Communications of the Association for Information Systems

Volume 47 Article 9

10-22-2020

Blockchain Regulations and Decentralized Applications: Panel Report from AMCIS 2018

Hemang Subramanian
Florida International University, hsubrama@fiu.edu

Karlene Cousins
Florida International University, kcousins@fiu.edu

Lina Bouyad Bouyad
Florida International University, lbouyad@fiu.edu

Alpen Sheth
Portland State University, alpens@gmail.com

Dan Conway
University of Arkansas, dconway@fsu.edu

Recommended Citation

Subramanian, H., Cousins, K., Bouyad, L., Sheth, A., & Conway, D. (2020). Blockchain Regulations and Decentralized Applications: Panel Report from AMCIS 2018. Communications of the Association for Information Systems, 47, pp-pp. https://doi.org/10.17705/1CAIS.04709

Communications of the Association for Information Systems

Reports DOI: 10.17705/1CAIS.04709 ISSN: 1529-3181

Blockchain Regulations and Decentralized Applications: Panel Report from AMCIS 2018

Hemang C. Subramanian
Florida International University
hsubrama@fiu.edu

Karlene C. Cousins
Florida International University

Lina Bouayad
Florida International University

Alpen Sheth
Portland State University

Dan Conway
University of Arkansas

Eduardo Salcedo
Florida International University

Jose Pineda
Florida International University

Abstract:

Blockchain represents one of the 21st century's most impactful inventions. In addition to creating cryptocurrencies such as Bitcoin, this technology enables smart contract functionality and supports decentralized, secure, and private transactions. By design, blockchains enable decentralized functionality for many of today's business applications and transform traditional centralized information systems. In this paper, we summarize four research areas that will appeal to IS scholars that a panel at AMCIS 2018 discussed: 1) cryptocurrency regulation, 2) Etherisc (a smart contract-based application), 3) decentralized blockchain applications in healthcare, and 4) Bitcoin as a blockchain application and issues with decentralization. To account for the European Union's General Data Protection Regulation's requirements to provide people with the right to be forgotten and modify personal data, we modified Pedersen et al.'s (2019) framework to accommodate off-chain data storage requirements. We deployed Pedersen et al.'s (2019) modified framework to evaluate whether one can use blockchains for three different applications. We summarize several research questions and present a research agenda that emerged from the issues highlighted during the panel discussion.

Keywords: Blockchain, Cryptocurrency, Smart Contracts, Ecosystem, Regulation.

This manuscript underwent editorial review. It was received 06/07/2019 and was with the authors for seven months for two revisions. Lauri Wessel served as Associate Editor.

1 Introduction

Blockchain participation and adoption is, by design, democratic and unconstrained (Beck, 2018). However, blockchain adoption presents several challenges to organizations (Beck & Muller-Bloch, 2017). Researchers and practitioners continuously ponder: do blockchains really add business value to organizations? Should organizations change their existing application frameworks to decentralized blockchain-based models? Furthermore, what regulatory implications will arise when organizations or individuals adopt blockchain-based applications that exchange "digital assets"?

This debate represents a central issue for both information systems (IS) researchers and practitioners who endeavor to understand blockchain's sociotechnical and socioeconomic implications (Cousins, Subramanian, & Esmaeilzadeh, 2019). In this paper, we report on a panel discussion at the Americas Conference on Information Systems (AMCIS) in 2018 that discussed blockchains and information systems. The panel occurred amid a larger IS debate on whether to adopt blockchains and the implications of such adoption.

This panel made two important contributions. First, it highlighted key issues pertaining to the ongoing debate surrounding regulatory frameworks for blockchain smart assets. Second, it discussed blockchain's usefulness, business viability, and value across several industries. In doing so, it outlined the key regulatory implications for blockchain-based financial crypto-assets. Furthermore, it outlined emerging opportunities in smart contracts and decentralized applications in the insurance sector, healthcare industry, and payment networks. During the panel, the audience asked why blockchain technology was a good fit for the applications we presented. To explore this idea, we used the framework that Pedersen, Risius, and Beck (2019) developed, which provides guidelines for assessing whether blockchain technology suits each case. However, Pedersen et al.'s (2019) framework does not account for the European General Data Protection Regulation's (GDPR) requirements to give individuals the right to modify or permanently delete personal data. We suggest how one could modify Pederson et al.'s (2019) framework in this panel report. We then use the adapted framework as a lens to assess whether one can use blockchain technology for the applications the panel presented. Furthermore, we develop a research agenda based on the panel discussion.

2 Blockchain: Background and Significance

Blockchain-based systems have many different applications such as in supply chain management, Internet of things (IoT), and artificial intelligence (AI) systems that use automated reasoning (Subramanian, 2017). Due to blockchain's decentralization, immutability, security, and openness, it provides the ideal infrastructure for sharing data across different types of inter-organizational systems that require a permanent record of transmitted transactions that participating organizations can access. Such applications include supply chain transactional systems created over value-added networks and health information exchanges (HIEs). Blockchain can also guarantee user privacy in sensor- and IoT-based networks (Chanson, Bogner, Bilgeri, Fleisch, & Wortmann, 2019). Blockchain applications that focus on product certification such as organic produce allow one to add transactions about that product, from the farm to the customer's table, to the blockchain as they occur (e.g., Wyoming's beefchain.com, which certifies organic beef products). Blockchain's decentralized structure allows one to replace trusted third parties such as financial intermediaries and governing bodies with algorithmic forms of trust (Beck, Stenum Czepluch, Lollike, & Malone, 2016).

Blockchain also shows promise in implementing legal documents such as an individual's will where a trusted third party receives a fee upon execution. If one implemented a will as a smart contract, then the contract could monitor a government mortality database and distribute resources when it discovers a certified death. Other examples where blockchains can replace third-party intermediaries include vehicle titles, land titles, marriage certificates, fishing licenses, intellectual property registers, and financial instruments.

One can use various operating parameters (e.g., mining power and hashing rate) and algorithms (e.g., proof of stake, proof of work, proof of data, and distributed proof of stake) to configure blockchains. Blockchain developers and firms use two kinds of blockchains to develop large-scale applications: permissioned and permission-less blockchains. They use hyperledger blockchains to implement private, permissioned, or permissioned-private enterprise business applications. Similarly, organizations use Ethereum, Bitcoin, EoS, and Monero blockchains to implement public and permission-less smart contract-

based distributed applications (DApps). However, blockchain applications also introduce new risks and interoperability challenges with existing systems (Rossi, Mueller-Bloch, Thatcher, & Beck, 2019), which suggests the need for further research into performance, appropriate use cases, risks and regulatory issues, incentive mechanisms, and interoperability among blockchains and other information systems (Beck & Müller-Bloch, 2017; Beck, Müller-Bloch, & King, 2018).

