PRACTICAL BLOCKCHAIN

Uncovering a true potential of the disruptive technology.

About

Velmie is a leading provider of Blockchain solutions for Finance and Ecommerce. Being recognized as Top Blockchain Solutions Provider by Clutch.co in 2018, our company put a lot of efforts in order to educate executives and entrepreneurs about Blockchain and Distributed Ledger technologies, helping to identify the practical sense of it. Despite of a cryptocurrency hype, there are a lot of real-world use cases remain undiscovered or underestimated. Many also don't recognize Blockchain as something that can be used somewhere else except coin speculations and ICOs. This situation puts many companies at risk of being affected by disruptive presence of Blockchain and our mission is to help to figure out how this technology can contribute to your business, making it secure, scalable, more efficient, sustainable and, the most importantly, making it more profitable.

Whether you have an idea, on-going project, or you are just curious about Blockchain; we provide free consultations. We will educate you and your team on what it will take to accomplish a project and what technologies we recommend to do the job right.

For more information please visit Velmie.com

Or drop us a line at hello@velmie.com

Table of Contents

Introduction to Blockchain

'Blockchain' has become one of the most hyped technologies since the Internet. It is also one of the most poorly understood. A recent HSBC global survey found that 80% of those who have heard of 'Blockchain' said they don't understand it. This state of affairs exists despite the fact that significant effort has been made to explain blockchain technology to non-technical audiences through the mainstream media, industry reports, academic and online courses, and other channels.

What is Blockchain?

In simple terms, Blockchain is a type of database that is replicated over a peer-to-peer (P2P) network. However, this definition could also apply to other types of distributed databases that have no central database manager, such as ones sold by software vendors like Oracle. So, what makes Blockchain special?

The principal way in which Blockchain is different from other distributed databases is that Blockchain is designed to achieve consistent and reliable agreement over a record of events (e.g., "who owns what") between independent participants who may have different motivations and objectives.

Put in a slightly different way, participants in Blockchain network reach consensus about changes to the state of the shared database (i.e., transactions amongst participants) without needing to trust the integrity of any of the network participants or administrators. The agreement between Blockchain network participants over the state

of the database is achieved through a consensus mechanism, which ensures that each participant's view of the shared database matches the view of all other participants. The combination of the consensus mechanism with a specific data structure allows Blockchain to solve the so-called 'double spending' problem – the same digital file being 'copy-and-pasted' and transferred multiple times – without requiring a centralised ledger or party that prevents users from duplicating/spending the same digital file twice. Blockchain can thus facilitate the transfer of assets and other data without needing a trusted central authority.

The elimination of a central third-party administrator brings further benefits. Put simply, participants can independently verify that what they see (i.e., the content of the database at a specific moment in time) is consistent with what every other participant also sees. This ensures that all participants have a consistent view of the shared database state. As a result, any improper alteration of the data (e.g., tampering by a malicious actor) will be immediately detected and rejected by all participants. This ability of Blockchain network participants to independently verify the integrity of the shared database without having to rely on a trusted third party is one of the main value propositions of using Blockchain.

The Key Components of Blockchain

Blockchain generally has the following five components:

1. Cryptography

Use of a variety of cryptographic techniques including cryptographic one-way hash functions, Merkle trees and public key infrastructure (private-public key pairs).

2. P2P Network

Network for peer discovery and data sharing in a peer-to-peer fashion.

3. Consensus Mechanism

Algorithm that determines the ordering of transactions in an adversarial environment (i.e., assuming not every participant is honest).

4. Ledger

List of transactions bundled together in cryptographically linked 'blocks'.

5. Validity Rules

Common set of rules of the network (i.e., what transactions are considered valid, how the ledger gets updated, etc.)

Blockchain enable entities to have shared control over the access to and evolution of data. Blockchain can provide clarity around asset and data ownership by creating a complete, tamper-resistant record of ownership changes. Network participants can consider the blockchain as the authoritative data source of ownership claims. Moreover, a participant can 'own' the recorded asset or data in question when controlling the associated private key. This means that the owner is in complete control of the asset or data; it cannot be transferred without the owner's explicit consent.

A Brief History of Blockchain

Wider interest to Blockchain technology developed after the launch of Bitcoin by Satoshi Nakamoto in 2009. Bitcoin utilizes Blockchain as a transaction ledger to securely record transfers of Bitcoins from one party to another. However, Nakamoto's original paper does not mention the term 'blockchain', which first appears as 'block chain' in a comment in the original Bitcoin client C++ source code. Much of Nakamoto's writing focused on Bitcoin as an alternative currency and store of value, with much less attention given to the many different 'non-currency' uses of Blockchain technology (e.g., serving as a voting system). Similar to many other buzzword technologies (e.g., machine learning), Blockchain technology is less of a new technology than a clever combination of existing technologies (P2P networking, distributed timestamping, cryptographic hashing functions, digital signatures, and Merkle trees, among others) that have in some cases existed for decades.

A few years after Bitcoin was launched, attempts were made to go beyond simple P2P value transfers and offer functionality not available in Bitcoin. For example, in 2012, the concept of 'coloured coins' emerged, which enabled the Bitcoin Blockchain to be used to record and transfer 'non-native' assets and data.

In 2013, public awareness of cryptocurrencies dramatically increased, and a number of more established organisations began to inspect Bitcoin and related technologies to see how they could be exploited. The breadth of potential use cases facilitated by the technology was noted, but many concluded that using a public Blockchain such as Bitcoin was ill-suited for regulated corporations for a variety of reasons. For instance, financial institutions seemed

uncomfortable using a public infrastructure run by anonymous miners and powered by an unregulated, volatile currency. Legal and reputational issues also gave many organisations pause. However, many organisations recognised that the Blockchain – the particular data structure underlying Bitcoin and other cryptocurrencies forming an auditable log of transaction records – was a key innovation.

Work began on how best to adapt Blockchain technology for the needs of large and regulated organisations. For example, it was determined that substituting Bitcoin's anonymous miners with known participants would allow institutions to remove the native currency and replace the energy-intensive, computationally difficult proof-of-work (PoW) puzzle needed for reaching consensus in Bitcoin with a less resource-intensive and more efficient consensus algorithm.

Why to Use Blockchain?

Blockchain can be useful in situations where there is a desire to minimize the degree of trust required between participants, or where participants would like to reduce their dependence on an intermediary service provider (e.g., central securities clearing house). Problems arising from the abuse of trust, such as fraud, have significant negative impact on business and trade: the global financial cost of fraud is estimated to have been more than $4 trillion in 2016 alone.

Historically, we have either relied on informal trust (e.g., handshake agreement) or formal trust that functions by introducing intermediaries (e.g., courts) through which legal recourse can be sought in the event of misbehavior. However, these approaches are far from perfect. Blockchain hold the promise of reducing the 'trust gap' by making actions within the system independently verifiable by each participant, introducing or improving accountability, and dis-incentivizing misbehavior through public auditability.

There are a number of trust-related benefits that Blockchain bring: data records or digital assets cannot be counterfeited or forged once they have been recorded into the Blockchain. Assets and data records cannot be created 'out of thin air' without participants noticing, and 'miners' cannot transfer assets and data records of other participants without their explicit consent (expressed in the form of a digital signature).

