Internet of Things 10 (2020) 100079

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Research article

Perspectives on emerging directions in using IoT devices in blockchain applications

A. Ravishankar Rao [a,*], Daniel Clarke [b]

[a] Gildart Haase School of Computer Sciences and Engineering, Fairleigh Dickinson University, NJ, USA [b] Icahn School of Medicine at Mount Sinai, New York, NY, USA

articleinfo

Article history:
Received 5 April 2019
Accepted 22 June 2019 Available online 2 July 2019

Keywords:
Internet-of things
IoT
Blockchain
Cybersecurity
Trust
Distributed computing

abstract

พื้นที่ของ IOT ระเบิดด้วยอุปกรณ์ที่เชื่อมต่อกันหลายพันล้านเครื่องตั้งแต่เมนเฟรมไปจนถึงตู้เย็นและเทอร์โมสตรัท อุปกรณ์เหล่านี้เป็นสัญญาที่ขนาดใหญ่ของระบบอัตโนมัติและการควบคุมที่ดีขึ้นและความสามารถในการทำธุรกรรมระดับจุลภาคที่ไม่เคยมีมาก่อน. การถือกำเนิดของ blockchain นำเสนอเส้นทางที่น่าสนใจในการจัดการธุรกรรมแบบกระจายในระบบนิเวศใหม่นี้

การใช้ blockchain ในแอปพลิเคชัน IoT นั้นค่อนข้างใหม่, โดยเฉพาะที่ระดับล่างสุดของสเปกตรัมคอมพิวเตอร์. ดังนั้นแผนงานสำหรับอนาคตยังไม่ชัดเจนและมีความท้าทายและคำถามมากมายที่ต้องได้รับการแก้ไข เช่น ความไว้วางใจ ความปลอดภัย และประสิทธิภาพ. ในเอกสารนี้ ได้สำรวจแอปพลิเคชันที่มีแนวโน้มที่จะนำไปใช้งานร่วมกับบล็อคเชนทั้งในเชิง กระบวนการต่าง ๆ ที่ทำให้เกิดสินค้าขึ้นมา พลังงานอย่างชาญฉลาด และการดูแลสุขภาพ ได้ร่างกลยุทธ์ เพื่อเอาชนะความท้าทายมากมาย, ซึ่งน่าจะนำไปสู่ความสำเร็จในการนำ blockchain มาใช้กับ IoT. สุดท้าย, ได้แจ้งเตือนเกี่ยวกับผลกระทบด้านความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นในการใช้อุปกรณ์ IoT, รวมถึงการเพิ่มพื้นที่การโจมตีและช่องโหว่ของอุปกรณ์

1. Introduction and motivation บทนำและแรงจูงใจ

ทั้งสอง IoT [1] และ blockchain [2] เป็นส่วนประกอบสำคัญในอนาคตของการเชื่อมต่อระหว่างกัน และมีการเติบโตอย่างรวดเร็วในปัจจุบัน. จุดเปลี่ยนของทั้งสองอย่างนี้สามารถสร้างกรณีใช้งานที่น่าสนใจและปัญหาที่เกิดขึ้นพร้อมกัน. เหตุผลที่น่าสนใจในการขับเคลื่อนการทำงานร่วมกันระหว่างสองอย่างนี้คือไม่มีวิธีไหนที่สามารถไว้วางใจในความปลอดภัย และการแลกเปลี่ยนข้อมูลแบบเรียลไทม์ระหว่างอุปกรณ์ IoTและบล็อกเชนเป็นวิธีแก้ไขที่ใช้งานได้จริง[3].

