BLOCKCHAIN AND ITS REAL-WORLD APPLICATIONS

In conversation with Professor A Damodaran, IIM – Bangalore

It is widely believed that blockchain may be the next major digital revolution – one that is possibly 'bigger' even than the Internet. Blockchain has the potential not just to save significant amounts of time and money, but to also transform business practices. While the first generation of the technology was about cryptocurrencies like Bitcoin, the second was concerned with smart contracts, and the third/current era is about applications outside the financial markets, including in governance. To shed light on the many possible uses to which blockchain can be put – and to understand some of its limitations – we asked IIM-Bangalore Professor A Damodaran share insights.

A DISRUPTIVE – BUT ALSO VERY SIMPLE – INNOVATION…

A revolutionary technology…

Blockchain is a much simpler concept than it appears to be at first glance. A blockchain is nothing but a ledger of transactions generated in a digital form. Crucially, it has three salient features that can radically change how businesses *do* business:

…with three key features

- **Decentralisation**: Unlike a traditional, centralised system, which is often vulnerable to compromise, a blockchain is characterised by a distributed network, under which no single individual/party is in-charge and all the stakeholders are inter-linked.
- **Transparency**: As every node of the chain is connected to the other, there is no scope for manipulation of any kind.
- **Immutability**: The system is tamper-proof on account of end-to-end encryption. Changing any one block means changing the entire chain.

…WITH CRITICAL BENEFITS…

A potential game changer…

Any idea, no matter how ambitious on paper, is useless if it cannot offer solutions to real-life problems. The reason why many consider blockchain to be so important is its potential applicability in a wide gamut of areas:

…that could transform lives

- **Financial fraud**: Time and again, the traditional core banking system (CBS) has been shown to have major loopholes. In essence, the PNB fraud was a case of deceptive entry through CBS, which involved circumventing three layers of security (maker, checker and verifier), and the subsequent issuance of LoUs via SWIFT. With blockchain, though, every entry is cast in stone, and cannot be manipulated. For that reason, financial institutions across the globe are considering blockchain-based solutions. For instance, German bank Fidor recently switched from SWIFT to Ripple, resulting in considerable time-saving as well as a steep ~75% cost reduction.
- **Identity theft**: In 2018, identity theft cost consumers worldwide a whopping USD 16 billion. Blockchain can be a complete game-changer in this regard. Canada-based SecureKey Technologies is on its way to developing a blockchain-based digital identity-management and attribute-sharing network that will allow consumers to control the information they choose to share. Such initiatives will not just avert *benami* and identity fraud, but could also slash paperwork significantly, and eliminate redundant verification processes.

LEVERAGING DATA TO BECOME A 'CUSTOMER-FIRST' ORGANISATION

In conversation with Deep Thomas, Chief Data and Analytics Officer, Aditya Birla Group

Consumer markets have undergone profound changes in the last decade, and the adage, 'The Customer is King' holds truer now than ever. Today, it means that the consumers want to build brand relations on their own terms, and that companies need to meet that demand. In a market flooded by brands, both national and global, it is essential to secure customer loyalty. By making the best use of the vast data that CMOs have at their disposal, they can create, contextualise and curate lasting experiences for their consumers. Deep Thomas, Chief Data and Analytics Officer at the Aditya Birla Group, is a 'data evangelist' who uses analytics to drive growth. Mr Thomas highlighted the need to build data-analytics capabilities within marketing, and shared his own experiences in this domain.

CUSTOMER CENTRICITY IN A DIGITAL WORLD

Digital has brought customer-centricity to the fore…

Businesses today operate in an interconnected world. Digital has overtaken traditional ways of building customer and brand loyalty – and customer centricity is at the core of the digital world. Digital disruption is taking place at every point within the organisation. Whether it is humans interacting with machines or machines with machines, every interaction results in data accumulation. This is where analytics converges with customer centricity.

…but also enables data mining on an unprecedented scale

For their part, consumers have become much savvier. They want the 'three C's': to be in control, and to enjoy convenience and choice like never before. A good example is how social media has eclipsed the mainstream media. This has, though, also enabled companies, using data analytics, to mine vast amounts of consumer data. In turn, big data offers scale, speed, precision and intimacy. In fact, because it so closely replicates the way the human brain thinks, AI is nothing but 'intimate' intelligence at scale.