Separate entities using Blockchain network can leverage that shared infrastructure to effectively streamline inter-organizational business processes, with strong verifiability guarantees to have a consistent view of the data. This also enables the avoidance of costly and error-prone reconciliation processes between isolated data 'silos'. Moreover, the ledger gives participants the assurance that everyone is storing, seeing, using, and processing the same data as everyone else. Fraud can be immediately detected, and auditing is made significantly easier and less expensive as the Blockchain provides a real-time audit trail. Blockchain can also go much further than simply offering improved auditing or accountability. To paraphrase Muneeb Ali, Co-founder of Blockstack, Blockchain can help us move from a world where today we rely on 'good guys' and mottos like "don't be evil" to a world where Blockchain systems help ensure we 'can't be evil'. In other words, the rules governing Blockchain can effectively eliminate the types of unauthorized transfers or fraudulent activity that have become all-to-common in many areas of business and society.

Blockchain Myths

While the use of Blockchain may provide transformative advantages over other technologies in some cases, they are not a panacea and do not magically solve every problem. Many publications, reports, and news articles focus primarily on the 'pros' (and occasionally exaggerate the positive impact Blockchain technology can have) without mentioning or giving balanced attention to the 'cons'. We believe it is important to understand the limitations of Blockchain technology, as well as the different trade-offs that arise as a result of different architecture and design choices. Without a clear understanding of these trade-offs, it is impossible to know where Blockchain technology can be best applied, let alone whether it should be considered at all.

Debunking Common Myths

MYTH: Blockchain is 'trustless'

REALITY: Blockchain always require some degree of trust. Although Blockchain may help reduce the need for trust, they do not completely remove the need for trust. At the bare minimum, trust must be placed in the underlying cryptography. In the case of a permissioned network, trust must be placed in the operator(s) and/or the validators. If well configured, permissioned Blockchain is at best 'trust-minimizing' in the sense that they enable participants to independently validate transactions and verify the state of the system.

MYTH: Blockchain is immutable or 'tamper-proof'

REALITY: Transactions on Blockchain network can be reversed by network participants under specific circumstances. Similar to 'trustlessness', absolute immutability does not exist. The illusion that

Blockchain transactions are immutable stems from its append-only data structure that suggests that data can only be added to, but not removed from the database. However, blocks comprising transactions can, in theory, be reversed if enough nodes decide to collude. Reversing transactions may be even easier with permissioned Blockchain than public Blockchain, where colluding miners would at least need to spend computational power and/or cryptocurrency funds to do so. However, permissioned Blockchain actors are bound by legal contracts and agreements that are designed to dis-incentivize collusion or other misbehavior. If 'mining' in a permissioned Blockchain is sufficiently decentralized across separate entities with different motivations, one can consider the Blockchain to be tamper-resistant.

MYTH: Blockchain is 100% secure

REALITY: Blockchain is not automatically more secure than other systems. Blockchain employ cryptography for authentication, permission enforcement, integrity verification, and other areas. The mere application of cryptography, however, does not automatically make the system more secure per se. The system may be more resilient as data storage and permissions are distributed, but compromising the private keys of some network participants could give attackers full access to the shared database, including the ability to reverse transaction history. As a result, the management of private keys constitutes a crucial challenge. There is also the widely discussed "51% attack", where malicious nodes can double spend or wreak other havoc on Blockchain.

MYTH: Blockchain is 'truth machine'

REALITY: GIGO ('garbage in, garbage out') applies to every Blockchain that uses non-native digital assets and/or external data inputs. Blockchain is particularly well suited for the transfer of assets or data native to the respective Blockchain (e.g., Bitcoin). However, Blockchain cannot assess whether a given input from the 'outside

world' is accurate/true or not. If the input is inaccurate or wrong, the Blockchain will just treat it as any other input and consider all transfers involving the input as valid as long as certain conditions are met. This goes back to the first Blockchain myth of trustlessness: if 'off-chain' assets or data sources are digitally represented on the Blockchain, a trusted third party is required to verify and guarantee the accuracy of the input when inserting it into Blockchain.

Private vs. Public Blockchain

In order to distinguish these new permissioned Blockchain from the open, public Blockchain that power cryptocurrency systems, the industry started using terms like 'private', 'permissioned' or 'closed' to refer to Blockchain network where access is restricted to a specific set of vetted participants. In practice, these terms are often used interchangeably. However, Blockchain can be further segmented by distinguishing between different types of permission models. The permission model refers to the different types of permissions that are granted to participants of Blockchain network. There are three major types of permission that can be set when configuring Blockchain network: Read (who can access the ledger and see transactions), Write (who can generate transactions and send them to the network), and 'Commit' (who can update the state of the ledger).

The key differences between open and closed Blockchain relate to their security and threat model. Public permissionless Blockchain operate in a hostile environment with unknown actors, requiring the use of 'crypto-economics' – a combination of game theory and economic incentive design applied to cryptographic systems – to incentivise participants to behave honestly (e.g., by rewarding miners with tokens native to the system, such as Bitcoins) and to keep the network censorship-resistant – at least to a certain extent.

In contrast, private permissioned Blockchain operate in an environment where participants are already

known and vetted, which removes the need for a native token to incentivise good behaviour. Participants are held liable through off-chain legal contracts and agreements, and are incentivised to behave honestly via the threat of legal prosecution in the case of misbehavior.

For the remainder of this study, we will focus on Blockchain systems where access is restricted to a specific set of participants (i.e., private/permissioned/closed Blockchain). These terms will be used interchangeably when referring to closed Blockchain.

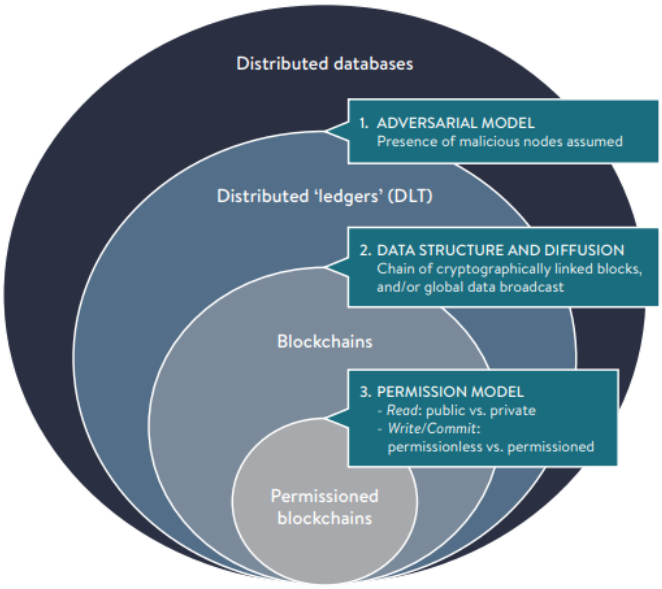
Deciphering Blockchain Jargon

A confusing number of new terms and buzzwords have emerged in the last few years to describe the technology underlying systems based on or inspired by Bitcoin. These different terms are often used interchangeably, adding to the general confusion Blockchain newcomers face. The first Blockchain were closely based on the architecture of Bitcoin, where transactions sent across the system are bundled into a new 'block'. This new block references the preceding block, effectively forming a chain of cryptographically linked transaction bundles. New database systems have emerged that are also often referred to as Blockchain, but which do not share the main characteristics of 'traditional' Blockchain used by cryptocurrencies. For instance, some are 'block-less' (i.e., not grouping transactions into blocks, but directly chaining them together), others do not broadcast all transactions to each participant, and yet others do not reach consensus on the state of the global ledger but rather on the state of sub-ledgers or channels. Some systems have no similarities with early Blockchain except that they use some of the same cryptographic primitives.

