BLOCKCHAIN TECHNOLOGY 101

Usman M. Sheikh (National Head, Blockchain & Smart Contracts)

2018 CLS Annual Compliance Conference – November 2018

GOWLING WLG

SIGNIFICANT IMPACT

- "You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990's." **– *Blythe Masters***
- "The technology likely to have the greatest impact on the financial services industry and the world of business has arrived." **– *Blockchain Revolution***
- "Financial Institutions are early adopters. It is estimated that 80% of banks are working on blockchain projects. … [B]lockchain will transform the world." **– *Ginni Rommetty, IBM***

WHAT IS BLOCKCHAIN TECHNOLOGY

- **LEDGER –** At its core, a blockchain is just a digital ledger or database of transactions ("distributed ledger technology" or "DLT")

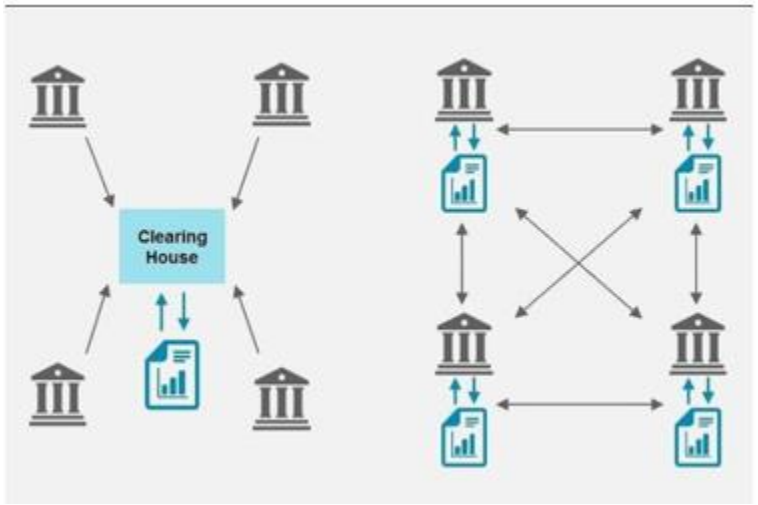
- **CONSIDER THE IMPORTANCE OF LEDGERS IN YOUR LIFE –**

  1. Bank Transactions
  2. Stock Transactions
  3. Real Estate Transactions
  4. Etc.

- **CRITICAL ELEMENT TO EACH OF THESE LEDGERS –** A trusted third party intermediary**.** Especially required for digital transactions: problem of double spend.

HOW IS THIS LEDGER UNIQUE?

- **NO NEED FOR A TRUSTED THIRD PARTY –** A ledger that allows transactions directly from one party to another without going through a trusted third party (e.g., a financial institution). Trust via cryptographic proof (not via third party).



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

GOWLING WLG

DISINTERMEDIATION

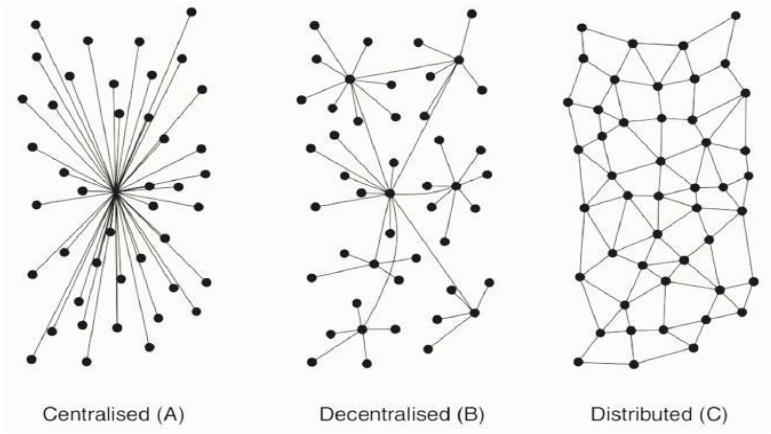
- "The blockchain protocol threatens to disintermediate almost every process in financial services." **– *World Economic Forum***
- "If the banks don't change, we will change the banks." **– *Jack Ma / Alibaba Group***
- "Banks may face a 'Kodak moment'" – ***former CEO / Barclays***

THE TECHNOLOGY

GOWLING WLG

HOW DOES IT DO THAT?

