

Vienna, 11.4.2018

Proposal for COMET K1-Center **ABC** (Austrian Blockchain Center)

Executive Summary

The K1-Center **ABC – Austrian Blockchain Center** - mission is to be the one-stop-shop Austrian Research Center for Blockchain (and related) technologies to be applied in industrial applications like industry 4.0 / IoT as well as financial, energy, logistics, government and administrative applications. Those new applications and business models resulting from collaborations between established players, innovative startups and top R&D institutes will be the key for the creation of new jobs and establishing Austria among the top ten innovative countries in Europe.

The R&D themes of the center have been organized in 5 Areas targeting economic, technological, applications as well as political and legal topics interfacing with existing COMET centers like CDP, SBA as well as international Blockchain initiatives.

Area 1 addresses the technical and theoretical foundations of distributed ledger technology. As we have seen in the past, understanding the mathematics and cryptography is important as these are the foundations for consensus building, which is again the very foundation of DLT. The area will also address technical aspects of different types of Blockchains and “Non-Blockchains”, Smart Contracts and transparency on the Blockchain.

Blockchain & similar distributed ledger technology (DLT) has the potential to fundamentally disrupt the current economic system by enabling the replacement of intermediaries by trust less peer-to-peer systems for value exchange. **Area 2** addresses the economic potentials and problems of this new paradigm. The area will study economic questions that arise in any peer-to-peer system and investigate DLT based decentralized business models in specific application domains.

Area 3 focuses on the technological aspects of Blockchains in Industry 4.0 and the Internet of Things. The convergence of Blockchain with emerging technologies in those fields such as semantic database solutions, machine learning, cloud manufacturing, 3D printing and machine-to-machine will be at the centre of the activities.

Understanding socio-economic and technical questions that arise in blockchain-based systems requires novel data-driven methods, services and tools. The goal of **Area 4** is to investigate, and develop scalable data science methods, tools and services that contribute to a better understanding of the structure and dynamics of blockchain-based ecosystems and environments. A central outcome will be a horizontally scalable platform that can be used by researchers and practitioners to answer scientific or business-related questions. This area will also have a strong interdisciplinary and community-oriented and focus and involve data

scientists, practitioners from the startup community, as well as scientists with various backgrounds within and outside the ABC initiative. From an organizational perspective, this area could be organized horizontally to other areas.

As a completely new technological concept, DLT also raises demanding legal questions throughout all fields on a national and international level. **Area 5** aims to address legal questions arising under current legislation including matters of private, public and tax law, tries to address concepts and suggestions for future legal frameworks and starts to analyse further political implications.

Research Areas and Projects

Overall Scientific Lead:

Prof. Taudes,
Institut für Kryptoökonomie,
WU Wien

<p>Area 1: Cryptography, Technology & Security</p> <p><u>Lead:</u> Dr. Weippl, SBA Research</p> <p><u>Partner:</u> Prof. Rinderle-Ma, Uni Wien Prof. Klas, Uni Wien Prof. Maffei, TU-Wien Prof. Pietrzak, IST Austria</p>	<ul style="list-style-type: none"> • Cryptography, Mathematics <ul style="list-style-type: none"> ○ “Game theory for Blockchains” • Types of DLTs <ul style="list-style-type: none"> ○ Blockchains ○ “Non-block Blockchains” ○ Upcoming/new types (e.g. IOTA) • Protocols, Algorithms (Machine Consensus) <ul style="list-style-type: none"> ○ Efficiency, environmental aspects (viz. Proof of work ...) ○ Byzantine Fault Tolerance ... • Tools/Frameworks for Development • Blockchain Code <ul style="list-style-type: none"> ○ Smart Contracts ... and beyond ○ Distributed Apps • Security <ul style="list-style-type: none"> ○ General aspects ○ Security ⇔ Privacy vs. Transparency ○ Security of Smart contracts ○ IoT-Security • Quantum Cryptography <ul style="list-style-type: none"> ○ Risks, Chances?
<p>Area 2: Cryptoeconomic Modelling & Blockchain Applications for Business</p> <p><u>Lead:</u> Dr. Shermin Voshmgir, Institut für Kryptoökonomie, WU Wien</p> <p><u>Partner:</u> Prof. Dr. Jochen Michaelis, Uni Kassel</p>	<ul style="list-style-type: none"> • Economic foundations of DLT enabled business models <ul style="list-style-type: none"> ○ Consensus Mechanism design ○ Identity and Reputation Systems ○ Application token design ○ Distributed application token design ○ Governance and DAO • Monetary aspects of DLT <ul style="list-style-type: none"> ○ Pricing theory for digital assets ○ Monetary theory and cryptocurrencies • DLT and sustainability in economic systems <ul style="list-style-type: none"> ○ Sustainability incentive design ○ Emissions pricing and trading • DLT and finance <ul style="list-style-type: none"> ○ Peer-to-peer banking and insurance ○ ICOs ○ Trade finance ○ DLTs in financial supply chains • DLT, innovation and business process design