The development of these new types of systems, loosely built on the original Bitcoin blockchain concept, has resulted in the emergence of a new, more generic term – distributed ledger technology (DLT). 'DLT' has replaced 'blockchain' or 'blockchain technology' in 2016 as an umbrella term to refer to all these new systems that are built on the premise of enabling a shared database between parties seeking to reduce the need for trust or depending on an intermediary. The trend seems to be reversing in 2017, however, with 'blockchain' recently gaining in popularity again. It can be observed that in practice, both terms are often mistakenly being used interchangeably.

Framework

The following figure introduces a simple framework that can be used to easily distinguish between traditional distributed databases, distributed ledgers, and Blockchain. Distributed ledgers are a subset of distributed databases, and Blockchain are a subset of distributed ledgers.



Distributed Database

Distributed databases are a type of database which have no central 'master database' that unilaterally decides on updating the database state. Rather, they are replicated across multiple nodes (and devices) that collaborate to maintain a consistent view of the database state. These systems are designed to provide fault tolerance, i.e., ensuring that the system continues to work in case some nodes fail and become unresponsive. However, it is assumed that all nodes are honest as they are all cooperating and freely sharing data with each other based on mutual trust. This means that

distributed databases are generally operated by a single entity that maintains strict access control to the network, which operates in a trusted environment.

Distributed Ledger

Distributed 'ledgers' are a subset of distributed databases that use a different assumption about the relationship between nodes. Their design is based on an adversarial threat model that mitigates the presence of malicious (i.e., dishonest) nodes in the network. They are designed to be Byzantine fault-tolerant, meaning that the database should be able to synchronise and run even if a certain number of nodes are acting maliciously. In contrast with traditional distributed databases that operate in a trusted environment, individual nodes do not trust their peers by default and thus need to be able to a) independently verify and validate transactions that update the database state, and b) independently recreate the transaction data log (i.e., the entire transaction history).

Blockchain

Blockchain can be thought of as a special subset of distributed ledgers that share the same adversarial threat model, but have additional characteristics that set them apart. Interestingly, in the enterprise Blockchain industry there is no clear consensus on the definition of Blockchain. Some argue that systems called Blockchain need to make use of a special, append-only data structure that is composed of transactions batched into blocks, which are cryptographically linked to each other to form a sequential, tamper-evident chain that determines the ordering of transactions in the system. Others use a broader definition that allows for the inclusion of 'block-less Blockchain' (transactions are not batched into blocks, but directly chained together and instantly confirmed), and determine global data diffusion (i.e., all transactions are broadcast to every node) as the distinctive characteristic.

Wrapping Up

In general, the term ‘distributed ledger technology’ refers to all initiatives and projects that are building systems to enable the shared control over the evolution of data without a central party, with individual systems referred to as ‘distributed ledgers’. If one wants to describe a system that has global data diffusion and/or uses a data structure of chained blocks, one should call it a ‘Blockchain’.

However, ‘Blockchain technology’ and ‘distributed ledger technology’ are still commonly used interchangeably despite attempts to semantically separate them by their different underlying architectures. It can be observed that both umbrella terms have evolved into including flexible architectures that apply some of the cryptographic principles used in early Blockchain to traditional distributed databases as well, although these systems may not provide the same independent verification mechanisms and thus may not truly work in adversarial environments.

Market Targeting And Usage

• Financial and insurance-related DLT use cases are the most heavily targeted industry sectors.
• 30% of identified DLT use cases are related to banking and financial services, followed by government (13%), insurance (12%) and healthcare (8%).
• Attention given to non-monetary uses (identity, supply chain, intellectual property, etc.) is increasing.
• Financial sector institutions (and banks in particular) currently constitute the most significant user base of DLT service providers.
• While the majority of infrastructure providers have a generic solution that can be applied to any industry, half of them target a specific industry sector or business case(s).
• The median number of projects supported by infrastructure providers amounts to seven; however large differences between respondents are observed, with figures ranging from three to over 400 projects.
• Some enterprise DLT frameworks have been downloaded as many as 20,000 times.
• Number of individual corporations using a specific platform or network ranges up to 70.

Business Models and Licensing Strategy

• Apache 2 and MIT license are the most frequently used open-source licenses; getting the product accepted in the space constitutes the main reason for open-sourcing the codebase (79%).
• It is more common for infrastructure providers to fully open-source their codebase (27%) than network operators (8%) or application providers (0%); one-third of infrastructure providers currently running proprietary platforms plan to open them in the near future.

• Significant uncertainty exists over DLT revenue models: most infrastructure providers use a combination of multiple revenue models, whereas 42% of operators are focusing on a single revenue model.
• 60% of infrastructure providers with open codebase monetise their platform by providing consulting services; 44% of proprietary software vendors are still undecided about what revenue model to use.
• Monetisation of DLT infrastructure platforms primarily occurs at higher stack levels (consulting, application development, support), effectively turning them into full service providers.
• Application developers are often moving down the stack and building networks themselves.
• Lack of clarity around roles and positioning of enterprise DLT actors indicates the ecosystem is still maturing.

Maturity

• 39% of study participants have production-ready platforms and 36% are running advanced pilots; software services are further ahead than operators.
• The current DLT landscape is highly fragmented, with dozens of competing protocol frameworks and hundreds of isolated, small-scale networks mostly used for testing purposes.
• While the infrastructure layer is maturing, the deployment of production-ready networks is lagging behind.
• We expect to see the emergence of large-scale networks (industry-specific, use case-specific, and geography-specific) in the near future; focus will gradually shift to the application layer with the main value created at the network layer.

Use Cases and Industry Sectors

50% of infrastructure providers provide a generic DLT platform or framework that can be used to develop networks or applications for any number of use cases in a variety of industries. Similarly, 40% of

application developers indicate that they build applications for any use case available and do not limit themselves to a specific industry sector. Nevertheless, some of them do currently specialise in various use cases and target particular sectors as part of their business strategy to promote their infrastructure platform, despite having general-purpose implementations that could be deployed for every imaginable use case. In contrast, all operators are focusing either on a specific industry or business case.
66% of study participants are explicitly focusing on developing sector-specific solutions that are purposefully designed to serve a particular set of use cases. Not surprisingly, infrastructure providers and application developers tend to focus on more use cases and sectors than operators: the latter often build a network or application that serves a specific business case.

We have compiled a list of 132 DLT use cases and segmented them by industry (the following figure). Findings indicate that almost a third of all use cases featured in the list are applicable to the banking and finance industry. This may be an indication that the current focus of DLT still primarily lies in monetary use cases, which may simply be a consequence of the first (public) Blockchain powering currency-related applications.

