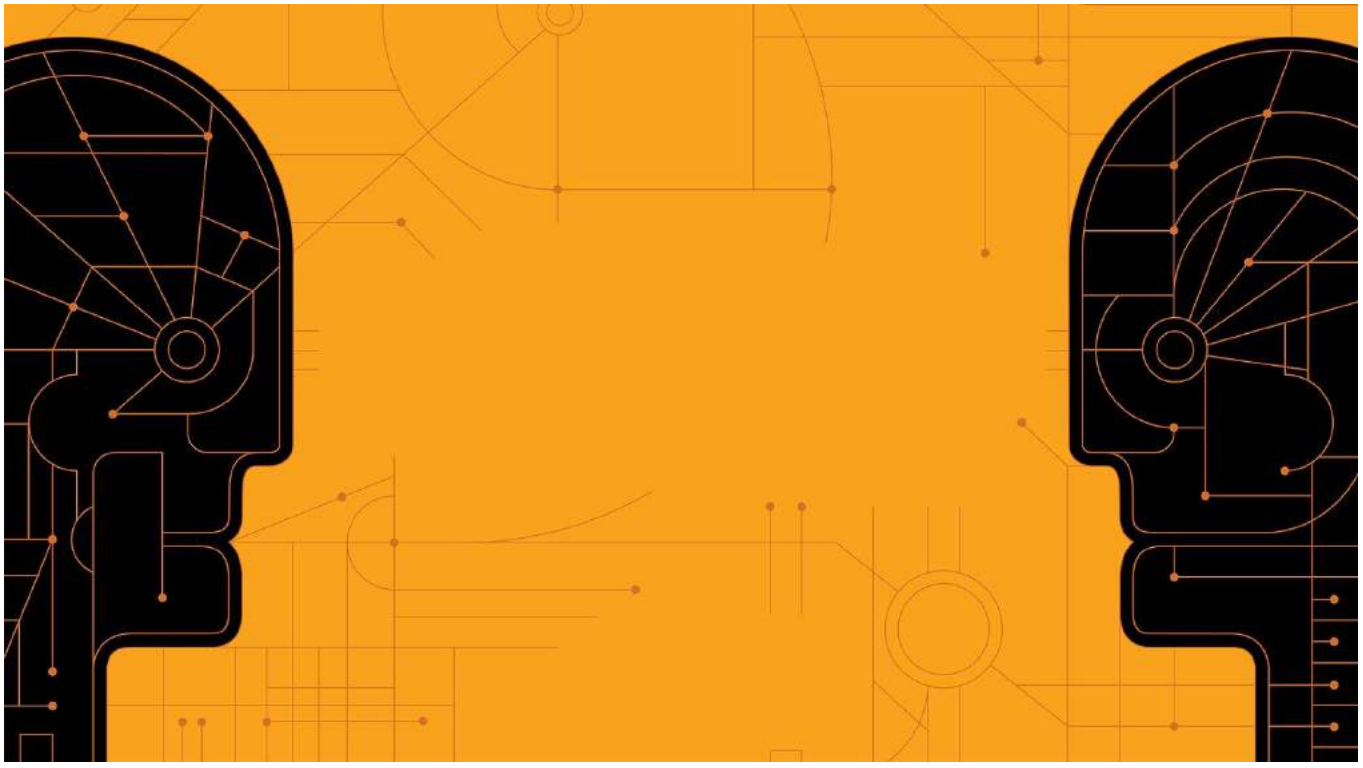
DATACHAIN

SMART DECENTRALISED INFRASTRUCTURE AS A SERVICE



Building the Internet of Value

Building the infrastructure for a data-driven world where AI will process trillions of data in real time to provide context-aware recommendations.

Disclaimer

This White Paper is for information purposes only. BRAINCITIES LAB does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or non infringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights. BRAINCITIES LAB and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. BRAINCITIES LAB does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided “as is”. In no event will BRAINCITIES LAB or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses. This paper is a description of the current and planned BRAINCITIES LAB ecosystem, the actors building it and the project that is working on it. It is neither a solicitation nor a prospectus. This paper may include predictions, estimates or other information that might be considered forward-looking. While these forward looking statements represent BRAINCITIES LAB’s current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forward-looking statements, which reflect the opinions of BRAINCITIES LAB only as of the date of this publication. Please keep in mind that BRAINCITIES LAB is not obligating itself to revise or publicly release the results of any revision to these forward-looking statements in light of new information or future events.

Table Of Content

Problem Overview

Information Reliability: A Trueless Reality

From Biased Opinions To Misinformation and Fake News

It seems that the Internet has become a large publique forum spreading individual opinions with limited to none controle. It is generating chaotic noises and counter results for machine learning projects like **Tay***, because current version of the Internet is not equipped with impartial mechanisms of information reliability assessment. The democratic and deregulated characteristics that made the strength and success of Internet in its early days, now, are plunging it into a digital dark ages.

Tay was an artificial intelligence chatterbot that was originally released by Microsoft Corporation via Twitter on March 23, 2016; it caused subsequent controversy when the bot began to post inflammatory and offensive tweets through its Twitter account, forcing Microsoft to shut down the service only 16 hours after its launch.[1] According to Microsoft, this was caused by trolls who "attacked" the service as the bot made replies based on its interactions with people on Twitter.[2] Microsoft's attempt at engaging ±millennials with artificial intelligence has backfired hours into its launch, with waggish Twitter users teaching its chatbot how to be racist. The company launched a verified Twitter account for "Tay" – billed as its "AI fam from the internet that's got zero chill"

The interdependency problem. Digital information platforms are valuating opinion based information because it help them develop and retain their audience to increase the revenue generated with ads. This new platforms intentionally feed the basic instinct people have to trust information that fit and reinforce with their believes. In 2016 a study analyzed 376 million Facebook users' interactions with over 900 news outlets and demonstrated that people tend to seek information that aligns with their views (ref. filter bubble effect). If data is the new oil, information is brut oil, the related economical interest make www noisy, full of biased opinions that create alternative truths that overwrite the reality. This phenomenon also explain why deregulation is a lie. Massive corporations like Facebook and Google took the power by controlling the information distribution pipe and became de facto and with no accountability obligations Internet's regulators. ~~but the lie on what rely the current version of internet consensus prevent them of any public accountability~~."

How do they use their regulatory power

Facebook do not ban or condemn racist, anti semite and homophobia publications on its platform because this topics has a large audience, and because Facebook prosperity rely on the rise of an unified digital world that will ensure the growth of its audience.

Facebook recently banned all ads for ICOs and cryptocurrencies to protect users from scams.

What if it was for its own interest? Facebook will soon become a digital financial operator. It provide payment solution and soon it will provide bank account. It would perfectly make sense if Facebook was planning to create its own cryptocurrency for its 1.5 billion users.

Information reliability constitute the cement on what social and historical consensus are built. But now a day, social medias allow group of interest to contrefaits the truth and reality itself. It create tensions and put democracy in danger.