Despite these challenges, blockchain applications have promising usefulness as a dis-intermediator in business sectors such as finance, healthcare, legal, and insurance. To emphasize these points, Rossi, Mueller-Bloch, Thatcher, and Beck (2019) stated that blockchain's properties of automaticity, autonomy, and enforcement enable blockchain applications that create "smart property" wherein the ledger tracks and inventories these hard assets. Furthermore, the ability to use blockchains to autonomously implement trust and an unalterable state of truth has several sociotechnical implications that profoundly alter how a firm implements information systems in the context of its business logic and sociotechnical interactions between individuals and in society (Rossi et al., 2019).

Overall, blockchain represents an exciting opportunity to change how we interact and exchange value with each other. The panel discussion corroborated these ideas by highlighting the legal implications of these "smart properties" in the form of crypto-assets and three widely used blockchain applications. In Section 3, we discuss the financial regulations landscape that influences how different regulatory organizations view crypto assets.

3 Crypto-assets and the Financial Regulation Landscape

Blockchain facilitates many innovative digital applications, assets, and organizations that raise concerns for financial regulators in the United States. Examples include smart contracts, decentralized autonomous organizations, decentralized autonomous applications (DAPPS), initial coin offerings (ICOs), crypto-tokens, and crypto-currencies. Each panelist discussed an example application from these categories. U.S. financial regulators mainly care about the threat these digital assets present to financial security. The panel discussed how financial regulators have different areas of oversight and view crypto-assets' regulation differently. Regulators may view crypto-assets as securities, commodities, money, or property. In Table 1, we summarize the key issues that the panelists addressed and the questions they raised and summarize their discussion pertaining to crypto-assets and financial regulation.

Table 1. Key Issues that the Panelists Addressed and the Questions they Raised

Key issues addressed	1) What implications arise if SEC treated crypto-assets as securities in the US? 2) What implications arise if FinCen treated crypto-assets as money in the US? 3) What implications arise if CFTC treated crypto-assets as commodities in the US? 4) What implications arise if IRS treated crypto-assets as property in the US?
Key questions raised	The complexity of the regulatory environment raises many pertinent research questions for the IS community. For instance, one can build regulatory oversight into blockchain applications. 1) What theoretical approaches can we use to explain the implications that decentralized governance have in different contexts? 2) How can we leverage know your customer (KYC), anti-money laundering (AML), and other existing regulatory approaches to deter individuals from using blockchain applications for criminal purposes? 3) How can we predict or explain the impacts of "hard-forks" and the possibility of roll-back operations that can revert smart contracts to a previous state and reset blockchains? In the legal context, an overload of pending lawsuits clogs the legal system. 1) How can we use blockchain protocols and AI to aggregate human judgment and make legal decisions to help alleviate this backlog? 2) What kinds of legal decisions are amenable to blockchain-supported legal decision making (e.g., in smart contracts)? 3) What legal and regulatory challenges do smart contracts present?
Summary	Different Federal organizations view crypto-assets differently, which creates conflicts in how they regulate blockchain-based applications.

3.1 Crypto-assets as Securities

The Securities and Exchange Commission (SEC), an independent federal agency, protects investors from fraudulent schemes and has primary oversight over the U.S. securities market. The SEC has taken a pro-regulation approach and views crypto-assets as securities. Securities are fungible, financial instruments that hold value, such as stocks, bonds, mutual funds, and exchange-traded funds. The SEC ensures that investors receive information concerning securities being offered for public sale to prevent deceit, misrepresentation, and fraud. The SEC accomplishes does so by requiring companies to disclose important financial information through registering securities to enable investors to make informed decisions about whether to purchase a company's securities. Under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"), one must register all securities that one offers and sells in the US with the SEC, or the securities must qualify for an exemption from the registration requirements (Douglas & Bates, 1933; "Securities Exchange Act of 1934", 1934).

Though lawmakers established these regulations in the early 1900s, the SEC has applied these laws to crypto-assets such as ICOs. For example, *SEC v. Howey* (1946) established the guidelines under which an asset would be considered a security subject to SEC regulation (Tew & Freedman, 1972). The Howey Test states that a security involves 1) an investment of money 2) in a common enterprise (e.g., pooling of funds) 3) with the expectation of profit and 4) solely from others' effort (passive investment) (Alcser, 1995). A crypto-asset must satisfy all four elements to constitute a security. Ultimately, the SEC does not regulate the technology itself but rather how one uses it and its consequences, which has two implications for blockchain-related initiatives. First, the underlying business that adopts the blockchain solution can issue a native security token (a crypto asset through initial coin offers) to raise capital and to assist with decentralized governance of the platform. Such a security token is a crypto asset which is tradable on platform exchange markets (Subramanian, 2019). Businesses that issue such tokens have to register with the SEC. Second, platforms that allow people to trade in such securities must register with the SEC as national securities exchanges unless they have exemption from such registration.

3.2 Crypto-assets as Commodities

The Commodities Future Trading Commission (CFTC), an independent federal agency, protects market participants from fraud. The CFTC regulates futures and option markets in the US for commodities such as oil, grain, precious metals, and electricity. In *CFTC vs. Patrick McDonnell and Cabbagetech d/b/a Coin Drop Markets* (2018), the court ruled that the CFTC can regulate Bitcoin as a commodity (Girasa, 2018). Under this ruling, the CFTC has taken a "do no harm" approach to crypto-regulation. The CFTC focuses on facilitating an environment that properly balances regulatory oversight and innovation to allow new technologies and the American marketplace to evolve in a responsible manner. As such, the CFTC granted LedgerX, a Bitcoin derivatives exchange and clearinghouse, the right to create a regulated Bitcoin futures market. Despite this approval, the CFTC, in conjunction with the SEC and other financial enforcement agencies, has proactively collaborated on prosecuting cryptocurrency schemes that involve fraud and manipulation. The CFTC has already taken civil enforcement actions against several virtual currency Ponzi schemes such as My Big Coin Pay and Coin Drop Markets.

3.3 Crypto-assets as Money

The Financial Crimes Enforcement Network (FinCen), a bureau of the U.S. Department of the Treasury, has full authority for KYC and AML matters. FinCen analyzes financial transactions to fight money laundering, terrorist financing, and other financial crimes. FinCen views crypto-assets such as tokens as money (Bryans, 2014; Kiviat, 2015). In 2015, FinCen, working in coordination with the U.S. Attorney's office, assessed a US$700,000 civil money penalty against Ripple Labs Inc. and its subsidiary XRP II, LLC, for violating the Bank Secrecy Act by acting as a money services business and selling its virtual currency, XRP, without registering with FinCen (Hughes & Middlebrook, 2016). Ripple also failed to implement and maintain an adequate AML program designed to protect its products from use by money launderers and terrorist financers. FinCen has registered over 100 virtual currency exchanges.