	<ul style="list-style-type: none"> ○ BPM and DLT ○ Novel BPM and governance structures in eGovernment, Knowledge Management and Supply Chain Management
<p>Area 3: Emerging Industries & Blockchains in Manufacturing</p> <p><u>Lead:</u> FH-Prof. DI Dr. techn. Fidler, Dr. Moser / FH St. Pölten</p> <p><u>Partner:</u> Univ. Prof. Dr. Bleicher, Dipl.-Ing. Mörzinger, Dipl.-Ing. Raschendorfer / TU Wien</p> <p>DI(FH) Helmut Loibl / FOTEC</p> <p>Univ. Prof. Soulla Louca, BA, MSc, PhD / University of Nicosia</p> <p>Prof. Dr. Horst Treiblmaier / MODUL University Vienna</p>	<ul style="list-style-type: none"> • Database Aspects/Single source of truth: <ul style="list-style-type: none"> ○ Integration of different Blockchain-based database solutions <ul style="list-style-type: none"> ▪ Quality documentation ▪ Asset sharing ▪ Digital Product Memory / Verification of spare parts ▪ Distributed manufacturing ▪ Supply chain tracking ○ Semantic Analytics in Blockchain-based database solutions and their implications in relational database systems & ontology-based data access applications. • Technological Aspects in Industry 4.0 & IoT: <ul style="list-style-type: none"> ○ 3D Printing & Smart Contracts ○ M2M Business Scenarios & Machine Learning ○ Blockchain/DAG-based Internet of Things ○ Blockchain-based traceability ○ Blockchain-based content distribution ○ Data sharing/ Decentralized Data market ○ Cloud Manufacturing • (Data Based) Decision Support <ul style="list-style-type: none"> ○ Visualization of large Blockchain data & relationships ○ Applicability of BC/DLT/DAG in emerging industrial applications ○ Process optimization using Blockchain-based technology
<p>Area 4: Data Science Methods for Blockchain Analytics & Predictions</p> <p><u>Lead:</u> Dr. Haslhofer, AIT M. Tarasiewicz, RIAT</p> <p><u>Partner:</u> Prof. Böhme, Uni Innsbruck</p>	<ul style="list-style-type: none"> • Blockchain Analytics Platform • Smart Contract Analytics and ICO Tracking • Market Understanding & Predictions • Empirical Analysis of Off-Chain Transaction Technologies • Centralization tendencies in distributed ledgers • Blockchain Monitoring for Governance and Sustainable Chain Quality
<p>Area 5: Legal and Political Implications</p> <p><u>Lead:</u> Prof. Kalss, WU-Wien</p>	<ul style="list-style-type: none"> • Legal aspects of the use of DLT <ul style="list-style-type: none"> ○ Private, public and tax law ○ International and national legislation • Governance and Smart Contracts <ul style="list-style-type: none"> ○ Changes to the current contract paradigm as a

Partner:

Prof. Winner, WU Wien

Prof. Eberhard, WU Wien

Prof. Owens, WU Wien

Prof. Forgó, Uni Wien

Prof. Wendehorst, Uni Wien

Prof. Blocher, Uni Kassel

result of DLT contracts

- Execution of contracts, incomplete contracts and judicial awards
- Self-regulatory codes of conduct
- Legal aspects of DAOs
- DLT and investment
 - ICO/ITO and capital markets
 - Regulatory law
 - Company law
 - Codes of conduct and enforcement
- Information Privacy and Information Security
 - Right of data protection, protection of privacy and the Blockchain
 - GDPR – General Data Protection Regulation
 - Enforceability of data protection rights (e.g. the “Right to be forgotten”) within Blockchain systems
 - Compromised Blockchains
 - Smart regulation
- Tax law
 - “Digital tax transformation”
 - Income tax, corporate tax and VAT implications
- Politics
 - Political implications of future legal frameworks
 - Cryptosystems for political and governmental processes

Area and Project Description

Overall Scientific Lead: Prof. Taudes, WU Wien

Area 1: Cryptography, Technology & Security

Lead: Dr. Weippl, SBA Research

Area 1 addresses the technical and theoretical foundations of distributed ledger technology.

