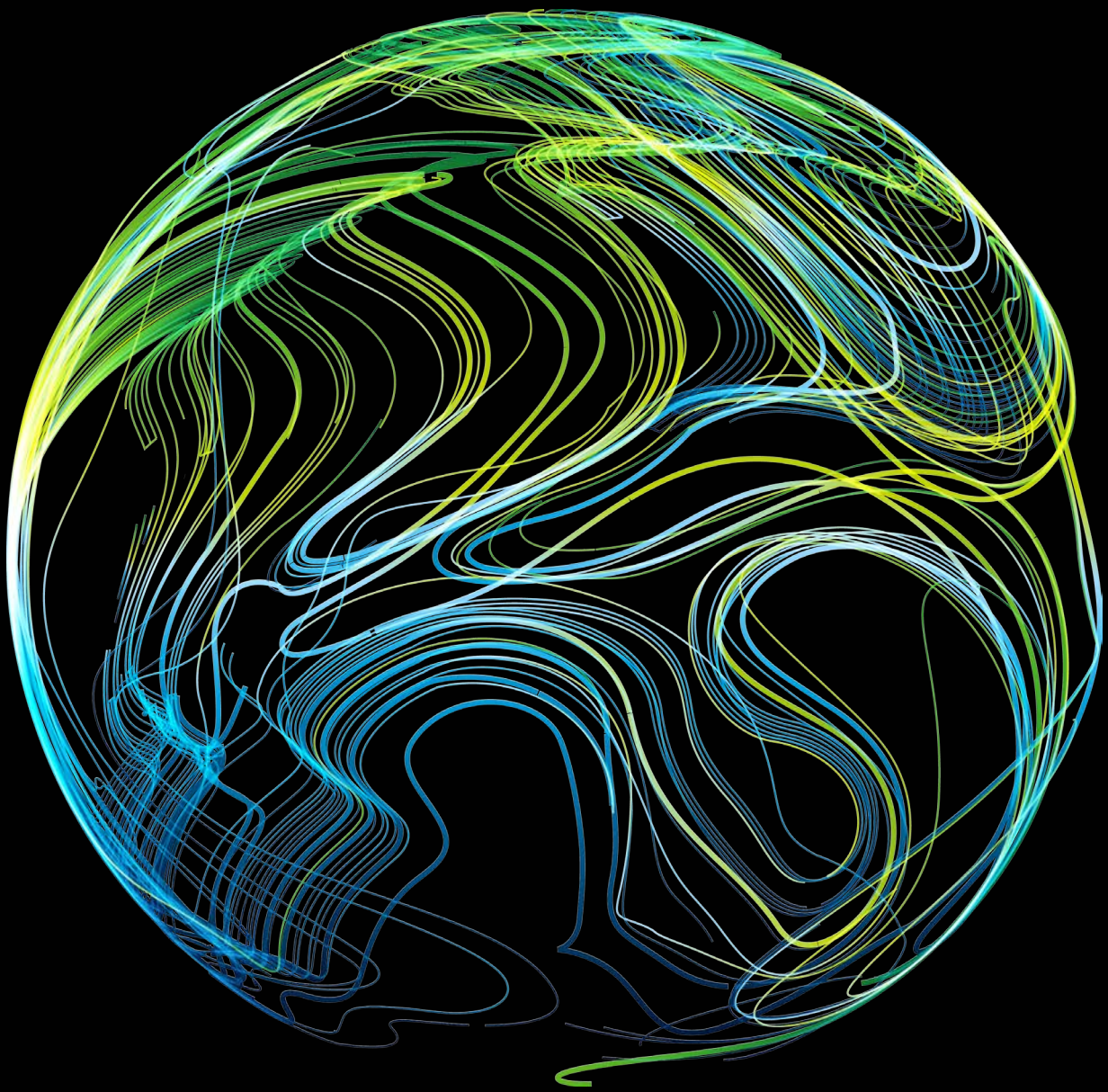
Deloitte.



2017 Technology, Media and Telecommunications Predictions

Middle East edition

Foreword

Welcome to the 2017 edition of Deloitte's Predictions for the technology, media and telecommunications (TMT) sectors.

For the first time in our 5 years of releasing our Middle East edition, we are including predictions for all three sectors together, and not splitting them into different sub-industries. This, by itself, is a reflection of the exciting industry we are in. An industry that continues to blur the boundaries of innovation, and reshape how operators, media players and technology companies collaborate and interact in an increasingly integrated market place.

