Does Blockchain mean higher transparency in the financial sector?

Amera Ibrahim
What is blockchain?

- Blockchain known to be a type of Distributed Ledger technology (DLT)
- Created in 2008 by Satoshi Nakamoto
- It is a combination of distributed timestamping, digital signatures, P2P networking, cryptographic hashing, Merkle tree, in addition to others
Transactions data are hashed and encoded into a Merkle tree. Each block contains a cryptographic hash of the previous block and a timestamp linking blocks together and forming a chronological chain.
How it works?

Systemic effect

Manipulated Block!

PEER A

Block: # 1
Nonce: 11316
Data: 
Prev: 00000000000000000000000000000000
Hash: 0001543b764259d38201

Block: # 2
Nonce: 35230
Data: 
Prev: 00015783b764259d38201
Hash: 00012ea9b916eb7e0788e68

Block: # 3
Nonce: 12937
Data: hello
Prev: 000013f9a9b916eb7e0788e68
Hash: 947809f9a07c4076b

Block: # 4
Nonce: 35990
Data: 
Prev: 947809f9a07c4076b
Hash: 9762853c403aa8d26

PEER B

Block: # 1
Nonce: 11316
Data: 
Prev: 00000000000000000000000000000000
Hash: 0001543b764259d38201

Block: # 2
Nonce: 35230
Data: 
Prev: 00015783b764259d38201
Hash: 00012ea9b916eb7e0788e68

Block: # 3
Nonce: 12937
Data: 
Prev: 000013f9a9b916eb7e0788e68
Hash: 947809f9a07c4076b

Block: # 4
Nonce: 35990
Data: 
Prev: 947809f9a07c4076b
Hash: 9762853c403aa8d26

ACCID

EAE Business School
We make it happen
Public key & private key

• Public key is associated with digital identity of participants in the system and it’s entirely different from the private key, and there’s no way to extract the private key from it, therefore, it can be published.

• The private key is used to authorize transactions by the owner of the account, this key is used as a validation signature to process transactions by the owner.

• Miners cannot transfer assets or records without the consent (i.e. digital signature) of the owner, manipulation or fraud can be detected immediately by other nodes.
Transaction validation process

Someone requests a transaction

The requested transaction is broadcasted to a P2P network consisting of computers, known as nodes

The network of nodes validates the transaction and the user's status using known algorithms

A verified transaction can involve cryptocurrency, contracts, records or other information

The transaction is complete

The new block is then added to the existing blockchain, in a way that is permanent and unalterable

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger

Image source: https://www.ecoinnomy.com/blockchain/
Double-spending problem
Costs associated with the centralized system

- Cross border payments are costly and time consuming
- Transactions in the foreign exchange market alone sum up to a total of $4.8 trillion on a daily basis
- Remittances market has been witnessing global growth since 2016 from $601 billion to $616 billion in 2018
- The cost of financial fraud has been estimated to more than $4 trillion in 2016 alone. In order to guarantee a transactions authenticity, intermediaries such as courts, lawyers and auditors are needed to verify and detect any misbehavior
Potential in the financial industry (1/2)

Blockchain technology is associated with a reduction in two key costs:
The **cost of verification**, and the **cost of networking** (Catalini and Gans, 2016).

- Costs associated with verifying transactions on a distributed ledger are almost down to zero
- The second statement is emphasizing the concept of no third parties are needed for verification
Potential in the financial industry (2/2)

• Blockchain reduces transaction costs that range from 5-20% to less than 1% where a reduction of only 5% will result in $16 billion in annual savings.

• Blockchain presents significant reduction in processing and bookkeeping around 50%-80%

• A report by Santander estimated savings of up to $20 billion per year for banks by 2022

• Utilizing this technology in the banking sector has the potential of increasing profits significantly by increasing their efficiency and automation.
Share X now belongs to A
Conventional transaction clearance

Blockchain-based transaction clearance
Banking industry

• Head of Santander InnoVentures, informed that they have further identified 20-25 use cases where the underlying technology can be applied in the banking industry, including:

  - Corporate payments
  - Crowdfunding
  - SME post-trade operations
  - Share registry
  - Cross border remittance and Foreign Exchange

• Central banks have observed great appeal in this. However, they are more hesitant to issue a virtual currency that will consequently narrow the banking system that could potentially lead to making sections of the financial industry “redundant”
Types of blockchains

- Public blockchain
- Private blockchain
- Consortium blockchain
- Federated blockchain

The New Networks

Centralized  Decentralized  Distributed Ledgers

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions (‘mining’)

- Users are anonymous
- Each user has a copy of the ledger and participates in confirming transactions independently

- Users are not anonymous
- Permission is required for users to have a copy of the ledger and participate in confirming transactions
Public blockchain (1/2)

- Public blockchain is a decentralised platform that has no restriction on participation, reading, processing or submitting transactions to be incorporated in the blockchain.

- Users are free to participate and create blocks of transaction and get involved in the validation/mining process.

Public blockchain (2/2)

Pros:
• Everyone can access and download a copy of the ledger
• Trustlessness
• Distributed authority
• Security is maintained and updated by the network
• Immutable records
• Transparency

Cons:
• Anonymous identities
• Ability to commit illicit activities
• Irreversibility of transactions or modification once a block has been added to the chain
• Electricity consumption of the consensus algorithm is equivalent to Austria
Consortium blockchain (1/2)

A consortium blockchain is partially private blockchain, where direct access to data and submission of transactions is restricted to a specified list of entities with known identities who are allowed to process transactions. Permissioned blockchain is divided into three tiers of accessibility:

1. Users are only able to access transactions that directly involve them.

2. Restrictions based on both creating new blocks of transactions and proposing new transactions to be included into the blockchain.