Our survey data confirms the use case estimate above: financial services, payments, and banking services are the most frequently targeted sectors by study participants (the following figure). Capital markets are clearly dominating, followed by insurance and trade finance. Although much focus is still put on monetary use cases, an increasing interest in nonmonetary use cases and applications can be observed (e.g., identity, supply chain).

Interestingly, only 8% of operators currently use their DLT network or application for payments. In contrast 81% of infrastructure providers indicate that their DLT platform is suitable for payments, and 85% of infrastructure providers are specifically focusing on capital markets. All operators composed of established banks and technology firms

are primarily focusing on DLT applications for digital identities and regulatory compliance, whereas 'start-up operators' are mostly engaged in activities related to capital markets. Application developers are currently most frequently involved in developing applications for insurance and regulatory compliance (80%).

Percentage of DLT Platforms Tracking Different

70% of study participants indicate that their DLT systems are suitable for tracking financial assets ranging from currencies, securities, and derivatives to syndicated loans and loyalty points, among others. Only the tracking of intangible data records (e.g., medical records, KYC records, ownership records, social media content, etc.) is cited more frequently (73%). 55% also indicate that their DLT solutions are used to track digital identities as well as physical items in tokenised form, such as diamonds and gold, artworks, and, generally, all types of goods that pass through a supply chain.

Types of DLT Users

The survey data on the major users of DLT are in line with the previously highlighted view that the financial sector is the main user of DLT: 72% of study participants indicate that banks are using their platforms and/or services, and 42% report that custodians and exchanges are engaged in activities involving their DLT solutions.

Interestingly, 'non-DLT' financial technology (FinTech) companies constitute the second largest user of DLT platforms (56%), and a fourth of platforms indicate that private individuals are also using their offerings. Another interesting data point is that 36% of study participants report that regulators and government agencies are using their services, indicating that the public sector is already significantly involved in DLT activities.

The figure also highlights the large diversity of user types that are engaged in DLT. The ‘Other’ category contains a variety of firms focusing on different types of technologies, system integrators, and Internet of Things (IoT) companies, but also includes service providers such as KYC aggregators. Moreover, energy companies, title and real estate companies, airlines, retailers, hospitals, and healthcare organisations are testing or using DLT applications as reported by study participants.

While the majority of infrastructure providers indicate that their main customers and users stem from the financial sector (mainly banks and FinTech companies), it is more difficult to determine a ‘typical’ user type for network and application operators as they are often focusing on specific use cases or industries. Unsurprisingly, infrastructure providers have a more diverse number of user types, although this is often limited to user types from the same industry sector. This reinforces the observed targeting of specific sectors by many software services. In contrast, operators generally have a lower number of user types that participate in their network: 78% of operators have four or less user types, compared to only 29% of infrastructure providers.

Enterprise DLT systems are being used by groups of users as small as five to as large as 12,000. Data obtained from survey participants indicates that software downloads range from 12 to 20,000 downloads per infrastructure provider, suggesting that the number of (loosely defined) ‘users’ could be as high as 20,000 for a single DLT framework.
The data suggest that the number of corporations using a specific platform or network remains rather small to date, with figures ranging from five entities to a maximum of 70.

Future Trajectory

We have yet to see the emergence of dominant networks with a considerable number of participants that have established themselves as platforms upon which applications can be built. For this reason, the number of publicly known applications built on enterprise distributed ledger networks is still rather small, and the majority constitute permissioned applications that are built on the public Bitcoin or Ethereum main nets. However, we anticipate that in the medium to longer-term, the core protocol layer will consolidate around a limited number of enterprise DLT frameworks and platforms that will co-exist and serve different business needs and requirements. A significant number of small- to large-scale networks will be deployed on top of that core infrastructure layer, and these networks will be operated by a wide variety of entities and institutions. The main focus will thus shift from the core protocol layer and the network layer to the application layer.

As a result, the main value will likely not be created at the protocol layer, but at the network layer operators that manage large networks composed of key players of a specific industry or region will be able to leverage their network to attract new participants, applications, and plug-ins that want to interact with the enterprise network.

Operators acting as the gatekeepers to the underlying network can then monetise the network by requiring access fees to applications and plug-ins that want to get access to the shared market infrastructure. After the major networks have been established, the key focus of developers will shift to the application layer. It is reasonable to assume that a rising number of applications will be ledger-agnostic and interact with various enterprise networks. Some

applications may also connect different enterprise networks and facilitate interaction between otherwise separate networks.

Four Blockchain Use Cases for Banks

Reduction of Fraud

Chris Mager of BNY Mellon Treasury Services acknowledged that "one of the main challenges facing the banking industry today is the growth of fraud and cyber-attacks." Traditionally, bank ledgers have been created within a centralised database. This model has been more susceptible to hackers and cyber-attacks as all the information is located in one place – usually secured behind outdated legacy IT systems. Hackers and cyber-criminals are well aware of evolving digital technology and have been able to bypass these security systems to commit data breaches and fraud.

In contrast, as the Blockchain is decentralized it is less prone to this type of fraud. By using Blockchain there would not only be real-time execution of payments but also complete transparency which would enable real-time fraud analysis and prevention.

How?

Chris Huls of Rabobank defined Blockchain as **"a ledger or database that can store all types of information or value exchange that is publicly available for all participants in a group where they all see exactly the same data."** Therefore, as Blockchain is checked at every step of a transaction by independent miners, with all data being open and publicly available, there is a real-time analysis and verification of every bit of data and all information during the transaction. The Blockchain ledger can provide a historical record of all documents shared and compliance activities undertaken for each banking customer. Malicious attempts to view or change the data become part of the data itself, making third-party hacks immediately obvious.

For example, this record could be used to provide evidence that a bank has acted in accordance with the requirements placed upon it – should regulators ask for such clarification. It would also be of particular use in identifying entities attempting to create fraudulent histories. Subject to the provisions of data protection regulation, the data within it could even be analysed by the banks to spot irregularities or foul play – directly targeting criminal activity. This would be an advantage over the current banking and payments systems, which are more susceptible to fraud and hacking. Chris Huls stated, though, that there would need to be collaboration to achieve this in Blockchain. Banks would need to partner with regulators and FinTechs to "develop credible, decentralised ledgers permitting rapid adoption of global real-time payments and settlement."

On 30 December 2015 Nasdaq announced that it had made its first ever share trade using Blockchain technology. Nasdaq used its proprietary Linq platform (developed in collaboration with Chain.com and global design firm IDEO) to sell shares.

As Nasdaq has pointed out, within the multi-step manual process used today in banks and financial institutions there is not only plenty of room for error but also for fraud. By utilising Blockchain, organisations can reduce risk and administrative burden, as well as saving time and money.

Nevertheless, banks must consider that Blockchain doesn't yet eliminate all types of fraud.

In August 2016, nearly 120,000 units of digital currency Bitcoin worth about US $72 million was stolen from the exchange platform Bitfinex in Hong Kong. The Bitcoin was stolen from users' segregated wallets and amounted to about 0.75% of all Bitcoin in circulation at that time. Since the hack, Bitfinex has taken steps to reimburse account holders with "BFX tokens" which are cryptographic tokens on the

Omni Blockchain that can be exchanged for $1 beneficial interests in iFinex (Bitfinex's parent company).