Across the global and regional predictions, we believe that the distinction between sectors is fast becoming obsolete. The introduction of dedicated machine learning capability to smartphones is relevant across all industry sectors, not just the technology or telecommunications verticals. The transition to 5G and resulting implications on machine to machine communication is a critical enabler to new technology adoption, starting with self-driving cars. IoT itself is the epitome of this borderless ecosystem with operators and technology companies working closely together to shape the cities and lives of tomorrow. Cybersecurity is an evergreen topic in the region raising threats to media companies and Telcos equally, and requiring cross sectorial regulations and safety measures.

With smart cities and nations so high in the agenda of the Middle East countries, our region is at the forefront of this borderless market place, with regional Telcos talking more about AI and IoT than network expansion. In this day and age, breaking borders, albeit at industry level, is a refreshing twist. 2017 promises to be yet another exciting year for the TMT sector. We wish you all the best for this year and trust that you and your colleagues will find this year's predictions a useful stimulant in your strategic thinking. We look forward to discussing them with you.

Emmanuel Durou
Partner, Head of Middle East TMT industry
Deloitte & Touche (M.E.)

Paul Lee
Partner, Head of Global TMT Research
Deloitte Touche Tohmatsu Limited

Tightening control of social welfare – A compelling use case for blockchain in the GCC

Deloitte predicts that blockchain will find widespread use in the GCC, where it will find uptake in the public sector potentially saving $3.5 billion in leakages over the next couple of years, by using blockchain-based identity management for the disbursement of social welfare. We further expect that four out of the of six countries in the GCC will pilot some form of implementation of digital identity on blockchain at the local or national government level, and 10 million identity records will be put on blockchain over the course of the year.

The GCC countries, by some estimates, spend over $150 billion cumulatively on a variety of social welfare schemes for their citizens. A significant portion of this amount is lost (colloquially called leakage) in fraud and in operational inefficiencies. Fraud usually pertains to a deliberate misappropriation of identity, and inefficiencies relate to high cost per welfare disbursement as well as inaccurate payments.

As it stands, welfare systems globally have to deal with the issue of fraud and inefficiencies. The United Kingdom Department of Work and Pensions has calculated that between 2.5 to 5.4% of the value of its disbursements are by fraud alone[21].

If we take this data and apply it to the situation in the GCC, we can safely assume an implicit greater leakage, incorporating both fraud and inefficiency, of around 7.5%. This is still a conservative estimate due to the larger bureaucratic machinery, lower technology threshold and a much larger administered welfare. This assumption results in a calculated loss of around $11 billion, which is about a third of the GDP of a country like Bahrain.

For a country like Saudi Arabia, where the GOSI (General Organization of Social Insurance) budgeted $4 billion for pensions and insurance benefits in 2012, a 7.5 % loss rate would equate to an annual loss of $300 million[22]. That's a significant amount lost every year for a country that is gearing towards a massive improvement in its public sector efficiency.

The imperative to bet on blockchain

In the region, a dramatic fall in oil prices, from upwards of $100/barrel to around $50/barrel at the time of writing this article, has shifted the focus of governments towards improving public sector efficiency. For example, Saudi Arabia reduced national spending in 2016 by around 11%, after running a $100 billion deficit in 2015.

The governments in the region also hold their social obligations to citizens sacrosanct, and in times of economic turbulence it is even more important that these vital welfare lifelines be provided efficiently to those dependent on them.

What constitutes social welfare?
Expenditure which comprises cash benefits, direct in-kind provision of goods and services, and exemptions with social purposes. Benefits may be targeted at low-income individuals, the elderly, disabled, sick, unemployed, or young persons. Disbursement of these benefits requires attestation of certain attributes about the person (e.g. income, age, employment etc.)

What is blockchain?
Blockchain is a way of creating a shared, encrypted "ledger" (or block) that cannot be manipulated once created. Inherent to the creation of a block is transparency, consensus, redundancy and immutability, which is useful because it allows the development of a single source of truth in unknown environments.

What is digital identity?
Digital identity is the mapping of a person's identity to a digital block using a unique secret that only the person knows (e.g. passwords), or can possess (e.g. biometrics)

How does digital identity on blockchain work?
The identity of an individual on blockchain is a cryptographically validated set of attributes about the individual (e.g. birth certificate, passport etc.), that is shared amongst trusted entities (government entities, banks etc.) and can be attested by these entities.

