Introduction to Blockchain and Distributed Ledger Technologies

Paul West
Hospitality Technical Services
pwest@gapspot.com

917.309.6451

Hospitality technology professional with a 30 year history of versatile international and domestic experience in directing IT operations, hardware implementations, software development, communication services, client services, vendor management and IT projects for property and portfolio operations around the world.

Global Hospitality Technology Consultant to hotels, casinos, restaurants, spas, clubs and related travel industries.

Founding member and current Secretary of the HFTP Greater Louisville Chapter.

Independent Broker providing benefit management solutions and risk related services to the industry.

Dedicated to bridging the communication gap between vendors and clients while providing technical services for companies seeking to derive business efficiency and profitability from their IT operations.

"The single biggest problem in communication is the illusion that it has taken place."

~ George Bernard Shaw ~

Introduction to Blockchain and Distributed Ledger Technologies

Session Contents and Introduction

- Overview of Cryptocurrencies, Cryptography, Blockchain and Distributed Ledger Technologies
- Basic explanation of related technology concepts
- Define some confusing terminology
- Review the Distributed Ledger Technology process and architecture
- Discuss how this new technology can be applied to business applications to help solve existing and/or new problems within the enterprise and beyond
- Review some current business application examples

General Blockchain Definition

- An empirical technology upon which an application is based that changes the approach to the current methods of how we exchange value and assets, enforce business contracts and share data
- A database of encrypted entries where each transaction is tracked as a common record to everyone on the network where no single entity is in control of the data
- A shared, secure ledger of transactions distributed among a network of computers in a peer to peer manner - as opposed to being provided from a central repository – where certain specific conditions must be met before the network agrees on any transaction
- A new method of sharing business processes and data across multiple organizations while eliminating waste, reducing the risk of fraud and creating new revenue streams
- Already being applied in banking, capital markets, insurance, logistics, retail and hospitality industries

Clarification of Definitions and Concepts

- Bitcoin was created circa 2009 in response to the global financial crisis of the previous year as a new way to transfer money, via the Internet, without an intermediary
- A Cryptocurrency is a programable, digital asset and medium of exchange not controlled or backed by any government
- Cryptocurrencies used for long term savings are saved in an offline “Cold Wallet” for storage while cryptocurrencies for more active everyday use are held in a “Hot Wallet” that could be secured by a Blockchain network online
- Blockchain has been used to define the overall data structure behind the Bitcoin concept; but, this term may be used too broadly to apply to everything on the spectrum when it is really a specific form or subset of Distributed Ledger Technology
- Blockchain is the underlying technology and type of distributed ledger used to track assets other than cryptocurrencies such as Bitcoin by actually constructing a chronological chain of blocks
- Blockchain Technology is a Peer to Peer Distributed Ledger Technology built on consensus
- Blockchain also consists of cryptography, time stamping, shared computational power and a defining consensus algorithm known as a Smart Contract

Brief History Review

- 20th century computing was a back and forth approach between centralized computing power and decentralized networks and protocols
- The advent of computing consisted of mainframes and then quickly became more accessible with mini computers (IBM, Digital Equipment, Wang Labs, etc) – all which provided access to data and resources via users connected with simple terminals via cables
- Personal Computing made the computer even more accessible and still with the desire to replicate data from server to server; but also now with the ability to be distributed between clients and servers
- Decentralized networks and protocols allowed for this more client server networking architecture (Novell NetWare, Banyan Vines, IBM Token Ring, etc.)
- Approaching the 21st century, a Peer to Peer approach grabbed some momentary attention with the advent of services like Napster that allowed any individual node or computer to push and pull music from point to point or from individual to individual
- The Internet soon opened device access further where mainframes drove the larger corporations while the booming cloud architectures which although decentralized in hardware became more centralized at the application level (Facebook, Google, Twitter, etc.)
- Today and as a result of Bitcoin and Blockchain, there may now be that shift back to decentralization with the use of Distributed Ledger Technologies and its Peer to Peer networking architecture where workloads and tasks are equally partitioned between peers (nodes or computers on the network)

Poll Question #1

What is Bitcoin?