William L. Schrader, PSINet's former CEO wrote, "Mankind has always lied, and always will; which is why the winners of wars get to write the history their way and others have no say, but with the internet, the losers have a say! So which is better? Both sides, or just the winner? We have both sides today."

Frederic Filloux explains: "'Misinformation' – a broader concept that encompasses intentional deception, low-quality information and hyperpartisan news – is seen as a serious threat to democracies. … The Dark Web harbours vast and inexpensive resources to take advantage of the social loudspeaker. For a few hundred bucks, anyone can buy thousands of social media accounts that are old enough to be credible, or millions of email addresses. Also, by using Mechanical Turk or similar cheap crowdsourcing services widely available on the open web, anyone can hire legions of 'writers' who will help to propagate any message or ideology on a massive scale. That trade is likely to grow and flourish with the emergence of what experts call the 'weaponized artificial intelligence propaganda,' a black magic that leverages microtargeting where fake news stories (or hyperpartisan ones) will be tailored down to the individual level and distributed by a swarm of bots. What we see unfolding right before our eyes is nothing less than Moore's Law applied to the distribution of misinformation: An exponential growth of available technology coupled with a rapid collapse of costs." Experts express deep concerns about people's primal traits, behaviors and cognitive responses and how they play out in new digital spaces. They said digital platforms are often amplifying divisions and contentiousness, driving users to mistrust those not in their "tribe."

Frank Pasquale, professor of law at the University of Maryland, says we need some sort of analysis and labelling process for data, which is not such an exotic concept: "We already accept labelling of drugs and food"... He also added "What we need as a second step in the information economy is, we need to have information about the information we get." That would help us decide what news we are going to trust, and what feeds are we going to follow... "We should require immutable audit logs," ... "We can at least have logs of the data that are influencing certain results on Google and could help identify certain sources of information".

Fake news, biased opinions and marketing are destroying trust and transparency on the internet Making www a less reliable source of informations for training bots , predictive analytics and reliable data modélisation...

Many of the early, optimistic assumptions about how the internet would create a public sphere with greater openness, transparency and accuracy have been battered by how it has actually been used and abused, according to Frank Pasquale, professor of law at the University of Maryland.

Information platform allow executives from all over the world to extract and analyze data they consider as necessaire to smarter, more agile and more competitive businesses. Across all sectors, more and more businesses are investing in, adopting and relying on data founded on platforms like Facebook, Youtube, Linkedin, Twitter to enrich their predictive model with behavioral, and social indicator then make critical business decisions.

In business environnement just like in political and daily life, reliability is the key factor for credibility evaluation, which is defined as believability, trust, trustworthiness, accuracy, fairness and objectivity, among others (Hilligoss and Rieh, 2008; Metzger et al., 2003). As such, the concept of information and data reliability is a key factor for AI adoption and generalisation [4]. It makes the dismantling of www data chaos a priority.

Data Insecurity : A trustless digital world

Over 70% of organizations and individuals connected to the Internet will be or have been the victims of an IP hijack, Data Breaches and ultimately Data Forgery.

In the last 10 years, nations and large companies have reported thousands of of IP hijacking. Henceforth any government agency, critical infrastructure company, financial organization or corporation that provide users with access to sensitive information is vulnerable.

Companies suffering significant attacks are: Amazon, JPMorgan Chase & Co., Google, Bank of America, Twitter, Apple, HSBC Hong Kong, Yahoo!, and Time Warner Cable.

IP hijack attacks have become a commonly employed technique by hostile governments and criminal organizations. The attackers impersonate to the victim on the Internet, allowing eavesdropping, recording and manipulating of Internet traffic. The attacker can implement various man-in-the-middle attacks against the attacked organization and its users, even when strong encryption is used.

In 2016, cyber attackers reach a new scale. This year was marked by extraordinary attacks, including multi-million dollar virtual bank heists, US electoral process disruption by state-sponsored groups, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices.

While cyber attacks managed to cause unprecedented levels of disruption, attackers frequently used very simple tools and tactics to make a big impact.

"Zero-day vulnerabilities and sophisticated malware now tend to be used sparingly and attackers are increasingly attempting to hide in plain sight. They rely on straightforward approaches, such as spear-phishing emails and "living off the land" by using whatever tools are on hand, such as legitimate network administration software and operating system features."

In the wrong hands, even relatively benign devices and software can be used to devastating effect.

Mirai, the botnet behind a wave of 2016 major DDoS attacks, was primarily composed of infected routers and security cameras, low-powered and poorly secured devices . Level 3 identified approximately 493,000 devices infected by Mirai bots.

Equifax says website vulnerability exposed 143 million US consumers
In July 2017 Equifax, one of the largest credit bureaus in the U.S., said that an application vulnerability on one of their websites led to a data breach that exposed about 143 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May.

"A data breach is the intentional or inadvertent exposure of confidential information to unauthorized parties. In the digital era, data has become one of the most critical components of an enterprise. Data leakage poses serious threats to organizations, including significant reputational damage and financial losses. As the volume of data is growing exponentially and data breaches are happening more frequently than ever before, detecting and preventing data loss has become one of the most pressing security concerns for enterprises. Despite a plethora of research efforts on safeguarding sensitive information from being leaked, it remains an active research problem. This review helps interested readers to learn about enterprise data leak threats, recent data leak incidents, various state-of-the-art prevention and detection techniques, new challenges, and promising solutions and exciting opportunities."[1]

"Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases," the company said in a statement. The statement goes on to say that those responsible for the data breach accessed records containing Social Security Numbers, birth dates, addresses, and in some cases driver's license numbers.

Moreover, 209,000 consumers also had their credit card data exposed. The data breach also included "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers."

“This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes,” said Chairman and Chief Executive Officer, Richard F. Smith in a statement. “I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will," Smith added.

Data broking isn't illegal, it takes advantage of a grey zone. A 2014 US Federal Trade Commission report identified data brokers as companies that “obtain and share vast amount of consumer information, typically behind the scenes, without consumer knowledge.” The main issue is the centralisation effect that accompany this unregulated business. Instead of stolling informations, future attaquants could inject, counterfeit, replace data. This kind of attacks will be invisible to their current monitoring tools eyes.

Data Forgery: Counterfeiting reality

The Biggest Threat To Ai & Digital Economy

So fare, attacks against traditional desktops and servers dominated the threat landscape in terms of numbers. In 2015 other platforms started being actively targeted by cyber-attackers. The widespread use of mobile devices and the mainstream adoption of cloud and Internet of Things (IoT) technologies has opened up whole new platforms and users for attackers to target, and in 2016 a number of emerging threats against these three increasingly high-profile areas could be observed.

Cloud is attractive to attackers as, depending on how it is used and configured, it allows attackers to bypass local security; data stored on the cloud can be more easily accessible and contrefait by attackers than data stored on local servers. Thus, targeting cloud services also allows attackers to cause maximum disruption with relatively little effort—as seen with the Dyn DNS DDoS attack. As a result, the newest target for cyberattacks on manufacturing and infrastructure facilities is not industrial control systems themselves, but rather the data on which they rely.

As the usage of cloud services becomes increasingly common, it stands to reason that such type of attacks also become more commonplace.

