Blockchain & Distributed Ledgers
Potential opportunities for the telecom and networking sectors

A Disruptive Analysis *thought-leadership* paper

August 2017

Commissioned by Juniper Networks Inc.

Author: Dean Bubley
Contact: information@disruptive-analysis.com

Introduction & Background

The term "Blockchain" has recently risen to prominence across the technology industry. Originally used as the underlying technology beneath Bitcoin, there has been a large amount of work turning the concept into a more general way of securely storing and accessing data, across distributed networks, without the need for central intermediaries.

By providing a way for databases to "self-certify" their own accuracy, and to prevent tampering, many believe that blockchains will be a core component of future IT systems – and may even change the way that business and society define "trust" more broadly. As well as the Bitcoin blockchain, there are now many other cryptocurrencies, ledger technologies, and platforms to create them. Ethereum is one of the most important, as it allows developers to create customised blockchains for particular public or private ("permissioned") use-cases. The Hyperledger Consortium is fast becoming one of the main open-source projects for enterprise-grade blockchains.

However, until recently the mainstream telecoms industry has mostly viewed the domain from afar, maybe just as a bullet-point on a slide about R&D projects or futurism. This is now changing. There is a growing recognition – across many industrial sectors – that some real-world use cases for distributed ledgers (the "official" general term for all sorts of blockchains) are starting to crystallise. And while much of the focus has been on the financial services sector, and perhaps healthcare and international trade, there is also an increasing amount going on in telecoms, as well as adjacent areas like network security, distributed computing and IoT.

This paper gives an overview of where the telecom sector should expect to see blockchain evolve in the short- and medium-terms, both as a way to reduce costs / improve efficiency of existing processes and infrastructure, and also a basis for new service and revenue opportunities. It considers both public blockchain examples, and the more-recent emphasis on private/permissioned ledgers. (The latter, broadly, are expected to be used for internal systems within and between large companies, while the former are better for publicly-offered services). It also touches on "tokenisation", especially where "coin offerings" are being used to help fund blockchain-based innovators and startups, including in the network arena.

For the sake of brevity, this paper does not give lengthy descriptions of either blockchain technology or cryptocurrencies. Both are well-explained elsewhere.

Disclaimer: The document has been written by Disruptive Analysis, an independent research and futurist company with long heritage in analysing networks, communications services and service provider business models. It has been commissioned by Juniper Networks, a vendor of hardware- and software-based network solutions for CSPs and enterprises. It is aimed at C-level executives, strategy, planning and technical staff at CSPs and related solution providers and partners.

Mentions of companies in this document are given as illustrations of market evolution and are not intended as endorsements or product/service recommendations. Note that Disruptive Analysis acts as a consultant or advisor to various companies and organisations mentioned here.


Background – what are telcos' underlying motivations?

Communication Service Providers (CSPs) of all types – fixed and mobile operators, cable providers, wholesale carriers and others – are struggling to find new sources of value, while simultaneously reining in costs for providing traditional services. They also face evolving regulation, plus rapid turnover in technologies, which competitive dynamics sometimes force into the market before the last iteration has been fully monetised.

Two broad sets of trends are occurring:

- **Costs:** A deep focus on costs, automation, and productivity, by taking "friction" out of existing assets, operations and external relationships. This ties in with "software-isation" of networks in the forms of NFV and SDN, as well as using third-parties as service and platform providers, shifting CapEx to Opex. These shifts frequently require re-assessing traditional vendors and intermediaries, and using new platforms, financial models and data flows to manage relationships.
- **Revenues:** A continued mission by CSPs to seek out new service opportunities, particularly where these arise from consumer Internet applications and content, or specific enterprise "verticals" that are seeing major technological revolutions. Such areas are well-suited to new entrants, and may allow greater differentiation than traditional commoditised telecom services. Many of these areas, again, bring new requirements for generating, storing or sharing data – for example around payments, IoT data-management, or content rights.

