These are highlights from a multi-disciplinary and multi-stakeholder IRGC workshop organised at the Swiss Re Centre for Global Dialogue in Zurich, in June 2017, on the topic of:

Governing Risks and Benefits of Distributed Ledger Technologies

with applications in insurance, medical and institutional governance, and with a focus on privacy and security issues.[1]

Highlights from the discussion include the following points[2]:

1. There is a broad variety of views about promises and pitfalls of the technology, which results from the large diversity in the types of blockchain technologies that support distributed ledgers for a large diversity of applications.
   Driven by digitalisation, dematerialisation and decentralisation, blockchain technology is a promising technology that could meet the demands of many industries and institutions. However, there is also much ambiguity, 'fuzziness' or even confusion about how various types of blockchains function and support the distribution of ledgers across nodes in a network. The technology is not mature yet, so caution is required, and in-depth work is needed on specific aspects. Conversations on the pros and cons of distributed ledger technologies (DLTs) should focus on specific implementation, because details matter for each application and are critical to understanding their trade-offs. Furthermore, discussion of the risks and benefits of DLTs necessitates an understanding of the key stakeholders and their preferences/values.

2. Blockchain technologies may be transformative and enabling. They can support the development of solutions to remedy existing inefficiency and governance problems, but are not the solution itself. Some of the stakeholders that work to develop blockchain-based solutions to problems they face begin to think holistically about the technical, legal, business and governance aspects, and about feedback on broader systems.

3. Through risks related to disintermediation, the technology may pose existential threats to many industries or institutions. Institutions, companies, or entire sectors should engage in research and experimentation in order to reduce uncertainty and clarify ambiguities. It is by trial and error, by starting small, failing often, learning and mastering that organisations can build their specific blockchain case.

4. It is necessary to differentiate more clearly between two basic types of blockchains: public (permission-less, bottom-up) blockchains and private (permissioned, top-down) blockchains. Both have their pros and cons.
   - Public blockchains can be useful in addressing certain fundamental governance issues, especially in instances where this no central authority, or when the central authority is not trusted. In most public blockchains, the ledger recording transactions is transparent and open for all to see.

[1] Prof. Bryan Ford (Decentralized and Distributed Systems Lab, EPFL) and Swiss Re provided support and important contributions.
[2] Questions discussed at the workshop can be found in appendix.

> Example: Bitcoin or Ethereum.
However, certain public blockchains have incorporated anonymising techniques.
> Example: Monero and ZCash.

- Private blockchains are being developed to benefit from the basic technology without suppressing the need for a central authority, or without destabilising the institution implementing it. With these systems, each institution decides who participates, no proof-of-work is needed (lower energy costs), and consensus protocols (validation rules) are different. When transactions are encrypted, only parties to a transaction can run the code and validate the data.
  > Example: Hyperledger Fabric (2017)
- In practice, every sector, application or organisation needs to adapt these generic types to their specific needs and objectives. This underlines the need for every organisation to review carefully its goals and constraints before asking the question of whether or not it should consider a blockchain technology to distribute ledgers among the nodes of its network.

5. Built-in cryptography can improve the security and privacy of blockchain technology, but it is not sufficient to make blockchains fully secure. This is a common misunderstanding, which needs to be clarified. Developers of methods to encrypt transactions and data must work together with those who develop the applications, to both bridge the knowledge and communication gaps, and help address the true problems. Privacy and security must inform the early design of blockchain systems and not come as an add-on consideration when it is too late.
   > The insurance industry is working to build privacy-preserving transparency with blockchains, using a layered approach to privacy in smart contracts, depending on the parties, the data and the business logic that need to be protected.

