

Accept, adopt, utilize: Making way for blockchain

By **Nicky Liu**
Technology Risk Consulting
KPMG in Canada

It has been nearly a decade since a programmer under the alias Satoshi Nakamoto entered the pantheon of technological innovators by designing the world's first blockchain. In the decade since, both the coder (or, perhaps, coders) and their distributed ledger technology (DLT) have transformed the way people and businesses trade funds, strategies, and critical data.

Blockchain / DLT technology continues to evolve; and while it could be easy to view its disruptive nature as a risk best left untouched, there is value to accepting, adopting, and utilizing Nakamoto's game-changing approach to human transactions.

A new way to transact

If there were a poster child for industry disruption, it would be blockchain. By design, it allows participants to share encrypted records over an open and decentralized peer-to-peer network.

Explaining the nuts and bolts (or rather, ones and zeroes) of blockchain would take a whitepaper in itself. And indeed, KPMG has a growing volume of papers dedicated to doing just that. For our purposes, though, an explanation of blockchain is best told through a run-down of a typical transaction. In this case, the trading of digital currency.

1. The Payer submits a transaction through a node in the chain, after which blockchain technology copies their ledger to verify their balance.
2. If the balance of the Payer is greater than the transaction amount, then the transaction is deemed legitimate and broadcasted to nearby nodes. The transaction requires validation from more than 12 nodes before it can proceed.
3. The transaction is moved to the pending pool for the node's tentative blocks. A blockchain 'miner' on the other hand – that is, someone using their computer to perform the complex

calculations required to verify and decrypt transactions – will continue to crack the hash puzzle from the latest block (i.e. block 1004), in order to link their tentative block to the chain.

4. Once the hash puzzle is solved and the tentative block is confirmed and added to the chain (block 1005), the node will broadcast this to other nodes in the network. At this point, the transaction made by the two customers has been recorded in the block and thus becomes tamperproof.
5. The other nodes receive the broadcast and drop this transaction in their pending pool and collect other pending ones in their tentative block. They then continue cracking the hash puzzle generated from the new block.

A blockchain primer

- **Blockchain:** A type of distributed ledger database that maintains a continuously growing list of transaction records ordered into blocks with various protections against tampering and revision.
- **Distributed ledger:** A digital record of ownership that differs from traditional database technology, since there is no central administrator or 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.
- **Consensus mechanism:** A method of authenticating and validating a value or transaction on a blockchain or a distributed ledger without the need to trust or rely on a central authority. Consensus mechanisms are central to the functioning of any blockchain or distributed ledger.
- **Nodes:** Members or systems of a consensus network or a server that holds a replicated copy of the ledger and can have varying roles: to issue, verify, receive, inform, etc. For all intents and purposes, a node can be a virtual machine (VM) instance.

Adopting blockchain for global payments

There are several advantages to blockchain transactions; particularly when applied to global payments. Take, for instance, a blockchain transaction between a customer in Canada to a business in China. Once sent, the payment is converted into an intermediary currency (e.g. a 'cryptocurrency' which all banks on the network accept) and sent to the nearby nodes within the blockchain network. Here, the customer's account and balance information are verified almost immediately via a distributed ledger available on the networks and the transaction is broadcast further and confirmed when a new block is created and linked to the chain. The processing time is totally controllable by the participating banks depending on how they design the technical protocol. The cryptocurrency received at the Chinese beneficiary bank is then converted into the designated currency according to customer instruction and transferred into the beneficiary's account.

Once the deal is done, the digital ledger is synchronized to all the participating banks in the network. This eliminates the need for reconciliation between the originating and beneficiary banks as transactions are kept at every ledger of all the banks within the network and is almost impossible to be tampered.

While only a hypothetical example, this scenario illustrates the advantages of blockchain compared to the traditional paperwork- and time-heavy process. Overall benefits include:

- **Pre-transaction verification:** Account and balance information verification is fully automated and confirmed instantly.
- **Authentication:** Blockchain's embedded cryptography system makes the transaction safer and transparent.
- **Transaction cost:** Correspondent bank(s) are no longer necessary as payment is made via a peer-to-peer network. The risk of exchange gains and losses is also minimized since the transaction is confirmed almost instantly.
- **Processing time:** Blockchain's verification technology and the elimination of a 'middle-man' (e.g., bank or financial mediator) accelerates the time it takes to validate and settle the payments.
- **Inter-bank reconciliation:** Blockchain's automated process cuts down reconciliation efforts by the banks. Down the road, it may even eliminate the reconciliation altogether.
- **Transaction efficiency:** The reduced processing time and transaction costs improve transaction efficiency and significantly increase the asset utilization to the customers.
- **Treasury management:** Totally controllable processing time and improved transaction efficiency provide better oversight of the banks' treasury management, which will reduce the liquidity risk and credit risk to the banks.

Contact:

Nicky Liu

Technology Risk Consulting
KPMG in Canada
nickyliu1@kpmg.ca

kpmg.ca/rethinkrisk
#rethinkrisk

Utilizing blockchain in your business

Many financial institutions are working to take advantage of blockchain technology. As described in the previous sections, global payments is just one of the examples that blockchain is capable of in the old school trade finance. The adoption is also scalable to include more complex transactions such as derivatives, cash equities sales and trading. However, considering the fact regulations are becoming heavier and the financial industry itself is transforming at unprecedented speeds, the cost to adopt can be challenging.

To begin unlocking the benefits of blockchain, institutions need to first consider some key questions:

- What business or process can use this new technology? And what is the priority for my investment? (**Scope**)
- How is the process done today versus using a blockchain application? How are agreements reached on the data, business, and industry level? (**Process**)
- What data needs to be shared? With whom does it need to be shared with, and when? Additionally, what kind of assets will be transferred, and where should the data be stored? Does it need to be authenticated and notarized? (**Data**)
- What does the underlying existing technology landscape look like and in which way would it be impacted? What is the underlying technology cost? Who can provide the assurance of the security of the technology? (**Technology**)
- What workforce skills, training, and changes are required to make the most of blockchain? (**People**)
- Does that solution help to address my regulatory requirements in a more efficient way? (**Regulatory**)
- Is there an industry-driven event requiring a refocus on current operations, to do things faster, with more trust? (**Industry**)
- What is the overall business case, including the consideration of implementation cost? What is the market size and compound annual growth rate? What is the return on investment? (**Business case**)
- Can the solution be scalable and transferable? (**Performance**)

Auditors take note

The world is changing – and so are auditors. Just as companies are warming up to the potential of blockchain technology, auditors are also embracing advanced tools and methodologies to tackle the challenges of examining blockchain records on behalf of investors to provide reasonable assurance as to their accuracy and integrity.

The evolution of the auditor is far from over. As blockchain evolves, and as automated audit procedure becomes more tangible, we must also accept, adapt, and utilize the new digital tools of the trade.