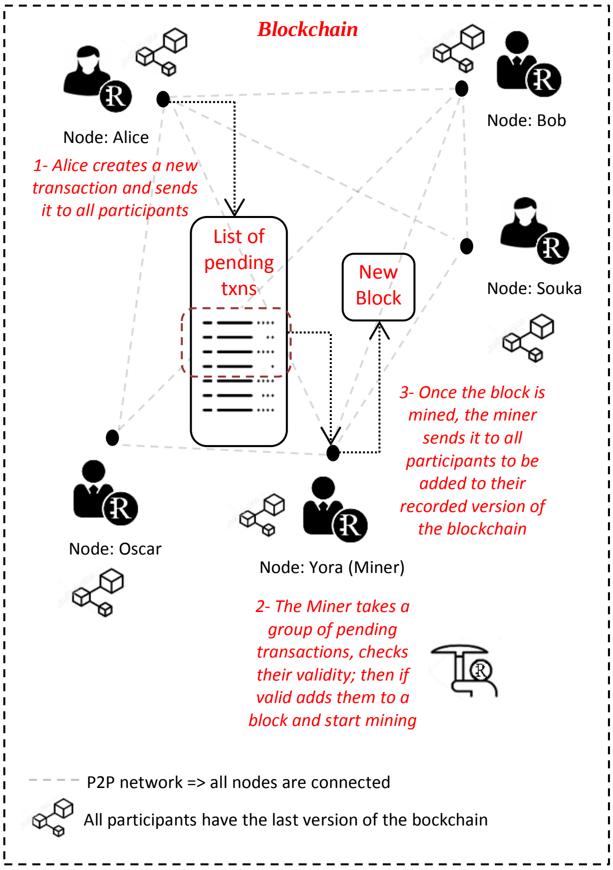

Blockchain
Node: Alice
Node: Bob
1- Alice creates a new transaction and sends it to all participants
List of pending txns
New Block
Node: Souka
3- Once the block is mined, the miner sends it to all participants to be added to their recorded version of the blockchain
Node: Oscar
Node: Yora (Miner)
2- The Miner takes a group of pending transactions, checks their validity; then if valid adds them to a block and start mining
P2P network => all nodes are connected
All participants have the last version of the bockchain

Figure 3: Blockchain/ Peer-to-Peer network

NB: in figure 3 only Yora is represented as a miner, however, in real world any participant can choose to be a miner. In this case, all miners compete on who will create the block first.

- ⇨ *Decentralized*: the ledger (data structure) is distributed among all participants (Peer-to-Peer network). hence, no need for a central third-party to keep records
- ⇨ *Public/private*: blockchain can be either public (Permission less: everyone can join the network) or private (Permissioned: closed ecosystem where only authorized individuals can join the network). In our case we will be interested in the Permission less family
- ⇨ *Highly secured*: the records (blocks) are immutable, meaning that once added to the blockchain they cannot be amended without altering all subsequent blocks.
- ⇨ *Cryptography*: is used to preserve integrity and security. All transactions are signed to prove authenticity and all blocks are protected by hash codes
- ⇨ *Consensus-based algorithms*: all nodes are adhering to a protocol for inter-node communication and validating new blocks.

NB: the term node will be used later and is functionally equivalent to say a participant in the blockchain (e.g. node Souka in figure 3).

Example of Blockchains: Multichain, Ethereum, Hyperledger…

INTRODUCTION TO THE PEER-TO-PEER TRADING SOLUTION

The objective of this document is to study the feasibility of applying the same functions and services mentioned in the first section to a decentralized network (peer-to-peer network), specifically, we will try to demonstrate that two investors A and B can exchange a quantity Q of share S at a price P without going through a clearing house, local custodians or a CSD and by preserving security and privacy. Moreover, their cash, share positions and corporate actions will be managed by the blockchain in an encrypted manner.

The general idea

For simplicity's sake, we will call our solution the "***Blockchain Trading Network (BTN)***" and the crypto money used the "***R-coin or R_{coin}***" Ⓡ (from now on cash = R-coin).

