UNLOCKING THE REAL BENEFITS OF BLOCKCHAIN THROUGH ITS "SWEET SPOT"
Various organizations are currently looking at a wide variety of applications for blockchain, the technology underpinning the cryptocurrency Bitcoin. However, in order to deliver the full capabilities of shared or distributed ledger technologies, it is necessary to focus on what its unique attributes and capabilities can provide to end-to-end business processes — rather than viewing it as a means to deliver what there is at present more efficiently, quickly and cheaply — principally through the removal of intermediaries.

This short paper describes the blockchain’s “sweet spot”, and where its key strengths and differentiating factors come into play.

1 BACKGROUND

The blockchain was developed in 2009 as the infrastructure supporting the Bitcoin cryptocurrency. However, it was soon realized that blockchain’s ability to provide a new form of distributed database or ledger could be applied across a broad range of applications in financial services. Hence, blockchain-based solutions have been developed and trialed by many different organizations. As the Monetary Authority of Singapore has said, “Distributed ledgers may be applied in any area which involves contracts or transactions that currently rely on trusted third parties for verification.”

2 KEY FEATURES

• Blockchain’s promise is “the decentralization of trust, enabling value flow without intermediaries”. It allows financial transactions to be verified and cleared without the need for a trusted third party sitting between market participants. Removing intermediaries reduces costs and complexity.

• The distributed ledger approach means that all the members of a financial market (the network) share an identical system of record, rather than each maintaining their own proprietary view of it. This replicated, shared ledger provides consensus, provenance, immutability and finality for the transactions concerned — payments, asset transfers, etc. This shared approach removes the need for reconciliations.

• New transactions are only accepted for posting to the distributed ledger (through the creation of new blocks for the chain) once all the computers in the network achieve consensus as to their validity. The verification of transactions by all network users reduces error rates and queries.

• At the heart of blockchain is a new type of distributed database. This provides for the exchange of information in a synchronous and even manner, as well as allows it to be updated constantly, providing near-instant clearing and settlement. The provision of faster settlement means less risk in the financial system and so reduces the capital requirements of market participants.

• The new distributed database functionality also allows code to run with the blockchain to modify data (both on and off the chain) automatically. This
enables the blockchain to support self-enforcing or “smart” contracts, allowing the automation of a variety of business functions.

- The blockchain’s security and privacy protocols are based on the use of a “cryptographic hash function” — each block (of transactions) in the chain is identified by its own “hash” key. This approach was developed to prevent the “double spending” of Bitcoins. The complexity of the crypto hash function reduces the blockchain’s susceptibility to fraud.

- Blockchains may be either:
  - Public or private, meaning they can be open to everyone or restricted to a defined group of users (e.g., institutions)
  - Permissioned or permissionless, meaning that either anyone can offer their services to add blocks to the chain or only a restricted group of users can do so
  - Bitcoin functions on a public, permissionless model and hence experiences performance issues with new blocks taking a long time to be added to the chain. Most blockchain use cases for other financial applications are based on the private, permissioned model which is less prone to performance issues, as the number of users can be controlled.

### WHAT BLOCKCHAIN IS

- A replicated, shared/distributed ledger of transactions or asset holdings which enables “collective bookkeeping”
  - It provides provenance, immutability and finality for the transfer of value within a business network.
  - It enables value exchange in real time, reducing costs and errors.
- Based on a network consensus approach, whereby trust between the parties involved in a transaction is provided by cryptography (i.e., mathematics)
  - This prevents “double spending” and protects the system from hacking, fraud, etc.
  - Cryptography replaces the need for third parties/intermediaries, which are not required to verify or clear transactions.

### WHAT BLOCKCHAIN ISN’T

- Despite some market sentiment, blockchain isn’t a panacea.
- Is yet to be appropriately regulated; however:
  - The EBA has started looking at a Europe-wide regulatory regime for virtual currencies.
  - There is some regulation in the U.S. via the NYDFS BitLicense regulations (but these are only applicable in NY State).
  - In the U.K., there is currently no specific regulation of the blockchain; however, regulators have expressed concerns over blockchain’s lack of controls over AML, ATF, etc.
- Cheap to operate
  - Public blockchains require significant power, space and energy to support them.
  - The nodes (or “miners”) require reward and incentivization to fulfill their essential network consensus role.
  - Once new regulations have been developed and introduced, blockchain will have significant compliance costs.
- Supported by internationally recognized and applied standards
  - However, some work is under way in this area — e.g., the R3 CEV initiative involving many large banks.