3.4 Crypto-assets as Property

The Internal Revenue Service (IRS), a bureau of the U.S. Department of the Treasury, collects taxes and enforces tax laws. The IRS views cryptocurrencies as property. Therefore, as published in Notice 2014-21, anyone who sells cryptocurrency for a profit will be subject to a capital gains tax. Payments received

or mined cryptocurrencies also have tax implications; payments using cryptocurrency to pay independent contractors, service providers, and employees are taxable. In 2018, the IRS ordered Coinbase, one of the largest cryptocurrency exchanges, to send information on 13,000 of its customers who used the exchange between 2013 and 2015 to the IRS to determine whether it should assess taxes for these customers. The IRS warned that taxpayers who do not report the income gains from their cryptocurrency transactions face the possibility of tax audits, penalties, and prosecution.

In addition to the aforementioned perspectives, the complexity of the regulatory environment raises many pertinent research questions for the IS community. For instance, in some cases, can one build regulatory oversight into blockchain applications? Because blockchains regulate themselves, they could use hard and soft forks, which roll back smart contract transactions and reset blockchains to a prior state. However, a blockchain cannot automatically decide to implement hard and soft forks; they require human intervention. It remains unclear how legal agencies would view such fundamental alterations to these crypto-assets.

While crypto-assets remain an important application, blockchains have a broader applicability for business processes. For instance, businesses have launched several crypto-assets in the form of ICOs, which ascertain the governance rules and facilitate trustful transactions among stakeholders. However, questions remain as to the types of business processes that suit blockchain technology. In Section 4, we explore this line of enquiry using three different blockchain applications as examples.

4 Blockchain Opportunities Framework: A Case of Three Blockchain Applications

Members in the IS community have considerably debated whether blockchain adoption provides any true business value to organizations and society (Rossi et al., 2019). To participate in this debate, we modified Pedersen et al.'s (2019) framework and used it to analyze three blockchain applications. Pedersen et al.'s (2019) framework helps decision makers decide whether to use blockchain technology and which type of blockchain to deploy. The framework provides 10 logical steps for analyzing whether one should use blockchain in a particular business application.

However, note that Pedersen et al.'s (2019) framework does not account for the privacy issues that the GDPR raises. Accordingly, in the following examples, we apply a modified version of Pedersen et al.'s framework to account for an 11th decision step to determine when one needs to store personal information off the blockchain. We include the 11th step because a blockchain deliberately makes data modification or deletion difficult (i.e., to achieve "immutability"). However, the GDPR requires that one modify (Article 16) or erase (Article 17) data under certain circumstances. The right to erasure (i.e., "right to be forgotten") in particular creates tension between blockchain and the GDPR. Therefore, blockchain architects need to recognize these requirements from the outset and ensure that they design their respective use cases in a manner that allows compliance with the GDPR. One approach to complying with the GDPR requirements in Articles 16 and 17 involves implementing off-chain personal information storage (Fink, 2019). We integrated Fink's approach into Pedersen et al.'s framework because we believe that such an approach can effectively allow one to modify or delete data once people invoke their right to be forgotten.

4.1 Modified Pedersen et al. (2019) Framework for Off-Chain Data Storage

Depending on the specific blockchain use case, it may not be prudent to store transactional data on the blockchain itself. One could store such data in an off-chain database and link it to the distributed ledger through a hash pointer. To comply with the GDPR requirements, one should (where possible) keep classified data (such as personal data) off the chain and link it to the blockchain ledger through a hash pointer (Fink, 2019). More specifically, the hash pointer would only contain information needed to access the personal data in the separate database. In this manner, one could confine personal transactional data to off-chain storage and avoid storing such data on the blockchain. Thus, off-chain storage would enable one to modify and erase personal data stored off-chain in databases in compliance with Articles 16 and 17 of the GDPR. An open question concerns the status of the remaining hash when one erases the off-chain data because that hash will remain permanently on the blockchain ledger.

The 11th step that we propose involves determining how to deploy blockchain technology to store personal data. If transactional data contain personal data, then the blockchain ledger should store only a hash pointer to personal off-chain data.

Using the extended framework in Figure 1, where we show the 10-step decision path to determine when to use blockchain technologies Pederson et al. (2019) and the 11th rule that we added (to enhance privacy and security of sensitive information and support the Rights to Be Forgotten and Data Modification), we analyzed three different blockchain applications: Etherisc (a smart contract-based insurance application), a blockchain-based healthcare information-sharing application, and Bitcoin.