- All participants to the BTN are represented by Nodes. Each node will have a unique identifier and a unique address called public address "PubA".
- The participants will pay, buy and sell shares using the R-coin which will have a market value (meaning the price P = n*R_{coin})
- Nodes can be defined as one and only one of the following profiles: investor, broker, dealer or clearing node (Only a limited number of nodes can be defined as clearing nodes, more on that later)
- Investors, dealers and brokers may create orders, however, only the clearer may match them and create transactions (more on that later)
- Investors and dealers will need a wallet consisting of a cash and share accounts, the others will mainly need a cash account to be paid.
- The cash state, equity state, orders and transactions will be encrypted in order to preserve privacy. All orders/transactions will be signed by their issuer in order to assure authenticity.
- Custody, cash/asset transfer and corporate actions will be managed by the BTN.
- Issuers/regulators may interrogate the blockchain access data they need within the limits of rights that will be granted to them. Consequently, they have to join the BTN as special nodes (this part will not be covered by our study)
- All nodes can choose to be Mining nodes or Memory nodes (nodes which stock and maintain the blockchain); they will be compensated by new created R-coins.

NB: only trade execution, clearing and settlement will be covered by this document; asset servicing is out of scope.

Centralized VS decentralized trading process

The table below compares the main features of centralized and decentralized trading processes from an investor's perspective. These differences are the main challenges to outpace in order to construct a functional and trustworthy ecosystem.

Features	Centralized	Decentralized
Prerequisites	• Investors have to create cash and share accounts with a custodian • Investors have to fill in a KYC with their brokers	• Investors join the blockchain as nodes • A wallet consisting of cash and share account will be automatically created and kept on the blockchain • It's difficult to perform controls (KYC) on investor's identity/profile • All nodes will have a unique identifier, a unique address and public/private keys. They will also have to keep their private key secret

Trade Execution	- Investors communicate their orders to the broker using phone or electronic messages - The orders should be recorded to avoid conflicts - Investors may agree on bilateral deal without going through a broker (OTC trade) - Privacy: Only the issuer, clearing house, custodians and eventually the broker know about Orders	- Investors have to send their orders through the blockchain network whether they go through a broker or a bilateral (OTC) trade - Orders should be signed by the issuer (verifiable by other nodes) in order to preserve authenticity and security - Cryptography will be used to preserve market privacy *NB: When you invest, you don't want others to figure out your strategy or what's in your portfolio)*
Clearing (CCP)	- Clearers are selected by regulators according to financial criteria - clearers should be very trustworthy - Clearers match the orders and act as a counterparty to the parties of the trade (to avoid default risk)	- Any node can pretend to be a clearing house. However ,only a limited number of clearers will be authorized (we will expose the logic behind this decision later) - Clearing may also be managed by smart contracts (this case is not covered by our solution) - Clearing nodes are selected by consensus according to financial and **IT** criteria - Clearing nodes do not need to be very trustworthy. Cryptography will be used to ensure trust - Clearing nodes will only match the trades, the default risk will be managed by the blockchain (this holds only for cash equity trades with no leverage) - Only clearing nodes will be allowed to issue transactions when orders do match
Settlement	- Local custodians manage cash and share accounts for their clients - Investors send the trade details to their local custodians - CCP send the trade confirmation t to the local custodians - CCP manage the transfer of assets and cash - The local custodians send the details to the central custodian (CSD) for further validations and position keeping - Privacy: Only the investor, local custodians and CSD will have details about cash and share accounts	- In order to be valid and included in a block, transactions have to be approved by Minors - Transfer of cash and shares will be managed by minors - The state of cash and share positions will be managed by the blockchain in an encrypted manner (to preserve privacy) - The state will be immutable meaning that we can only append new operations, no modification will be possible - The acceptance of a new created block will be done following rules of the consensus (to avoid a malicious Miner)
Asset Servicing	- maintain up-to-date records of shareholders' information for issuers - executes corporate actions, data analytics, and shareholders' communication/ voting/ meeting organization	- The issuer may interrogate the blockchain to have the state of shareholders - Proxy/voting may be managed by the blockchain - Corporate actions may be managed in the blockchain through smart contracts or special nodes (Asset servicing will not be covered by this study)
Market participant needed	- Investors - Brokers - CCP - Local custodians - CSD - Transfer Agent - Issuer	- Investors - Brokers - Clearing nodes - Issuer - Miners

Table 1: Centralized Vs Decentralized trading process

NB: in our solution we have reduced the role of clearing nodes to matching orders; the reason is that we are dealing with the simple case of trading cash equity products. In next publications, we will evoke more complex products, especially derivatives, and their role may expend to margin call and trade life cycle management.