### WHAT BLOCKCHAIN COULD BE

As mentioned above, there are a plethora of companies currently leveraging blockchain technology to develop new applications. During the first 10 months of 2015, venture capitalists invested $921 million in Bitcoin and blockchain companies. Current market developments suggest the best opportunities for the deployment of the blockchain in financial services are in the following areas:

- Currency exchange – payments and remittances, interbank clearing and settlement
The diagram below illustrates how the key features of the blockchain can come together to create truly compelling use cases for the financial services industry.

**THE BLOCKCHAIN’S “SWEET SPOT”**

The diagram below illustrates how the key features of the blockchain can come together to create truly compelling use cases for the financial services industry.

**DEFINITIONS OF TERMS USED IN THE DIAGRAM**

There are two key types of blockchain where access level is either public or private:

- **Public** – where anyone can read and submit transactions to the blockchain
- **Private** – where the permission to read and submit transactions is restricted to users within an organization or group of organizations

and where participation level is either permissioned or permissionless:

- **Permissioned** – where a set of trusted parties carry out the verification, and additional verifiers can only be added with the agreement of the current members or a central authority
- **Permissionless** – where anyone can participate in the new transaction verification process; i.e., no prior

**TRUE BLOCKCHAIN BENEFITS ARE ONLY PROVIDED AT ITS SWEET SPOT**

**TYPE OF BLOCKCHAIN**

- Public
- Private
- Permissioned
- Permissionless

**TYPE OF INFORMATION/ACTIVITY**

- Rich Information
- Transaction-Based Data/Payment
- “Smart Contract” Programmable Money
- Dumb Data Transmission

**PROVIDING KEY BENEFITS**

- Mathematics used to enable trust between parties
- Secure yet shared view
- Full provenance and immutability
- Provision of comprehensive, rich information
- Automated verification/reconciliation
- Self-enforcing contract capability
authorization is required and a user ("miner") can contribute their computational power, usually in return for monetary reward.

The information within the blockchain can be either:

**Rich information or transaction-based data**

- Rich information – this is the value-added information which is not included in transaction data at present, e.g.:
  - The verified digital identities of all parties to the transaction (e.g., evidential KYC checks)
  - The verified AML and ATF “watch list” databases against which the transaction has been checked, e.g., those of U.K., European and U.S. authorities
  - Together with any “false positives” which have already been reviewed and discounted
  - Broad information around the context of the transaction, e.g., information on the overall supply chain to which it relates
  - The information necessary for the blockchain to undertake any “smart contract” processing
- Transaction-based data – this comprises the basic information for the transaction (e.g., payment) concerned, such as:
  - PKI/hash-tag information assuring the transactions authenticity and validity (standard blockchain verification)
  - The transaction type, e.g., payment, asset transfer
  - The parties to the transaction, e.g., payer and payee
  - The amount, currency, value date and, possibly, asset type
  - Transaction narrative and references

**The blockchain can use the information in two ways:**

- Dumb data transmission – whereby the blockchain merely processes (actions/“posts”) the instruction without considering contingent or other types of standing instructions (“if, then...

- “Smart contract”/programmable money – whereby the blockchain itself is able to evaluate whether the transaction it is processing meets certain criteria, in which case it automatically instigates other actions
  - This enables the blockchain to support and enable various types of “self-enforcing contracts”.
  - It can provide automation of sophisticated business processes and decision making.

- Hence, the blockchain itself can police, regulate and control the totally impartial processing of transactions between parties against a set of pre-agreed rules and in an entirely (code-driven) impartial manner.

---

**FINANCIAL SERVICES USE CASES THAT MISS THE BLOCKCHAIN “SWEET SPOT”**

Having identified the components of its “sweet spot”, it is clear that many applications either in place or in development do not harness the blockchain’s key attributes. By way of an illustration of this, consider a payments application which:

- Is not a true blockchain P2P solution, as it doesn’t interface directly with consumers
- Is still based on intermediaries as the service is offered via banks, payment processors and money transfer companies
- Requires the use of network “miners” to receive, validate and post new blocks to the chain — these all require to be paid for their work

Such an application doesn’t hit the sweet spot because:

- It’s just a means to deliver what’s there at present (supposedly) more efficiently, quickly and cheaply
- It’s based on a public/permissionless (not a private/permissioned) network — so it requires “miners” to function
- It’s based on the processing of simple transaction-based data, not rich information — so KYC and AML remain “off-chain”
- It doesn’t utilize blockchain’s “smart contract” capabilities
The following types of business processes readily lend themselves to enabling the blockchain’s “sweet spot” to be brought into play:

**Supply chain and trade finance**
- Plays directly to many of the blockchain’s principal strengths
- Mathematics is used to achieve trust between the parties to a transaction
  - The current role of banks in trade transactions is principally to accept risk, thereby allowing the parties to trust each other.
- Allows shared access for all parties within the supply chain (buyers, suppliers, banks, logistics companies, insurance companies, customs and health authorities, etc.) to the single view of the truth
- A private, permissioned blockchain can restrict access only to those parties involved in the supply chain concerned
- The delivery and use of rich information — i.e., transactions on the chain would include invoice numbers, certificates of origin, bills of lading, bills of exchange, insurance documents, customs documents, health certificates, etc.
- “Smart contract” capabilities enable automated decision making and information handling
  - Again, the current role of banks in trade transactions is all about considering whether to make a payment based on an assessment of the documents presented to them — classic “smart contract” territory.

**Securities post-trade**
- The total cost to the finance industry of clearing, settling and managing the post-trade environment is estimated in a 2014 Oliver Wyman report at between US$65 billion and $80 billion per year.
- There are already a number of industry-level initiatives investigating and developing applications for the use of blockchain in this area — e.g., R3 CEV which is developing new standards for use on blockchain.
- These initiatives feature the participation of all the key market players (stock exchanges, clearing houses, banks, brokers, etc.).
- The back-office elements of much current post-trade activity are based on archaic, complex processes of which many still lack automation — manual reconciliation, fax machines are still used, etc.
- Further, the clearing and settlement of transactions requires the intervention of a variety of intermediaries and third parties (e.g., exchanges, clearing houses, depositaries and custodians) all adding complexity and cost.
- However, the nature of this post-trade processing plays to the blockchain’s “sweet spot” because:
  - Mathematics is used to achieve trust between the parties, this removes the need for intermediaries
  - It allows shared access for all parties to the asset transfer transaction — buyer, seller, brokers, banks, depositaries, custodians, etc. — to the single, view of the truth
  - A private/permissioned blockchain can restrict access only to those parties involved in the asset transfer concerned
  - The delivery and use of rich information — i.e., transaction on the chain — would include all the relevant information: the asset class/type, full provenance of the asset (its full ownership history since issuance), the asset's coupon/interest rate, etc.
  - “Smart contract” capabilities enable automated decision making and information handling, thus providing much greater speed, efficiency, accuracy and lower cost to the existing clearing and settlement processes

**Hidden payments**
- Hidden payments are:
  - Transactions undertaken through non-bank providers which are both not subject to the same regulation as banks and not required to report their payment transactions
  - Include cash stored on digital wallets, points stored on store loyalty programs, the Starbucks mobile app, etc.
- The World Payments Report 2015 highlighted the issue of hidden payments and estimated that c.40 billion hidden payment transactions were completed in 2014 and that this volume is increasing very quickly.
Hidden payments and the digital wallets supporting them are becoming an increasingly important issue for regulators who are unable to either monitor or control the transactions concerned. This lack of regulation also means that the huge sums stored by consumers on their digital wallets — either in the form of cash or loyalty points — are not protected unlike bank deposit under legislation such as the U.K.’s Financial Services Compensation Scheme.

- There is believed to be over $1 billion of funds lodged on the Starbucks app alone.

The nature of this hidden payments market also plays to the blockchain’s “sweet spot” because:

- Mathematics is used to achieve trust between the parties
- It allows shared access for all parties to the transaction — card holder, digital wallet issuer, the store, regulators, etc. — to the single view of the truth
- A private/permissioned blockchain can restrict access only to those parties involved in the digital wallet concerned
- The delivery and use of rich information, e.g., about the card holder’s eldentity and spending patterns; for regulators, the total amount of value stored (i.e., at risk) on the digital wallets issued by specific organizations (e.g., Starbucks)
- “Smart contract” capabilities enable automatic decision making and information handling, so consumers could set rules so that their eWallet could be topped up when required from their bank account, that any balance above a certain amount be returned to their bank account from their digital wallet, etc.

What follows is a summary of their views and the approaches they are taking to look at blockchain in a way that goes beyond the hype and responds to increasing pressure to turn blockchain activities into more tangible and measured assessments of the technology’s pros and cons.