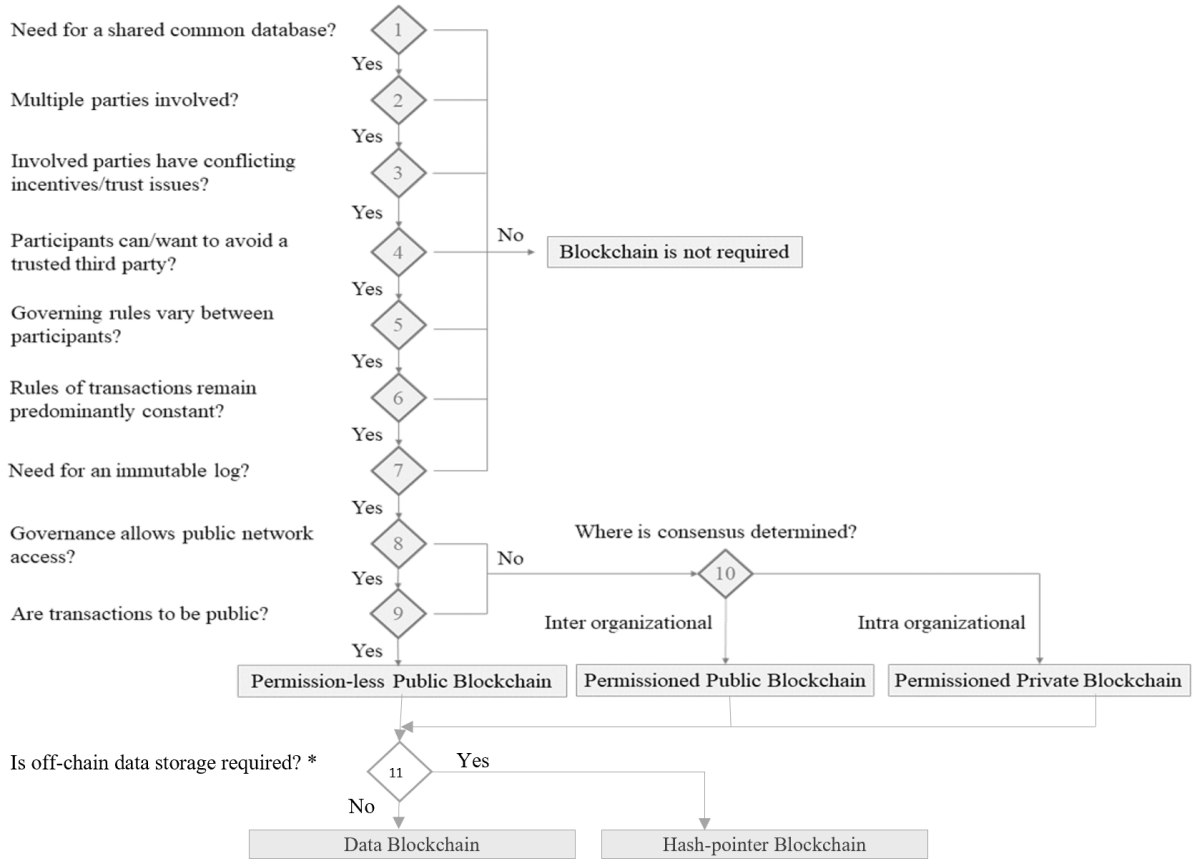

Figure 1. Decision Path for Using Blockchain (Adapted from Pederson et al., 2019)

In Sections 4.2 to 4.4, we highlight the three blockchain applications and how Pedersen et al.'s (2019) modified framework would apply to these applications.

4.2 Etherisc: A Smart Contract-based Insurance Application

Nick Szabo (1997) provided the earliest known definition of smart contracts:

> *The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive for the breacher.*

Ethereum, a blockchain platform, enables smart contracts by providing a distributed, reliable, and verifiable contract enforcement mechanism through software code. Smart contracts provide consensus mechanisms (e.g., proof of work, proof of stake, proof of authority) and an auditable trail of contract execution that can reduce legal institutions' involvement and penalties by reducing potential breaches and conflicts during contract execution.

Etherisc, a smart contract protocol, allows one to build DAPPS that cater to the insurance industry to automatically process insurance claims based on a triggering event (Etherisc, 2018). Etherisc-based DAPPS such as Flight Delay (see https://fdd.etherisc.com/) run on Ethereum's virtual machine blockchain

and encode entire insurance workflows including policy pricing, policy issuance, claims processing, claims settlement, and payout. Such smart contracts require an external component—a third-party data source called the "oracle"—that triggers the blockchain to execute contracts via application program interfaces (APIs). For example, once Etherisc detects a flight delay from the oracle and validates contractual conditions, the smart contract bytecode executing on Ethereum automatically processes the claims transfers money to the insured party. In this scenario, the oracle sources data from sources such as flight trackers, weather databases, KYC data, and banks and provides this input to the smart contract.

We summarize the key issues that the panelists addressed and the questions they raised with respect to Etherisc in Table 2. Subsequently, we discuss key insights and discussions from the panel.

Table 2. Key Issues that the Panelists Addressed and the Questions they Raised Pertaining to Etherisc

Key issues addressed	• What are smart contracts? How can we use them to create a decentralized insurance application marketplace? • How do smart contracts play a role in enabling a decentralized insurance marketplace? • How can we analyze whether blockchain presents an appropriate business opportunity in the decentralized insurance marketplace?
Key questions raised	Smart contracts raise the following research questions pertinent to IS scholars: 1) Protocol functionalities that link multiple smart contracts will create complex interoperable frameworks across multiple organizations. What kinds of protocol frameworks will assist one in creating smoother cross-functional and cross-organizational business process functioning? 2) How will different actors in a particular industry benefit from specific smart contract applications? For example, in the insurance segment, how will market participants, such as underwriters, insurance agents, resellers, and insurance providers, benefit from the smart contract functionality that Etherisc provides? 3) How can we design smart contracts to overcome barriers to interoperability? 4) How can we standardize smart contract languages to operate on different blockchains? 5) What risks do smart contracts present? What auditing tools and services do we need to reduce these risks?
Summary	Though smart contracts provide an efficient mechanism for creating decentralized applications in the insurance sector, issues with respect to system-level and blockchain-/smart contract-level interoperability remain.

4.2.1 Decentralization of Insurance

Among other reasons, one could implement a decentralized approach to insurance to align incentives in insurance contracts whereby insurance firms, insurance agents, and customers engage in profit-maximizing activities with different incentives (Sheth & Subramanian, 2019). Such market behavior leads to overly restrictive insurance contracts due to a financial interest in not paying out claims on time. Smart contracts incentivize efficiency and facilitate a broad innovation base by pooling risks among different participants. Current Etherisc insurance products include Flight Delay, Hurricane Guard, Collateral Protection, Crop Insurance, and Social Insurance. These products use modified smart contracts with a backend that includes an Ethereum blockchain and third-party APIs to price, underwrite, monitor, trigger, and pay out claims. In Table 3, we propose how the Etherisc Flight Delay Insurance application benefits from the blockchain using Pedersen et al.'s (2019) modified framework. As we show in Table 3, insurance applications such as Etherisc use permission-less public blockchains to provide a common database and an immutable transaction log, which provides access to the public and avoids the need for third parties but requires off-chain personal data storage.

Depending on the investment mode and how one sells insurance products (e.g., via crypto-tokens), one may implement blockchain-based insurance DAPPS such as Etherisc as ICOs that may fall under U.S. securities regulation. One should also store personal data off chain to comply with the GDPR's right to be forgotten and modify personal data. Such an application will also have to comply with insurance regulations.

Table 3. Pedersen et al.'s (2019) Modified Framework Applied to Etherisc Real-time Flight Delay Insurance

