Enterprising the Blockchain

By Robert P. Smith II

bob@rpsmith.net www.rpsmith.net

As the Internet transformed communications and commerce in less than a decade, Blockchain will profoundly change how we acquire and convey property. Read on for a description how Blockchain works in less than 400 words using just nine words of jargon.

Electronic transactions have been displacing cash for convenience and safety for 50 years. In many third world countries, making payment by text is now the fastest growing form of cash.

All electronic transactions require third party institutions acting as arbitrators. Underlying faith comes from the countries where they operate creating stability or even regulation guaranteeing funds like the FDIC. However, this certainty comes with the quid pro quo of *imperial entanglements*.

Therefore, *trust, security, convenience and privacy* are factors considered in every transaction.

Blockchain is already disrupting property in fundamental ways:

Trust	Public, consensus driven and auditable ledger
Security	Unbreakable encryption based on unsolvable mathematics
Convenience	Allows transactions anywhere the Internet can reach
Privacy	Personal identity not required to transact

What is Blockchain and How Does It Work?

Blockchain came to being in 2008 by Satoshi Nakamoto, a pseudonym for a person or group through a whitepaper, Bitcoin: A Peer-to-Peer Electronic Cash System.

They also released open source code ultimately named Bitcoin Core forming the operational foundation of Blockchain that maintains records referencing any physical or virtual asset and tracks the transfer from one party to another.

Blockchain tracks two computer generated codes as:

Public key	Identifies a participant
Private key	Sending this code transfers ownership (*transaction*)

This 35 character code is an example key:

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Breaking it requires 2^{32} or 4.29 billion guesses hardly a practical exercise ensuring, if the key isn't compromised by its owner, complete trust.

Blockchain performs these functions through a federation of computers (*nodes)* owned and operated by volunteers (*miners)*.

Nodes collect and post transactions to a *block* containing:

Reference to the previous block *(chain)*
New transactions
Computationally-difficult math problem *(proof of work)*
Miner identity (*coinbase*)

Nodes compete to be the first to solve the proof of work. Solution *difficulty* adjusts designed to generate new blocks about every 10 minutes. Miners are paid in Bitcoins collecting having collected $1.8B in mining revenue to date

For a sense of size, there are dashboards and over the last 24 hours showed:

280k transactions
5,000 nodes active in 93 countries
spawning 553 new blocks

Blockchain is transparent, every transaction is public (go and see them here), and this is the point, moving governance out of the hands of third parties and governments to the vast consensus of miners.

Blockchain is secure coming from the highly distributed community of miners operating nodes worldwide. Breaching the system requires an impossibly larger and much more coordinated mob of "dark" miners to overwhelm a system that reinvents itself every ten minutes. Only obtaining the private key can theft occur leaving physical security completely in the hands of the participant.

Blockchain has no back door because Bitcoin Core is completely open source. With every line of code is in the open. Unless a majority of miners were secretly cooperative, third party backdoors can't exist.

Blockchain is private operating peer to peer only. Identity is not part of the system and therefore no role exists for a third party, including governments except by consensus.

Blockchain is smart able to carry out conditional tasks enforcement called contracts. Conditions can include anything publicly verifiable like a date, death or employment status. A derivative could be paid out when a financial instrument meets a certain benchmark.

The Future

Much like the Internet of 1995, Blockchain is pre-infancy with massive potential. Over $1.1B of land grab investment in any company that can put *block* and *chain* together is in place around the world. Aware incumbents are participating as well for instance MasterCard offering Blockchain resources for programmers developing new payment systems.

Some additional glimpses are:

> Peer-to-Peer (P2P) – bypass third party involvement and exposure of sensitive user information including credit card numbers enabling ecommerce networks in which buyers and sellers interact directly without hackable stored records.
>
> Keyless Security Infrastructure (KSI), using hash-function cryptography and public ledgers bypassing the required third party of Public Key Infrastructure (PKI) that limits scale and is exposed to brute-force attacks.
>
> Central Security Depositories (CSD) settlement process is expensive and can take days to settle. Blockchain decentralizes the system cutting out the third party drag and expense.
>
> Counterfeiters get product to market, like drugs, by exploiting wholesale distribution systems. Blockchain transparency enables authentic supply chain brand, merchant and marketplaces.

About the only certainty at this point is Blockchain will be the most transformative concept of the first quarter of this century if not sooner.

As a technology marketing leader, Bob holds that customer experience is the highest aspiration and ultimate judge of any enterprise. He further believes that persistent curiosity, transformative vision, and collaboration are the most critical factors to getting this right.

Disruptive product and marketing innovation highlight Bob's career along with predictable data analytics and methods increasing share and investment returns. Close interlink of sales and customer systems using automated marketing processes maximize customer satisfaction and mitigate unplanned events.