BLOCKCHAIN TRADING NETWORK (BTN) CONSRUCTION

To illustrate in an easy way the construction of our target trading system we will go back to our example of investors A and B who are respectively willing to sell and buy a quantity Q of share S at a price P. First A and B must create their accounts to join the blockchain network (Join the network as nodes).

Account creation:

In order to trade on the BTN, investors A and B must have a unique identifier, a unique address, a private & public keys (to communicate and sign their orders) and a wallet consisting of cash and share accounts for position keeping.

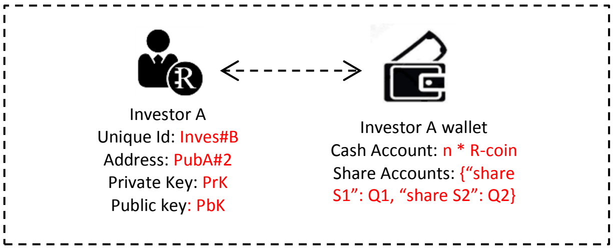


Figure 4: Investor account creation

In the same way brokers, dealers and clearers will create their accounts to add their nodes to the network. Please note that each address/ identifier will be associated with one and only one profile and one and only one account. Therefore, if investor A is willing to participate as an investor and as a broker, he will have to create two separate accounts.

Trade execution:

I do not believe that blockchain technology will have a big impact on the trade execution process, except that the orders have to be encrypted, signed and issued via the blockchain network. In our case, we will use the BTN network to create secure a communication channels.

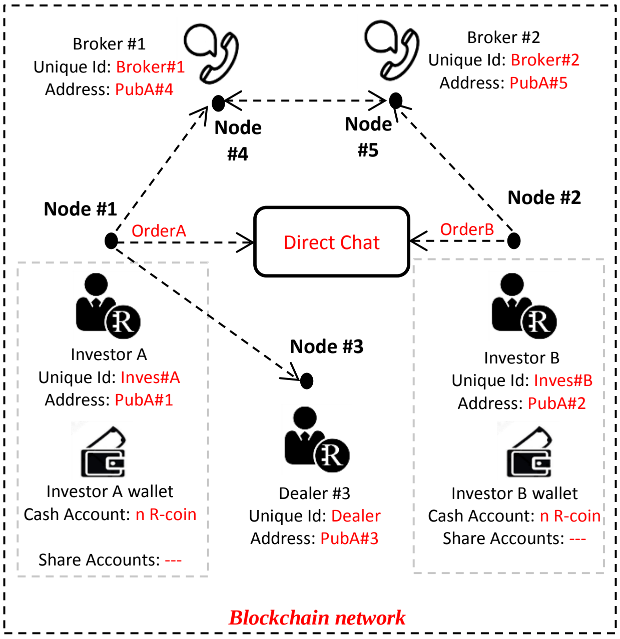


Figure 5: Trade execution process on BTN

When two investors agree on a deal without going through an exchange (e.g. using direct chat as in the figure above) we say that the trade is OTC or over the counter. From here, and for simplicity stake, we will only consider this case, meaning that investors A and B have agreed on their deal via direct chat.

Clearing:

Now that A and B have agreed on their deal, they have to choose a clearing node and send trade details for matching:

⇨ A sends OrderA:

Party	Ctpty	Direction	Qtity	Price	Asset	Signature
A	B	Sell	Q	P	S	SignA

⇨ B sends OrderB:

Party	Ctpty	direction	Qtity	Price	Asset	Signature
B	A	Buy	Q	P	S	SignB

NB: Communications between A, B and the clearing node should be encrypted to protect against other participants listening to their transactions.

Once clearing nodes receive the orders, they:

- Validate the authenticity of the issuer by verifying signatures
- Verify that the orders' details do match
- Check that each leg of the trade has the required amount of R-coins (cash) and quantity of shares (may be done using ZKP assuming that clearing nodes do not keep records of a plain state)
- Send the orders to all other clearing nodes to inform them of the ongoing transaction (to avoid double spending, we will come back to that later)
- Check that there is no other ongoing conflicting transaction, to avoid double spending (e.g. we want to make sure that A is not trying to sell the same shares to another investor at the same time)