Need for common database	• Provides a single view of the insurance policy and related transactions to multiple parties. • Enables multiple parties involved in a transaction (e.g., insurance firms, an insured customer, and insurance agents such as travel companies) to track and maintain a claim's status. • Allows one to validate the triggering event and whether insurance payouts occurred in real time. • Provides a log of all transactions and helps improve the main analytical model that models the risk profile of a particular insurance policy.
Multiple parties involved	• Insurance companies, insured individuals, insurance agents, insurance regulatory authorities, resellers, Insurance validators, and intermediaries
Involved parties have conflicting incentives/trust issues	• Insurance firm wants to maximize its profits and reduce payouts. • Insurance agents who multihome have an incentive to sell only those insurance policies with maximum commissions. • Insurance resellers who multihome have an incentive to only sell those policies with maximum commissions. • Insurance customers want to protect against risk while paying the optimal price for the insurance policy (Sheth & Subramanian, 2019). • Insurance regulators want to provide a legal and operable market for insurance and protect customers.
Participants can/want to avoid a third party	• Third parties, such as insurance validators and actuaries, involved in this transaction increase costs to the insurance firm and to the insurance customer. • Third party can use data to model, resell, or upsell existing insurance policies on the market. • The market is straightforward, and one can make it efficient if one implements direct payouts and develops risk models to increase optimal profitability in the sector.
Governing rules vary among participants	• For insurance firms, the governing rules stem from their ability to create configurable, affordable insurance policies that they can customize to individual customers. • For the resellers and insurance agents, their governing rules imply reducing the costs to reach out to end consumers and have the ability to sell it to them. Therefore, configurability presents a disincentive to agents and resellers because the time taken to sell increases with product variation. • For insurance validators, the key governing rule involves proving beyond reasonable doubt that the event of interest occurred, such as a flight delay, and that everyone accepts their proof. • For the insurance customer, rules that govern the processing of claims include that the policy should repay him the amount for which he has been insured if a flight delay event occurs.
Rules of transactions remain predominantly constant	• Consistent transactions. • The governing rules for each agency in this relationship remain the same. • Individual insurance firms/participants and policy sellers can participate according to their smart contract rules.
Need for immutable log	• To provide for non-repudiability of each transaction that has occurred on the blockchain (as validation mechanisms in case of a future event).
Governance allows for public network access	Anyone in the public domain can access Etherisc including: • Insurance company • Insured individual • Insurance agent • Insurance regulatory authority • Resellers • Insurance validators and intermediaries
Public transactions?	• Yes. Etherisc has a permission-less public blockchain design and anyone can access the smart contract on the Ethereum blockchain and observe its execution. • Nevertheless, oracles, which Etherisc uses as a source of KYC, AML, and personal data, protect consumer data.
Off-chain personal data storage required?	• One needs to store personal data to process insurance-based smart contracts. • This system requires off-chain personal data storage to facilitate parties' right to be forgotten and right to modify data.

4.3 Healthcare Information Sharing

Healthcare providers and other relevant actors have generated much patient- and health-related data from implementing electronic health records. These data help healthcare providers improve healthcare outcomes and facilitate research that improves care quality. However, frameworks that today's hospital systems use for digitizing health processes digitization lack efficiency due to poor data quality. Major stakeholders such as insurance providers, practitioners, and patients often have an erroneous and incomplete copy of health records. Given that healthcare providers have begun to introduce sensor-based data for tracking and monitoring patients' health, we can expect volumes of health data and their associated quality issues to increase exponentially. Such exponential growth calls for systems and processes that can consolidate and distribute health data in a reliable way. One popular solution is the HIE. In Table 4, we summarize the key issues that the panelists addressed and the questions they raised with respect to HIEs.

Table 4. Key Issues that the Panelists Addressed and the Questions they Raised Pertaining to Healthcare Information Sharing

Key issues addressed	• What importance do blockchains have with respect to health information data? • Do blockchains present an appropriate business opportunity in the decentralized, personal healthcare information-exchange system? If so, why?
Key questions raised	We present the panelists' views on important research questions in this area that could interest the IS community at large: 1) Can one securely share protected healthcare information (PHI) on the blockchain? If so, how would such a system impact both health outcomes and patient satisfaction? 2) How can one implement off-chain PIH storage? How can one implement a hash pointer for off-chain to reduce the risk of identification from the hash once one deletes personal off-chain data? 3) How will blockchain-based systems such as HIEs or clinical data pathways help resolve interoperability challenges across heterogeneous healthcare systems? 4) How will blockchain-based healthcare systems affect provider efficiency and cost of care?
Summary	Although blockchains present a secure, privacy-enabled, and accurate mechanism to store and exchange healthcare information, we need to study issues that arise from legacy healthcare system integrations and analyze benefits to end users in terms of improving cost and healthcare efficiency. We need to develop efficient methods to implement off-chain PIH data storage.

In research settings, HIEs have enabled multiple providers to collaborate and, thus, reduce the extent to which they duplicate medical procedures (Bardhan, Ayabakan, Zheng, & Kirksey, 2014), lower costs, and improve patient health outcomes (Saef, Melvin, & Carr, 2014). In practice, HIEs have suffered from sustainability issues (Kruse, Regier, & Rheinboldt, 2014) and experienced varying degrees of success. Barriers to HIE adoption include privacy concerns, technical barriers due to incompatible systems, and limited interoperability among heterogeneous healthcare systems (Furukawa et al., 2014). These barriers only grow in contexts where providers share anonymous healthcare information with the public. A blockchain-based HIE can potentially enable one to securely share health information (Dubovitskaya, Xu, Ryu, Schumacher, & Wang, 2017; Ichikawa, Kashiyama, & Ueno, 2017) across multiple participants. Broadly, a generic blockchain-based solution for sharing healthcare information could include the following features:

1) At the patient level, the solution would store each health encounter as a transaction in a block. Due to blockchain's immutability and ability to enable permission-based access using cryptographic protocols, the blockchain would constitute a single "source of truth" for an individual patient's record.
2) Patients can save various types of health data, collected through different devices, onto the blockchain.
3) Patients may grant permission to different players in the healthcare system to view and insert information into their records as needed for treatment and billing.
4) The consolidated patient information saved on the blockchain can potentially reduce the extent to which providers duplicate diagnostic and treatment procedures, which can improve health outcomes and reduce costs.
5) Multiple entities such as insurance providers would validate transaction in a decentralized fashion via a peer-to-peer system.

In the panel, we discussed how one could use blockchain technology to develop a prototype for sharing treatment data among breast cancer patients. In this solution, corresponding peers on the network would securely share data pertaining to patients. Patients, doctors, and hospital systems in the network receive permission to participate in various network functions such as requesting patients' records and accessing clinical pathways for treatment and other diagnostic-related information. Because such records reside on the blockchain and actors transfer them directly from the hospital system, this approach has three advantages: 1) immutability: one cannot alter the healthcare record, 2) accuracy: the network contains accurate data because consensus from the peer-to-peer network verifies each record, and 3) privacy: one can design the application to protect the privacy of healthcare information. This approach results in a true and validated repository of clinical pathways. Patients often drive current peer-to-peer patient networks, and they lack a mechanism to ascertain data's accuracy and authenticity on the network. In Table 5, we analyze the aforementioned healthcare application using Pedersen et al.'s (2019) modified framework. As the table shows, the healthcare applications such as those used in online patient communities may use permissioned public blockchains to provide a common database and an immutable transaction log, which provide access to multiple healthcare organizations and peer-to-peer access. Such a healthcare blockchain-based application avoids the need for third parties but requires off-chain personal data storage.