ความท้าทายที่สำคัญในด้าน blockchain คือเป็นเทคโนโลยีที่ค่อนข้างใหม่และยังไม่เห็นการนำไปใช้อย่างแพร่หลายในอุตสาหกรรมต่าง ๆ. ด้วยเหตุนี้จึงขาดเอกสารทางวิชาการที่ให้ความกระจ่างเกี่ยวกับปัญหาเกี่ยวกับการยอมรับ blockchain ขอบเขตของบทความนี้มีวัตถุประสงค์เพื่อให้ภาพรวมของพื้นที่แอปพลิเคชันที่เกิดขึ้นใหม่ซึ่งเกี่ยวข้องกับการโต้ตอบระหว่างอุปกรณ์ IoT และเทคโนโลยีบล็อกเชน. เรานำเสนอและแสดงความคิดเห็นเกี่ยวกับประเด็นสำคัญ 3 ประการ ประกอบด้วยการดูแลสุขภาพ supply chain management(SCM) การจัดการห่วงโซ่อุปทานและ energy grid มีคำถามเปิดมากมายในด้านการดูแลสุขภาพ เช่น

การปกป้องความเป็นส่วนตัวของเวชระเบียนในขณะที่ให้ผู้ป่วยมีอิสระในการแบ่งปันกับฝ่ายที่เชื่อถือได้.ในกรณีของการจัดการห่วงโซ่อุปทานความพร้อมใช้งานของเซ็นเซอร์ IoT สามารถใช้เพื่อสร้างที่มาและเปิดใช้งานการดำเนินการตามสัญญาอัจฉริยะ ในบริบทของกริดพลังงานการทดลองในช่วงต้นกำลังอยู่ระหว่างการใช้บล็อกเชนเพื่อความชาญฉลาด

* Corresponding author.
E-mail addresses: ravirao@fdu.edu (A.R. Rao), danieljbclarke@gmail.com (D. Clarke).

https://doi.org/10.1016/j.iot.2019.10 0 079

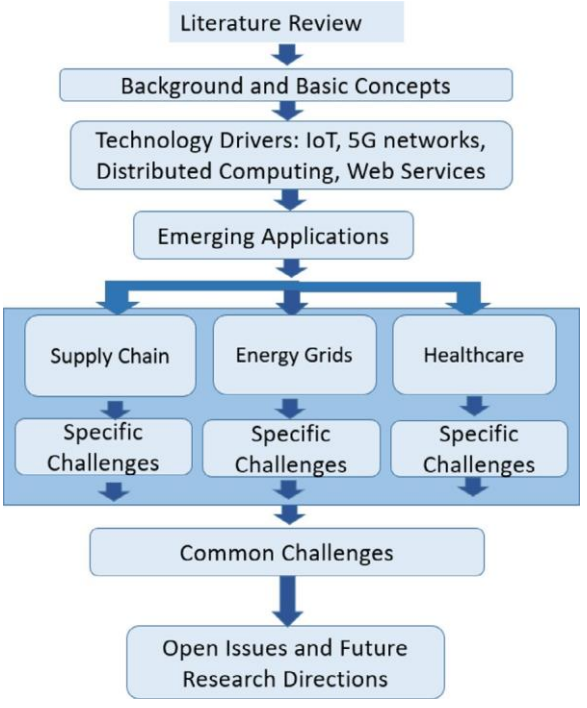

Fig. 1. This figure describes the organization of the material in the current paper.

การวัดและทำธุรกรรมพลังงานแบบกระจาย เราเลือกประเด็นสำคัญสามประการนี้เนื่องจากเป็นพยานที่เพิ่มพูนการวิจัยการลงทุนและการเติบโต