KYC

Know Your Customer ("KYC") requests currently can cause delay to banking transactions, typically taking 30 to 50 days to complete to a satisfactory level. Current KYC processes also entail substantial duplication of effort between banks (and other third party institutions). While annual compliance costs are high, there are also large penalties for failing to follow KYC guidelines properly.
The average bank spends £40 million a year on KYC Compliance, according to a recent Thomson Reuters Survey, which also revealed that some banks spend up to £300 million annually on KYC compliance, Anti Money Laundering ("AML") checks and Customer Due Diligence ("CDD").

Since 2009, regulatory fines, particularly in the USA, have followed an upward trend with record-breaking fines levied during 2015. On-going regulatory change, with no one internationally agreed standard, makes it increasingly hard for banks to remain compliant. Thus, as it can take such a long time to on-board a new customer because of lengthening KYC procedures, this is having an increasingly negative effect on customer experience.

Chris Huls of Rabobank proposed the use case that "KYC statements can be stored on the Blockchain." Once a bank has KYC'd a new customer they can then put that statement, including a summary of the KYC documents, on Blockchain which can then be used by other banks and other accredited organisations (such as insurers, car rental firms, loan providers etc.) without the need to ask the customer to start the KYC process all over again.

These organisations will know that the customer's ID documents have been independently checked and verified so they will not need to carry out their own KYC checks, reducing their administrative burdens and costs. As data stored on Blockchain is irreversible, it would provide a single source of truth thereby minimising the risk of duplication or error.

There is also the advantage for the customer that they only have to supply KYC documents once (until they need to be updated) and that they are not then disclosed to any other party (except for their own bank) as the other organisations will not need to see and check the ID documents but will just rely on the Blockchain verification.

SWIFT has established a KYC Registry with 1,125 member banks sharing KYC documentation – however, this is only 16% of the 7,000 banks on their network. The KYC Registry meets the need for an efficient, shared platform for managing and exchanging standardised KYC data and it's free to upload the documentation to the Registry and to share it with other institutions.
SWIFT validates the data rigorously, informs the client if it's incomplete or needs updating, and sends out alerts to correspondents whenever the data changes.

There will still be issues surrounding security and privacy of customer's KYC information but, as long as all KYC is held on a private Blockchain rather than a public one, these issues should be minimal from a bank customer's point of view. The data on the Blockchain will merely be a reference point with a digital signature or cryptographic hash – which would give individuals access to the relevant client information in a repository separate to the Blockchain, ensuring a secure and private way of conducting and storing a customer's KYC information. Equally important, though, is ensuring financial institutions only have permissioned access on a temporary basis so that access to KYC information is only granted when strictly necessary for that purpose, and for no other ancillary reason.

Therefore, it is evident that Blockchain could have a major role in streamlining these KYC and AML processes – although this may require cross-border consensus as to what is regarded acceptable KYC documentation and what needs to be done in terms of acceptable verification of those documents.

According to a Goldman Sachs Report, Case Study 7, the banking sector can achieve 10% headcount reduction with the introduction of Blockchain in the KYC procedures. This amounts to around $160 million in cost-saving annually.

Blockchain will also reduce the amount of budgetary resources allocated for employee training, there will be 30% headcount reduction amounting to $420 million.

Overall operational cost savings are estimated to be around $2.5 billion dollars. AML penalties will also be reduced by estimated amount between $0.5 to $2 billion dollars.

Trading Platforms

A bank could set up a new trading platform (or move across an existing trading platform) on Blockchain protocol. The Blockchain technology offers a potential new medium to exchange assets without centralised trusts or intermediaries – and without the risk of double spending.

As already discussed, Blockchain can eliminate the threat or the risk of fraud in all areas of banking, and this could equally apply to a trading platform. Furthermore, Blockchain would also address issues such as operational risk and administrative costs as it can be made transparent and immutable.
The traceability and the permanent historic record that would exist on Blockchain backing up every asset or item of value that was

traded would provide assurance and authenticity all the way through the supply chain.

In practice, when a high-value item is first created, a corresponding digital token is issued by a trusted central authority which acts to authenticate the product's point of origin. Then, every time the product is bought and sold the digital token is moved in parallel so that a real-world chain of ownership is created and mirrored by the Blockchain history of that digital token.

The digital token is acting as a virtual "certificate of authenticity" which would have the advantage that it is far harder to steal or forge than a piece of paper. Upon receiving the digital token, the final recipient of the product will then be able to verify the chain of custody all the way back to the point of creation.

The Blockchain gives the benefit of distributed and verifiable trust that was not present before.

As a non-banking example, Everledger, a permanent ledger for diamond certification, has adopted the use of Bitcoin as a mark of authenticity providing transparency for all parties involved – a clear attempt to prevent diamond fraud.

Similarly, the immutability and digital uniqueness inherent in Blockchain offers the ability to provide a secure transfer of value and delivery of a solution to the trade finance problem of endorsement.

The challenge of maintaining data privacy among counterparties to trade transactions is also overcome by utilizing Blockchain technology where tokenization, in the form of cryptography, is used to protect the trade data with parties only allowed to access to permissioned information with the correct security key. This should enable the most confidential of transactions, especially financial transactions, to still take place on such a trading platform.

Clearing and settlement costs billions and, according to Santander's 2015 report, it is estimated that moving this into a digital record, near real-time and over the internet, will save the industry $20 billion a year or more in overhead costs due to D+3. D+3, or T+3, is the three-day clearing and settlement cycle common to most investment markets today.

Many firms are leading the charge to digitalise the clearing and settlement structures from Blythe Masters' Digital Asset Holdings with the Hyperledger to Overstock with T0, along with many other key and emerging players such as Epiphyte, Clearmatics and SETL.

Payments

The main use case that is focused on when looking at the possibilities of blockchain for banking is that of payments. Chris Huls of Rabobank said that Blockchain could be used as "another way of paying each other, not depending on SWIFT and other payment schemes."

Chris Mager of BNY Mellon also recognises that there is a potential role for Blockchain in payments and that currently there is an "unprecedented period of change and transformation." Mager recognised that blockchain could have benefits for not only bank customers, but this could also lead to operational efficiencies and cost savings for banks themselves. He also stated that payment systems collectively are currently under a lot of pressure, as there has been urgency to modernise payments and to address the questions of safety and security since the 2008 financial crash. This has led to new market entrants,

such as FinTechs, looking to solve these problems using Blockchain.

The existing payment system has always gone through banks and central banks, a process that was first put into place in the 1970s and 1980s. Apart from speeding up money transfers, blockchain could also help banks to operate continuously, 24 hours a day. This is now somewhat expected by customers who want an omni-channel banking experience at any time day or night – especially, according to Chris Mager, for "millennials who are now firmly within the workforce and want a better, quicker and easier way to make payments."

Rabobank has been heavily involved in the on-going development and use of Ripple Lab's Blockchain Ripple protocol. It was announced in December 2014 that the three banks had started to test Blockchain technology in making payments to customers and cross-border transactions. Ripple has said that its technology could give banks a 33% reduction in their operating costs during the international payment process and allow lenders to move money "in seconds."

Ripple is a "real-time gross settlement system" (RTGS), currency exchange and remittance network. Released in 2012, Ripple purports to enable "secure, instant and nearly free global financial transactions of any size with no chargebacks." It supports tokens representing fiat currency, cryptocurrency, commodity or any other unit of value. Ripple can be used by banks for an open-source approach to payments to replace many of the common intermediaries in the payments industry, thereby passing on savings to partner institutions, and thus by extension, to their customers.

Thus Blockchain can be used to make payments in real-time globally, with real-time execution, complete transparency, real-time fraud analysis and prevention and also at a reasonable cost. The

only issue with Ripple, at the moment, is that it is a proprietary Blockchain network that cannot yet connect with other systems. In order to connect Ripple to other Blockchain protocols an inter-ledger protocol will have to be developed, tested and put in place.

There are, however, other Blockchain protocols in limited use and in development for the payments industry. In Estonia, LHV Bank is experimenting with Blockchain through coloured coins called "Cuber" as a "cryptographically protected" certificate of deposit. The project would enable the bank's FinTech offshoot, Cuber Technology, to develop mobile apps using Blockchain to provide free P2P fiat currency transfers.

Rain Lõhmus, Chairman of the Supervisory Board of LHV Bank, said that all Estonian government and finance infrastructure relies on public-key cryptography, which makes exploring Blockchain to be a natural next step.

As Chris Mager from BNY Mellon also highlighted, VISA Europe Collab and BTL Group are working on a separate concept to make cross-border payments between banks using distributed ledgers. The project will use BTL's crossborder settlement platform Interbit to explore the ways in which a distributed ledger-based settlements system (as well as utilising "smart contracts") can reduce the friction of domestic and cross-border transfers between banks. This is a similar goal to Ripple but, as it is based on the Ethereum smart contracts concept, it is not proprietary like Ripple and thus is potentially more scalable.

Chris went on to explain that, similarly, UBS, Deutsche Bank, Santander and BNY Mellon have teamed up with blockchain developer Clearmatics and trading company ICAP to create a new digital representation of fiat currency called the "Utility Settlement Coin." Although this is still a proof of concept, it could potentially reduce friction in delivery versus payment scenarios by providing a

faster and less expensive settlement mechanism than existing funds transfer and currency exchange mechanisms.

Use Cases for Blockchain in Energy & Commodity Management

Intermittent renewable power generation is on the rise, and system stability on local, national and European level is the key objective of power grid management. Direct peer-to-peer trading with aggregation to virtual power plants (VPP) is a viable solution and could build on Blockchain technology.
A prerequisite for local P2P trading is the reduction of traded lot sizes. In energy & commodity trading, standardised units are defined according to size, quality and quantity. Standardised criteria and lot sizes are necessary to overcome transaction costs in the current market configuration. Actors are not able to sell on wholesale power markets if the offer does not match the standardised criteria.

They are required by third-party intermediaries (brokers, banks) to draft contracts. Thus, commodity traders are de facto big clients or specialists. Blockchain is able to reduce transaction costs through standardisation via smart contracts and the automatic execution of orders. Transaction costs decrease dramatically, allowing smaller lot sizes and bypassing intermediaries. In fact, one application of Blockchain technology is in the distributed generation of renewable energy using smart meters to track electricity use.

In this setting, "prosumers" not only consume commodities but also dispose of generation capacity in the form of solar systems, small-scale wind turbines or CHP plants. Blockchain technology strengthens the market role of individual consumers and producers. It enables prosumers to buy and sell energy directly – manually or via automation – with a high degree of autonomy.

Aggregation of Microgrids to Virtual Power Plants

The term virtual power plant refers to clusters of electricity generators, loads and storage systems that are pooled in an intelligent manner and controlled jointly. The VPP proper represents a central platform from which dispersed assets can be monitored and controlled remotely. As VPP fleets are an aggregation of various asset types and energy sources, they provide a certain level of flexibility, allowing VPP operators to respond to market and price changes within very short time frames.

In order to be able to participate in energy exchange, plant operators have to produce forecasts so as to minimise fluctuations. The complexity involved in producing forecasts varies for each type of generation facility; deriving forecasts for wind and solar power output is a more complex task than for controllable power plants like gas-fired power plants. If a plant operator fails to forecast its output accurately, it will incur imbalance charges. Plant operators who can provide accurate forecasts can benefit from higher revenues.

If controlled intelligently, VPPs aggregating widely dispersed and strategically clustered assets can be used to optimise power flows, thus serving as a power flow optimisation tool complementing network development. Even today power flows can be optimised with the help of renewable power generation facilities, for example by aggregating wind turbines and controlling them jointly. In this way VPPs can contribute to compensating for and bridging insufficient network development.

A central actor could deploy Blockchain solution that automatically integrates local information and optimises local grids. The local grids are then aggregated to virtual platforms, providing stable power capacity at low cost. This aggregation can include multiple actors and have a central player or only one player could deploy it for several distributed grids.

In the past, the organisation and management of VPPs of different sizes was complex and costly. Blockchain technology has the potential to make this process more efficient. On a lower level the VPPs can – based on smart contracts – optimise themselves to a certain degree, and if the balance of the current optimisation level is not sufficient, then optimisation against the next higher level (e.g. distribution grid) can be done via Blockchain very efficiently as well.

Examples for Local Trading Between Small Consumers and Prosumers via Blockchain

Ponton developed a simulation of a local energy market based on EPEX SPOT next-hour prices. This price curve is used to drive the behaviour of participating batteries and an electrolyser. For the electrolyser, Ponton developed a trading strategy with two goals: consume 1 MWh within the simulated runtime of 24 hours and buy hourly chunks of electricity, depending on the actual head-hour market price.

The system uses an agent-based architecture connecting the devices as market participants to the local marketplace. Each agent is controlled by an individual behaviour – acting as a consumer, a generator or both. The marketplace itself was built based on Blockchain technology.

Asset Tracking, Bill of Lading, Transfer of Title

In the logistics chain all parties require continual consensus with other parties. These actors usually use completely different information tracking systems, leading to significant challenges for the optimisation of the shipment process. The key challenges Stratum identifies are sharing information between systems, unsynchronised payments and deliveries, and auditing.

Currently, each party in the supply chain purchases goods, adds value and sells these goods to the next actor in the chain. The related transfers of ownership are often still recorded on paper and fraud remains a persistent risk. Blockchain solution for the tracking of physical commodities along the supply chain addresses the key challenges and can reduce costs significantly.

Financialisation of Commodities

Physical trading between a buyer and seller in different countries is costly, prone to error and involves a financial intermediary to process the transaction. Commonly, letters of credit (LC) with security and guarantees from banks are used for these transactions.

Making use of Blockchain technology tackles the disadvantages while maintaining the security LCs provide. The typical smart-contract application in goods trading could be designed as follows: via his node, the selling party receives a payment confirmation that will take place later, once a set of conditions is met. On the physical side, goods are tagged with QR codes that are linked to the smart contract. Upon arrival of the goods, the payment is

automatically triggered through the execution of the contract.

The QR code/smart-contract solution is an example of how Blockchain can improve the traceability of physical commodities. Today only the front end of commodities trading has been financialised, in the form of electronic trading. With blockchain, the infrastructure could be financialised as well.