LEVERAGING DATA

CMOs must understand their customers…

Today's CMOs need to be 'marketing technologists.' In order to better leverage data, they need to first understand their customers: their preferences, needs, loyalties, passions, how they deal with different brands, and so on. Various channels can be used to build this type of understanding: social media, chat-box interactions with consumers, augmented reality platforms, and other forms of digital data. Next comes product design. Based on the information collected, companies should create offerings that appeal to the consumer. Essentially, this boils down to selling an experience, and not just a product. It is then the CMO's job to 'curate' 3-4 products that enhance the customer experience.

…and play a lead role in curating the customer experience

DirecTV leverages data on people shifting homes…

Using its internal data, DirecTV, an American direct-broadcast satellite service provider, found that people relocating to a new neighbourhood are particularly good target customers. It tied up with US Postal Service to identify when people move homes, and used that information to 'hook' them to DirecTV. Pretty Secrets, an online lingerie brand, created purposeful campaigns targeted specifically at 'tech savvy' women. It combined internal research with external data from an agency to develop more personalised products for this clientele.

...while Pretty Secrets tailor-makes its campaigns

CYBER SECURITY: THE NEW CFO MANDATE

In conversation with Venkat Raman Srinivasan, Partner, PwC and Monil Gala, Partner, Assurance Practice, PwC

In an age where technology is driving key business decisions and outcomes, data ownership and cybersecurity both figure high on Boardroom agendas. Certain kinds of cyber-attacks can cripple a company's operations and even threaten its very existence. As the company's de facto risk officer, CFOs must not only comprehend the risks around digital adoption, but also take the lead in drafting a cyber-security response plan. They also need to be able to partner with security leaders, business managers and CIOs to manage these risks. Ironically, many Finance leaders continue to believe that cyber security is outside their purview, instead belonging to Operations or IT. Venkat Raman Srinivasan and Monil Gala from PwC provided an expert's perspective on today's cyber challenges, and shared best practices on how leading companies are proactively dealing with cyber threats.

THE CURRENT STATE OF CYBER THREATS: WORRISOME

India has emerged as the third-biggest target for cyber attacks

Cybercrime in India has evolved dramatically in both nature and scope. Data from the Indian Computer Emergency Response Team (CERT) indicate that between January and October 2019, it experienced 313,649 cyber-attacks – 50% more than the total recorded in 2018. In fact, India is next only to the US and China as a target for such attacks, which are spread across sectors and geographies. Increasingly, cybercrime syndicates are using sophisticated tools, combining one or more attack techniques. They are also unfolding faster taking mere seconds, compared to several days in earlier times. In August 2018, a daring attack on Cosmos Bank in Pune by an 'ethical' hacker resulted in the theft of personal data of 17 million users. In July, Canara Bank ATM servers were targeted, wiping off Rs 2 million from different bank accounts. The UIDAI data breach in early 2018 is believed to have compromised the personal information of 1.1 billion citizens, including their Aadhaar, PAN and mobile numbers.

Cyber security concerns both industrial and new-age companies, and it is a sub-set of information security

Some ill-conceived notions can accentuate a company's cyber risks. Many believe that cyberattacks are a threat only to new-age companies, but in fact traditional manufacturing companies are an easier target for hackers owing to their poor cyber-security standards. Further, cyber security is wrongly believed to be distinct from information security, whereas it is really a sub-set that rests on three pillars: integrity, confidentiality and availability. Moreover, not only do cyber breaches often result in commercial losses, but they can also cause major health and safety issues – such as, for instance, if an attack on a power grid leads to major power outages.

MANAGING CYBER THREATS

Invest in planning, preparation and training

In a dynamic and complex environment, rapid and efficient responses to cyber breaches are possible only if the company decides in *advance* how it will respond. This requires regular investments in planning, preparation and training. In this regard, the experience of class-leading companies can offer valuable insights.

Make it a business priority

- **Align cyber security with business strategy:** As cyber risks evolve, organisations are starting to realise that their approach to security cannot be separated from their business strategy. Accordingly, cyber security is now firmly on the C-suite's radar.