Today's Biggest threat to AI and digital economy is data forgery.

According to Vernon Turner, senior vice president at IDC, by 2025, approximately 80 billion devices will be connected to the Internet genérating over 180 zettabytes of data.

All the data generated by the IoT will dramatically expose private and sensitive information to attackers. The gap between the volume of data produced today that requires a certain level of security and the amount of data secured is huge, and this gap will grow 100 times. A major threat in an AI-powered world driven by data.

The convergence of cloud storage, cloud computing, digital agent adoption, serverless application and modern world dependency to data enforce the spread of new cyber-attack trend: Data Forgery.

"Current cloud services make cyber attacks such as data forgery undetectable."

Data Forgery will result in almost symptomless information system control hijack, allowing attackers to hide in plain sight. The nightmare of a data driven and AI powered world.

"Computer forgery can be applied to both forgery of a physical document, carried out with the use of computer hardware and software (e.g. counterfeiting of official forms with the use of a scanner and software for processing graphic documents), as well as forgery of a document created, stored and transmitted in electronic for (e.g. changes in electronic trade books)."

Approximately 11 billion devices are connected to the Internet today. We are already familiar to digital assistant. Self-driving cars are coming, humanoid robots are popping in every bank and 4D factory are built all over the world relying on the data produced by their sensors and their environments.

The figure should triple to 30 billion by 2020, before tripling again to 80 billion five years later. 90% of all data created by this interoperable and interconnected networks of networks will require the highest level of security, but less than 50% will be secured (30% today).

Here is the problem, how to create a trustful and sustainable society if the information used by people and machines are not reliable at 100%?

It is not only about securing data storage. It is about creating a secured stream for the data fueling AI and other autonomous systems to guarantee the integrity and the resilience of the data used for services, decision making, driverless car, healthcare, energy production, manufacturing, education, finance, cryptocurrency analysis and many more...

“Current solutions focus on keeping hackers outside critical systems, but attacks like the one that took down the power grid in Ukraine clearly show that sophisticated attackers will eventually penetrate these systems,” said Bergerbest-Eilon. “Once attackers breach a system, they must blind the operators and protection mechanisms by falsifying data in order to inflict severe and long-lasting damage.” Thus we need to rethink Data Forgery Protection (DFP) as it is the key to keep autonomous devices and AI secured, accurate and reliable.

Why should data forgery be a concern for every AI focused startups?
Well, AI eats data. Poor food mean weak AI, irrelevant analysis, trustless outcomes.
Data integrity is key. In fact, IDC estimates that by 2025, nearly 20% of the data in the global datasphere will be critical to our daily lives and nearly 10% of that will be hypercritical.

We all agree that AI is reshaping the world in an unprecedented way as it leverages the power of the data contained in business siloed databases and people daily life to uncover meaningful stories. It brings the why, the what and the when. What would happen if the data were falsified. Would a recruiter make the right choice? Would investors choose the right business opportunities, would the judges sentence the right person?

AI dependency to Data

It is a misunderstanding to qualify actual AI as 'intelligent' mainly because, current learning method like deep learning, are based on the 'brute force' of computers and limited by the amount of available training data and the system ability of identified patterns. To summarize, no data, no AI. In today AI vision, Intelligence (the capacity to understand environments, contexts, situations) and Experience (interactive or environmental learning and capacity to extract, historize and recognize environmental patterns) are extremely limited because it only rely on one of the 3 dimensions that make intelligence: reasoning, emotion and experience. Current AI industry is focused on human reasoning capabilities simulation through the use of Mathematics and Logic, because it is the easy and simpler way to simulate intelligence.

Gary Marcus, a professor of cognitive psychology at NYU to complete our argument "We are born knowing there are causal relationships in the world, that whole can be made of parts, and that the world consists of places and objects that persist in space and time," he says. "No machine ever learned any of that stuff using backprop."

François Chollet, a researcher at Google explain "People naively believe that if you take deep learning and scale it 100 times more layers, and add 1000 times more data, a neural net will be able to do anything a human being can do," "But that's just not true." To be clear, what if the data used by AI are falsified thus not reflecting the reality? what about the outcomes?

The Data Ownership Challenge

Everydays billions of users are dutifully feeding massive corporations siloed databases with terabytes of data. Gathering tweets, Facebook posts, Google inquiries, banking details, birthday and location information [...]. Businesses leverage this data to generate substantial revenues with ads and fuel business processes.

In a world full of data breaches and threatened by data forgery, the current Data Governance paradigm applied in business environment is a threat by its own. According to a post published by Data Governance Institute on September 28, 2013, "Enterprise data doesn't 'belong' to individuals. It is an asset that belongs to the enterprise. However it still needs to be managed". Since, the increasing value of Data in everyday business, have seen the rise of accredited and delegated data ownership embodied in new functions within the organization like Chief Data Officer, This shift instead of securing people data, Increased the hackable surface and diversified the nature of possible failure. making data protection much more complicate.

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. A common aggregation purpose is to get more information about particular groups based on specific variables such as age, profession, or income. The information about such groups can then be used for digital services personalization, content and advertising targeting to appeal to an individual belonging to one or more groups for which data has been collecte. Online Analytics Processing (OLAP) is a simple type of data aggregation in which the marketer uses an online reporting mechanism to process the information.

When we use Google, Amazon, Facebook or Apple services – like, carrying out a search on Google, getting directions on Google Maps or watching a video on YouTube – the service provider collect data to make these services work for you and stock it on their server. This can include:

What you do

Things that you search for
Websites that you visit
Videos that you watch
Ads that you click on or tap
Your location
Device information
IP address and cookie data

What you create

Emails that you send and receive
Contacts that you add
Calendar events
Photos and videos that you upload
Docs, Sheets and Slides on Drive

What define you

Name
Email address and password
Date of birth
Gender
Telephone number
Country

Data Is An Increasingly Valuable Assets.

It Is Growing In Volume, In Value And In Accuracy.

Current rush on data leads us to the current Internet Dark Age
"1/ We have lost control of our data. And internet and Massive organisation behave as if no one was in control of this phantasmagoric entities. Everywhere and nowhere in the same time. This leads to the end of privacy, to the end of autonomy, it's also bad for the security of people's online identity.

2/ The huge quantities of data produced every day offers the potential for insights which could benefit all of society. With the data controlled by a handful of monopolies, this data is inaccessible to people and organisations who want to create solutions and services for public benefit.

3/ The monopolisation of data creates economic inefficiencies and inequalities. This threatens to undermine trust between citizens, public institutions, and companies, which is essential for a stable, sustainable and collaborative economy.

4/ The current digital ecosystem and Internet of Things (IoT) landscape is highly fragmented, with a multitude of non-interoperable vertical solutions, all offering their own set of devices, gateways and platforms, and means of data handling in data "silos". This fragmentation makes data unmanageable and end users ultimately lose control over it

5/ Data producers and owners have little or no ownership over the digital information they create or the value that derives from it. All of it goes into the gaping maws of tech giants and corporations that use it to monetize their services."

