GBBC Global Blockchain Business Council

BLOCKCHAIN PRIMER

The Blockchain is potentially the most transformational technology since the inception of the Internet. While the World Wide Web revolutionized commerce, communication, media and more, assets of value — currency, passports, votes and land titles –have yet to be digitized. This is, in part, because information transferred on the internet is usually copied when it moves from one owner to the next (think of email). But for assets to retain their value, they must be moved without being duplicated in the process. This demands a system with greater security and transparency. Blockchain technology provides a digital mechanism for anyone with an internet connection to transfer any asset—anywhere, anytime, with unmatched security and integrity.

HISTORY

The first Blockchain (now known as the public Bitcoin Blockchain) was conceived in 2008, in the wake of the global economic crisis. Presented in a white paper by a person or a group of people known as Satoshi Nakamoto, the Bitcoin Blockchain has grown rapidly to become a global technology, adding a much-needed layer of security to the Internet and changing the way governments, organizations, businesses and individuals operate in our increasingly digital world.

WHAT MAKES BLOCKCHAIN DIFFERENT?

Today, most people place their trust in middlemen or intermediaries, like banks, to provide security. But too often intermediaries are inefficient, expensive or insecure. Blockchain eliminates the need for intermediaries, allowing people to directly and securely transact peer to peer. No central authority is necessary to verify blockchain transactions because the technology acts as the intermediary. Trust is embedded into the Blockchain's very code—a decentralized, cryptographically secured database that can be seen and downloaded by everyone on the network.

Because information stored on the Blockchain is copied across a vast network of computers worldwide, there is no central-point of attack or failure. A paradigm-shifting approach to digital security, the Blockchain prevents fraud by requiring verification from every source computer before approving a transaction. This decentralization makes hacking or falsifying information on the Blockchain almost impossible. To hack into the Bitcoin Blockchain, bad actors would need to hack ~10,000 data centers simultaneously. In almost a decade of use around the world, the Blockchain has never been successfully hacked.

HOW DOES IT WORK?

Each asset transferred on the Blockchain is recorded and packaged into a group of transactions called a "block." Every "'block" is mathematically authenticated before

being linked to the immutable chain of previously verified data. Before being verified, mining nodes or "miners" (members in the network with high levels of computing power who secure the Blockchain) compete with each other to solve the mathematical problem of each block. This mathematical problem is a hash function of all the transaction information in the current block, the mathematical solution to the previous block and a random number. Once the solution is found, the block is considered "solved" and assigned a unique ID. After solving the block, the winning node broadcasts their success to the rest of the nodes, who, in turn, verify the transaction. On the Bitcoin Blockchain, the winning node is rewarded for solving the block with a bitcoin— incentivizing miners to continue securing the Blockchain. After the verified block is officially added to the Blockchain, it can no longer be altered. This immutability is created by the mathematical link between each block in the chain. Tampering with an individual transaction or block requires altering the mathematical function of multiple blocks at myriad points on the Blockchain. This would mean changing millions of geographically dispersed computer nodes *simultaneously*.

The Bitcoin Blockchain is the oldest and most secure, publicly used blockchain. Bitcoin is the "token" or vehicle which moves assets across the Blockchain. Put another way, if the Bitcoin Blockchain is the train track, Bitcoins are the train cars upon which goods are moved from one place to the next. And while the Blockchain can be used to move bitcoin, the digital currency, users can put anything of value on top of the bitcoin, as each bitcoin can be divided into as many pieces as needed to move the asset traveling on top of it. While anyone can create their own blockchain, the older the blockchain –and the wider the network of nodes verifying the information on it –the more secure it becomes.

BENEFITS OF BLOCKCHAIN

The Blockchain's immutability, decentralization and cryptography protect against both hacking and internal fraud. These components allow for real-time and retrospective auditability – further reducing costs while increasing transparency. Blockchains effectively establish a single, authoritative source of truth for institutions, providing a comprehensive digital paper trail for both internal reference and external auditors, regulators and business clients wishing to access data. The technology creates real trust and real security. The Blockchain is transforming the internet from an avenue of information exchange to a mechanism for moving real value.

USES OF BLOCKCHAIN

The most obvious applications for blockchain technology are in the financial services industry. Reducing costs and complexity associated with financial transactions has the potential to open the global economy to billions of unbanked individuals. But blockchain goes far beyond finance—from agriculture to supply chain, foreign aid delivery to identity management, insurance to governance, medicine to media, education to property rights–and everything in between. All around the world, blockchain technology is being piloted to improve many of the underlying systems which make our lives possible. It can be used any time someone needs a secure, immutable and efficient way to store or transfer value.