Table 5. Pederson et al.'s (2019) Modified Framework Applied to Blockchain Applications in Online Patient Communities

Need for common database	• Provides a single view of patient data • Enables patient matching • Enables one to mine past treatments to assess significance of specific patient-reported outcomes
Multiple parties involved	• Patients with different variations/at different stages of the same disease • Patients with different treatments • Patients with different health outcomes • Patients with different mental, socioeconomic outcomes • Patients from different geographic regions • Hospitals and doctors provide medical records at patients' request
Involved parties have conflicting incentives/trust issues	• Newly diagnosed patients care about the validity of the information that other patients provide. • Survivors participating in the platform care about 1) the privacy risks associated with sharing personal health information and 2) third parties' misusing health information (e.g., insurance firms that might refuse future coverage).
Participants can/want to avoid a third party	• Having all patients' posts verified by a qualified moderator would require tremendous resources.
Governing rules vary among participants	• The platform offers various levels of privacy depending on patient preference. • Blockchain rules allow survivors to specify the participants authorized to view the data. • Tracking of all sharing transactions increases the accountability of the patients posting the information.
Rules of transactions remain predominantly constant	• In each patient category, the same rules apply at all times.
Need for immutable log	• To increase accountability of patients posting information
Governance allows for public network access	• Patients have the right to share their own data with other patients and with healthcare organizations.
Public transactions?	• Transactions are not public but are shared with peers and multiple healthcare organizations. • A permissioned public blockchain is recommended.
Off-chain personal data storage required?	• This system requires off-chain personal data storage to facilitate parties' rights to be forgotten and modify data. • For added privacy and security, blockchain stores hash pointer to off-chain personal health information.

Depending on the investment mode (e.g., via purchasing a crypto-token), healthcare DAPPS may require compliance with U.S. securities regulation. If entities such as healthcare providers, healthcare plans, and healthcare clearinghouses participate in sharing personal health information via the healthcare DAPPS, they need to comply with the Health Insurance Portability and Assurance Act of 1996. Off-chain personal data storage will also facilitate compliance with the GDPR's requirements for people to exercise their rights to be forgotten and to modify personal data.

4.4 Bitcoin: a Peer-to-peer Payment System

In Table 6, we highlight Bitcoin, a blockchain-based cryptocurrency. Bitcoin network participants trust that the blockchain constitutes a neutral source of truth (Subramanian, 2017). The Bitcoin blockchain represents the first case of a decentralized autonomous system with distributed control (Anderson & Bogusz, 2019). However, the open source community can still manipulate it through forks and modifying its source code—a process that researchers often refer to as generativity (Anderson & Bogusz, 2019). Table 6 describes the key issues that the panelists addressed and the questions they raised pertaining to decentralization in the Bitcoin blockchain.

Table 6. Key Issues that the Panelists Addressed and the Questions they Raised Pertaining to Bitcoin's Peer-to-peer Payment System and Decentralization

Key issues addressed	• What importance does decentralization have in a peer-to-peer payment system such as Bitcoin? • What components in the Bitcoin sociotechnical ecosystem contribute to this decentralization? • Does the Bitcoin blockchain present an appropriate business opportunity for a decentralized peer-to-peer value-transfer system?
Key questions raised	The following research questions explore the key challenges that the Bitcoin ecosystem faces: 1) What design mechanisms in the blockchain ecosystem will ensure that a single entity in the ecosystem can never dominate the network? 2) What risks do centralized components in the blockchain ecosystem pose? 3) While different components in the Bitcoin system relate to one another, how can networks of influencers and policy makers design effective governance mechanisms to prevent centralization?
Summary	Centralization poses several risks; nevertheless, with Bitcoin's enablement of peer-to-peer asset transfer, incentive mechanisms constitute one component in Bitcoin's ecosystem that we will need to address to provide a true peer-to-peer decentralized value exchange.

Centralizing any component in a blockchain ecosystem poses a threat to blockchain's neutrality and decentralized trust (Murray, 2019). Bitcoin's ecosystem comprises six main components: miners, node implementors, bitcoin implementations, developers, exchange operators, and investors. As a peer-to-peer payment system, Bitcoin's founders envisioned a decentralized, autonomous, and network-based validation system that facilitates value exchanges pseudonymously. In Table 7, we apply Pedersen et al.'s (2019) modified framework to evaluate whether one can suitably apply blockchain to Bitcoin's peer-to-peer value-exchange solution. Blockchain technologies suit efforts to design cryptocurrencies such Bitcoin. As Table 7 shows, cryptocurrencies such as Bitcoin use permission-less public blockchains to provide a common ledger and an immutable transaction log, which provide access to the public, avoids the need for third parties, and do not require off-chain personal data storage.

Given the conflicting incentives among the different stakeholders in the Bitcoin ecosystem, we calculated the Gini coefficient of each component in the Bitcoin ecosystem from various Bitcoin data sources to determine their concentration (see Table 8). The Gini coefficient is a statistical measure of distribution that gauges inequality. A Gini coefficient of 0 represents perfect equality (an equal distribution condition), and a Gini coefficient of 1 represents perfect inequality (highly concentrated). We can see from Table 8 that five out of six components were centralized (i.e., Gini > 0.70).

From these results, we inferred that a small number of exchanges control most of the cryptocurrency deposits and transactions. We observed that most Bitcoin nodes that transmit transactions and perform checks such as double spending reside in a few countries. For example, with Bitcoin, a country's government can disrupt the Bitcoin network if it decides to terminate all Bitcoin nodes. Similarly, the small number of source code versions (or Bitcoin protocol implementations) suggests a high concentration of blocks mined per implementation. If this small number of implementations develop bugs or have security vulnerabilities, they could easily affect how the entire Bitcoin network functions.

Similarly, disagreements on technical directions for developing the source code could lead to incompatible blockchains through four different means: pseudo-forking, development forking, bifurcation, and speciation (Anderson & Bogusz, 2019). Consequently, if the top 10 core developers who contributed to the cryptocurrency software code colluded maliciously, they could disrupt the crypto-ecosystem's decentralized and neutral nature.

In the future, although the underlying algorithms support decentralization, the concentration of power in the six components could prevent the Bitcoin ecosystem from realizing the full potential of a decentralized architecture.

Table 7. Pedersen et al.'s (2019) Modified Framework Applied to Bitcoin's Blockchain as a Peer-to-peer Value-exchange Solution

Need for common database	• Enables senders and receivers to track transactions between themselves. • Validates whether the sender has the requisite balance to transfer to the receiver or not • Provides a log of all transactions perennially
Multiple parties involved	• Investors (senders and receivers), Bitcoin miners, node implementers, Bitcoin code maintainers (developers), exchange operators, regulators and government
Involved parties have conflicting incentives/trust issues	• Sender needs assurance that the transfer has happened and needs the ability to view the transaction in near real time. • Miners have the incentive to select those transactions with the highest transaction fee. • Receivers have incentives to track transactions in real time. • Developers want to improve the network's speed and provide for redundancy. • Miners do not want to implement hard/soft forks due to uncertainty in rewards.
Participants can/want to avoid a third party	• Third parties involved in value exchange transfers often charge a transaction fee, which makes certain types of transactions difficult. For example, micro-lending or micropayments have higher transaction fees compared to the value exchanged. • Third parties often compromise transactions' security and privacy by sharing (storing) transaction details without senders' and receivers' explicit consent. • Third-party transactions have high fees when peer-to-peer value exchange happens using conventional payment transfer methods.
Governing rules vary between participants	• For the sender, the money has to reach the receiver in near real time with confirmation of the transaction available publicly. • For the transaction's value to remain fixed and to be given access to the exchanged fiat currency, access must be limited to the true identity of the participants on the network.
Rules of transactions remain predominantly constant	• Transactions are consistent and follow the same sending and receiving process. • Transactions should be consummated in a definite period.
Need for immutable log	• To provide for non-repudiation of each transaction by the sender and receiver.
Governance allows for public network access	• Yes; by design, the Bitcoin blockchain allows public access.
Public transactions?	• Permission-less public blockchain by design
Off-chain personal data storage required?	• Bitcoin is pseudo-anonymous by design and does not need to store personal data. Does not require off-chain personal data storage.

Table 8. Description of the Ecosystem Components, Data Sources, and Gini Coefficients[1]

Ecosystem Component	Data source	Unit of measurement	Gini coefficient	Implications
Exchanges	Coinmarketcap.com	Value of transactions in billions of USD on Bitcoin exchanges	0.718	Highly concentrated. A minority of Bitcoin exchanges control a majority of Bitcoin transactions, such as Coinbase and Binance.
Miners	Blockinfo.com	Blocks mined per mining pool	0.370	Equitable distribution. Mining power is widely distributed across mining pools.
Nodes	Nodes.info	Number of Bitcoin transaction nodes per country	0.844	Highly concentrated. Nodes are located in a few countries, primarily the US and Germany.
Implementations	Blockinfo.com	Blocks mined per code base (collection of source code)	0.901	Highly concentrated. Bitcoin is mined using few implementations.
Developers	github.com/bitcoin	Number of commits of Bitcoin source code per developer on GitHub	0.894	Highly concentrated. Only a minority of software developers develop a majority of the code.
Investors	Block.info	Binned values indicating count of wallet addresses with average number of Bitcoins per wallet—how much each investor holds	0.790	Highly concentrated. Only a minority of investors own a majority of Bitcoin holdings.

5 Conclusions and Future Research Directions

This panel highlighted important research avenues pertaining to blockchain regulations and decentralized applications. In this paper, we discuss the regulatory framework in the US and the European GDPR requirement for providing persons with the right to be forgotten and to modify personal data. Using this argument, we modified Pedersen et al.'s (2019) framework and applied it to analyze three decentralized applications: Etherisc (a Flight Delay insurance application), a health information-sharing application for cancer patients, and Bitcoin. We also include key research questions that the IS research community can pursue in future.

In Table 9, we summarize important research questions that the panel members and the audience highlighted that can guide research agendas for the IS research community

Table 9. Key Discussion Themes and Future Research Directions

Themes	Future research directions
Regulatory landscape and its applicability	1) Designing regulatory frameworks that application writers themselves or blockchain designers can build into blockchain's and smart contract applications' governing mechanisms 2) How can one enhance contract theory and contract law to pertain to the implications of decentralized governance, especially in the smart contract context? 3) Exploring and mandating legal frameworks for hard and soft forks and rollbacks as existing properties laws mandate 4) Proposing blockchain protocols and AI to aggregate human judgment and legal decision making to alleviate backlogs

[1] Data updated on 5 June, 2019.

Smart contracts and interoperability	1) Designing, implementing, and analyzing cross-chain smart contracts that are interoperable among blockchain-based and legacy systems without violating structured decentralization principles 2) Developing frameworks to analyze the economic, technical, and social implications in terms of costs and benefits for all stakeholders in a situational environment wherein one rolls out a blockchain 3) Developing models that analyze smart contract risks, smart contract auditing tools, and smart contract services
Private and hybrid healthcare blockchains	1) Designing, developing, and analyzing healthcare information (PHI) that enables secure and accurate information sharing 2) Developing metrics to measure health outcomes, efficiency, and patient satisfaction of such blockchain-based information sharing—plausibly providing a feedback loop to these system designers 3) Designing, developing, and analyzing how blockchain-based HIEs or clinical data pathways can interoperate with different blockchain or legacy systems across heterogeneous health care systems
Risks that centralized blockchain ecosystems pose	1) Developing, implementing, and testing design mechanisms in the blockchain ecosystem that will ensure the network's non-centralization 2) Developing, implementing, and testing risk-based models to analyze blockchain applications that depend on centralized blockchains. 3) Developing a peer-to-peer payment system that works with networks of influencers and policy makers who design effective governance mechanisms that prevent network centralization

We hope the IS research community can leverage the research agenda we suggest above.

References

Alcser, M. G. (1995). The Howey test: A common ground for the common enterprise theory. *UC Davis Law Review*, *29*.

Andersen, J. V., & Bogusz, C. I. (2019). Self-organizing in blockchain Infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems*, *20*(9), 1242-1273.

Bardhan, I., Ayabakan, S., Zheng, E., & Kirksey, K. (2014). Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals. In *Proceedings of the International Conference on Information Systems.*

Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. *Computer*, *51*(2), 54-58.

Beck, R., & Müller-Bloch, C. (2017). Blockchain as radical innovation: A framework for engaging with distributed ledgers as incumbent organization. In *Proceedings of the 50th Hawaii International Conference on System Sciences.*

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1020-1034.

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S., (2016). Blockchain—the gateway to trust-free cryptographic transactions. In *Proceedings of the European Conference on Information Systems.*

Bryans, D. (2014). Bitcoin and money laundering: Mining for an effective solution. *Indiana Law Journal*, *89*(1), 441-472.

Cousins, K., Subramanian, H., & Esmaeilzadeh, P., (2019). A value-sensitive design perspective of cryptocurrencies: A research agenda. *Communications of the Association for Information Systems*, *45*, 511-547.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems*, *20*(9), 1274-1309.