As we have seen in the past, understanding the mathematics and cryptography is important as these are the foundations for consensus building, which is again the very foundation of distributed ledger technology. Game theory can explain the probabilistic guarantees of the Nakamoto consensus that solves (a specific case of) a previously unsolvable problem of Byzantine Fault Tolerance. Research in the last years, however, has revealed new powerful attacks on this consensus model such as Selfish Mining and Stubborn Mining.

This foundations area is important to really understand the intricacies of this technology. While companies and many “crypto-market experts” see the dawn of a new society, global-scale attacks can bring down such as a system within minutes and we have seen spectacular hacks in the past that were technically not sophisticated at all.

Topics that we plan to address are comparing different types of Blockchains and “non-Blockchains” including upcoming concepts such as IOTA. In addition, efficiency, scalability and environmental aspects (i.e. power and resource requirements) of protocols is another important topic.

In the context of Smart Contracts we will also explore distributed apps including API options, call to external systems, and possible malicious behaviour of both apps and VMs.

One aspect that is not widely discussed in the public is the transparency that public Blockchains offer. Partial transparency and selective pre-emptive disclosure of certain attributes is a challenging and important topic that we plan to address. For instance, a company might want to prove to its customers that it provably paid its value added tax of all its previous transaction but not reveal its total turnover or the amount of taxes paid.

Area 2: Cryptoeconomic Modelling & Blockchain Applications for Business

Lead: Dr. Shermin Voshmgir, WU Wien

Distributed ledger technology (DLT) has the potential to fundamentally disrupt the current economic system by enabling the replacement of intermediaries by trust less peer-to-peer systems for value exchange. Area 2 addresses the economic potentials and problems of this new paradigm. On the one hand we will study economic questions that arise in any peer-to-peer system, on the other hand we will investigate DLT based decentralized business models in a number of application domains.

Consensus mechanism, identity, application token, distributed reputation management and governance / distributed autonomous organizations design have to be dealt with in any DLT-based organization. Using game theoretical methods we will study more sustainable and egalitarian alternatives to PoW and PoS like Proof of Identity or Proof of Time and investigate governance structures for peer-to-peer systems. We will look into mechanism design methods for designing sustainable application tokens and research methods to make distributed reputation mechanisms interoperable and resistant to manipulation.

Given the breadth of expertise present at RIAT and WU's research institute of cryptoeconomics we are able to apply these general findings in a number of important areas of application:

In the project monetary aspects of DLT we will develop a pricing theory for digital assets and study the linkage between classical monetary theory and cryptocurrencies. We will study peer-to-peer banking and insurance business models and the impact of DLT on financial supply chains. We will look at ICOs as novel financing instruments and regulatory design in this area. Novel ways of trade finance will be studied, too.

Project DLT and sustainability in economic systems will study the potential of DLT and cryptocurrencies for new ways of incentivising for sustainable behaviour of consumers and industry. We will also explore the potential for emissions pricing and trading.

Project DLT, innovation and business process design will explore the implications of DLT on the design of business processes and innovation processes utilizing application scenarios in eGovernment, Knowledge Management, Energy Markets and Supply Chain Management.

Area 3: Emerging Industries & Blockchains in Manufacturing

Lead: FH-Prof DI Dr. techn. Fidler / Dr. Moser, FH St. Pölten

Area 3 focuses on the technological aspects of Blockchain in Industry 4.0 and the Internet of Things. The convergence of Blockchain with emerging technologies in those fields such as semantic database solutions (relational database systems and ontology-based data access), machine learning, cloud manufacturing, 3D printing and machine-to-machine will be at the centre of the activities. On the one hand, Blockchain will be used to improve the named technologies in the industrial context by, for example, researching distributed network consensus as additional trust layer in data sharing scenarios and therefore enabling M2M business scenarios and cloud manufacturing. On the other hand, technologies such as machine learning and data visualization can be applied to improve Blockchain-based processes in emerging industries. The three main topics that will be addressed are