6. In a world where data security is challenged, we must consider carefully how DLTs can protect information integrity (the system must store and retrieve the correct data, and yield correct answers -it must "tell the truth"), confidentiality (the system must by default protect sensitive information from improper disclosure -it must keep secret any information that an individual or organisation considers is private or confidential), and availability (the system must reliably deliver requested information in a timely fashion).
   The current state of play in respect of these criteria is as follows:
   - Integrity is what a blockchain is naturally designed to do. But it may be a false promise, so some caution is needed. The reality is that a chain of blocks may be hacked or forced to perform certain operations if a majority of users (possibly tricked by powerful arbitraries) or if a consensus threshold in the community decides to violate the pre-established rules. Many private blockchains have single points of failure or compromise. This potentially allows an attacker to violate the integrity of the entire blockchain by successfully compromising only one participant. So the assumption that decentralisation brings security and protection may be challenged. At the edge, a blockchain may provide un-correct answers, for example if a bug in a smart contract is exploited.
   - Confidentiality is in general not well protected by blockchain technologies. The pseudo-anonymity that is created to replace anonymity aims to manage identities to facilitate

transactions but does not fully protect identities. Even when transaction data on the blockchain is encrypted, unencrypted metadata about it –such as the timing and patterns of transaction- can leak potentially sensitive information. Therefore, privacy and data protection cannot be taken as a given, except in some cases, which should be described more explicitly by developers. Those cases rely on using the right type of encryption, which is also the only way to protect collective integrity (except with zero-knowledge proofs). At the edge, the blockchain technology itself can neither prevent a user's computer from being hacked, nor can it prevent on-chain transaction metadata to leak confidential information. What will matter there (as usual) is the quality and accuracy of the algorithm that the blockchain will execute.

- Availability is built into the very fabric of blockchain, but latency can be an issue. The early type of public blockchains used for cryptocurrencies (e.g. Bitcoin) does not respond promptly enough for some applications, either in the case of block congestion or if network outage severely splits validators. But not all applications need quick response time.

  > Transactions on public registries such as land ownership or insurance claims do not need to be instantaneous, in contrast to payment systems that replace cash or credit cards. In the case of medical records, it is not a problem if it takes some time to share the data, except in the case of an emergency, when the data must be quickly available.

In the current state of the technology, and depending on the type of blockchain and cryptography, applications will have to make trade-offs between confidentiality and integrity, and between confidentiality and availability. They will also have to consider interoperability, and some standardization may be needed for some sectors.

7. Blockchain-embedded 'smart contracts' are a promising development, which can be expected to deliver efficiency improvements for businesses and administrations. Smart contracts are a technology to make blockchains fully programmable. They can be read and executed by the blockchain network they are deployed on, thus decreasing the transaction costs associated with an exchange. The smart contract code sets out its core functionality, the conditions under which it is triggered and the source of data used to make a decision. However, current smart contract systems are still suboptimal and, because of the inherent weaknesses of blockchain technologies, interpretation and dispute resolution must be planned, as for any contract. Various models and systems can be considered. These will likely depart from existing arbitration systems to better deal with the technical nature of smart contracts.

8. Law can be supported by the technology, and the positive contribution that blockchain can make to how regulations are implemented and contracts are executed is underestimated. However, for that purpose, the technology must be supported and authorised by the law (at least for those applications that are regulated). Legal and regulatory aspects are too often ignored by those who develop the technology.

   > The EU GDPR[3] will require that personal data is stored under the control of the individual. This is something that proper use of blockchain technology can make possible; or that improper use can infringe. In that context, proper use of DLTs implies that the data stays where it has been generated.

[3] European Union General Data Protection Regulation. Will come into force in May 2018

> In Estonia, blockchain is used to verify how citizens' private and confidential data are accessed and by whom (for transparency), but the actual data is not stored on the blockchain itself (for privacy and security). The blockchain only records the transactions (for integrity), and the government and its administration remain the central authority (for accountability).

9. Distributing trust among the nodes in the system in order to create digital trust to substitute or complement trust in central institutions can work in some cases. However, it will not and should not be expected to replace trust between individuals and organisations. Blockchain opens new opportunities but can contribute to improving trust only if it is accompanied by and serves to support the building of trust between people. In many cases this implies a new role for institutions and central authorities.
   > Many current private blockchain systems do not fully distribute trust because they still contain single points of compromise where any single failure of any participant can compromise the integrity, confidentiality and/or privacy of everyone relying on the blockchain.
   > Regarding the perceived lack of efficiency of some institutions affecting trust in those institutions, technologies such as blockchain should necessarily try to remedy this problem because inefficiencies are often associated with other factors of trust such as proximity to citizens or clients, or simply human relations.