3. Restriction to a limited number of institutions such as Banks, granting their clients access to read their transactions to guarantee the safety of the client’s funds (full access is granted to central parties).

Central Banks or legal entity

Transaction is validated by the Banks and legal entities

- Inserts the Public key of the receiver
- Amount to be paid
- Signs the transaction with her private key

- Decrypts the message using his private key and receives the money

Receiver B

Payer A

Embedded text: permissioned Blockchain transaction

Central Banks or legal entity

Transaction is validated by the Banks and legal entities

- Inserts the Public key of the receiver
- Amount to be paid
- Signs the transaction with her private key

- Decrypts the message using his private key and receives the money

Receiver B

Payer A
Consortium blockchain (2/2)

Pros:
• Partial centralization will result in validation efficiency
• Reduction in transactional costs
• Modification can be implemented (data is not immutable)
• Elimination of power consuming economic game

Cons:
• Accessibility is centralized restricted to certain parties of the organization
• Modification and validation is restricted to central authority
• Level of security is low in comparison to public blockchain
• Flexible transparency
Private vs Public blockchains

- Reduction of intermediaries will be significant, but not eliminated
- Depends on certain entities criteria
- Cryptocurrencies
- Transparency
- Limited Access to read, write, and participate
- Mining: Private blockchain is questionable, potential recentralization or semi-centralized
- Immutability
- Decentralization

Unlimited access to read, write, and participate depends on certain entities criteria. Reduction of intermediaries will be significant, but not eliminated. Cryptocurrencies and transparency are key features of blockchain technology. Private blockchain mining is questionable due to potential recentralization or semi-centralized structures. Immutability and decentralization are essential properties of blockchain technology.
Blockchain’s misconceptions

• One of the strategies used by the notorious investment bank Lehman brothers was to run two parallel ledger to hide their debt and overestimate the value of their assets to deceive regulators and the.

• The existence of blockchain back then would have helped with the maintenance of records in order due to scalability limits of the existing bookkeeping system as Lehman’s balance sheets grew in complexity and tracking records of assets to their origin became extremely obscure.
Consortium blockchains & financial institutions

• A permissioned blockchain can aid central banks in the process of decision making and managing monetary policy.

• The platform will allow for the central bank to make a clear precise decision based on the transparency provided such as monitoring the impact of lowering interest rates.

• Regulators can also have access and monitor the performance of banks to see whether banks are taking on excessive risk and the possibility of an upcoming credit crunch.
Regulations & legal issues

• Judicial problems arise due to the anonymity of the bitcoin miners
• Agreeing to the level of transparency provided by DLT raised two main issues:
  - Data privacy
  - Insider trading and market abuse
• **Data privacy**
  - The distribution of private data under some jurisdiction are subject to heavy penalties for violating the data protection laws.
  - Once inaccurate or private data is stored on a DLT it would be extremely difficult if not impossible to delete.
  - Immutability contradicts the human’s right law “the right to be forgotten”, victims instead will turn to damages compensation instead.
  - Difficulty in halting fraudulent transfers or removing them from the chain after they are posted.
  - Tampering data prior to being stored on blockchain.

• **Insider trading and market abuse**
  - The ESMA (European Securities and Market Authority) is concerned with the transparency and public features of Blockchain that may allow and ease the process for unlawful acts concerning excessive manipulation of records, recent trades, inventory levels and manipulation of prices.
Cyberattacks

- MTGox, a Japanese bitcoin exchange, reported a hack that resulted in a total loss of 850,000BTC. The loss amounted to $473 million when the declared bankruptcy.

- The Luxembourg and London based Bitstamp suffered a loss around 19,000BTC, that is, $5.1 million
• Ease of traceability with public keys lead to the creation of HD wallets that generate new public key for every transactions in order to increase anonymity

• The decentralized nature and lack of supervision has allowed for this technology to be an easy way for buying illegal drugs and weapons on the dark web e.g. *Silk Road*
Transparency

Transparency in blockchain defines the ability to view public addresses where you will be able to access transaction history, assets, etc without limitations or boundaries. Which has never existed within the financial system.

- Consortium blockchains are not as transparent as public.
- Law clashes with the technology due to anonymity.
- Transparency can be greatly decreased or even eliminated by setting accessibility and viewing restrictions.
- The consensus power consuming algorithm poses centralization threats.
Blockchain increasing transparency?

• The incentive mechanism is authenticating the legitimacy of the fund transfer of the transacting parties without any additional information regarding identity, location or the source of funds.

• The technology appears to promote controlled tailored transparency enabling its users taking full advantage of handling their accounts and transactions

• In a private blockchain, the same public key will need to be utilized in order to link the account to the owner, otherwise transparency will turn into opacity and tracking the account will be nearly impossible, and more challenging than the existing system.

• Both private and public blockchains require regulation in order to impose transparency
Several banks are hesitant with experimenting/adopting the technology due to:

• Compatibility and efficiency
• Initial investment requirement
• Changes and upgrades requirements
• Existing systems and operations
• Maintenance, regulation and control
Conclusion

In this example, a Private Intranet is performing the tasks of the Internet but is not accessible to outside connections.
Thank you for your attention!