The prudent use of a technology such as blockchain ensures the fastest improvements in cost in providing welfare in the shortest period of time.

The Identity crisis of welfare

When it comes to reducing fraud in disbursement of social welfare, the most important factor is establishing the identity of the individual to whom the welfare is being provided. In the current situation in GCC countries, identity is managed centrally by the government entities providing the welfare, which leads to a single point of failure, and control. This, in turn, creates potential security and privacy issues, along with an implicit lack of trust in the system where controls and data governance are not transparent to the end-benefactor. An example would be the GCC nations, where the Ministry of Interior and National ID authority both collect and maintain details about individuals. Here, an improvement would be the creation of a single source of truth built using blockchain.

Fragmented delivery

Currently, different welfare providers hold the same piece of information in multiple databases, replicating information, and competing with themselves to be the single source of truth. This leads to wasted effort in maintaining separate instances of the same data, and entails the alteration of data in each distinct database whenever an update is required. These actions are considered as highly inefficient.

The promise of no-paper automation

A key factor to improving efficiency is automating welfare payments, based on agreed-upon terms between the government and the individual. These terms, when put on blockchain, form a type of smart contract that can allow for a paperless automation of welfare disbursement. For example, an armed forces veteran of a certain rank might be entitled to a particular welfare payment due to a certain disability he might have encountered in war. This payment can be automated using blockchain, and if the contract terms are changed by policy, his blockchain entry should automatically be used to verify his eligibility and make autonomous changes to any periodic payment entitlements.

Case Study: Guardtime

Since 2013, Estonian government registers — including those hosting all citizen and business-related information — have used Guardtime to authenticate their held data. Guardtime allows the Estonian government to guarantee a single source of truth of any component of the state within the network and data stores.

Through incorporating blockchain technology, Guardtime ensures that every alteration of data is recorded. In addition, it gives proof of time, identity and authenticity, providing data integrity, backdated protection and verifiable guarantees that there has been no interferences with the data. Moreover, all transactions are transparent, as citizens can see who reviewed their data, why, and when. In addition, any alterations to their personal data must be authorized.

Digital authentication reduces the administrative burden on the state and the citizen. Over 200 million digital signatures have been made using the smart ID card system: this is equivalent to some 39 per capita per year and rising. Guardtime works by allowing citizens to use their ID card to fulfill around 3,000 functions including, but not limited to ordering prescriptions, voting, online banking, reviewing their children's school records, applying for state benefits, filing their tax returns, submitting planning applications and uploading their wills.

Entrepreneurs can also use the ID card to file their annual reports, issue shareholder documents, apply for licenses, etc. Government officials use the ID card to encrypt documents for secure communication, review and approve permits, contracts and applications, and submit information requests to law enforcement agencies.

The use of blockchain allows the government to know if its records are the right records, and that they have not been altered from the inside, or by a cyber-attack. In the case of an incident, the government is assured that rogue alterations of public data will be 100% detectable. Nevertheless, this does not sacrifice security, as blockchain removes the need for a trusted authority: its signed data can be verified across geographies, and it never compromises privacy because it does not ingest customer data.

Ultimately, blockchain means that while the Estonian ID card may never be immune to breach (although there have been none so far), the government and citizens can be assured of the confidentiality of their data and can remain reassured since they will be notified in case of any lapse in security.

Source: UK Government: Distributed Ledger Technology: Beyond the Blockchain

The bottom line

If governments in the region are to harness the true value of this technology for disbursement of social welfare, they need to take a multifaceted approach which addresses both the regulatory as well as the technological facets of implementing the concept.

On the regulatory front, governments need to relook at their data laws related to privacy and residency of information. Privacy laws, which are practically non-existent in most GCC countries, might need to be supported by the inherent enablers of privacy. Also, since data reside on multiple nodes, which might be outside the government's entity using the data, data residency laws need to be reexamined to allow this sharing of data between trusted entities.

On the technology front, a pilot is recommended in which a government entity responsible for providing social welfare can start by building a small network of nodes within the entity and integrate it with existing systems. This can be scaled to other trusted entities (e.g. banks) which are also involved in providing welfare to the end-benefactor.