Fewer Intermediaries Through Immutable Records and Reconciliation Reporting

Blockchain technology is increasingly being seen as a commercial tool for transparency, visibility and security in numerous sectors. It could hence play the role of clearinghouses and brokers. The technology inherently and automatically provides all the confidence needed. In over the counter (OTC) energy & commodity trading, both counterparties confirm the deal details in order to minimise the risk of misunderstandings or errors. This process of "confirmation matching" is traditionally performed via fax or electronically at each commodity trader's back office.

According to Ponton, Blockchain could be used to completely automate this process. With Blockchain technology, the exchange of trade confirmations could be done on a peer-to-peer basis, i.e., directly between the counterparties without any middleman. OTC commodity derivative trading in particular could be a quick win for blockchain: OTC commodity derivatives have fewer clearing requirements and, overall, the smaller market size could favour a smart-contract rollout.

Ponton has launched its own Blockchain platform, Enerchain. Enerchain is a platform for peer-to-peer trading in the wholesale energy market. The software allows traders to anonymously send orders to a decentralised order book, which can also be used by

other organisations. Thanks to this technology, Enerchain does not require a central authority. To date, 23 European energy suppliers and traders have joined the Enerchain consortium.

Developments and Outlook

As of now, Blockchain offers an opportunity for large utilities and commodity traders. They could individually or in consortia move to Blockchain solutions, reducing transaction costs for their processes and maintaining their current position. One example of this development is the newly founded Energy Web Foundation. Another example is Poton's Enerchain project, where European utilities seek to create a standard for Blockchain technology in the energy sector.

A less known application of Blockchain technology are business processes. These processes are based on a case-by-case analysis of business processes with the identification of pain points that can be tackled with Blockchain solutions. This approach can be applied in the very short term, aiming at increasing process efficiency and increasing automation.

The real potential of Blockchain technology unleashes with the Internet of things (IoT). In an IoT environment machines communicate directly without any human interaction. This machine to machine (M2M) communication could be managed with blockchain(s), leveraging its benefits, such as immutability, speed and automatisation. It will be interesting to see, how these will create even more use cases in future.

Blockchain in Logistics

Achieving excellence in logistics involves working collaboratively with others to optimize the flow of physical goods as well as the complex flow of information and financial transactions (see the figure above). But today there is a significant amount of trapped value in logistics, largely stemming from the fragmented and competitive nature of the logistics industry. For example, in the US alone, it is estimated that there are over 500,000 individual trucking companies. With such a huge number of stakeholders involved in the supply chain, this often creates low transparency, unstandardized processes, data silos and diverse levels of technology adoption.

Many parts of the logistics value chain are also bound to manual processes mandated by regulatory authorities. For example, companies must oftentimes rely on manual data entry and paper-based documentation to adhere to customs processes. All this makes it difficult to track the provenance of goods and the status of shipments as they move along the supply chain, causing friction in global trade. Blockchain can potentially help to overcome these frictions in logistics and realize substantial gains in logistics process efficiency. This technology can also enable data transparency and access among relevant supply chain stakeholders, creating a single source of truth. In addition, the trust that is required between stakeholders to share information is enhanced by the intrinsic security mechanisms of Blockchain technology.

Furthermore, Blockchain can achieve cost savings by powering leaner, more automated, and error-free processes. As well as adding visibility and predictability to logistics operations, it can accelerate the physical flow of goods. Provenance tracking of goods can enable responsible and sustainable supply chains at scale and help to tackle product counterfeiting. Additionally, Blockchain-based

solutions offer potential for new logistics services and more innovative business models.

Faster and Leaner Logistics in Global Trade

Logistics is often considered the lifeblood of the modern world, with an estimated 90% of world trade carried out by the international shipping industry every year. But the logistics behind global trade is highly complex as it involves many parties often with conflicting interests and priorities as well as the use of different systems to track shipments. Therefore, achieving new efficiencies in trade logistics is likely to have significant impact on the global economy. According to one estimate from the World Economic Forum, reducing supply chain barriers to trade could increase global gross domestic product (GDP) by nearly 5% and global trade by 15%.

Blockchain technology can help alleviate many of the frictions in global trade logistics including procurement, transportation management, track and trace, customs collaboration, and trade finance.

With over 50,000 merchant ships involved in the global shipping industry and multiple customs authorities regulating the passage of freight, a major area of focus for efficiency gains is ocean freight. Blockchain technology has huge potential to optimize the cost as well as time associated with trade documentation and administrative processing for ocean freight shipments. One example that highlights the complexities behind ocean freight today is the estimate that a simple shipment of refrigerated goods from East Africa to Europe can go through nearly 30 people and organizations, with more than 200 different interactions and communications among these parties.

To unlock efficiency in ocean freight, Maersk and IBM have started a venture to establish a global Blockchain-based system for digitizing trade workflows and end-to-end shipment tracking (see the

following figure). The system allows each stakeholder in the supply chain to view the progress of goods through the supply chain, understanding where a container is in transit.

Stakeholders can also see the status of customs documents, and can view bills of lading and other data. Blockchain technology ensures secure data exchange and a tamper-proof repository for this documentation. The two companies expect this solution to track tens of millions of shipping containers annually. It has the potential to significantly reduce delays and fraud, which could lead to billions of dollars in savings in the logistics industry.

Ocean carrier company ZIM has conducted a pilot to digitize the actual bill of lading, often hailed as a 'holy grail' application in logistics. The bill of lading is one of the most important documents in ocean shipping, and it acts as a receipt and a contract for the goods being shipped. The information stored on a bill of lading is critical as it contains all necessary details such as the shipment description, quantity and destination, as well as how the goods must be handled and billed. During the trial of Blockchain-based system developed by Wave, ZIM and pilot participants issued, transferred, and received original electronic documents successfully through the decentralized network.

The containers, shipped from China to Canada, were delivered to the importers (i.e., consignees) without a problem. Although still in pilot phase, industry adoption of a digital bill of lading would be significant. It could greatly support supply chains in reducing costs, enabling error-free documentation and fast transfer of original documents.

Accenture is developing Blockchain-based system also focused on replacing the traditional bill of lading as well as facilitating a single source of truth for all supply chain stakeholders for freight inquiries up to issuance of trade documents. Here, a decentralized network connects all parties in the supply chain and enables direct

communication, eliminating the need to go through central entities and rely on intermediaries. According to Adriana Diener, Global Freight & Logistics Lead at Accenture, the proven value of this project is surpassing expectations: “Using Blockchain to replace the traditional bill of lading documentation to ship goods will drive millions of dollars in process efficiency and operational cost reduction benefits across the supply chain for multiple parties in the trade ecosystem including shippers, consignees, carriers, forwarders, ports, customs agencies, banks, and insurance companies”.

Improving Transparency and Traceability in Supply Chains

Many projects are underway using Blockchain technology to improve supply chain transparency and monitor provenance. These initiatives amass data about how goods are made, where they come from, and how they are managed; this information is stored in the Blockchain-based system. This means that the data becomes permanent and easily shared, giving supply chain players more comprehensive track-and-trace capabilities than ever before. Companies can use this information to provide proof of legitimacy for products in pharmaceutical shipments, for example, and proof of authenticity for luxury goods. These initiatives also deliver consumer benefits – people can find out more about the products they are buying, for example, whether a product has been ethically sourced, is an original item, and has been preserved in the correct conditions.