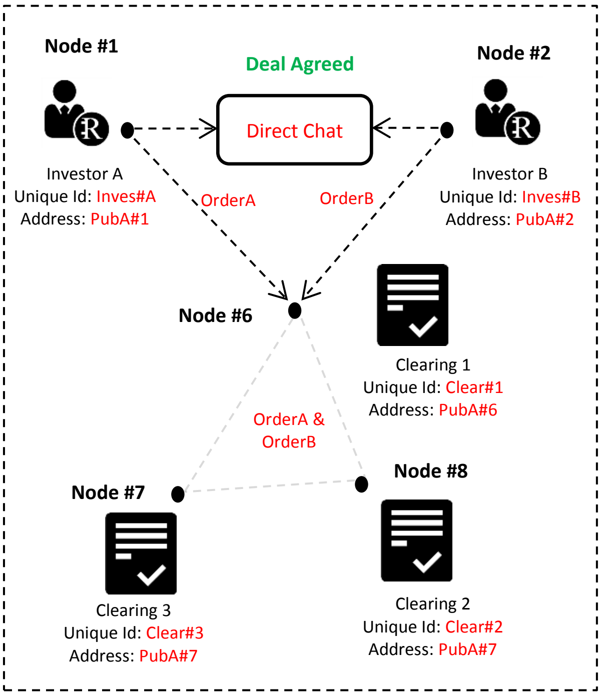


Figure 6: Clearing process

If the orders pass the checks successfully, the clearing node issues the following transaction:

⇨ Clearing node issues TxnAB:

Seller	Buyer	Qtity A	Qtity B	Price A	Price B	Share	Sig A	SigB	Sig Clearing
A	B	EncH$_A$(Q)	EncH$_B$(Q)	EncH$_A$(P)	EncH$_B$(P)	S	SignA	SignB	Sign CLR

EncH is a homomorphic encryption.

The transaction above will be added to the list of pending transactions waiting for settlement. A transaction is confirmed if and only it's included in the blockchain, otherwise, it's pending.

NB: for simplicity's sake we chose to encrypt the quantity and price only, but in real word we may also encrypt investors' identities and exchanged share's identifier.

NB: you may wonder why we are using clearing nodes in the case of cash equity trading. If you think about it, the minors can do the job! They can match the orders before creating and including transactions in a block. We are doing it to avoid order matching problems and double spending (we will explain these two points after next section).

Settlement:

Now that the transaction TxnAB was added to the list of pending transactions, the minors come into play:

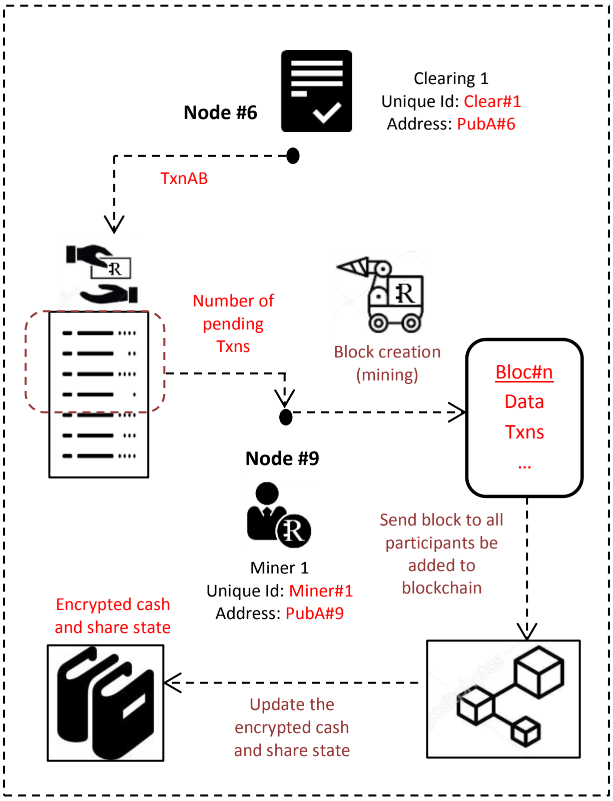
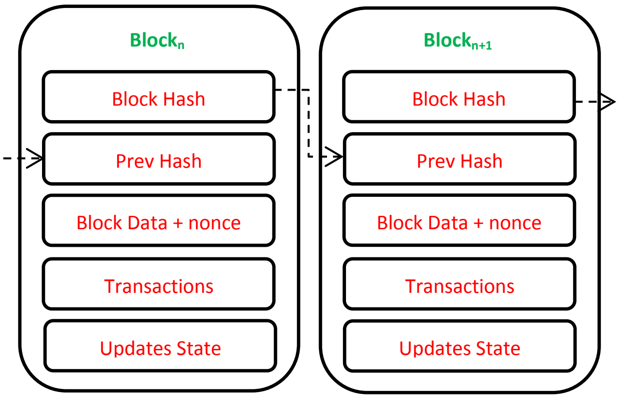