Blockchain ใช้บัญชีแยกประเภทสาธารณะแบบกระจายต่อท้ายเท่านั้นเพื่อเปิดใช้งานธุรกรรมแบบไม่ระบุตัวตนที่เชื่อถือได้[4]ปัญหาสำคัญที่ blockchain อยู่คือเรื่องของตัวกลางซึ่งผู้ซื้อจับคู่กับผู้ขายผ่านบุคคลที่สามที่เชื่อถือได้ โดยทั่วไปเป็นธนาคารหรือนายหน้าในการทำธุรกรรมทางการเงิน. ธุรกรรมปัจจุบันจำนวนมากเกี่ยวข้องกับรูปแบบการรวมศูนย์[5]. Blockchains เสนอกลไกในการรับหน้าที่เป็นตัวกลางนี้ [6] , และย้ายเราออกจากโมเดลรวมศูนย์ไปสู่แบบจำลองที่ไม่รวมศูนย์. ทุกฝ่ายสามารถตรวจสอบการทำธุรกรรมของบุคคลอื่นผ่านบล็อกเชน. ไอโอทีขนาดใหญ่ครอบคลุมอุปกรณ์หลายพันล้านเครื่องซึ่งอาจต้องการทำธุรกรรมระหว่างกัน. ความท้าทายที่สำคัญในสถานการณ์นี้คือการทำงานร่วมกันของอุปกรณ์หลายพันล้านเครื่อง รูปแบบรวมศูนย์ไม่สามารถใช้ได้ที่นี่และ blockchain นำเสนอโซลูชันแบบกระจายอำนาจ[7] .

Blockchains ยังมีฟังก์ชั่นที่ต้องการมากมายรวมถึงความถูกต้องของธุรกรรมการคงอยู่ของธุรกรรมและความเป็นส่วนตัวแบบข้ามชาติ [7] . พวกเขากล่าวถึงปัญหาของอำนาจอธิปไตยของข้อมูลซึ่งบุคคลจะได้รับการควบคุมข้อมูลส่วนบุคคลของพวกเขาและสามารถแบ่งปันกับบุคคลที่พวกเขาไว้วางใจเท่านั้น[8].เราจะตรวจสอบคุณสมบัติที่พึงประสงค์เหล่านี้ของ blockchain ร่วมกับแอพพลิเคชั่นโฟกัสสามส่วนที่เราเลือกเพื่อกล่าวถึงในเอกสารนี้

โดยคำนึงถึงการพัฒนาเหล่านี้เราจึงนำเสนอโครงสร้างของเอกสารของเรา Fig. 1 . เนื่องจากมีบทความบทวิจารณ์หนังสือและนิตยสารที่ยอดเยี่ยมมากมายที่อุทิศให้กับการอธิบายพื้นฐานของบล็อกเชนเราจึงให้ข้อมูลสรุปสั้น ๆ เพื่อเก็บคำศัพท์ไว้ในเอกสารนี้. ผู้อ่านจะอ้างถึงแหล่งที่มาต่อไปนี้สำหรับคำอธิบายของ blockchain [2,9,10] และการสำรวจก่อนหน้านี้ของ blockchain สำหรับ IoT [10] .

2. Background: basic concepts and terminology ความเป็นมา: แนวคิดพื้นฐานและคำศัพท์

2.1. Internet of Things

คำจำกัดความที่ได้รับการยอมรับอย่างกว้างขวางของ Internet of Things (IoT) คือ "เครือข่ายทั่วโลกของวัตถุที่เชื่อมต่อกันซึ่งระบุตำแหน่งได้โดยไม่ซ้ำกันโดยอาศัยโปรโตคอลการสื่อสารมาตรฐาน" [11] . นับตั้งแต่มีการใช้คำจำกัดความนี้มีการระเบิดของอุปกรณ์ IoT การวิจัยและการใช้งานในพื้นที่นี้[12] . อุปกรณ์ IoT ไม่ได้เชื่อมต่อเพียงอย่างเดียว แต่ทำการคำนวณที่ซับซ้อนหลากหลายรวมถึงการตรวจจับ[13–15] , การควบคุมอัตโนมัติ[15,16] , และการสนับสนุนของ smart cities [15,17–19] .