- Database Aspects and „Single source of truth“ characteristics: Systematic studies are done on the integration of different Blockchain-based database solutions in scenarios such as quality documentation, asset sharing and tracking, digital product memory or the verification of spare parts, distributed manufacturing or supply chain tracking. Semantic technologies such as ontology-based data access will be used to improve such Blockchain-based database solutions and their implications in relational database systems further.
- Trust Layer: The additional trust layer functionality together with the possibility to transfer values next to pure information leads to important research topics which are centered around traditional machine-to-machine communications or the (real-time) industrial Internet of Things.
- (Data Analytics Based) Decision Support: Based on the results of the aforementioned topics decision support workflows utilizing the visualization of large Blockchain data and relationships will lead to possible process optimizations in emerging industries using Blockchain-based technology

Our research will uncover the relevant questions on optimal approaches of (autonomous) Blockchain based functionalities within Emerging Industries focusing on Industry 4.0 and the Internet of Things. Possible real-world scenarios for prototypical evaluation within the research context of the “Pilotfabrik 4.0” will for example be:

- 3D Printing & Smart Contracts
- M2M Business Scenarios & Machine Learning
- Blockchain/DAG-based Internet of Things
- Blockchain-based traceability
- Blockchain-based content distribution
- Data sharing/ Decentralized Data markets
- Cloud Manufacturing

Area 4: Data Science Methods for Blockchain Analytics & Predictions

Lead: Dr. Haslhofer, AIT; M. Tarasiewicz, RIAT

Understanding socio-economic and technical questions that arise in blockchain-based systems requires novel data-driven methods, services, and tools. The goal of this area is to investigate, and develop scalable data science methods, tools and services that contribute to a better understanding of the structure and dynamics of blockchain-based ecosystems and environments. A central outcome will be a horizontally scalable platform that can be used by researchers and practitioners to answer scientific or business-related questions. This area will also have a strong interdisciplinary and community-oriented and focus and involve data scientists, practitioners from the startup community, as well as scientists with various backgrounds within and outside the ABC initiative.

The Area will address the following topics in detail:

- Blockchain Analytics Platform
- Smart Contract Analytics and ICO Tracking
- Market Understanding & Predictions
- Empirical Analysis of Off-Chain Transaction Technologies
- Centralization tendencies in distributed ledgers
- Blockchain Monitoring for Governance and Sustainable Chain Quality

Area 5: Legal and Political Implications

Lead: Prof. Kalss, WU-Wien

New technological developments provide great challenges for every legal system. The distributed ledger technology (DLT) is a completely new concept and potentially revolutionary technology. Therefore it raises demanding questions throughout all legal fields at both a national and an international level. Area 4 aims to address legal questions arising under current legislation, tries to address concepts and suggestions for future legal frameworks and starts to analyse further political implications.

A starting point of the area is to discuss legal questions the use of DLT raises under current legislation, including aspects of private, public and tax law. Matters of interest may comprise disclosure requirements, prevention of money laundering and international aspects. With coins and tokens attracting more and more attention, another area of interest is DLT and investment. Facing the tremendous developments in the field of financial regulations during the last decade, some questions immediately occur: Are there any legal restrictions? Is there a need for regulation and authorisation, codes of conduct or similar enabling legal frameworks? Research will address regulatory aspects as well as selected questions of company law.

Blockchains and self-executing Smart Contracts also raise fundamental questions related to governance. These concern the governance among the participants of DLT-networks and the economic and legal relations among them, the enforcement of contracts, incomplete contracts, and alteration through judicial awards. Do, for example, the current concepts of contracts suffice to govern the relations of the participants and towards market partners? Do self-executing Smart Contracts prevent the enforcement of court rulings?

From a public law perspective, the area will focus on data protection law on national and European level (GDPR). Not only the applicability of rules is of relevance, but also how certain data protection rights such as the “Right to be forgotten” can be enforced within the Blockchain. The internet has shown that disruptive new technologies often force lawmakers to implement new legislation. Although huge steps have been made in the past, the development of legal systems is still behind the technical development in the IT sector. ABC offers the opportunity to identify the legal areas where additional legislation is needed to ensure that our legal system is poised to deal with new developments and to maintain the rule of law.

Mentioning the digital revolution, a main topic on the agenda for tax-related matters apart from income tax, corporate tax and VAT issues is “digital tax transformation”, focusing on taxes and technology. Technical developments may not only bring challenges, but also numerous opportunities. Therefore the agenda includes, for instance, how to use technology to improve tax compliance and how to support value added processes with new technology.