The reason for this is the centralized architecture that has dominated internet services and information society for the past decades. Under this model, we entrusted our digital informations to unelected Internet regulators like Facebook, Amazon and Google that don't need to be accountable for the use they make of it. These digital natives and institutions like banks, insurers, mobile service providers store our data, take responsibilities for its security and integrity, and use it to improve their services. But they also leverage it for other business purposes, Without asking for our consent or in exchange of insignificant compensations, they sell it to data brokers like Epsilon, Equifax and Experian that generate sophisticate and accurate people data sets for marketing, risk mitigation, people search.

Foreseeing the future

A New Paradigm

Peer to peer networks provide an alternative that gives the ownership of data back to people. Individuals who generate and store their informations on the network can retain access to it through encryption keys, independent of the service or application that generated or require access to it. Many companies are exploring the opportunity offered by the blockchain to create new services and platforms relying on business models allowing users to keep full control over their data accessibility. Some are engaged on a path that may lead to the creation of a decentralized web using the blockchain.

Decorolating data from the service and application using it to work, ensure user data-privacy and prevents service providers from risk like data breaches or the temptation to stockpile and mine user data.

No doubts are allowed, data is Internet main assets and it has become the backbone of a society that will rely at +70% on daily recommendations made by autonomous systems such as BRAINCITIES AI. According to Saadia Madsbjerg, Managing Director at Rockefeller Foundation, your personal data is worth an estimates $1,000 per year, a number that should double by 2025. Data brokers centralised the value generated by people on the Internet and social medias. Data broking is a $200 billion industry and it is all built on a free commodity our personal data. Marketing products generate over 50% of the total generated revenue, risk mitigation constitutes approximately 45% of the revenue, people search constitutes the remainder.

In its latest report on global advertising market trends, released December 4, 2017, MAGNA forecasts Digital and mobile advertising sales to grow by +13% in 2018 to reach $237 billion or 44% of global advertising revenues. Approximately 54% of this was shared between Google and Facebook. The two giant platform will benefit of 50% of total advertising sales by 2020. Magna expects the 2018 44% of global advertising revenues share to rise to 50% of the total by 2021 (i.e., $300 billion of an estimated $600 billion). The big opportunity is in the disintermediation of ads targeting.

The emergent new paradigm of data ownership brings the concept of consentment and mutual interest to the table. We envision this new internet as the infrastructure of a decentralized marketplace for Artificial Intelligences providing Outcomes As A Service. Imagine alexa or Siri integrated at the root of current internet. The said context aware recommendation system (AI) main goal would be to match service providers offers with data-owner needs. The requiring or need-based approach supported by AI and reliable data would allow accurate targeting and contextualized product and services recommendations. For making their data accessible and for alerting services and products provider of their need such internet users would be rewarded and paid with coins in line with the agreed smart contract.

“Today’s Biggest threat to AI and digital economy is data forgery and Blockchain may help solve it.”

BRAINCITIES Proposal

From A Declarative To A Proof Based Internet

Data forgery threat and AI generalisation call for the raise of a proof based internet relying on a Proof based and decentralized approach of information production and distribution. Blockchain genuinely notarize the origin of transactions, documents, actions and even relations. It enables proof based authentication of data origins and it increases information reliability. It is the best attempt to design a secured communication protocol over an insecure by design medium such as the current internet.

In a centralized digital world, big corporations are the sole beneficiaries of the financial benefits generated by the exploitation of personal data gathered by data Brokers. The 2016 attacks on Equifax exposed 145.5 million U.S. Consumers financial data, and critical data such as passport information, and credit card numbers. The CFPB is reportedly pulling back from its investigation in the data breach at Equifax, wrote Ben Lane, Senior Financial Reporter for HousingWire on February 5, 2018. The data Broker responsibilities won't be engaged, no accountability is required mainly because data is not a regulated asset. It is brut oil. BRAINCITIES technology aim to disintermediate data broking by giving data owners the opportunity to autonomously convert their data into revenue. Our Federated Decentralized Network for AI and Autonomous Systems will support the raise of a trustful and equitable internet. Such network will enable the development of a sustainable society that benefit everyone by bringing durable solution to challenge like universal revenu and human disruption by robots in the workplace.