หนึ่งในตัวเปิดใช้งานพื้นที่ IoT คือความพร้อมใช้งานและการเติบโตของแพลตฟอร์มคลาวด์คอมพิวติ้งซึ่งสามารถจัดเก็บและประมวลผลข้อมูลจำนวนมหาศาลที่สร้างโดยอุปกรณ์ IoT [20] . เนื่องจากอุปกรณ์ IoT และระบบคลาวด์เป็นสิ่งที่ช่วยเสริมกันได้. ในขณะที่อุปกรณ์ IoT มีความสามารถในการจัดเก็บการคำนวณและการสื่อสารที่ จำกัด คลาวด์มีมากกว่าปัจจัยเหล่านี้ตามลำดับขนาดต่างๆ. ตัวอย่างเช่น, ในขณะที่กล้องรักษาความปลอดภัยของ Amazon Blink มีพื้นที่เก็บข้อมูลน้อยมาก (1 MB) ระบบคลาวด์สามารถเก็บข้อมูลได้อย่างน้อย 2.5 เอ็กซาไบต์ที่สร้างขึ้นทุกวัน [21]

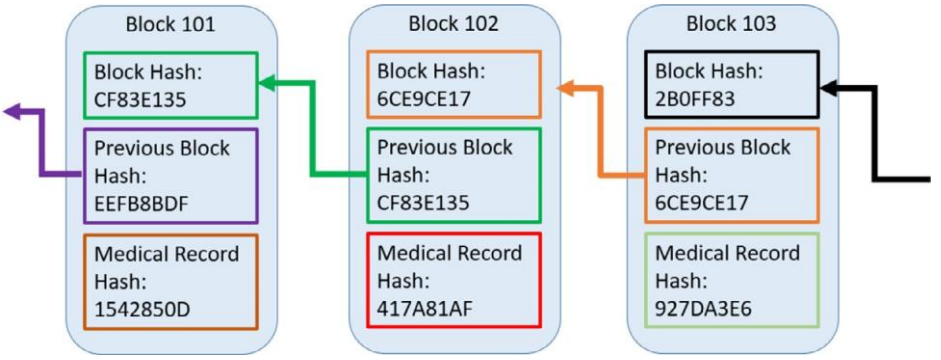

Fig. 2. A simple depiction of a blockchain. For instance, we can consider each block to represent a medical record. This medical record could combine data related to patient vitals with biometrics collected by IoT devices.

ผลการทำงานร่วมกันระหว่างคลาวด์และอุปกรณ์ IoT ทำให้เกิดพื้นที่ใหม่ในการประมวลผลเรียกว่า CloudIoT [20] ในทำนองเดียวกันเราจะตรวจสอบการบรรจบกันของ blockchain และ IoT ในเอกสารปัจจุบัน.

พื้นที่การวิจัยที่เพิ่มขึ้นในพื้นที่ IoT เกี่ยวข้องกับการพัฒนาเครือข่ายหมอก(fog networks)[22] อุปกรณ์ IoT มีความสามารถในการสร้างข้อมูลจำนวนมากซึ่งโดยทั่วไปแล้วจะมีการจัดการโดยแพลตฟอร์มคอมพิวเตอร์ระบบคลาวด์.สิ่งนี้ทำให้เกิดความต้องการอย่างมากในช่องทางการสื่อสารบนเครือข่ายและเซิร์ฟเวอร์คลาวด์ที่ค่อนข้างรวมศูนย์. ในฐานะที่เป็นวิธีหนึ่งในการปรับปรุงการทดลองนี้และทำให้การคำนวณและการจัดเก็บมีการกระจายอำนาจมากขึ้นเครือข่ายหมอกใช้อุปกรณ์มากขึ้นที่ขอบเครือข่ายเพื่อยกเลิกการคำนวณจากเซิร์ฟเวอร์คลาวด์ [22] . มีผลกระทบที่น่าสนใจที่เกี่ยวข้องกับขอบของเครือข่ายคอมพิวเตอร์ดังที่แสดงโดยโครงการ Argonne National Laboratories เกี่ยวกับอาร์เรย์ของสิ่งต่างๆ[23–25] , ซึ่งใช้อาร์เรย์เซ็นเซอร์แบบกระจายเพื่อเปิดใช้งานเมืองอัจฉริยะ[24] . ตัวอย่างเช่นอุปกรณ์ IoT ไม่จำเป็นต้องส่งข้อมูลทั้งหมดที่รวบรวมไปยังเซิร์ฟเวอร์ระบบคลาวด์และเพียงพอที่จะส่งข้อมูลในสถานการณ์ที่ผิดปกติเท่านั้นเช่นน้ำรั่วบนถนน สิ่งนี้จำเป็นที่อุปกรณ์ IoT จะประมวลผลและกรองข้อมูลของตนเองก่อนที่จะส่งข้อมูล ความสามารถนี้มีประโยชน์จริง ๆ จากมุมมองของความเป็นส่วนตัวเนื่องจากต้องมีการส่งข้อมูลโดยรวมเท่านั้นเช่นจำนวนคนที่เดินผ่านสี่แยกจราจรไม่ใช่ภาพของผู้คนเอง อาร์เรย์ของ Argonne Laboratories [23–25] สถาปัตยกรรมจงใจหลีกเลี่ยงการส่งข้อมูลที่ไม่จำเป็นและเป็นส่วนตัวไปยังคลาวด์ เนื่องจากความสามารถในการคำนวณของอุปกรณ์ IoT ยังอยู่ภายใต้กฎหมายของมัวร์จึงมีความเป็นไปได้มากสำหรับการประมวลผลที่ซับซ้อนรวมถึงอัลกอริทึมการเรียนรู้ของเครื่องที่จะดำเนินการโดยอุปกรณ์เหล่านี้ [26] .