A.) A unit of currency whose owners are identified by name or location

B.) A cryptocurrency used as a worldwide currency

C.) A valuable piece of metal that is mined with a pick and shovel 150 meters below ground

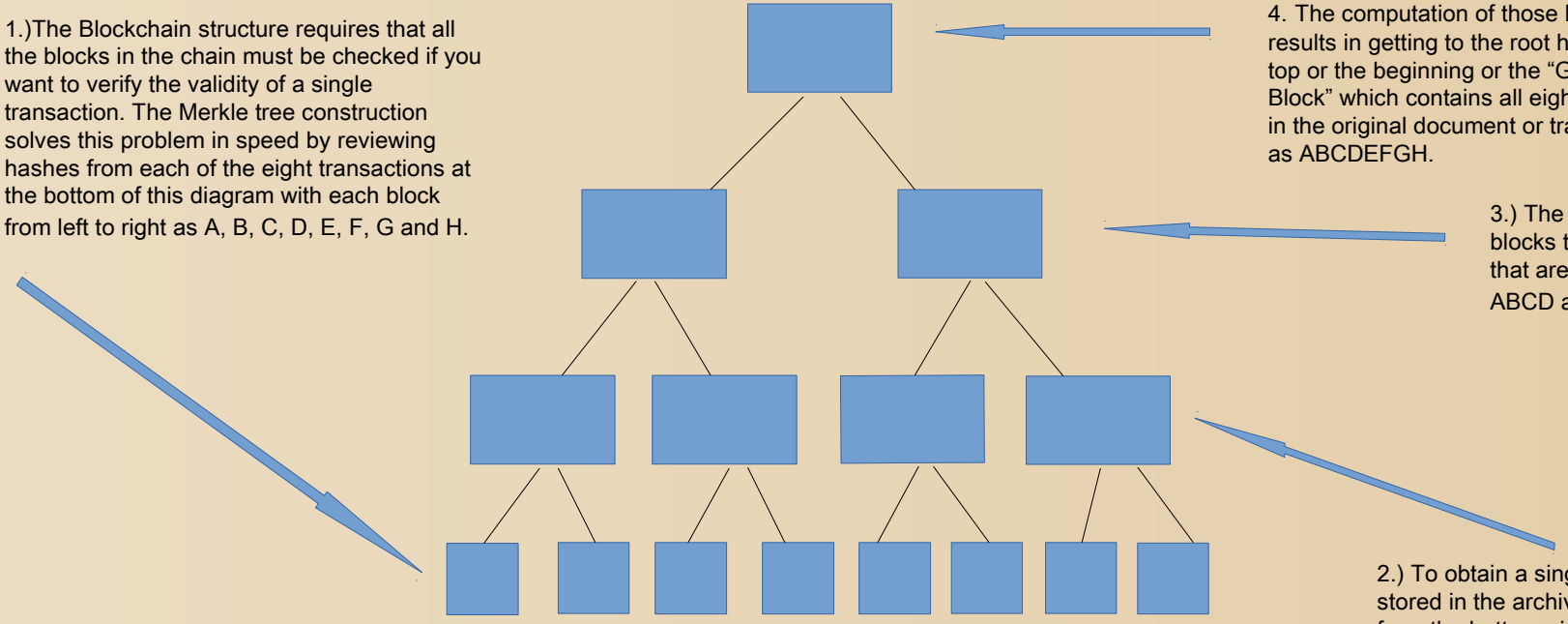
Distributed Ledger and Blockchain Concepts, the “Mining” Process and the Block Structure

- In a Bitcoin network, miners solve a cryptographic challenge to propose the next block or “Proof of Work”
- Proof of Work is one of several mining methods (depending on the Distributed Ledger Technology framework in use) that succeeds when proven, much in the way continually guessing the combination to a lock is proven when the correct number actually opens the lock
- This particular method of mining requires extremely intensive computing power where each block is time stamped and each new block refers to the previous block using cryptographic hashes that refer all the way back to the very first block known as the “Genesis Block”
- Immutability of Data where nothing is ever changed in the ledger without leaving a record of that change that is then distributed to everyone on the network
- Each block on the ledger chain contains four pieces of metadata:

    1) Reference to the first block
    2) Proof of Work or “Nonce” (the specific value in the message)
    3) Timestamp
    4) Merkle Tree Root or Binary Hash Tree or the Digital Fingerprint of the transaction within the block

Simple Example of Merkle Tree Blockchain Structure

1.)The Blockchain structure requires that all the blocks in the chain must be checked if you want to verify the validity of a single transaction. The Merkle tree construction solves this problem in speed by reviewing hashes from each of the eight transactions at the bottom of this diagram with each block from left to right as A, B, C, D, E, F, G and H.