Figure 7: Settlement process

The minors choose a bunch of transactions and perform the following controls:

- Verify that the signatures of investors A, B and the clearing node are valid (Authenticity)
- Verify using Zero Knowledge Proof that the two legs of the trade have the required R-coins (cash) and quantity of share S
- Verify using other controls that the clearing node didn't manipulate transaction details (reliability)

If the transaction passes the checks, the minors update the cash and share states using homomorphic properties of the encryption. The Transactions and the updates state are then included in a block and, after mining (bloc creation), are added to the blockchain => TxnAB is confirmed.



NB: the updated state in the last created block will be used by minors for zero knowledge proof verification of pending and coming transactions.

Why do we need clearing nodes for cash equity trading?

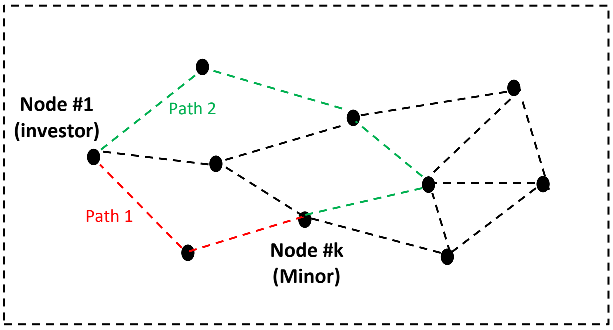


Figure 8: simplified Peer-to-Peer network

Saying that in a blockchain network all participants are connected is an exaggeration. In fact, it's technically almost impossible to connect with all nodes in a peer-to-peer network unless it's very small. What's in real world is that a node is connected to a limited number of nodes which are connected to a number of nodes and so on.

As you can see in figure 8 there are 2 paths node #1 (the investor) can use to reach node #2 (the minor). You will also notice that path 1 is shorter than path 2, hence if clearing nodes do not exist (meaning that minors are in charge of order matching and transaction creation) some issues will rise:

Double spending: if node #1 is a malicious investor, he may for example send order#1 selling a Q quantity of share S to investor B via path 1, and then send a conflicting order#2 selling the same shares to investor C via path 2. The minor will receives order#1 first; he may manage it before receiving the conflicting order#2. Therefore, the transaction with investor B will be validated while that of investor C will be rejected causing an opportunity cost.

The use of a limited number of clearing nodes and the technical criterion of being all connected for instant communication can resolve this issue.

Order matching problems: The fact that some paths are longer than others may cause delays or problems in the reception of orders, in other worlds, the minor can receive order details from investor A and spend a long time before receiving those of investor B. Also, if A and B make the same deal a second time, the orders may collide.

The use of a clearing node can resolve this issue as investors A and B agree on a clearing node and send instantly their order's details for matching.

CONCLUSION

We presented a functional description of a peer-to-peer ecosystem for trading cash equity assets, said differently, we have demonstrated that investors A and B can exchange assets without going through CCP, custodians, CSD or other central institution. We didn't cover asset servicing or regulatory constraints; they also can be managed by the BTN if the issuer and regulators are part of the blockchian. However, adding more features generates more technical and cryptographic challenges.

The applications of blockchain technology to the investment industry are at an early stage; therefore, there are many aspects like applied market regulations, managing equity's static data, corporate actions and maintaining relationships with issuers that make the implementation of a peer-to-peer trading solution very difficult for cash equity assets. In the next publication, we will study the case of a more practical product called contract for difference (CDF) on equity assets.

REFERENCES

[1] European Central Bank, World Economic Forum, Richard Gendal Brown (R3), Moody's Investor Services

[2] Cryptography from Wikipedia, https://en.wikipedia.org/wiki/Cryptography

[3] Homomorphic Encryption from Wikipedia, https://en.wikipedia.org/wiki/Homomorphic_encryption

[4] Homomorphic Encryption and Applications from Yi, Xun, Paulet, Russell, Bertino, Elisa

[5] Zero Knowledge proof from Wikipedia, https://en.wikipedia.org/wiki/Zero-knowledge_proof

[6] Comparing encrypted data from Thijs Veugen

[7] Les Blockchains - De la théorie à la pratique, de l'idée à l'implémentation from de Billal CHOULI, Frédéric GOUJON, Yves-Michel LEPORCHE