2.2. Blockchain

คำจำกัดความของบล็อคเชนมีมากมาย สิ่งที่ค่อนข้างง่ายมีให้ที่นี่:“ บัญชีแยกประเภทแบบกระจายสาธารณะถาวรต่อท้ายเท่านั้น” [27] . ข้อเสนอเดิมสำหรับ bitcoin และการถือกำเนิดของ blockchain เป็นวิธีแก้ปัญหาการใช้จ่ายซ้ำซ้อนในเครือข่ายแบบเพียร์ทูเพียร์ซึ่งไม่ต้องพึ่งพาความไว้วางใจ[28] . ทำได้โดยการสร้างกลไกฉันทามติที่โหนดจะลงคะแนนเสียงด้วยพลัง CPU ของพวกเขาผ่านการคำนวณหลักฐานการทำงานในรูปแบบของแฮช SHA-256 ที่ยากขึ้นเรื่อย ๆ สำหรับบล็อกที่กำหนดซึ่งขึ้นอยู่กับงานที่ มาก่อน (ด้วยเหตุนี้คำว่า blockchain) บล็อกเชนดังกล่าวถือได้ว่าเป็นชุดเอกสารที่เป็นของสาธารณะต่อท้ายเท่านั้นซึ่งมีการกำหนดโดยแฮช SHA-256 ที่ยากต่อการคำนวณ ในระบบนี้ตราบใดที่พลังซีพียูรวมของโหนดที่ซื่อสัตย์มีค่ามากกว่าผู้โจมตีที่กำหนดก็จะเป็นไปไม่ได้ที่ผู้โจมตีจะปรับเปลี่ยนเส้นทางของบล็อกเชนที่ไม่ได้รับการยกย่องได้สำเร็จ

เนื่องจากคุณสมบัติที่เป็นเอกลักษณ์และเป็นที่ต้องการของบล็อกเชน ได้แก่ การกระจายอำนาจการคงอยู่การไม่เปิดเผยตัวตนและความสามารถในการตรวจสอบ เทคโนโลยีนี้จึงได้รับการพิจารณาสำหรับการใช้งานอื่น ๆ นอกเหนือจากการเงิน[29]แม้ว่าในช่วงวัยเด็กสัญญาอัจฉริยะที่ขับเคลื่อนด้วย blockchain เป็นข้อตกลงทางสัญญาที่รับประกันว่าจะดำเนินการตามเงื่อนไขที่กำหนด[30] . สิ่งนี้ส่งผลให้เกิดความสามารถทั่วไปสำหรับ blockchains และวางรากฐานสำหรับการขับเคลื่อนบริการทุกประเภทผ่านเครือข่ายที่กระจายอำนาจและยืดหยุ่นได้ อย่างไรก็ตามสัญญาที่ชาญฉลาดสามารถรับประกันสิ่งต่าง ๆ เท่าที่บล็อกเชนสามารถทำได้ กระตุ้นให้เราพิจารณาว่าเราสามารถขยายขอบเขตทางไซเบอร์ - กายภาพของสังคมของเราไปได้ไกลแค่ไหน นอกเหนือจากสกุลเงินไซเบอร์แล้วอาจเป็นไปได้ที่จะแสดงโครงสร้างทางสังคมอื่น ๆ บนบล็อกเชน[31] , เพิ่มพลังให้กับสัญญาอัจฉริยะ อย่างไรก็ตามสิ่งที่ต้องระวังคือในการกำหนดขอบเขตของความไม่ไว้วางใจเนื่องจากมันครอบคลุมเฉพาะสิ่งที่บล็อกเชนสามารถเข้ารหัสได้