DATACHAIN: A Federated Decentralized Network For AI

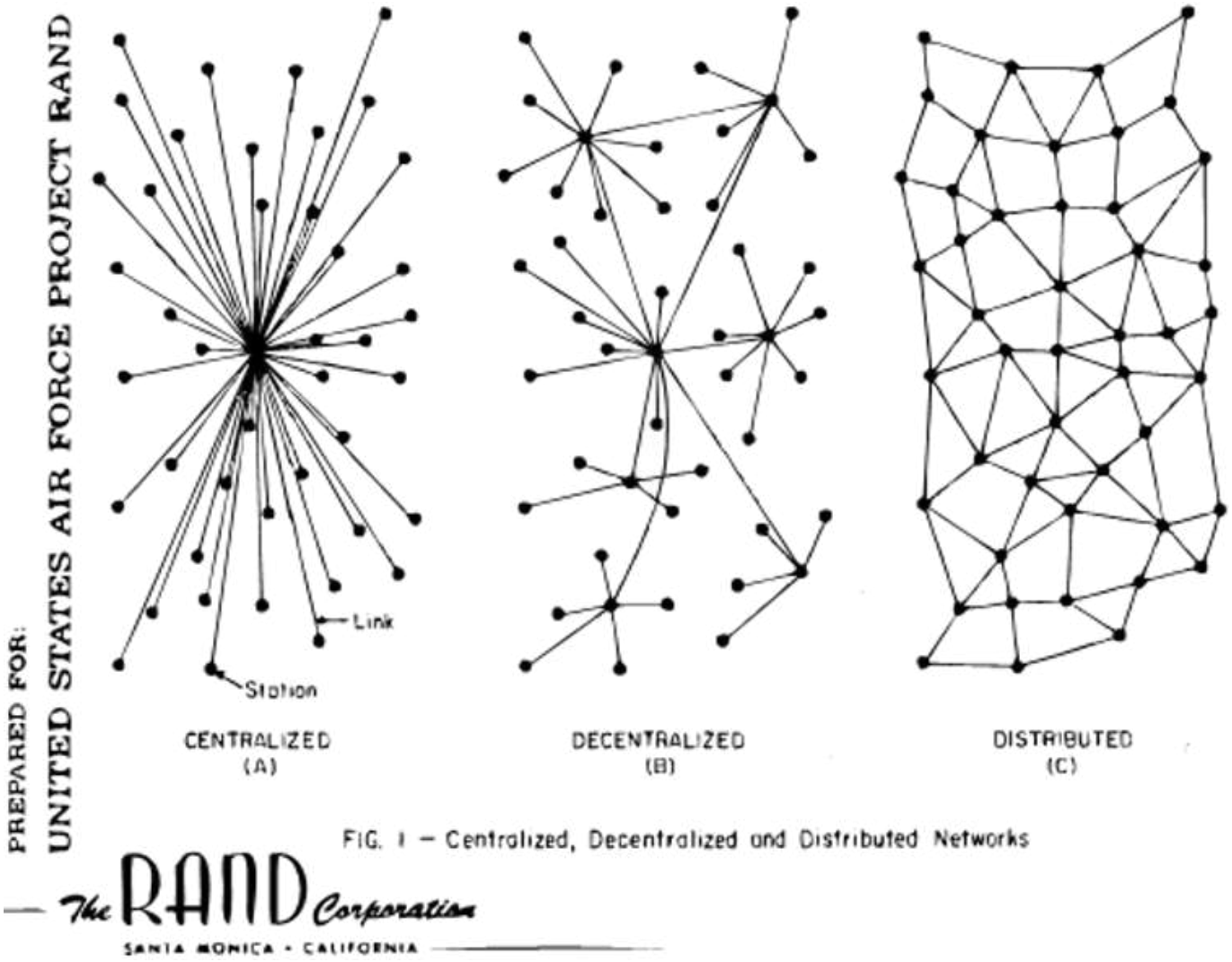
RAND Corp. and Paul Baran initiative

RAND (Research and Development) Corporation, founded in 1946 and based in Santa Monica, California, is to this day a non-profit institution that provides research and analysis in a wide range of fields with the aim of helping the development of public policies and improving decision-making processes. During the Cold War era, RAND researchers produced possible war scenarios (like the hypothetical aftermath of a nuclear attack by the Russians on American soil for the US government. Among other things, RAND's researchers attempted to predict the number of casualties, the degree of reliability of the communication system and the possible danger of a black-out in the chain of command if a nuclear conflict suddenly broke out.

Paul Baran. Ohio State University

Paul Baran was one of the key researchers at RAND. In 1964 he published a paper titled On Distributed Communications in which he outlined a communication system resilient enough to survive a nuclear attack. Though it was impossible to build a system of communication that could guarantee the endurance of all single points, Baran posited that it was reasonable to imagine a system which would force the enemy to destroy "n of n stations". So "if n is made sufficiently large", Baran wrote, "it can be shown that highly survivable system structures can be built even in the thermonuclear era".

Baran was the first to postulate that communication networks can only be built around two core structures: "centralised (or star) and distributed (or grid or mesh)". From this he derived three possible types of networks: A) centralised, B) decentralised and C) distributed. Of the three types, the distributed was found to be far more reliable in the event of a military strike.



Baran/RAND - Types of Network. RAND CORP

A and B represented types of systems where the "destruction of a single central node destroys communication between the end stations". By contrast, the distributed network **C** was different. In theory, one could remove or destroy one of its parts without causing great harm to the economy or function of the whole network. When a part of a distributed network is no longer functioning, the task performed by that part of the network can easily be moved to a different section.

Unfortunately, Baran's ideal network was ahead of its time. Redundancy – the number of nodes attached to each node – is a key element to increasing the strength of any distributed network.. Baran's required level of redundancy (at least three or four nodes attached to each node) can only be properly sustained in a fully developed digital environment, which in the 1960s was not yet available. Baran was surrounded by analogue technology; we, by contrast, live now in a rapidly expanding digital age.

Thanks, but not interested

Nevertheless, Baran's speedy store-and-forward distributed network was highly-efficient and required very little storage at node level; the entire system had an estimated cost of $60 million to support 400 switching nodes and in turn service l00,000 users. And though RAND believed in the project, it failed to find the partners with whom to build it.

First the Air Force and then AT&T turned down RAND's proposal in 1965. AT&T argued that such a network was neither feasible, nor a better option to its own existing telephone network. But according to Baran, the telephone company simply believed that 'it can't possibly work. And, if did, damned if we are going to set up any competitor to ourselves.'

If AT&T had accepted the proposal, the Internet could have been a commercial enterprise from the start, and may well have ended up completely different to the one that we use today.

The Department of Defence (DoD) also got involved, but failed to seize the moment - and with it the chance of turning Baran's project, from its early stages, into a military network. After examining RAND's proposal in 1965, the DoD, for reasons of political power struggle with the Air Force, decided to put the project under the supervision of the Defence Communication Agency (DCA). This was a strategic mistake. The Agency was the least desirable manager for the project. Not only did it lack any technical competence in digital technology, it also had a bad reputation as the parking lot for employees that had been rejected by the other government agencies. As Baran put it:

If you were to talk about digital operation [with someone from the DCA] they would probably think it had something to do with using your fingers to press buttons.

There was, however, some truth in considering Baran's network model impracticable. It was, at least, a decade ahead of its time. Some of its component didn't even exist yet. Baran had, for example, imagined a number of mini computers to be used as routers, but this technology simply wasn't available in 1965. Hence, Baran's vision became economical only when, a few years later, the mini-computer was invented

ARPANET begins to take shape

It was only in 1969, at UCLA (not that far from Santa Monica where Baran worked), that the first cornerstone of the Internet was finally laid, and the ARPANET, the first computer network was built.

Paradoxically, what had began a decade earlier as a military answer to a Cold War threat (the Sputnik), turned a completely different kind of network.

Blockchain

Blockchain technology brings security structures and incentives in line with the way we share information in the 21st century.

On 31 October 2008, at 2.10 pm New York Time (Vigna-Casey, 2015) a white, seminal, paper, written under the pseudonym of Satoshi Nakamoto (SN), was diffused by email to a very large list of computer science experts suggesting how to design a protocol for a peer-to-peer cryptocurrency, called Bitcoin. The paper spurred several reactions (Extance, 2015; Popper, 2015) which then developed into the current implementation of Bitcoin. It describes how bitcoin transactions should be recorded, how to solve the potential problem of double spending (Eyal-Emin, 2014), how to change the supply of bitcoins over time, how to keep pricacy and sustain security and other important features. It also pointed out that trust can be replaced by a cryptographic proof, and that no mediating figures are needed to agree and validate transactions.

The suggested method for registration of bitcoin transactions was the inception of the blockchain technology (BL), a protocol where the relevant information is recorded in subsequent blocks on a ledger, that is shared by all the nodes of the network. Since then other cryptocurencies, such as Litecoin, Feathercoin, Peercoin, Novacoin and others (Halaburda-Sarvary, 2016) and platforms such as Ethereum, based on BL have been introduced and the potential of the technology began to unfold in areas other than cryptocurrencies (Walport, 2015; Nomura Research Institute, 2016; Deloitte, 2016). As of now, its development and applications have been identified as Blockchain 1, 2 and 3 (BL1-2-3) (Swann, 2015). Blockchain 1 refers to the initial applications to currencies, Blockchain 2 refers to contracts while Blockchain 3 concerns applications to further legal and economic aspects. More specifically, BL3 includes value attestation services, notary services, identity and property verification, intellectual property rights protection and others. Public institutions across the world are also becoming interested in BL3 services (Walport, 2015). For example, recently in 2017 the government of Georgia announced an agreement with a specialised company to implement its land property cadastre on a blockchain. The main goal of such operation is to make sure that information on land property is shared among the stakeholders and is non-manipulable, since attempts to change it could be reliably identified. As well as states, banks and corporations are also becaming interested in BL to enhance security and efficiency in information management. Unlike permissionless applications of BL such as cryptocurrencies, where any individual could enter the network and operate, access to states and corporate applications is restricted. The interest of Governments in BL may be seen as somewhat surprising, since the initial bitcoin application was strongly motivated by a libertarian and authority-free approach.