10. Criteria of trustworthiness include accountability and transparency.
    Accountability may become a central concept in the future. Although current blockchain systems are not performing well on the accountability properties mentioned in point 6, ongoing research on those aspects could help.
    > In the medical sector, trust may be established if (a) patients are confident that the technology will help provide the best treatment for them and (b) they trust that the technology will not use private data in a way that will cause prejudice to them. Needless to say that this must be achieved without the need to explain the algorithm!
    - Blockchain technology provides a capability to (a) implement the rule of who has the right to access the ledger/data (and the right to revoke the right), and (b) know or verify who has accessed the data.
    - The provision of transparent audit trails of who accesses the data may be the second major advantage of blockchain technology (and a means to build accountability). This is especially the case if there are varying views about privacy in society and if a cornerstone of privacy law is the right of individuals to withdraw consent or data (also including the right to be forgotten).

11. The blockchain logic that distributes ledgers and trust can help us start thinking about new ways of doing things in a new world, for new types of ecosystems. In this respect, and whatever is achieved in the short term, it is necessary to invest deep thinking into the paradigm that supports the blockchain technology and the governance context. Both influence the technology and will be influenced by it.
    > Many of those who invent new open blockchain systems (e.g. Ethereum to provide a decentralised platform for smart contract development) do not ask permission before deploying them. They do not respect the conventional norms of governance.

Technology that intends to support institutional move into the digital era will translate a culture of decentralisation and global security into operational mechanisms. The challenges of decentralisation (scalability, usability, security, privacy and sustainability) will have to be addressed upfront so that the decentralised systems that will be deployed can secure information-centric societies. A 'next-generation' blockchain may be needed for that.
It is thus important that the technology is not overkilled by the way it is currently used, not least because it will most probably trigger new norms and ways to handle privacy and security.

About IRGC

The **EPFL International Risk Governance Center** (IRGC) is a neutral platform for dialogue about emerging risks as well as opportunities and risks related to new technologies, with the aim of providing recommendations for their governance.

More information about IRGC is available on irgc.epfl.ch

This workshop on Governing Risks and Benefits of Distributed Ledger Technologies is part of an on-going **IRGC project on cybersecurity**, which includes a series of expert workshops.

More information about this project is available at irgc.epfl.ch/projects/cybersecurity

Appendix: Questions discussed

Participants in the workshop were invited to discuss the following questions:

- To what extent do you trust that DLTs will be very helpful to address cybersecurity and data protection issues, and how? Please consider in particular, and perhaps separately: privacy, confidentiality, integrity and availability.
- What are the pros and cons of the various distributed ledger / blockchain technologies, for application in the medical and health sector, in insurance and in institutional governance?
- Is there a knowledge or communication gap between those who develop the technologies and those who implement and use them?
- What must an organisation do before making a decision about DLTs for providing services?
- Could DLT contribute to building trustworthy applications, which in turn contribute to building societal trust in institutions?

Specific themes were discussed in breakout groups:

A. Algorithms ('rule of code') and the rule of law – smart contracts

- "Thinking through law and code, again"
- Smart contracts and private commercial relationships
- Blockchain smart contracts and the EU General Data Protection Regulation (GDPR)

B. Protecting sensitive data against cybersecurity risks

- Should we be concerned about the risk of a "51% attack", where gaining control of a majority of nodes could lead to control over the entire blockchain?
- How can DLTs enable data sharing, while preserving confidentiality?
- What is recommended to enable data protection and privacy for medical and health data transactions or for e-voting, according to specific legislations ("must know who" versus "must not know who")

C. The trust issue: DLTs can help restore trust in institutions

- What does it mean that "trust will be decentralised, or distributed"?
- To what extent can 'technical (digital)' trust substitute for social trust?
- To what extent is disintermediation an opportunity? Or a problem?
- In what cases are permissioned ledgers preferable to permission-less ledgers?

D. Performance issues: cost-efficiency, scalability, interoperability, etc

- How can DLT-based institutions coexist with non-DLT systems?
- How to handle the transition and issues of interoperability?
- Scalability issues
- Might the introduction of DLT systems add a level of complexity that is unsustainable?