Fig. 2 แสดงแผนผังอย่างง่ายของ blockchain ซึ่งรายการใหม่จะถูกผนวกเข้ากับรายการที่มีอยู่ การใช้ฟังก์ชันแฮชกราฟิกเข้ารหัสลับร่วมกับความเห็นพ้องแบบกระจายจะช่วยป้องกันการปลอมแปลงรายการเหล่านี้ที่อาจเกิดขึ้น คุณลักษณะของ blockchains นี้ช่วยปกป้องข้อมูลเพิ่มเติมในกรณีที่มีการโจมตีทางอินเทอร์เน็ต

2.3. The intersection of IoT and blockchain

Blockchain มีแอปพลิเคชั่นที่มีศักยภาพมากมายใน IoT ซึ่งเป็นที่พึงปรารถนาของสถาปัตยกรรมแบบกระจายอำนาจที่ทนทานต่อโหนดที่ทำงานผิดปกติ อย่างไรก็ตามข้อกำหนดการประมวลผลและการจัดเก็บที่สำคัญสำหรับบล็อกเชนทำให้การนำมาใช้ค่อนข้างท้าทาย ข้อกำหนดที่หนักหน่วงเหล่านี้จำเป็นสำหรับความปลอดภัยและความยืดหยุ่นสูงสุด แต่สถาปัตยกรรมเริ่มปรากฏขึ้นซึ่งทำให้เกิดการแลกเปลี่ยนเพื่อให้สามารถทำงานได้มากขึ้นในการตั้งค่าที่รองรับอุปกรณ์ที่ใช้พลังงานต่ำ[32] . เมื่อระบบฝังตัวมีความสามารถมากขึ้นจึงเป็นเพียงเรื่องของเวลาก่อนที่ความมีชีวิตจะไม่เป็นปัญหาอีกต่อไป

ความปลอดภัยของ Blockchain มาจากผู้ใช้อิสระที่หลากหลายจำนวนมาก นี่เป็นกรณีของ IoT อาจจะมากกว่าในโดเมนเดิมการเงินเนื่องจากจำนวนอุปกรณ์ที่ระเบิด คำถามยังคงอยู่: สิ่งที่สามารถเข้ารหัสบน blockchain ในโลกของ IoT ได้? นอกจากการใช้บล็อกเชนเป็นอุปกรณ์อำนวยความสะดวกในการจัดเก็บและประมวลผลข้อมูลที่รวบรวมโดยอุปกรณ์ IoT อย่างปลอดภัยแล้วเว็บเซ็นเซอร์ IoT จะช่วยเชื่อมช่องว่างระหว่างโลกไซเบอร์กับทางกายภาพทำให้สัญญาอัจฉริยะที่ขับเคลื่อนด้วยเซ็นเซอร์ ในความเป็นจริงพื้นที่การใช้งานโฟกัสของเราสร้างขึ้นจากแนวคิดนี้ พฤติกรรมที่ไม่เหมาะสมในแง่ของการจัดการกับสิ่งที่จับได้สามารถบรรเทาลงได้ แต่ยังคงมีที่ว่างสำหรับการจัดแงะอุปกรณ์ ยังคงต้องสร้างระบบไซเบอร์ - ฟิสิคัลอย่างรอบคอบโดยคำนึงถึงวิธีการตรวจสอบการอ่านทั้งจากการทำงานที่ผิดปกติและอุปกรณ์ที่ถูกดัดแปลง ตามแนวเหล่านั้น RFID เสนอวิธีที่เชื่อถือได้ในการติดตามแหล่งที่มาของการอ่านโดยอย่างน้อยก็จัดให้มีกลไกในการยืนยันที่มาของการอ่าน[33] .