Therefore, the question is: what are the main features of BL becoming so widely attractive in both the private and public spheres? Tapscott-Tapscott (2016) identify “seven principles underlying BL, which may help explaining the wide spread interest for it: “networked integrity, distributed power, value as incentive, security, privacy, rights preserved, inclusion”. Below we briefly comment on two of them.

Broadly speaking, security on BL is based on the cryptographic principle of a private public key approach (Swann, 2015; Narayan et al, 2016; Antonopoulos, 2017; Holden, 2017;). The intuition behind it can be drawn from our every day email experience. Email communication is based on two main elements. A personal credential to enter the system, which plays the role of the private key and the email address, which corresponds to the public key. Credentials have to be well managed and safely kept by an individual, as they represent the instrument for writing and reading messages. The email address is publicly known, and used by those who want to transmit messages to that individual. However, messages sent to that address, public key, could only be read by accessing the system with the corresponding individual's credentials, private key.

Hence, messages sent to a specific address could only be read using the credential of the receiver. Therefore security and privacy of the message content is guaranteed by the protocol and by the fact that personal credentials can not be traced back from the public address. This is clearly true unless the sender/receiver transmits the message to other addresses or the credentials are appropriated by somebody else. In fact, the relation between credentials and addresses is formally a function; that is, the same credential could be used for different addresses while for each address there is only one credential that could allow to read the message. As we shall see, information security is one of the most important features of BL. Personal privacy is almost complete since actors, in a permitted network such as bitcoin where anyone can operate, act under a pseudonym, the digital address, and not under full anonymity. That is, in principle it seems that some inference could be made on the real identity of a trader (Narayanan et al, 2016) by looking at the history of his transactions. However, this can still be very difficult and require large computational power.

2. Blockchain, Distributed Consensus and Coordination

As said, the fundamental technology underlying cryptocurrencies, smart contracts and more in general smart services is BL. This definition, drawn from Wolport (2015) captures the main elements for our discussion "A block chain is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions. There are many ways to corroborate the accuracy of a ledger, but they are broadly known as consensus (the term 'mining' is used for a variant of this process in the cryptocurrency Bitcoin)".

The following important feature is what distinguishes BL from a standard database

"The real novelty of block chain technology is that it is more than just a database — it can also set rules about a transaction (business logic) that are tied to the transaction itself. This contrasts with conventional databases, in which rules are often set at the entire database level, or in the application, but not in the transaction".

Therefore, broadly speaking BL is a list of connected blocks of data, whose contained information is typically validated peer-to-peer by the nodes of the relevant network. Indeed, in some of the most important applications consensus on the recorded data is obtained via some majority rule, without a trusted third party mediating between the interested subjects. As a matter of fact, savings on costs for verification and networks formation are identified as the main economic advantages of BL

(Catalini-Gans, 2016) A simple representation of BL could be as follows. If Bt stands for the union of all blocks of information available at time t, and bt for the block of information added at time t, with t = 1,2, … then

$$B_t = B_{t-1} \cup b_t = B_o \cup \bigcup_{i=1}^{t} b_i$$

with B_o being the initial block. A fundamental cryptographic element of BL information security, is the hashing function $\hbar = H(x)$, that is a function assigning a string of symbols of limited size $\hbar$ to a list of symbols of any size x. Then, a hash $\hbar$ can be seen as a summary of x, which can be very large, with two remarkable properties: the first one is that inversion of $H(x)$ is virtually impossible and, moreover, even a slight variation of the input x to x' will produce an output $\hbar' = H(x')$ which is meaningfully different from $\hbar$ (Narayanan et al, 2016).

These two properties, as well as others, are fundamental for the bitcoin implementation and in general for BL. For example, in bitcoin the private key is first generated as a random number, then a public key is obtained through some mathematical transformation of the private key and, finally, a bitcoin address is obtained as a hash of the public key (Antonoupoulos, 2017). Therefore, from the bitcoin address, which is public information in the network, is neither possible to trace back the public key nor the private key. Hence, as long as it is well managed, the private key remains secret.

Moreover, the content of a block (bitcoin transactions, time stamp and others), is hashed as a unique string of symbols and, if the block information for some reason is tampered with its hash would meaningfully change. Therefore, since the hash computation is immediate, the block hash represents a very quick test to verify if a block content has been altered.

The methodology for registration of transactions, which besides the amount of currency exchanged includes a time stamp, can be interpreted as an example of the so called triple-entry book keeping, an accounting methodology originally introduced to specify the time dimension, as well as the monetary details of the exchange, payer and receiver (Ijri, 1982). Therefore, such registration technology allows to trace back from its initial introduction the path followed by each single bitcoin, keeping the memory of its ownerships. Such feature of bitcoin evokes the view that money is memory, advocated by Kocherlakota (1998).

If security concerning blocks content alteration is guaranteed, the question for BL applications is how to agree on the information to be inserted in the block. In the next paragraph we discuss consensus formation in distributed systems.

Indeed, if a "trusted third party" may not deserve trust or be competent enough, in a decentralised environment nodes too could behave opportunistically, for example trying to validate false information, or perhaps involutarily approving wrong information. Therefore for the correct functioning of a BL with decentralised, peer-to-peer, validation it is important that honest nodes reach a consensus and be sufficiently numerous, so that a majority could emerge to support correct information registration.

But what is correct information? For example, with reference to financial transactions, suppose an individual draws x€ from an ATM machine in country A. Hence, the system should charge his bank account in country B by the sum $-x$€. If instead, because of a computer malfunctioning or other reasons, the bank account was charged $-y$€, with $y \neq x$, then the system would produce information discrepancies and become unreliable. Therefore, for the system to continue functioning in a proper way a majority of nodes should form to validate information where the charge in country B is $-x$€. If some very occasional, minor, mistakes and inconsistencies can be tolerated, as long as they could be timely fixed and do not harm customers, major mistakes due to technical problems or to opportunistic alterations of the data, by some of the nodes in a network, would seriously hinder the correct functioning of the system and eventually its adoption. Therefore, unforgeability and consistency of the relevant information among the nodes of a distributed system is a fundamental requirement for its acceptance and success. However obtaining such consensus, in the presence of nodes who could behave opportunistically, raises some critical issues that we are going to discuss in the next paragraph.

2.2 The "Byzantine Generals"

The main conceptual problem for reaching consensus in an unreliable distributed system has been originally presented within the Artificial Intelligence community under the metaphores of the Coordinated Attack with two generals (Akkoyunlu et al., 1975; Gray, 1978) in its simplest version, or as the Byzantine Generals in the general version with more than two generals (Pease et al, 1980; Lomport et al, 1982; Dolev 1982; Turek-Shasha, 1992). The main problem, in both versions, is that generals of different divisions of an army have to coordinate their attack to defeat the enemy. If they do not do so attack would fail to succeed; failure to coordinate may take place because while some generals are honest, following the initial command of a (loyal) general, others can be traitors, hence with an incentive to alter the information on the attack to make it fail.

