Blockchain Essentials

Conatum Consulting LLC
Bernard S. Donefer

We associate the blockchain with the Bitcoin cryptocurrency. The news focuses on the currency aspect, with its soap opera of volatility and scams, forgetting the more important underlying technology, the blockchain. Major banks, financial firms, exchanges and startups are investing hundreds of millions of dollars in projects promising a revolution in securities and payment processing efficiencies. Why are they doing so and are their expectations achievable? Mangers need to get beyond the hype and understand what is the blockchain, its potential uses, operation and risks. We will examine and compare the Bitcoin and Ethereum blockchains and look at current projects at JPMChase and Facebook among others.

Blockchain Essentials is intended for managers in finance, accounting, compliance, IT, risk, legal, compliance and others who need to understand the technology and its potential. It requires no programming or mathematical expertise. Our objective is to provide the background to enable attendees to enter the discussion, understand the issues, benefits and pitfalls and make well-reasoned decisions.

The one day seminar topics to be covered include:

1. Cryptography and hashing, the basis of the blockchain
    a. Secret key (symmetric) cryptography
    b. Public key infrastructure (PKI) encryption
        i. RSA and ECC
    c. Hashing ensuring data integrity and password protection
    d. Transport Layer Security (TLS) safeguarding our internet transactions
    e. Digital signatures
        i. Non-repudiation of transactions and their legal standing
        ii. Assurance of asset ownership
2. Brief history and context of blockchain and cryptocurrency
    a. Investments in blockchain
    b. What were the drivers in the creation of the first accepted cryptocurrency
    c. Satoshi Nakamoto and his paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*
3. Peer to peer file sharing
    a. Distributing transactions to multiple ledgers and authenticators

4. Ledgers
    a. How to ensure single spending/transfer of assets
    b. Single trusted ledger
    c. Distributed ledgers and the double spend problem
5. The blockchain
    a. Hashed linked list, digital signatures and Merkle tree ensure immutability of transactions
    b. Walk through a Bitcoin transaction
        i. Creation of blocks from transaction pool
        ii. Bitcoin trading, exchanges and hot/cold storage
    c. Bitcoin forks - how changes are implemented
6. Gaining consensus – mining , process and payment
    a. How to confirm transactions on a distributed ledger
    b. Mining and its technology requirements
        i. Proof of work and alternatives
            1. Cost of power and infrastructure
            2. The 51% attack
7. Issues and considerations in using blockchains
    a. Regulatory and compliance
    b. Capacity, latency
8. Initial coin offerings (ICOs)
    a. Purpose, risk and regulatory issues
9. Cryptocurrency
    a. Exchanges and how they work
    b. Bitcoin transaction example - full life cycle
10. Permissioned blockchains
    a. Open only to approved participants
    b. Consensus on permissioned networks
11. Ethereum – Virtual Machine – World Computer
    a. Compare to Bitcoin blockchain
    b. Use of gas for payments
12. Smart contracts
    a. Use of external oracles
    b. Rules based processing – use case examples
13. JPMChase (Quorum) and Facebook (Libra) projects
    a. New consensus alternatives
14. Current blockchain proof of concepts projects
    a. Private securities
    b. Diamonds, gold
    c. Payment systems
15. Reference materials and sources