Douglas, W. O., & Bates, G. E. (1933). The Federal Securities Act of 1933. *The Yale Law Journal*, *43*(2), 171-217.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. *arXiv*. Retrieved from http://arxiv.org/abs/1709.06528

Etherisc. (2018). *White paper.* Retrieved from https://etherisc.com/files/etherisc_whitepaper_1.01_en.pdf

Fink, M. (2019). Blockchain and the General Data Protection Regulation. *Scientific Foresight Unit.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Furukawa, M. F., King, J., Patel, V., Hsiao, C.-J., Adler-Milstein, J., & Jha, A. K, (2014). Despite substantial progress in EHR adoption, health information exchange and patient engagement remain low in office settings. *Health Affairs*, *33*(9), 1672-1679.

Girasa, R. (2018). *Regulation of cryptocurrencies and blockchain technologies.* Berlin: Springer.

Hughes, S. J., & Middlebrook, S. T. (2016). Developments in the law affecting electronic payments and financial services. *The Business Lawyer*, *71*, 361-372.

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth and Uhealth*, *5*(7), e111.

Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal*, *65*(3), 569-608.

Kruse, C. S., Regier, V., & Rheinboldt, K. T. (2014). Barriers over time to full implementation of health information exchange in the United States. *JMIR Medical Informatics*, *2*(2), e26.

Murray, M. (2019). Tutorial: A descriptive introduction to the blockchain. *Communications of the Association for Information Systems*, *45*, 464-487.

Pedersen, A., Risius, M., & Beck, R. (2019). A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive*, *18* (2), 99-115

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agend*a. Journal of the Association for Information Systems*, *20*(9), 1390-1405.

Saef, S. H., Melvin, C. L., & Carr, C. M. (2014). Impact of a health information exchange on resource use and Medicare-allowable reimbursements at 11 emergency departments in a midsized city. *Western Journal of Emergency Medicine, 15* (7), 777-785.

Securities exchange act of 1934. (1934). Retrieved from https://www.nyse.com/publicdocs/nyse/regulation/nyse/sea34.pdf

Sheth, A., & Subramanian, H. (2019). Blockchain and contract theory: Modeling smart contracts using insurance markets. *Managerial Finance.*

Subramanian, H. (2017). Decentralized blockchain-based electronic marketplaces. *Communications of the ACM*, *61*(1), 78-84.

Subramanian, H. (2019). Security tokens: architecture, smart contract applications and illustrations using SAFE. *Managerial Finance*.

Szabo, N. (1997). The idea of smart contracts. *Satoshi Nakamoto Institute.* Retrieved from https://nakamotoinstitute.org/the-idea-of-smart-contracts/

Tew, J. A., & Freedman, D. (1972). In support of Sec v. W.J. Howey Co.: A critical analysis of the parameters of the economic relationship between an issuer of securities and the securities purchaser. *University of Miami Law Review, 27*(3), 407-450.

About the Authors

Hemang Subramanian is the panel organizer and is an Assistant Professor of Information Systems and Business Analytics at Florida International University, USA. He is a member of the AIS, IEEE, INFORMS and POMS and has presented his research therein. His work has appeared in *Information Systems Research, Communications of the AIS, CACM, IEEE Software, Journal of Managerial Finance, Journal of Database Management, IEEE blockchain*, and others. He has presented his work on blockchains at MIT-Code, CMU conference on data analytics, AMCIS, ICIS, etc. and a few industry panels. He holds a PhD from the Scheller College of Business, Georgia Tech specializing in Information Technology Management. His research focuses on analyzing the behavior of market actors using data analytics, market efficiency in product markets, blockchain technology, and cryptocurrency disruption.

Karlene C. Cousins is associate professor and chair of the Information Systems and Business Analytics in the College of Business at the Florida International University where she teaches courses in technology innovation, information systems strategy and governance and healthcare information law. She is recognized for her research on mobile technologies and the legal and regulatory issues impacting the use and innovation of information technology. She serves as an expert panelist and speaker in the mobile technologies area. Dr. Cousins has published her research in journals such as the Communications of the ACM, Journal of the AIS, Decision Sciences, Communications of the AIS and the European Journal of Information Systems. In addition, Karlene served as faculty director of the MSIS Program and Director of the ATOM Think Tank - FIU's first faculty technology consulting practice.

Lina Bouayad is an assistant professor in the Information Systems and Business Analytics Department at the Florida International University, and a Research Associate at the VA HSR&D/RR&D Center of Innovation on Disability and Rehabilitation Research. With a background in computer science and management information systems, her research involves the use of innovative analytics methods to augment provider effectiveness and improve patient experience. Such solutions include the development of develop a blockchain-based solution that would enable patients to share their validated comprehensive treatment records with peers, an on-demand scheduling system in non-urgent settings, and a real-time clinical recommender system that provides recommendations for medications along with associated cost information at the time of prescription.

Alpen Sheth holds a PhD in Urban Planning from MIT. He currently works as Senior Technologist, blockchain at Mercy Corps and is an adjunct faculty at Portland State University School of Business. He previously was of Head of Product at Etherisc, a smart contract-based insurtech firm attempting to reinvent traditional insurance so as to make it affordable to everybody, and, to make insurance marketplaces more efficient. Prior to Etherisc, Alpen was co-founder of Economic Space Agency, that developed smart contract applications using Gravity and Space, 3rd-generation blockchain technologies. His work experience spans systemic risk management related to weather risk, smart sensors for infrastructures, and disaster risk financing in the US, Carribbean and South Asia. He has worked with the World Bank Group, Risk Management Solutions, MIT, INURED and the Miami Downtown Development Authority.

Daniel Conway holds a PhD in Decision Sciences from Indiana University, and is currently a Professor in the Information Systems Department at the University of Arkansas and the director of the blockchain Center of Excellence, Walton school of Business. His research interests involve blockchain, analytics, data science, and artificial intelligence. Prior to joining USF, Conway served on faculty in business and engineering schools at Notre Dame, Indiana, Iowa, Northwestern, Florida, and Virginia Tech. He is currently in the SAE IoT program committee and a columnist for CognitiveWorld. He is also Chief Decision Officer at Qlytix, Chief Operating Officer at blockchain startup Apollo Group, an advisor to blockchain companies Nexus Embassy and KoreConX, and was one of the first 25 Bitcoin miners many years ago.

Jose Pineda (Moderator 1) is currently a fifth-year PhD candidate in business administration at Florida International University (FIU) where he also obtained a Master of Science in Information Systems degree. Before joining the program, he was part of World Fuel Services rotational leadership program within the information technology side of the firm. His research interests include the application of business analytics, blockchain technology, and human-computer interaction. Jose has developed and taught courses on business analytics, and database systems including special topics sessions on blockchain technology and NoSQL databases.

Eduardo Salcedo (Moderator 2) is a fourth-year PhD candidate at Florida International University's department of Information Systems and Business Analytics. Before joining the PhD program, he worked in management in the retail sector. His research interests lie in blockchain technologies, cybersecurity, and the negative influences of technology. Currently, he works on a study involving the use of the blockchain in business settings.