เป็นที่ถกเถียงกัน [34] ว่า blockchain เป็นโซลูชันที่ใช้งานได้ในการจัดการขอบเขตที่ขยายและความซับซ้อนของภูมิทัศน์อุปกรณ์ IoT ผู้บริโภคอาจต้องไว้วางใจผู้ผลิตอุปกรณ์ IoT ก่อนที่จะติดตั้งและใช้งานอุปกรณ์เหล่านี้ blockchain ช่วยในการจัดหาโมเดลเพียร์ทูเพียร์ที่ปรับขนาดได้และเชื่อถือได้ซึ่งโปร่งใสและกระจายข้อมูลอย่างปลอดภัย[34] .

สัญญาอัจฉริยะถูกเสนอให้เป็นกรณีการใช้งานที่สำคัญสำหรับบล็อกเชน [7] . อย่างไรก็ตามการตรวจสอบอย่างใกล้ชิดพบว่าพวกเขาไม่ใช่สัญญาที่มีผลบังคับใช้ตามกฎหมายหรือฉลาด[35] . Orcutt ตั้งข้อสังเกตว่า“ ก่อนที่สัญญาอัจฉริยะจะทำอะไรที่เป็นประโยชน์จริง ๆ พวกเขาต้องการวิธีที่เชื่อถือได้ในการเชื่อมต่อกับเหตุการณ์ต่าง ๆ ในโลกแห่งความเป็นจริงและนั่นก็พิสูจน์แล้วว่าเป็นไปไม่ได้เลย” วิธีแก้ปัญหาที่นำเสนอคือการมี“ oracle” นำเสนอเหตุการณ์จริงในรูปแบบของฟีดแบบเรียลไทม์เช่นข้อมูลสภาพอากาศหรือข้อมูลเที่ยวบิน นี่คือจุดที่อุปกรณ์ IoT มีบทบาทสำคัญและสามารถให้ข้อมูลเพื่อตรวจสอบเงื่อนไขสัญญา. ตัวอย่างเช่น, หากคาดว่าภาชนะที่ใช้ในการขนส่งผลิตภัณฑ์อาหารจะได้รับการบำรุงรักษาที่อุณหภูมิที่กำหนดเซ็นเซอร์ IoT จะตรวจสอบได้ว่าตรงตามเงื่อนไขนี้ ด้วยการใส่

หลักฐานเงื่อนไขนี้เป็นระยะ ๆ ในบล็อกเชนคู่สัญญาที่เกี่ยวข้องในสัญญาสามารถตรวจสอบได้ว่าเป็นไปตามเงื่อนไขในสัญญา สิ่งนี้ถือว่าเซ็นเซอร์ IoT เองได้รับความไว้วางใจจากคู่สัญญาในสัญญาซึ่งเป็นประเด็นแยกต่างหาก. ปัญหานี้คล้ายกับการถกเถียงในปัจจุบันเกี่ยวกับอุปกรณ์ Huawei 5G ที่มีแบ็คดอร์ซึ่งยังไม่ได้รับการพิสูจน์หรือหักล้างอย่างเด็ดขาดในขณะที่เขียนบทความนี้[36] .