Figure 1: Telecom operators are seeking new roles & revenue opportunities
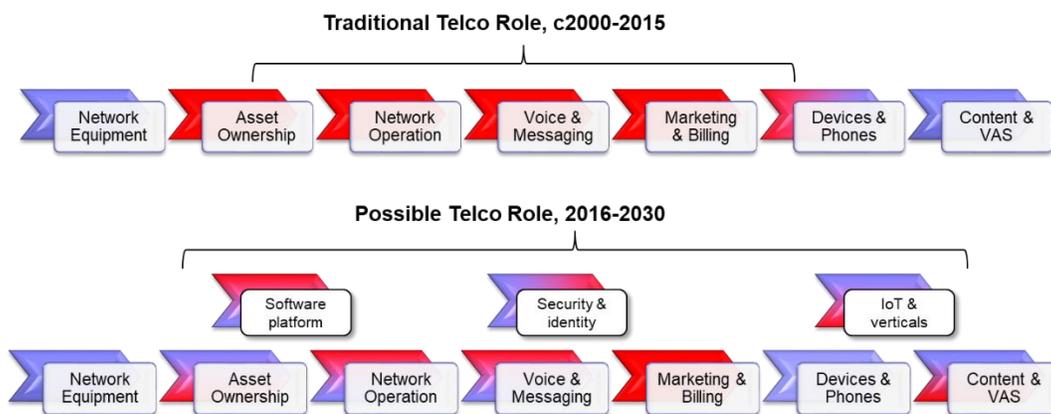
Source: Disruptive Analysis

On the cost side, there is potential for blockchain to remove intermediaries, or otherwise reduce business-process friction where centralised functions act as bottlenecks. Distributed ledgers may also align better with other decentralised functions and capabilities, such as edge-computing or the desire to manage some security capabilities as close to the end-user as possible.

For new services and revenue opportunities, telcos are looking at rapid, inexpensive, innovation and service-creation cycles. This puts a premium on using lightweight technology components, maximising automation, and avoiding complex implementation and integration projects, for functions like billing and management.

Operators are also developing niche solutions for industry "verticals" such as healthcare, e-government, transportation, "Industry 4.0" manufacturing, or public-safety. These will often have very different sets of products, regulations and deployment contexts to traditional telecoms – and the network/communications products may be used to circumvent legacy structures in *those* industries.

For example, electricity supply is changing from centralised huge power-stations and monolithic grids, to distributed solar and wind power generation, "feed-in" from end-users, and probably localised storage in future. This will require new forms of (secure) network and communication to control – a potential opportunity for telcos if they can align their assets (e.g.4G/5G spectrum and networks) to this highly-specialised marketplace. They are looking for tools and partners that might help them to compete in this, and many other, changing end-user sectors.

A major contextual trend is that *all* industries will be embedding networks and communications functions deeply into their structures. While some can use generic telco connectivity offers, others will need more thoughtful, customised variants. Part of the challenge will be dealing with new value-chains and stakeholder groups, while considering alternative payment/accounting methods to traditional telco subscriptions.

While blockchain is not the only answer to these problems, it is likely that *some* of the new service opportunities can exploit networks "enabled by distributed trust".

Trust relationships are central to telecoms

A very general issue of trust, which spans telecoms – and every industry and other walk-of-life - is the simple-sounding question "Who controls the database?"

That then breaks down into a number of associated questions:

- Do I need to pay that person/organisation to control the database? Do I have to pay to enter data, store it, look it up, or change it?
- Can the data in the database be changed or tampered-with in some way?
- How long does it take to put data into the database, or access it afterwards?
- When transactions occur, does everyone involved agree on the changing data, before and afterwards?
- Is the data secure and private? On what terms?
- Who needs access to the data? Just a closed group, or the wider world?

The telecom industry has databases (sometimes "registries" or even just data in a server) everywhere. Your billing details, your call records, what services you have, your interactions with customer-service, your payments and much more – and that's just at a consumer retail level.

But *internally* both within individual telcos, and across the broader sector, there are many other repositories of data. Who has access to radio-spectrum and what are the terms of the license? What equipment and software does an operator have (or use from the cloud), where is it, how is it configured, who's responsible for maintaining it, and so on? Who has rights to a specific phone number – and what happens if it is ported or forwarded? What records or statistics need to be shared with law enforcement or regulators? What data is used for operational and financial decision-making, and where is it kept?

All of these imply *trust* in the data-store, and therefore by extension, trust in the body or mechanism that is storing it, or transmitting it during transactions.

Yet if we look across the telecoms industry today, we sometimes see examples of trust breaking down, or being abused. Various forms of fraud occur, for example around network interconnect. Subscriber databases get hacked. Insecure endpoints are corralled and used as botnets for denial-of-service attacks. Privacy is sometimes insufficient for end-users. Organisations may have old, stranded or non-productive assets or services, for which they may still be paying bills years later. Supposedly "neutral" or non-discriminatory connections may be misconfigured by accident or design.