4. The computation of those hashes results in getting to the root hash at the top or the beginning or the “Genesis Block” which contains all eight records in the original document or transaction as ABCDEFGH.

3.) The hashes of those four blocks then point to two nodes that are on the second level as ABCD and EFGH.

2.) To obtain a single hash that is stored in the archive, the hashes from the bottom eight blocks here are grouped into four at the third level of nodes as AB, CD, EF and GH.

Overview of the Blockchain and Distributed Ledger Technology Network Infrastructure

- Blockchain is a form of Distributed Ledger Technology with a data structure residing across multiple computer devices, locations and regions
- Distributed Ledger Technologies utilize “Smart Contracts” which are the actual computer programs that execute algorithms or predefined actions when certain conditions within the system are met to create a new transaction that is tracked in the ledger
- Nodes or machines on a distributed ledger network then group those transactions and send them through the network in a peer to peer manner
- Data is synced along the way using a Consensus or Agreement among the network peers so that eventually each machine will have an exact copy of the Blockchain throughout the network
- “Consensus” is the system of ensuring parties agree to a certain state of the system as the true system state using a synchronized series of transactions within the decentralized database
- Distributed Ledger Technologies process captures the current state of the ledger, provides a transaction language to change the state of the ledger and uses a protocol to build consensus for which transactions will be accepted - and in what order - by the ledger

Security Within the Network

Security in a Distributed Ledger network is driven by “Consensus” within the Peer to Peer design that:

- Ensures data is the same for all nodes on the network
- Prevents malicious actors from manipulating data
- Is not dictated by any central authoritative figure and so operates in a more democratic manner

Security is further enhanced within the Distributed Ledger network by:

- Operating in an environment without the concept of human trust – assuming that any insider or outsider can compromise the system at any moment
- Cryptography that allows secure communication between parties – ensuring authenticity and immutability of the data being communicated
- Handling every transaction as a group of blocks that is cryptographically secured with a digital signature, verified, ordered and bundled together to form a record or event on the network
- Using a permission-ed or closed, private network as opposed to a permission-less or open, public network
- Company firewalls and security monitoring that are still necessary if the Distributed Ledger solution operates with nodes outside its network where there may not be a direct connection between nodes

Permission-ed Networks and Permission-less Networks

Variations in Distributed Ledger Technologies and Frameworks

- A permission-less or open network is basically a public network (used by Bitcoin and another popular framework called *Ethereum* which has its own digital asset called *Ether*)
- Permission-less networks are where one can commoditize trust such that it is not necessary to identify the parties involved and usually includes a sale or distribution to the general public
- A permission-ed network is a closed network where all parties involved are known and is deployed behind a firewall for local participants while using a VPN to connect to outside, known participants and is a most suitable choice for companies looking to develop enterprise solutions
- *HyperLedger* open source projects that operate for the most part in permission-ed or closed networks offer different frameworks such as *Fabric, Sawtooth and Iroha* – all which utilize a variety of consensus protocols
- Parties involved in permission-ed *HyperLedger* blockchains are authenticated and authorized to participate with the goal of creating enterprise grade, open source, distributed ledger frameworks and code bases that support business use cases

Basic Cryptography Overview

- Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those for whom it is intended, can read and process that data
- An important tool for cryptocurrencies is the concept of signatures that as in real life, should provide verification of the signer, should be non forgeable and should be non repudiating
- The use of keys (both public and private) within the digital signatures of cryptography are that next layer of security not afforded to one with a real life signature; but, proven reliable with such cryptographic keys as used with Bitcoin
- Essential to blockchain management is the cryptographic hash or digital fingerprint that is created by converting an input of letters and numbers into an encrypted alphanumeric output of fixed length
- Kudos to many a mathematician for working out the plethora of key and encryption options to end up with the type of cryptography used by cryptocurrencies and distributed ledger technologies of the blockchain

Some Consensus Type Algorithms

- Proof of Work
- Requires much energy to solve computationally heavy algorithms used by Bitcoin and Ethereum within permission-less networks

- Proof of Stack
- Nodes are selected randomly to act as validators of transactions for a fee that depends on the amount of stake held.

- Proof of Elapsed Time
- Developed by Intel and similar to Proof of Work but uses no competition to solve the cryptographic challenge. Instead its nodes are allotted on a first come, first server basis where the one with the shortest wait time is elected to create the next block on the chain

- Proof of Authority
- Used in permission-ed ledger networks that use authorities or designated nodes to create nodes and secure the ledger

- Simplified Byzantine Fault Tolerance
- Used in permission-ed ledgers where the validator is a known party and used in an improved version of the original Bitcoin protocol

- Proof of Activity
- Created as an alternative structure for Bitcoin that is a hybrid version of Proof of Work and Proof of Stack but still energy intensive

- Proof of Burn
- Instead of investing in expensive computer equipment, coins are “burned” or sent to an irretrievable address to obtain lifetime privileges

- Proof of Capacity
- Algorithm creates “plots” of space stored on the hard drive where chance to find the next block increases as space increases

Poll Question #2

Who has been around long enough to have used a centralized hotel property management system that was hosted on a mini computer and accessed by users via thin client terminals?

A.) Yes

B.) No

C.) Not Sure

Business Value of Blockchain and Distributed Ledger Technologies

- A distributed consensus among potentially distrusted parties
- A method of possible collaboration among competing entities that manipulate the same data
- Automation of repetitive, tedious, manual processes with integrity
- Validation in real time instead of batch processing for immediate reconciliation
- Immutable data with a write only data structure where new entries get appended
- Smart Contracts that provide an arbitrary, sophisticated business logic to define the rules of the game
- Designed for decentralization of data unlike traditional databases designed for centralized applications
- Decentralized applications or “D’Apps” provide zero business downtime as they can never be switched off

Challenges in Adapting and Deploying Distributed Ledger Technologies

- Lack of standards in the supporting services of identity, privacy and data governance
- Regulatory challenges by city, state, country and global unions
- General lack of knowledge on distributed ledger technologies
- Same challenges facing anyone looking to replace an existing infrastructure with another infrastructure
- General alignment of competing businesses with varying business models to coordinate across boundaries to deliver products and services to the same desired clients
- In 2016, Organization for Standardization for Blockchain and Distributed Ledger Technologies established to create some standards in the technology:

    1) Short Term = Terminology & Vocabulary
    2) Medium Term = Security, Privacy, Data Governance, Enduser Identity, Interoperability
    3) Long Term = Provenance Tracking and Other Technical Aspects

International Organization for Standardization (ISO)

In May of 2017, International Organization for Standardization plotted a similar but more detailed course for the development of Blockchain and Distributed Ledger Technology standards:

- Reference Architecture
- Taxonomy and Ontology
- Use Cases
- Security, Privacy and Identity
- Smart Contracts

Engaging a Distributed Ledger Technology Solution in the Enterprise

- Define current business requirements and assess future objectives
- Ascertain business processes that rely heavily upon trust
- Distinguish areas where multiple parties manipulate or manage the same data
- Measure the importance of data integrity to the business
- Review intermediaries controlling any single source of truth
- Determine any business processes that involve low-value, manual verification steps
- Understand your target user for the solution
- Determine any thresholds for what is an acceptable processing time for your application
- Discuss requirements for scalability, confidentiality, compliance, workflow complexity and security which differ by industry and scenario
- Establish if solution can operate in a permission-less, open, network or if the security of a closed, permission-ed and private
- network is necessary before choosing an appropriate platform (Ethereum, HyperLedger, Corda, etc)
- Determine the measurement for success of your solution
- Consider beginning with a smaller ecosystem to test the waters of your distributed ledger solution
- Involve everybody at all levels of the organization in the process - from the technical level - to the business level - to the operations level

Blockchain and Distributed Ledger Technology
Developments within Other Industries

