BLOCKCHAIN

A Financial Regulatory Cryptogram

Dr. Evan C. Gibson

June 2022

A Financial Regulatory Cryptogram?

Cryptogram:

- A puzzle involving code
- Text transformed into code

The challenge of regulating blockchain technology, which is designed around cryptography, in the financial sector

Outline

- Applications
- Design Considerations
- What is Blockchain?
- Types of Blockchain
- A Financial Regulatory Cryptogram
- Research: Moving Forward
- Q & A

Applications

- Blockchains are being promoted as a financial system revolution
- New and proposed applications, for example:
  - Trade finance
  - Payment systems
  - Settlement and clearing
    - Relatively slow implementation

Design Considerations

- Blockchains are not generic
  - Type of blockchain
  - Technological design

Design Considerations

- Fundamental question - why use blockchain?
  - Factors influencing the design
    - Financial markets and behaviour
    - Legal and regulatory objectives
    - Legal and regulatory parameters
      - Fit for the purpose?

What is Blockchain?

- Distributed ledger technology (DLT)
  - A distributed network of computers or a computer system
  - Record, disseminate and validate data across the network / system
- A blockchain is a type of DLT with specific qualities:
  - Shared database arranged in a chain structure
  - Consists of blocks that are chained in a chronological sequence
  - Each block represents a ledger - a digital account of transaction data

What is Blockchain?

- Data stored across a chain of computers
- Together forms digital database infrastructure
  - Continuously distributes, validates and stores data
  - Ensures that the blockchain is accurate and up to date

Cryptography

- How does the blockchain ensure that the data is accurate?
  - Cryptography:
    - Security protocols to protect data from being compromised
      - Third parties and corrupt nodes
    - All transactions and blocks across the network are
      - Connected and protected by cryptography

Cryptography

- Several different types of cryptography
  - For example:
    - Key cryptography
      - Digital signatures
    - Hash function
    - Consensus mechanisms

Key Cryptography

- Symmetric Key Cryptography
  - One algorithmic key to encrypt and decrypt
  - Fast
  - Requires sharing the key
    - Transferring the key can undermine security

Key Cryptography

- Asymmetric Key Cryptography
  - Two algorithmic keys
    - Private and public key pair
  - Managed by blockchain software
    - Held in a digital wallet

Key Cryptography

- Asymmetric Key Cryptography
  - Public key
    - Anyone can view the public key
    - Represents the owner of the public / private key pair
    - To send transactions to the key pair owner
    - Used by the key pair owner to receive transactions
    - Similar to a public email address and a bank account number

Key Cryptography

- Asymmetric Key Cryptography
  - Private key
    - Provides control over the public key
      - Encrypts and decrypts transactions sent from the public key
    - Generates a digital signature
      - Used to sign and send transactions from the public key
    - Similar to a password and signature

Digital Signatures

- Identifies a key pair holder for both a transaction sender and recipient
- For a transaction, verifies
  - Key ownership
    - The authenticity of the data sent
    - That a transaction is legitimate
- One digital signature corresponds to one transaction

Digital Signatures

- Trusted identity system
- Proves that a person owns a private key without having to reveal the private key
- Consist of two parts:
    1. Signing - using the private key to generate a digital signature
    2. Verifying - using the public key to verify that a digital signature has been generated from a private key

Verifying Digital Signatures

- Matching the hashes produced by a key pair for a transaction
  - If the signature is not verified, the transaction will be rejected
    - Transaction is void
    - If necessary, the algorithm performs restitution
    - Not recorded on the blockchain
  - If verified, the transaction is provisional and unconfirmed (i.e., unvalidated)

Hash Function

- Transactions are hashed by a one-way cryptographic algorithm
  - Transformed into a fixed length output - hashing
    - A hash is almost impossible to reverse engineer (i.e., change)
  - Every block (and transaction) is assigned a hash value
    - Each block records the hash of the preceding block in the chain (c/f genesis)
      - Connects the blocks in the chain together

Hash Value

- Identifies the data held in each block
  - Every block's hash value is different (i.e., collision-free hashing algorithm)
  - A block should always have the same hash value
    - Any changes to a transaction will be reflected in the block hash value
      - Compare a block's hash value with the next block (i.e., audit trail)

Consensus Mechanisms

- Transactions are not validated until there is consensus
  - Reach an agreement on the state of the network
  - Once a block reaches its fixed length, adds the next block to the chain

Consensus Mechanisms

- Different types have different features
  - Security and resilience levels
    - Fault tolerance
      - Continue functioning despite node failure or malicious activity
  - Transaction settlement times
  - Transaction costs
    - Energy usage

Consensus Mechanisms

- Mechanisms vary depending on the type of blockchain and its functionality
  - Some examples:
    - Proof-of-work
    - Proof-of-stake
    - Proof-of-elapsed-time

Blocks in the Chain

- Blocks are validated and authenticated by the consensus protocol
- Data contained in a block is not generic
- Consists of two parts:
  - Header: metadata
  - Body: input data

Blocks in the Chain

- Metadata:
  - Software version
  - Root hash (used to calculate the hash value)
  - Parent block hash
  - Other information to function
    - E.g., time stamp, consensus goal

Blocks in the Chain

- Input data
  - Ledger of transaction data
  - Merkle tree structure
  - Transactions are hashed
  - A pair of hashed transactions represents a leaf
  - A pair of leafs are consolidated into a parent leaf

Types of Blockchain

- Public
  - Decentralised
- Private
  - Centralised
- Consortium
  - Private
- Hybrid
  - Public with private / Private with public

Types of Blockchain

- Distinguishing Features:
  - Access
    - Permissionless, permissioned or hybrid
  - Degree of centralisation
    - Public, private or hybrid
  - Cryptography

A Financial Regulatory Cryptogram

- Fundamental questions need to be addressed:
  - Does the technology provide any distinct advantages over the status quo?
    - Are the advantages sufficient to justify changing the status quo?
    - What are the trade-offs?
      - What financial market weaknesses are introduced by the technology?
      - Risks (e.g., technology-based); design flaws; market inefficiencies and behaviour

A Financial Regulatory Cryptogram

- Fundamental questions need to be addressed:
  - Are existing financial regulatory frameworks fit for the purpose?
    - If not, what amendments or new regulatory frameworks are needed?
  - Will financial regulations shape the blockchain design?
  - Will RegTech or SupTech influence the design?

A Financial Regulatory Cryptogram

- Viability
  - Determine whether blockchain is a viable alternative
  - Where viable, each application will need to be tailor made
    - From a technological standpoint
    - From a legal and financial regulatory standpoint
    - Business case - satisfy a cost / benefit analysis

A Financial Regulatory Cryptogram

- What we do know:
  - Not merely an application of the law to determine viability
    - Requires a holistic approach
    - Intersection between technology, finance and regulation
  - Financial market infrastructure is being redesigned
  - In most cases financial regulatory frameworks will need to be redesigned

Research: moving forward

- Research focuses on the regulation of financial markets
  - From a technological, financial and legal perspective
    - Interdisciplinary comparative analysis
  - Determine both viable use cases and unviable designs
  - Appraise the parameters and limitations of current financial regulatory frameworks
    - Domestic and cross-border
    - Propose regulatory amendments and / or new regulatory frameworks
      - Is there a role for RegTech or SupTech?

Q & A