To be fair, telecoms probably does not suffer from breakdowns of trust – or as catastrophic possible outcomes – as badly as some areas of financial services. Neither does it have some of the cumbersome manual trust-related processes still involved in international trade – faxing letters of credit, or requiring paper certificates for imports.

But as operators look at new business areas – as most of them recognise that they need to – these almost always involve even more new data domains, which may come with other technical constraints and opportunities. Many telcos are looking at IoT applications, which may involve "thin" network connectivity, periods where equipment is offline, or new low-latency tolerance. New service areas may also have their own regulatory requirements on data/trust - for example, telemedicine and healthcare data-protection and confidentiality. Aspects such as asset- and identity-management are inherently predicated on trust, as are (more obviously) payments and creditworthiness.

Consider these examples of instances where "trust" is needed in telecoms, and the tools used to enable it:

- Call-termination CDRs
- Number porting databases
- Lawful intercept requests
- VNF utilisation data
- Privacy protection for user data
- Quota-management for users' plans
- Credit checks for handset subsidies
- SIM / Network mutual authentication
- Spectrum rights
- Service level agreements for network performance
- Data integrity protection

There are hundreds of "trust points" in telecoms already, and the number is increasing. These generally need a basis for immutable (non-changeable) records, and different

models of shared/distributed data ownership and read/write privileges. For some of these, the existing technologies and business processes are efficient and well-proven. Others are changing in various ways, as software or regulation evolves.

It is probable that *some* of these will start adopting shared ledgers to improve or create trust relationships, although it is important to recognise the hype which suggests it is the only future architecture. There will be many alternatives, and blockchain-based solutions will need to be justified in each case.

Categorising blockchain use-cases

This throws up one of the problems here. A central challenge of discussing blockchain in a telecoms context is that there are so many *possible* uses and applications. If you consider the huge number of *existing* instances of databases and storage, that might be replaced or improved with distributed ledgers, you start to recognise the scope.

Then add the immense diversity of new service domains, plus the ways the current architectures might be evolved, and the problem swiftly becomes intractable. Should operators have a central "blockchain strategy" driven from the CTO's office? Or is it best seen as a pervasive trend, that cuts across organisational silos, and will likely emerge in numerous diverse instances?

To counter this complexity, Disruptive Analysis has developed a series of tools that help companies in the telecom sector categorise – and prioritise - the blockchain opportunities, and consider where in their organisations they are best addressed. The two most important are:
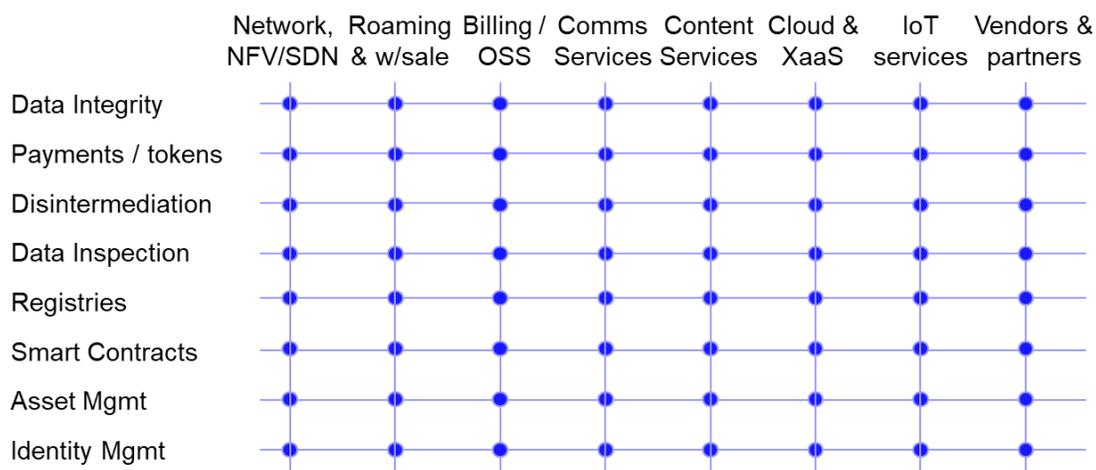
- A matrix of possible "intersections" between generic functions of blockchains, and the operational domains within a stereotypical CSP
- A description of the possible stakeholder groups that may be relevant for any potential blockchain use-case.

The matrix maps generic "horizontal" uses of blockchain (which broadly apply to *any* industry) against functional domains within typical telcos (network, content, cloud etc). The "horizontal" use-cases that Disruptive Analysis expects from distributed ledgers include:

- **Data integrity protection:** Essentially "anti-tamper" for data records, to prove there have been no covert changes made, between data creation, storage and access. Providing a "chain of trust" for data is likely to be ever more important as software and AI systems start to allow for easier "fake" information of all types to be created
- **Micropayments:** The roots of blockchain are in cryptocurrencies, especially Bitcoin. For telcos, we should expect to see both existing public coin types used to pay for services (e.g.content such as music tracks), and potentially new and specialised tokens for things like peer-to-peer sharing of network capacity. Telcos could also potentially become payment-as-a-service providers for verticals. One possibility is a way of storing very small micropayments for later bulk settlement, rather than incurring the transaction costs of dealing with each individually in realtime.

- **Disintermediation:** This refers to the use of blockchain to remove existing central authorities or intermediaries. While telecom doesn't have the multi-layered settlement processes seen in some parts of finance or international trade/shipping, there are still areas such as roaming, WiFi offload and content/app partnerships where third parties are involved and generate extra costs.
- **Data inspection:** This refers to the ability to keep data "in escrow" in situations where there are non-trusting partners, in order to allow select instances of external visibility. For example, a third-party VNF provider might want to check usage records for their software instances, used within another vendor's orchestration framework.
- **Registries**: These are long-term databases where information changes perhaps only in months or years. Some use commercial providers, or industry associations, to keep track of certain variables. These could potentially be replaced with distributed ledgers. For example, a future number-portability database could use a blockchain, to reduce lookup / transaction costs of using a third-party database administrator. More interestingly, this might enable new registry-type operations, for example shared-spectrum usage rights and allocation.
- **Smart Contracts:** One of the most interesting general use-cases for blockchain is "computational law", or "smart contracts". Basically this involves encoding legal agreements directly into software, so that they execute (and settle) automatically, based on specified conditions being met.
- **Asset Management:** Slightly overlapping with other categories, this relates to the ability to encode ("hash") large chunks of digital information, such as media-content or bulk data, directly into a blockchain itself. This allows such assets' distribution to be controlled, as well as ensuring they cannot be easily changed.
- **Identity Management:** Public blockchains enable new ways to create and assert unique identities, for example creating digital versions of passports or financial account data.

Figure 2: Blockchain use-cases may appear in numerous telco intersection-points

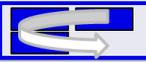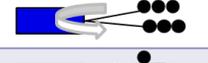|	Network, NFV/SDN	Roaming & w/sale	Billing / OSS	Comms Services	Content Services	Cloud & XaaS	IoT services	Vendors & partners
Data Integrity	●	●	●	●	●	●	●	●
Payments / tokens	●	●	●	●	●	●	●	●
Disintermediation	●	●	●	●	●	●	●	●
Data Inspection	●	●	●	●	●	●	●	●
Registries	●	●	●	●	●	●	●	●
Smart Contracts	●	●	●	●	●	●	●	●
Asset Mgmt	●	●	●	●	●	●	●	●
Identity Mgmt	●	●	●	●	●	●	●	●

Source: Disruptive Analysis

It is important to realise that the matrix is, essentially, fractal. You can "double click" on each point to explode a sub-matrix of more-detailed use-cases. There are literally 100s of plausible intersections.

Stakeholders for telecom blockchain uses

Another way to think about blockchain use-cases is to consider the various stakeholders that could participate in a given application. Obviously, this is going to align with the public/private split in ledger types, but drilling down further is also informative.

In particular, the near-term opportunities are likely to occur where there are like-minded trading or interacting partners – which have broadly similar levels of knowledge and "power". These are sometimes called "market counter-parties", implying rough equality, and without one set needing extra protection by laws or regulators - but having imperfect trust between them. Areas like international settlements and roaming, between two or more telcos, are good examples.

Figure 3: Blockchain stakeholder map

	Within one telco's functional unit / opco	🟥
	Between a telco's functional units / opcos	🟧
	Between "peer" telcos / counter-parties	🟩
	Along a telecom vendor supply-chain	🟨
	Between telco & customers for a service	🟨
	Managed by telco for a community	🟩
	Between telco & regulators/government	🟨

Source: Disruptive Analysis

Potentially, telcos could also use their role as a "trusted intermediary" in a totally separate community, as sometimes occurs for mobile payments today. In a way, telephony itself is a community, where calls between peers are assisted by the telco, which is trusted with routing, counting of time elapsed, and appropriate charging. Something similar could be performed in other domains, perhaps using blockchain tokens as identifiers and payment instruments.

Other stakeholder groups seem less relevant, or at least slower to evolve. There seems little point using distributed ledgers internally within a single telco, given the very high demands placed on systems like billing and rating engines – most blockchain technologies cannot easily scale to millions of transactions per hour, at least without needing huge computing and energy resources.

The medium-term possibilities (yellow on the chart) covers some of the most interesting domains – although they are likely to need considerable development and testing. The fragmenting telco supply chains, and a shift to software and virtualised models, will introduce requirements for new forms of data-integrity management, smart contracts (e.g.for service level agreements, SLAs) or better/more-thorough regulatory intervention. For example, in a world of NFV-based networks, lawmakers may request historic details of software configurations, to investigate claims about failures or unfairness. Blockchains could be a way to prove "state" of software at a given point in time.

Current market status (Q3 2017)

Various telcos and vendors have made public comments about their interests in blockchain over the last 6-18 months. Some have made investments in startups, while others have focused on lab demos and prototypes, or taken roles in one of the industry bodies working on the area.

At the time of writing, there are no fully-commercial blockchain services that have been launched (or at least, announced) by operators or other telecom-industry stakeholders, but the level of "noise" has increased in both quantity and quality since the beginning of the year. It is worth noting that Disruptive Analysis meets far more telcos' representatives at blockchain events than have publicly announced involvement.

Among the most interesting developments have been:

- Orange investment in chain.com
- Verizon investment in filament + other projects discussed at industry events
- TMForum working-group on Blockchain (especially for SLA management) plus at least one "Catalyst" R&D project for IoT exhibited at the May 2017 event in Nice (which involved AT&T, Microsoft, Ericsson and others)
- BT announcement of a security-related blockchain patent, plus broad attendance at multiple industry events
- AT&T patent for blockchain-based HSS (authentication database for mobile)
- Du (UAE telco) announcement of a prototype for healthcare IT using blockchain
- Telstra announcement of an IoT firmware anti-tamper & biometric identity verification concept and that it is "Also experimenting with blockchain for legal interception, environmental sensor monitoring, car safety, agriculture, network operations, fraud, compliance and audit, and e-voting"
- A reference to an (undescribed) proposition by Sprint / Softbank with a startup called TBCASoft, although it references "*..clearing and settlement, personal authentication, IoT applications, and other services provided by telecommunication carriers*"
- Swisscom, NTT Data, NEC, Huawei, Nokia, Cisco, Samsung all members of Hyperledger, although it is unclear if they are working on telecom-specific projects
- IBM and Microsoft have a significant presence at events that blend telecom and blockchain, and seem to both want to be platform providers and/or integrators
- Some blockchain generalists have shown a strong telco focus, e.g.GuardTime (data integrity protection) & Sytel

- Various startups using "initial coin offerings" to raise funds for telecom / network-related services or products. Encryptotel is working on a VoIP / cloud-PBX offer; Dent Mobile is promising an aftermarket for unused mobile data quota; Ammbr is working on a mesh-network proposition (disclosure: this report's author is an advisor)
- Other industry bodies such as GSMA are known to be interested, but have said nothing in public yet. Regulators and law-enforcement bodies are also watching closely.

Going back to the mapping tool, it is also possible to overlay the matrix diagram shown previously with a "heat map" of where real development is occurring, or where the ultimate potential is strongest. Based on current trends, the most action is currently around:

- IoT in general, especially data integrity protection and identity-management, as well as connection-tolerant networking.
- Other domains for data-integrity, such as anti-tamper controls for data provided to law enforcement.
- Smart contracts being explored as tools for network and service SLAs, including as part of an ongoing project by TMForum.
- Cryptocurrencies and tokens, either as payment for basic services (e.g.micropayments for content), or as the basis of secondary marketplaces for network capacity. Disruptive Analysis has recently written an article on the rise of "tokenisation" in networking, and the new phenomenon of "Initial Coin Offerings"[1]
- Various opportunities within NFV and virtualisation more broadly – either to check validity of software versions, or record usage.
- Telcos acting as integrators/platforms for a range of verticals, such as government and healthcare, using blockchains to store identity or encrypted user data

Conclusions & Recommendations

Overall, blockchain technology has huge opportunities in many industries and contexts. It is also in danger of being over-hyped by some of its more enthusiastic advocates. To a large degree, its trajectory will be driven by sectors outside telecoms. Financial services, international shipping and healthcare are probably leading at present, and getting large shares of investment and attention.