A standard version of the Byzantine Generals communication protocol is as follows. Suppose there are n generals; one of them will send a message to the other generals to communicate whether tomorrow they should attack the enemy camp, at a certain time, or retreat. The general sending the first message is the chief, main, commander and will take a decision after having collected as much relevant information as possible on the enemy's position, forces, weather conditions etc. To simplify, as in the original version of the problem, we assume the main general to be honest, that is he will communicate to the others what he truly believes in the interest of his army. As we shall see, the situation may differ depending on whether or not honesty of the chief general is commonly known by the other generals. For this reason we do not consider so, although we assume that any other loyal general will follow the command received, if they only receive one command.

Each general thinks the other generals may be loyal or traitors. Again, also this assumption could be further specified by saying that everyone knows that at least a share s of the generals, where $0 \leq s \leq 1$, hence sn generals, are traitors. However, again to simplify, in what follows we shan't discuss this. In the original version of the problem the main question asked was the following: is there a way for the main general to send the command that the loyal generals will follow?

We now see how, for this to occur, it is fundamental the modality with which the message is sent (oral or written) and whether it is delivered sequentially or simultaneously 7 As for the modality of the command, we can conceive the message as being (i) oral (ii) written but forgeable (iii) written and unforgeable.

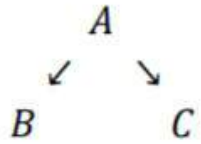
Cases (i) and (ii) are important for successful coordination when the message is transmitted sequentially from one general to the other, or when even if the initial message is sent simultaneously by the main general, the other generals can communicate wih each other. To gain insights on the above points, consider this simple example, inspired by Lomport et al (1982), with three generals A, B and C. If mi stands for the message sent by general $i = A, B, C$, then for simplicity we assume mi can only be of two types: $mi = \{a, r\}$, for a=attack or r=retreat.

Start considering (i) and (ii), and suppose

(a) the message is sent sequentially by A to B and then by B to C: that is $A \rightarrow B \rightarrow C$ meaning that A sends it to B who in turn sends it to C.

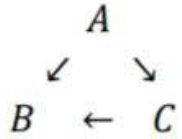
Assume A is honest and that any honest general receiving a message will communicate-execute the same message, while if a traitor receives message a then will communicate message r and viceversa. Moreover, a traitor will always implement action r. First observe that if either B, or C, or both are traitors and $mA = a$ then clearly one general will not attack. Indeed, suppose B is a traitor while A and C are honest. Since $mA = a$ then $mB = r$ and both B and C will retreat. For this reason, the plan of attacking ordered by the chief commander will not be followed by all honest generals. If B is honest, C is a traitor and $mA = a$ then $mB = a$ but C will not attack though, in this case, all honest generals will attack. If both B and C are traitors and $mA = a$, then $mB = r$ and both B and C would retreat. Trivially, also in this case, all honest generals will attack. If $mA = r$ and B is the only traitor then $mB = a$ and C only will attack. Instead if C is the only traitor then $mA = r$, $mB = r$ and all will retreat, as well as when both B and C are traitors.

(b) the message is sent simultaneously, and separately, by A to B and C. Moreover, B and C do not communicate with each other: that is



Still assuming A to be honest, if $mA = a$ and at least one between B and C is a traitor then at least one of them will not attack, though again all honest generals will. Under the same conditions, if $mA = r$ then all will choose r.

Suppose instead that now B and C can communicate with each other. In particular, suppose B is loyal general and C is a traitor. If $mA = a$ then C may say to B that he received $mA = r$.



In this case B may be uncertain as to whether A or C are traitors, and undecided on what action to take. The simple example shows that consensus among honest generals, who will execute the order, can be difficult to obtain even when only one traitor is present within three generals. Indeed, more extensively, if at least 1/3 of the generals are traitors then Lomport et al (1982) show that it is impossible for the plan to be followed by all honest generals.

Therefore, how can the message go through and the related action implemented by all loyal generals? Suppose now (iii) messages are written and transmitted in an unforgeable way. Moreover, each message sent by a general keeps record of the messages received by that general.

For this reason, now a message will contain the following information $mi = \{mj\}$ where mj , with $j \neq i$, are the messages received by general i before sending his own message. More specifically, consider again the sequential communication $A \rightarrow B \rightarrow C$

Suppose that A is honest, B is a traitor and C is honest. If $mA = a$ then now $mB = \{mA = a\}$ Indeed, because of non-manipulability of $A's$ message, although B is a traitor he could not send messages other than what A sent to him. Therefore, action a will be implemented by the two honest generals.

It is easy to see that, with unforgeability, the above conclusion holds for any number of generals, whether with sequential or simultaneous communication. As a result, the protocol is implemented by all honest generals.

The Blockchain technology solves the distributed consensus problem as with the written, unforgeable, messages introducing the new information to be registered in blocks, which is added to previously accepted registered blocks. As said before, hashing functions make forgeability virtually impossible.

A more general way to analyse the Byzantine Generals problem, is to assume that being a honest general or a traitor, is the outcome of a strategic choice. Though we won't enter into the analysis, it may be interesting to sketch, in a very simple way, how the problem could be modelled as a game. Consider the sequential, simplified, procedure $A \rightarrow B$ with only two generals. In the following table we represent all the possible sequences of moves that could take place.

State of the world	*A sends message*	*(A action, B action)*	*Payoff*
α	m_A =α	(a, a)	?
α	m_A =α	(a, r)	?
α	m_A =α	(r, a)	?
α	m_A =α	(r, r)	?
α	m_A = r	(a, a)	?
α	m_A = r	(a, r)	?
α	m_A = r	(r, a)	?
α	m_A = r	(r, r)	?
r	m_A =α	(a, a)	?
r	m_A =α	(a, r)	?
r	m_A =α	(r, a)	?
r	m_A =α	(r, r)	?
r	m_A = r	(a, a)	?
r	m_A = r	(a, r)	?
r	m_A = r	(r, a)	?
r	m_A = r	(r, r)	?

That is, the first column on the left reports what nature chooses as a first move, that is whether it would be right for the army to attack or retreat. We call nature's choice the state of the world, with p being the (commonly known) probability of a. Then general A will observe the state and send a message mA to general B, which again could be either to attack or retreat. However, since B cannot observe the state he may not perfectly deduce it from $A's$ message. Finally, generals A and B will simultaneously choose whether to attack of retreat.

To each possible profile of actions, there will be payoffs associated, and based on such payoffs choices will be made. The game can be solved by backward induction. Hence, in the final, simultaneous, subgame Nash Equilibria will be identified. Based on those, A will decide which messages to send after the state realises.