- Chain Core by a Chain that is used by financial institutions, in securities, bonds, gift cards, loyalty points and has collaborations with NASDAQ, Visa and Citicorp
- Corda Distributed Ledger Platform that records, manages, automates legal agreements between businesses (created by the company R3 which is a consortium of over 100 global institutions
- Quorum – a permission-ed, data privacy, implementation of Ethereum created by JP Morgan to allow data visibility on a need to know basis for the financial industry
- IOTA – an organization with a cryptocurrency in a permission-less environment that enables machine to machine transactions in sort of a Blockchain generalization with a protocol involving peer to peer validation
- A variety of HyperLedger products and other more enterprise oriented approaches from companies like IBM, SAP, Microsoft and Cognizant
- Dock.io – a Blockchain application running on the Ethereum platform to create a single shareable source for one's social profile, network and professional reputation (updates all information from all your connected apps like Facebook, Linked-in and Google, etc., from one location)

Blockchain and Distributed Ledger Technology
Application Development for the Hospitality Industry

- Loyalty or Rewards Programs and Reverse Reward Usage
- Supply Chain Procurement / Facilities Management
- Food Industry Distribution
- Reconciliation, Tracking and Securing of Wholesale Rooms on the Online Distribution Chain
- Wine and other High Value Counterfeiting Detection
- Removal of the Middle Man Commission Fees (Online Travel Agencies, Travel Management Companies, Banks)
- Guest Tracking and General Guest Experience Enhancement
- Human Resources and the Payroll Process

Poll Question #3

Has anybody been around long enough to remember which application that was run from a floppy disk made the personal computer a huge hit in the Accounting department?

A.) Yes

B.) No

C.) Not Sure

A Steady Worldwide Growth of Companies, Organizations and Councils for Blockchain, Digital Currencies and Distributed Ledger Technologies

Companies:

- STOX – a prediction market platform
- Hashed Health – a healthcare innovation firm
- GLobaCap – a digital capital raising platform
- CoinCheck – a Japanese cryptocurrency exchange
- GuardTime – a data security startup founded by an Estonian cryptographer
- CashAA Holdings – one stop shopping platform for all your financial needs
- Follow My Vote – uses elliptical curve cryptography to manage voter registration and casting of ballots to make the election process as transparent as possible

Organizations and Councils:

- Chamber of Digital Commerce – a global trade association for digital assets
- Global Blockchain Business Council – provides industry insight on potential impact of blockchain applications and development
- The Global Blockchain Foundation – focuses building a blockchain sustainable worldwide community
- The Government Blockchain Association – international association to join government, business and technology sectors
- The Wall Street Blockchain Alliance – serving financial market professionals in all aspects of the distributed ledger global ecosystem

Summary and Recap

- A brief history on the rise of Cryptocurrencies, Blockchain and Distributed Ledger Technologies
- A review of the Blockchain, Distributed Ledger Technologies and immutable data with proof of origin
- Definitions of cryptography, smart contracts, mining or “cracking the code”, consensus of varying types, permission-ed (closed or private) networks and permission-less (open or public) networks
- Decentralized or peer to peer networks versus centralized networks and the impact of each
- How a distributed ledger solution can a benefit business with transparency, security, streamlining and problem solving
- Overview of how a company may approach engaging a distributed ledger solution
- Current company and solutions from other industries
- Current and potential application solutions for the hospitality industry
- Scenarios for implementation are numerous, contribution to world economies appears to be optimistic and the future impact to business and industries globally is yet to be realized

CLOSING

Blockchain and Distributed Ledger Technologies are the beginning of a change in how business is done; but for any new technology to reach its full potential, a certain number of achievements must be reached:

- Recognition by a critical mass which is necessary before any systemic efficiencies can be realized
- A collaboration of all major competitive players in the market to define standards

The contributions introduced by implementing this network infrastructure to current applications and business processes include:

- Reducing Business Costs
- Increasing Speed
- Increasing Security
- Reducing Fraud
- Reducing Risk

"Anything that you can conceive of as a supply chain, blockchain can vastly improve its efficiency – it doesn't matter if its people, numbers, data, money."

-

Ginni Rometty CEO IBM

THANK YOU VERY MUCH!

QUESTIONS?

Paul West
Hospitality Technology Consultant

Hospitality Technical Solution Services | Hospitality IT Project Management Services

Independent Broker
Benefit Management and Risk Management Solutions

917.309.6451

pwest@gapspot.com

"Plans are worthless. Planning is essential."
~ Dwight D. Eisenhower ~