But that will bring along telecoms with it – and there are also numerous signs of "grassroots" effort by the communications industry, especially when linked to new areas such as IoT.

This mirrors general trends towards what Disruptive Analysis calls "TelcoFuturism" – the blending of traditional telecoms concepts, networks and value-chains with a broad set of adjacent enablers. Blockchain, AI, robotics, AR/VR, sensor technologies, new payment vectors and many other developments are impinging on telecoms – often in diffuse and unpredictable fashion.

---

[1] http://disruptivewireless.blogspot.co.uk/2017/08/blockchain-for-telecoms-and-networks.html

That said, development of blockchain applications in telecoms is taking a rather different evolution path to, for example, AI. There are some big "framework" plays around telecoms AI, including massive shared "data lakes" relating to customer data, network status and other variables. These can help drive more-reliable operations, better planning and happier customers who are prepared to spend more. Conversely, interest in blockchain and distributed ledgers is (for now) much more dispersed. Individual projects and functions are looking at these as solutions for "point problems" – cheaper registries and databases, ways to secure identity, whether smart contracts could help create enforceable SLAs and so forth.

As such, it's harder to see telcos developing a centralised, coherent "blockchain strategy" – instead, it is going to be used tactically in specific niches, for the next 1-2 years at least. There will be a lot of pilots and prototypes – and each domain will also have a wide range of alternative options to consider. Data-integrity as-a-service could be an early winner for telcos, in terms of new service and also integrated into anti-tamper mechanisms for NFV and law-enforcement requests. There is also scope for various slow-moving registries and databases to transition to blockchains, although regulatory issues may slow these.

We might see more strategic use in IoT in future, as that seems to be a focus of quite a lot of work. There is also strong interest from the OSS/BSS community in developing newer, low-footprint ways of managing and charging for telecoms services. The various token/coin approaches to shared resources are interesting, but have a lot of work to do, to live up to some advocates' utopian-seeming hype.

This fragmentation of effort also means that multiple vendors, integrators and blockchain platforms (private, but also potentially public blockchains) are likely to be relevant.

In terms of recommendations, Disruptive Analysis encourages telcos and vendors to continue experimentation and prototyping blockchain-based concepts. The diversity of possibilities suggests that this responsibility should be devolved to many separate operating groups, ideally with visibility from the CTO's office but not heavy-handed control.

Market participants should also look at working groups within TMForum, GSMA and other bodies in order to collaborate on real-world projects. Membership of Hyperledger or other consortia is also an option – especially if there is scope to help start a telco-specific group or project.

Lastly, Disruptive Analysis would also advise regulators and governments to assess if blockchain makes certain new concepts more viable – for example whether spectrum policy could allow for better sharing of some bands, based on time/location, using a blockchain-based way of recording allocations and usage rights.

Disruptive Analysis

Don't Assume

About Juniper

Juniper Networks believes that Blockchain should be a part of the broader cybersecurity discussion that every company is having today. Millions, perhaps billions, of new peer to peer connections resulting from distributed ledger technologies will create additional strain on network management, orchestration, and security systems, and drive the need for intelligence and distributed cloud architectures further toward the edge.

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

About Disruptive Analysis

Disruptive Analysis is a technology-focused advisory firm focused on the mobile and telecoms industry. Founded by experienced analyst Dean Bubley, it provides critical commentary and consulting support to telecoms/IT vendors, operators, regulators, users, investors and intermediaries. Disruptive Analysis focuses on communications and information technology industry trends, particularly in areas with complex value chains, rapid technical/market evolution, or labyrinthine business relationships. Currently, the company is focusing on 5G, NFV, private cellular, spectrum policy, blockchain, AI, eSIM, operator business models, the Future of Voice, smartphones, Internet/operator ecosystems and the role of governments in next-generation networks.

Disruptive Analysis attempts to predict - and validate - the future direction and profit potential of technology markets - based on consideration of many more "angles" than is typical among industry analysts. It takes into account new products and technologies, changing distribution channels, customer trends, investor sentiment and macroeconomic status. Where appropriate, it takes a contrarian stance rather than support consensus or industry momentum. Disruptive Analysis' motto is *"Don't Assume".*

For more detail on Disruptive Analysis speaking engagements, workshops, publications and consulting / advisory services, please contact **information@disruptive-analysis.com**

Website: www.deanbubley.com   **Blog: disruptivewireless.blogspot.com**
Twitter: @disruptivedean   **LinkedIn: https://www.linkedin.com/in/deanbubley**

Intellectual Property Rights / Disclaimer