- **DISTRIBUTED –** There is a distributed digital master ledger of transactions and assets that is shared among participants in the system (“nodes”)



- **TRANSACTION VALIDATED BY CONSENSUS –** For any new transaction, the master ledger can only be updated by consensus of a majority of nodes.

GOWLING WLG

HOW DOES IT DO THAT?

- **ACHIEVE CONSENSUS –** Cryptographic process; “proof of work”

  1. Proposed transaction is first confirmed by nodes to be *valid*
  2. Transaction then joins a *block* of transactions (block contains a set of all cleared transactions within a short period of time, e.g., 10 mins)
  3. The new block is formally added onto the blockchain only after certain nodes (“*miners*”) solve a very difficult math problem (“*hash*”). Miner receives a *reward*.
  4. The new block contains a time stamp and reference to the prior block – creating a *chain*
  5. The new block will populate on the *master ledger* maintained by all nodes in the system.

KEY FEATURES

- **ELIMINATES DOUBLE SPEND PROBLEM –** If someone tries to sell the same asset twice, the transaction will be rejected by network as having already been spent.
- **NO CENTRAL TRUSTED AUTHORITY REQUIRED –** Strangers can hold / exchange assets without having to trust each other or a central authority
- **TRANSPARENT YET PRIVATE –** Every transaction (since inception) is available to be viewed, but privacy / anonymity of the parties can be maintained
- **IMMUTABLE RECORD –** Once validated, transactions are immutable (cannot modify, cancel or revoke; irreversible)
- **SECURITY –** Blockchain is considered tamper proof

KEY BENEFITS

- **CUTTING COSTS –** Reduces the need for multiple intermediaries (transaction costs), need for reconciling individual ledgers, etc.
- **REDUCING COMPLEXITY AND INCREASING EFFICIENCY –** Fewer intermediaries, streamlines / simplifies processes, reduce errors and delays, reduces data duplication
- **SPEEDING UP TRANSACTIONS –** Enables near to or real time processing of transactions
- **INCREASING SECURITY / RESILIENCE –** No single point of failure
- **TRANSPARENCY –** Obtain real time view of information
- **ENHANCE TRUST –** Enhance trust among parties

PUBLIC / PRIVATE BLOCKCHAINS

- Blockchains can be private or public
- **PUBLIC –** A **public blockchain** is a blockchain where there are no restrictions on reading blockchain data and submitting transactions for inclusion into the blockchain (e.g., Bitcoin)
- **PRIVATE –** A **private blockchain** is a blockchain in which direct access to blockchain data and submitting transactions is limited to eligible persons/entities (e.g., Linux Foundation Hyper Ledger)

SMART CONTRACTS

- Term coined in 1990s by Nick Szabo (computer scientist / law professor)
- Many different usages of the term. Oftentimes, describes contracts whose terms / conditions are programmed into computer code; allows for self-execution of the contract upon specified occurrence or performance
- Allows parties to determine now what future outcome will be in the future and bind themselves to that outcome
  - **Legal contract:** parties bind themselves to that outcome by becoming legally bound (enforcement via courts)
  - **Smart contracts:** parties become technically bound to the outcome by agreeing to run a computer code that will execute their intended outcome automatically on the occurrence of certain triggering conditions

SMART CONTRACTS (CONT'D)

Why Smart Contracts are Particularly Synergistic with Blockchain Technology?

1. Coding the contract on a blockchain ensures that the code is immutable
2. Smart contract can rely upon the ledger as proof of the occurrence of the conditions
3. Smart contract can trigger the transfer of digital assets on that platform

Numerous Applications

- Storing assets in escrow; insurance contracts; facilitate trade finance; etc.

GOWLING WLG