Therefore, the analysis would suggest who strategically behave honestly or as a traitor, based on the profitability of such choices. It would also include the standard approach previously discussed, where generals are by definition loyals or traitors, as a particular case. Indeed, payoffs in that case will be such that being honest or traitor is a dominant strategy, at any state of the world. Finally, notice that players may be uncertain as to the opponent's payoffs, in which case the final stage of the game could be modelled as a Bayesian game.

Having introduce some of the main conceptual issues behind BL we now proceed discussing Datachain, its original and first use cases.

DATACHAIN

Smart Decentralised Infrastructure As A Service

Paul Baran and RAND Corporation networks was initially designed to resist to a Nuclear major attack… What if AI was the new Major threat… In a data driven and AI powered world, how would we overcome the effect of a major attack of our information infrastructures by a malicious autonomous system created by an hostile group of hackers? We all know about Skynet the fictional neural net-based conscious group mind and artificial general intelligence system that features centrally in the Terminator franchise and serves as the franchise's main and true antagonist. Such general purpose artificial intelligence may not raise before 50 years. But we do believe that in the next 10 years, attacks processed by humans using advanced AI will have impact that will outmatch artificial intelligence such as determined as skynet. To prevent the promising Data driven and AI powered digital era from such threat we have designed a federated decentralized network for AI.

The designed network rely on a live data streaming platform using Blockchain key properties to secure and retrace data integrity. Our DATACHAIN fills the identified security breach in the data storage and data streaming industries (Ip Hijacking, Data breaches, Data forgery). We provide a secured decentralized data storage solution making data injection and data forgery impossible to ensure point to point data integrity. Our solution is designed for a data-driven world where AI will have to process Zettabytes of data in real time to provide accurate and relevant context-aware recommendations to people and machines.

Datachain provides a secured by design Smart Decentralised Infrastructure As A Service. Datachain Factory generate individualised permissioned Blockchains.

Each individual Blockchain is connected to a Data Wallet enabling its owner to control the access to their data. To leverage Blockchain capabilities to solve real life and business problems requiring Blockchain technologies, we designed an agnostic technology. This means that people willing to use DATACHAIN Smart Decentralised Infrastructure As A Service can use any ledger of their choice: Datachain native ledger
Ethereum
Hyperledger
EOS
Neo
...
All this various Blockchain are integrated within the multichain factory's P2P components library and can be deployed on demand.

The system provides to accredited entities the capability to read, write data in format such as Json files. The Datachain Factory contains the logic to provide its services over various blockchain technologies, such as Hyperledger Fabric, Ethereum, Eos, MultiChain, depending on its configuration. Datachain Factory manage the access to off-chain API independent of any underlying blockchain technology.

Using the entity generator, DATACHAIN users can create two kinds of entities: Federations and Communities. Entities are endowed with wallets. They perceive portion of the transaction fees to pay for infrastructure cost (data center, calculation power, custom protocol development)..

DATACHAIN provides a set of enabled functionalities to support the coordination and execution of services, such as federation and communities generation, smart data wallet generation, access to AI Library, access to third parties smart data wallets, consensus execution, consensus auditing, access control, and monitoring.

FEDERATIONS
Federations are accredited entities, this means that they can view and edit the content of third parties Data wallet.

Administrations, corporations and institutions gathered by topics and industries form accredited federations. Banks, Real estate, Humanitarians and healthcare federation are electable accredited federations. This entities are managed by federation operators.

Federation operators run federation node and all the operation executed using custom protocols designed for the federation business need (Ex: in banking KYC). All the member of the federation of the federation can use the protocol and or smart layer (AI) to run their daily business operations.

Members of a federation do have access to the resources provided by DATACHAIN (Protocols, Biaseless and diversified AI, access to secured and reliable data). They are also endowed with transactional Data Wallet connected through webservices to the data warehouse.

Federation operators running a federation node are incentivised :
- They perceive a portion of the fees paid by the member of their federation for using the resources provided by DATACHAIN.
- They buy service on the platform with a discount.

The consensus validating the transactions processed in a federation is a PoA (Proof of Authority). The Proof of Authority Consensus Model overcomes many of the obstacles presented in Proof of Work (PoW), Proof of Stake (PoS), Designated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) to make a platform that has low computational power requirements, no requirement for communication between nodes to reach consensus, and is optimized for system continuity. This is the ideal solution for enterprises relying on a timely and secure consensus.

It is when their identities and reputations are at stake that all the stakeholders can be held accountable and incentivized to work in the best interest for the networks growth and security. To achieve this state, Federation Operators will go through a strict Know Your Customer (KYC) procedure to satisfy the DATACHAIN's minimum requirements.

We summarize the main characteristics of the PoA protocol implemented as:
Low requirement of computational power;
No requirement of communications between AMs to reach consensus;
System continuity is independent of the number of available genuine AMs.

COMMUNITIES
Communities are structured (cities), unstructured (real Madrid supporters) and autonomous entities (Machine to Machine, AI, Bots).
Communities members own their own Data Wallets.

Communities Smart Data Wallets are composed with

Datachain main properties are:
Asynchronicity
Persistency
Resiliency
Elasticity
Security

Datachain main properties are:
Asynchronicity
Asynchronous communication is often viewed as a single entity, the counterpart of synchronous communication. Although the basic concept of asynchronous communication is the decoupling of send and receive events, there is actually room for a variety of additional specification of the communication, for instance in terms of ordering.
A highly secure, virus resistant, tamper resistant, object oriented, data processing system for depositing, withdrawing and communicating electronic data between one or more individual and/or networked computers comprising one or more computers for processing electronic data including one or more shared electronic storage devices for the temporary and/or permanent storage of said electronic data, each of said computers including custom configurable system programs for asynchronous depositing, withdrawing and communicating said electronic data to commonly shared electronic storage devices, and said programs permitting data archival, accountability, security, encryption and decryption, compression and decompression, and multi-processing capabilities.

Persistency

To be define

Resilience

To be define

Elasticity

To be elaborate

$$E_{1D}(\varepsilon) = 2\frac{n}{L}\int_0^{L/2} E_{cl}(\varepsilon x)\,dx.$$

Security

BRAINCITIES

DUBAÏ

Emirates Towers
Sheikh Zayed Road
Dubai, UAE - Po Box 31303
International. +447 413 341 581

PARIS

21 Boulevard Haussmann
75009 Paris France
phone +33 156 036 752

BRAINCITIES

DUBAÏ

Emirates Towers
Sheikh Zayed Road
Dubai, UAE - Po Box 31303
International. +447 413 341 581

PARIS

21 Boulevard Haussmann
75009 Paris France
phone +33 156 036 752

SMART LAYER

A piece of algorithm run on a specialized folder within a Smart Data Wallet.

DATA WALLET

Introducing the Embedded Vault

- Turn any Laptop or Computer into a secure hardware wallet for data, documents, cryptocurrency more secured than traditional hardware wallet device because keys are not stored on the device and can only be recreated by the user using dynamic key creation.

- Turn Laptop or Computer into secure crypto communicator:

- Applications that might be built using the Data Vault.

Secure Messaging

Secure Calling:

Secure Document Transfer:

Media Vault:

Decentralised database:

Ø knowledge browser: