CHAIN OF ACTIONS

Initiate the transaction.

- Multiple parties transact
- All transactions are recorded, including each transaction's date, time, parties and amount.

Post and record the transaction to the network.

- The transaction is added in order into a network's "block" and presented.
- Entries can be added but not deleted.
- Each node in the network owns a full copy of the ledger.

Broadcast.

- Each "block" is broadcast to every party and their nodes in the network.
- The network of computer nodes verify and validate by running a software that continuously replicates the ledger.

THE BLOCKCHAIN

'Blockchain' seems to be on everyone's lips. But what does it mean,

BLOCKCHAIN IS AN EMERGING technology that has the potential to disrupt transaction processing, settlements, accounting, reporting and auditing in a wide range of industries, and most certainly the media business.

In the future, blockchain – or distributed ledger technologies – may be able to provide significant value to the media industry in areas such as royalty reporting, digital rights management, piracy prevention and licensing payments.

The reason why blockchain is starting to gain attention is understandable. There's an explod-ing amount of transactional data that accounting systems need to capture. As traditional accounting systems strain to keep pace, blockchain seeks to become a new tool to enable businesses to process and record transactions more efficiently

HOW IT DEVELOPED

First proposed in 2009, blockchain enabled the first major digital currency, known as Bitcoin. The concept was to create a decentralized currency that did not rely on banks or other financial institutions for its utility. Blockchain has the potential to expand far beyond Bitcoin and now is being tested in a

Validate by consensus and confirm.

- The network verifies, validates and approves; the confirmation is broadcast to the other nodes.
- Consensus (agreed mathematical mechanism) is recorded and provides the basis for the trust mechanism.

Immutable encrypted block.

- The confirmed block is added in a linear and chronological order to the chain.
- This provides transparent record of the transactions, audit trail and traceable digital fingerprint.

Transaction completed.

- Nodes have access to a single shared source of truth.
- A completed block gives way to the next block in the block chain.

Consensus Mechanism Applied

REVOLUTION

By
PADRAIC KELLY

and how is it changing the way media companies transact business?

broad range of business and financial applications.

Blockchain can disrupt the current financial system because it decentralizes trust in financial transactions by distributing it among the participants. In a distributed blockchain ledger, transactions are validated across many computers. The intent is that records could not be altered unilaterally without altering all subsequent blocks, which would be readily apparent to participants in the peer network.

If there is an attempt to corrupt a transaction, the nodes would not arrive at a consensus and would refuse to incorporate the transaction in the blockchain. Every transaction is accessible, and all nodes need to agree unanimously about the key transaction attributes. So, in theory, everyone would have access to a shared single source of truth.

Blockchain has sparked a new wave of digital innovation. Today, most industries, such as media, banking and healthcare, rely on intermediaries to help manage the integrity of the value chain. With blockchain, all transaction records are stored in a shared ledger and all participants have access to all records, which can streamline accounting, reconciliation, settlement and reporting activities for counterparties.

The media industry has experimented using

blockchain technology to track distribution of licensed music and used the capability of digital currencies to execute micro-payments for settlement of licensing fees.

A streamlining of the licensing process would make it possible for artists to claim a higher percentage of the total revenue generated by their creativity while at the same time providing safeguards against fraud. To verify transactions, auditors may one day directly access evidence from the blockchain rather than from invoices, disbursements, reconciliations and confirmations.

SMART CONTRACTS

Media companies may soon use "smart contracts," a feature of certain blockchains, in the distribution and pricing of their digital goods. Smart contracts are self-executing digital contracts that use the blockchain. They can set prices or other variables depending on demand, point in time or other factors.

Artists could use smart contracts, for instance, to price newly released songs at a premium price, and then dynamically scale down the price as demand slackens or the content ages.

Blockchain could also permit any content creator to monetize his or her online content. Blockchain can track who created content, who viewed it and who values it. So content producers can capture more of the value they create with their content, instead of ceding monetization to the social network or another platform on which the content is viewed.

CHALLENGES TO CONSIDER

Blockchain is not a panacea to eliminate all fraud and unauthorized transactions, as evidenced by recent publicized thefts exploiting programming flaws in early ventures centered on the technology. If implemented properly, it does, however, make it much more difficult.

Companies seeking to use blockchain are smart to apply a risk assessment lens to management of private keys. They should also utilize consensus mechanisms and network access permissions, in addition to the security lessons learned over decades of technology innovation.

Another challenge is that transactions on the blockchain, in particular cryptocurrency transactions, currently can take longer to process than credit card transactions, which may slow the pace of adoption.

Blockchain is one part of a larger digital transformation that is disrupting transaction processing and accounting methods employed by organizations across myriad industries. In today's digital world, where financial information is being created faster than ever, digitizing transactions is an effective response to address the explosion of data. Blockchain is likely to gain even more popularity as companies continue to modernize their technologies.

A MINI BLOCKCHAIN GLOSSARY

Authentication: The process of proving the counterparty identities and the existence of assets via private and public keys.

Blockchain: A type of distributed ledger that maintains a continuously growing list of transaction records ordered into blocks with various protections against tampering and revision.

Consensus Mechanism: A method to authenticate and validate a set of values or a transaction without the need to trust or rely on a centralized authority. It can be constructed on and off a blockchain; a variety of approaches exist.

Cryptography: The process of enforcing the authentication and cryptographic validation integrity of transaction integrity via quorum structures and confirmation via code. This is done without the need to trust or rely on a centralized authority.

Cryptographic Signature: A method to mathematically validate the owner of a piece of data beyond any doubt if the user has kept the private key to sign the transaction safe.

Distributed Ledger: A digital record of ownership that differs from traditional database technology, since there is no central data storage. Instead the ledger is replicated among many different nodes in a peer-to-peer network, and each transaction is uniquely signed with a private key.

Nodes: Members of systems within a consensus network or a server that holds a replicated copy of the ledger and can have varying roles to issue, verify, receive and inform. For all intents and purposes, a node can be a virtual machine.

Public Blockchain: A network in which anyone can participate by reading data, submitting transactions and participating in the validations process.

Public Key: The public address where other wallets send transaction values.

Private Key: The encryption key uniquely linked to the owner and known only to the parties exchanged in a transaction. It is secretly held in a digital wallet.

Privacy: Ensuring that only the receiver intended can read the message. The field of computing cryptography addresses many security and privacy issues of distributed consensus through the use of mathematical formulas for specific secure communication requirements within the context of any application-to-application communications.

Security: Distributed ledger security is the process for protecting and safeguarding business and personal data, as well as transaction information. It includes an assurance to the receiving node that a message received has not been altered in any way and a mechanism to prove that the sending node truly sent the message. Security can include digital signatures as a feature.

Padraic Kelly is an audit partner at KPMG, LLC. He can be reached at pkelly@kpmg.com or (415) 963 7373.

This article is based on information within the KPMG research document Consensus: Immutable Agreement for the Internet of Value.