There is a general recognition that blockchain will have a transformative impact on the financial services industry. However, today it is viewed as immature, and the timeline typically quoted during which its potential will be realized is three to five years. Few see immediate gains, but they are nonetheless investing in assessing blockchain’s value.

The extent to which interviewees believe blockchain-based applications are dependent on, or linked to, other innovative activities in financial services varies. Some see the growth in digital services, open data initiatives and expansion of markets to accommodate new ideas and entrants as supportive of blockchain, while others believe it is so disruptive it will have an independent, explosive effect and drive a range of new services.

When it comes to the proliferation of industry groups looking at blockchain, interviewees believe the collective “herding” is a “comfort to the industry” and a low-cost way in which to keep each other informed and aware of developments as a “club”.

“There is no harm in a club that helps us all collectively look at the opportunity and speeds up the potential to rule use cases in or out,” said one. Investment in industry groups is simply “entry membership” and affordable at this time. The representative of one software provider said blockchain has the potential to strip out billions of costs in the market and banks paying an advisory fee to collectively pursue the benefits is acceptable — but that investment in a single solution is not.

This led to discussions around the public and private images of blockchain technology. There is increasing activity in banks to pilot projects and evaluate blockchain-based developments without a deliberate, clear focus on the commercial benefits. Instead, attention is focused on the core technology and the potential for how a distributed ledger that maintains a continuously growing set of data records securely offers value, for example through operational efficiencies, governance controls and innovative client services. The projects are not significant in terms of resource and cost, but they are focused on satisfying increasing demand from senior executives and board
members to prove the benefit of blockchain. As one interviewee said, “actually understanding it ourselves”.

In summary, the focus on blockchain has shifted and is now on understanding the technology and the value it offers, as opposed to some months ago when it was more of a collective huddle and a focus on collaboration and shared intent. However, there is still no clear emergence of where blockchain sits in terms of technology, business benefits and application. “We don’t know who will own it and who will benefit so maybe the wrong group within a bank is looking at the benefit?” said one interviewee.

There is acceptance that the hype, media attention and general misunderstanding has to be balanced, and increasingly there is a more pragmatic, considered approach to blockchain and its application.

Interviewees endorsed the concept of the “sweet spot” as a more structured approach to the core tenets of what blockchain is and what it can be in terms of financial services. In particular, a sweet-spot approach is perceived as extremely helpful in raising the level of debate about blockchain to a management and executive level. It prompts alternative thought processes and a rethink of the questions to ask of an emerging technology that has until now been clouded by the supposed multiple levels of value it brings, driven by hype and self-interest.

There is a growing acceptance among interviewees that a permissioned distributed ledger offers greater potential to launch a service to a core group (including banks and clients) with speed, control and safeguards — and exploiting common standards, protocols and governance.

So where next? The banks did not plan for blockchain, but the direction is clear. Few people fully understand blockchain within banks, but everyone is asking powerful questions as to what it is and what it offers. It is not seen as a lethal threat to banking, but it is seen as disruptive new technology they have to understand more fully, and for which they must develop a strategic approach to deployment. As one interviewee said: “I actually don’t understand how we have reached such a stage of involvement in the bank without ownership or control. We need a blockchain czar.”

What is absolutely clear is the recognition that there is a need to separate the hype from the reality and from an executive and strategic perspective, to take a fresh look at what blockchain offers banks, and what banks must do to adopt it.
Finextra Research is the world’s leading specialist financial technology (FinTech) news and information source. Finextra offers over 100,000 FinTech news, features and TV content items to visitors to www.finextra.com. Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organizations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra’s unique global community consists of over 30,000 FinTech professionals working inside banks and financial institutions, specialist FinTech application and service providers, consulting organizations and mainstream technology providers. The Finextra community actively participates in posting its opinions and comments on the evolution of FinTech. In addition, they contribute information and data to Finextra surveys and reports.

For more information, visit www.finextra.com, follow @finextra, contact us at contact@finextra.com or call +44 (0)20 3100 3670.
ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.

LEARN MORE

WWW.ACIWORLDWIDE.COM
@ACI_WORLDWIDE
CONTACT@ACIWORLDWIDE.COM

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2017
ACI, ACI Worldwide, ACI Payment Systems, the ACI logo, ACI Universal Payments, UP, the UP logo, ReD, PAY.ON and all ACI product names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties’ trademarks referenced are the property of their respective owners.

ATL6445 07-17