One key application is the use of Blockchain technology to combat a major challenge in the world today: the counterfeiting of drugs and false medication. According to Interpol, around 1 million people each year die from counterfeit drugs, 50% of pharmaceutical products sold through rogue websites are considered fake, and up to 30% of pharmaceutical products sold in emerging markets are counterfeit. To answer this challenge, DHL and Accenture are driving Blockchain-based serialization project providing sophisticated track-

and-trace capabilities to the pharmaceutical industry (see the following figure).

Pharmaceutical serialization is the process of assigning a unique identity (e.g., a serial number) to each sealable unit, which is then linked to critical information about the product's origin, batch number, and expiration date. Serialization effectively enables a unit to be tracked at virtually any moment, and traced to its location at any stage of its lifecycle. A key serialization challenge is maintaining traceability and transparency especially when these units are repackaged or aggregated from unit to case to pallet for logistics purposes and then disaggregated back down to unit level for consumption.

The DHL /Accenture proof-of-concept was established to overcome this and other challenges by demonstrating the effectiveness of Blockchain technology in product verification. The aim is to show that pharmaceutical products have come from legitimate manufacturers, are not counterfeit, and have been correctly handled throughout their journey from origin to consumer. Most importantly, this initiative proves how end customers can verify the legitimacy and integrity of pharmaceutical products, especially compliance with handling requirements. This not only reassures the end customer at the point of purchase that their medicines are genuine and in perfect condition, but has potentially life-saving implications.

To achieve this, the partners have established Blockchain-based track-and-trace serialization prototype comprising a global network of nodes across six geographies. The system comprehensively documents each step that a pharmaceutical product takes on its way to the store shelf and eventually the consumer (see the figure on next page). The prototype was a lab performance simulation that demonstrated how Blockchain technology could handle volumes of more than 7 billion unique pharmaceutical serial numbers and over 1,500 transactions per second.

The project illustrated how Blockchain can be used to capture all logistics activities relating to an item of medication – from production to purchase – and ensure this information is made secure, transparent, and immediately available. “Our proof of concept demonstrated the opportunities blockchain presents in the fight against counterfeit pharmaceutical goods. Together with our partners we are actively refining the solution as well as working with key industry stakeholders to operationalize the concept” states Keith Turner, CIO Chief Development Office at DHL Supply Chain.

In the consumer goods and retail industry, companies like Unilever and Walmart are exploring the use of Blockchain technology to improve supply chain transparency and to track provenance. Walmart is focusing specifically on food tracking, traceability, and safety.

Together with partners, Walmart has conducted Blockchain test designed to trace the origin and care of food products such as pork from China and mangoes from Mexico. To begin with, this initiative documented the producer of each specified food product so that Walmart can easily address any case of contamination, should this arise. Secondly, the test put mechanisms in place to identify and rectify the improper care of food throughout the journey from farm to store. For example, since meat shipments must not rise above a certain temperature, the test took temperature data from sensors attached to the food products and committed this data to the Blockchain-based system. From there, automated quality assurance processes notified relevant parties in the event of suboptimal transport conditions. Since launching this test, Walmart has also announced the creation of Blockchain Food Safety Alliance, an extensive partnership to apply tracking, traceability, and safety benefits to food supply chains in China.

Moving forward, a key requirement for track-and-trace applications will be to adopt more secure and intelligent forms of digital identity for each physical product – moving from the provision of a passive

barcode or serial number to, for example, enabling interactivity with the use of Internet of Things (IoT) sensors. Smart devices can be securely tied to or embedded in the physical product to autonomously record and transmit data about item condition including temperature variation, to ensure product integrity, as well as any evidence of product tampering.

Automating Commercial Processes in Logistics with Smart Contracts

Current industry estimates indicate that 10% of all freight invoices contain inaccurate data which leads to disputes as well as many other process inefficiencies in the logistics industry. This problem is so prevalent that in the oil and energy industry alone, Accenture expects that at least 5% in annual freight spend could be reduced through improved invoice accuracy and reduction of overpayments.

Blockchain has the significant potential to increase efficiency along the entire logistics and settlement process including trade finance and help to resolve disputes in the logistics industry. As digitized documents and real-time shipment data become embedded in Blockchain-based systems, this information can be used to enable smart contracts. These contracts can automate commercial processes the moment that agreed conditions are met.

One of the first startups to pursue such smart contract applications in the logistics industry is ShipChain. ShipChain is an early-stage company which has designed a comprehensive Blockchain-based system to track and trace a product from the moment it leaves the factory to final delivery at the customer's doorstep. The system is

designed to encompass all methods of freight and there are plans to include an open API architecture that can integrate with existing freight management software. All relevant supply chain information is recorded in an immutable Blockchain-based database that can execute smart contracts once the conditions have been met (for example, as soon as the driver transmits confirmation of successful delivery). A key element to automating the settlement process is through ShipChain's digital currency called "SHIP tokens". Participants of ShipChain's platform purchase these tokens in order to pay for freight and settle transactions on the platform.

In this use case, Blockchain in combination with the Internet of Things (IoT) in the logistics industry will enable even smarter logistics contracts in future. For example, on delivery a connected pallet will be able to automatically transmit confirmation and the time of delivery as well as the condition of the goods to the Blockchain-based system. The system can then automatically verify the delivery, check whether the goods were delivered as per agreed conditions (e.g., temperature, humidity, tilt) and release correct payments to the appropriate parties, greatly increasing efficiency as well as integrity.

Blockchain can further be used in the context of IoT to automate machine-to-machine payments (e.g., connected machines negotiating and executing price based on the logistics activities performed).

Another example of smart contracts in the logistics industry is the digitization of letters of credit (L/C) in order to accelerate the preparation and execution of a standard paper-based L/C – a process which currently tends to take from a few days to a few weeks. The Bank of America Merrill Lynch (BofAML), HSBC and the Infocomm Development Authority of Singapore (IDA) have developed a prototype to bring the paper-intensive L/C process onto Blockchain. The system essentially enables the sharing of information between exporters, importers and their respective banks

on a secure Blockchain-based platform. This allows trade deals to be executed automatically through a series of digital smart contracts. In the trial, each of the four parties involved in an L/C transaction could visualize data in real time on a mobile tablet and see the next actions to be performed.

In a joint statement, the consortium partners state that the proof of concept shows potential to streamline the manual processing of import/export documentation, improve security by reducing errors, increase convenience for all parties through mobile interaction and make companies' working capital more predictable. The partners now plan to conduct further testing of the concept's commercial application with selected partners, such as companies and shippers.

Startups are also working in this space with one example being Libelli. This company is developing a solution to essentially act as an escrow agent between any seller and any buyer to create a smart contract, bypassing the need for buyers and sellers to engage banks and eliminating the paperwork traditionally associated with L/C. The company aims to provide transparency to all stakeholders during the process, and claims that the automation of this commercial process reduces L/C time-to-execution down to a few minutes, with costs ten times lower than currently charged by banks.

Other functions that could be automated include outsourced transportation management, normative compliance, route planning, delivery scheduling, fleet management, freight forwarding, and connectivity with business partners.

Velmie

Velmie is a leading provider of Blockchain solutions. This document is intended for general informational purposes only, does not take into account the reader's specific circumstances, and may not reflect the most current developments. Velmie disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Velmie does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

For more information, visit Velmie.com