อย่างไรก็ตามการใช้เซ็นเซอร์ IoT เป็นวิธีที่มีประสิทธิภาพในการทำให้สัญญาอัจฉริยะทำงานได้จริงและเปิดใช้งานแอปพลิเคชันที่เกี่ยวข้องกับบล็อกเชนจำนวนมาก. เราจะตรวจสอบโดเมนแอปพลิเคชันเฉพาะสามโดเมนในเอกสารนี้ซึ่งได้รับการคัดเลือกจากผลกระทบทางเศรษฐกิจที่คาดว่าจะได้รับและความเป็นไปได้ที่โดเมนเหล่านี้จะถูกนำไปใช้อย่างกว้างขวางในอนาคตอันใกล้. พื้นที่การใช้งานอยู่ในห่วงโซ่อุปทานการดูแลสุขภาพ และกริดพลังงาน

3. Drivers for integration of IoT and blockchain

มีโมเมนตัมจำนวนมากในการปรับใช้อุปกรณ์ IoT ที่มีขนาดใหญ่ขึ้นซึ่งจะย้ายการประมวลผลออกจากเซิร์ฟเวอร์ส่วนกลางไปยังขอบของเครือข่าย ผลที่ตามมาคือสัญญาและการเจรจาระหว่างอุปกรณ์ IoT นั้นสามารถทำได้ดีกว่าโดยอุปกรณ์เหล่านี้เองแทนที่จะเกี่ยวข้องกับเซิร์ฟเวอร์ส่วนกลางในฐานะ "คนกลาง" เราตรวจสอบตัวขับเคลื่อนที่อยู่เบื้องหลังการเติบโตของ IoT และบล็อกเชน

3.1. The exponential growth of IoT devices

Fig. 3 แสดงให้เห็นว่าจำนวนอุปกรณ์ IoT เพิ่มขึ้นเกือบสองเท่าในทุกๆสองปีและคาดว่าจะมีถึง 20 พันล้านเครื่องภายในปี 2020

แม้ว่าจะมีการเปิดใช้งานแอปพลิเคชันใหม่ ๆ ผ่านอุปกรณ์เหล่านี้เช่นแอปพลิเคชันบล็อกเชน แต่ก็เป็นความท้าทายในการจัดการอุปกรณ์เหล่านี้ตามขนาด ปัญหาล่าสุดที่ บริษัท General Electric [37] ส่วนหนึ่งเกิดจากสถานะที่ไม่ถูกต้องของธุรกิจ IoT และแสดงให้เห็นถึงปัญหาเกี่ยวกับอุปกรณ์ IoT อุตสาหกรรมเช่นเซ็นเซอร์ที่วัดประสิทธิภาพของเครื่องยนต์เจ็ท. มีข้อมูลจำนวนมหาศาลที่สร้างขึ้นและเป็นไปไม่ได้ที่จะส่งข้อมูลทั้งหมดนี้ไปยังศูนย์จัดเก็บข้อมูลบนคลาวด์ประมวลผลแล้วส่งกลับไปยังจุดดำเนินการ[38] . นอกจากนี้การตั้งค่าบริการจัดเก็บข้อมูลภายในองค์กรยังเป็นปัญหาที่ท้าทายและ บริษัท อย่าง GE อาจตระหนักว่าไม่คุ้มค่าที่จะลงทุนในการสร้างความสามารถดังกล่าวหากมีให้บริการผ่านผู้จำหน่ายพื้นที่เก็บข้อมูลบนคลาวด์ [38] .

อุปกรณ์ IoT ส่วนใหญ่มีต้นทุนต่ำและสิ่งนี้สร้างแรงกดดันให้ผู้ผลิตรวมกลไกการป้องกันที่จำเป็นเพื่อป้องกันการโจมตีทางไซเบอร์เช่นการออกแพตช์ปกติและการอัปเดตซอฟต์แวร์[39] .

3.2. The emergence of 5G networks

คาดว่าเครือข่าย 5G จะแพร่หลายในปี 2019 เครือข่ายการสื่อสารไร้สายเหล่านี้จะให้อัตราข้อมูลที่สูงมาก (ตามลำดับ Gbps) เวลาแฝงต่ำและการปรับปรุงคุณภาพของบริการที่สำคัญ

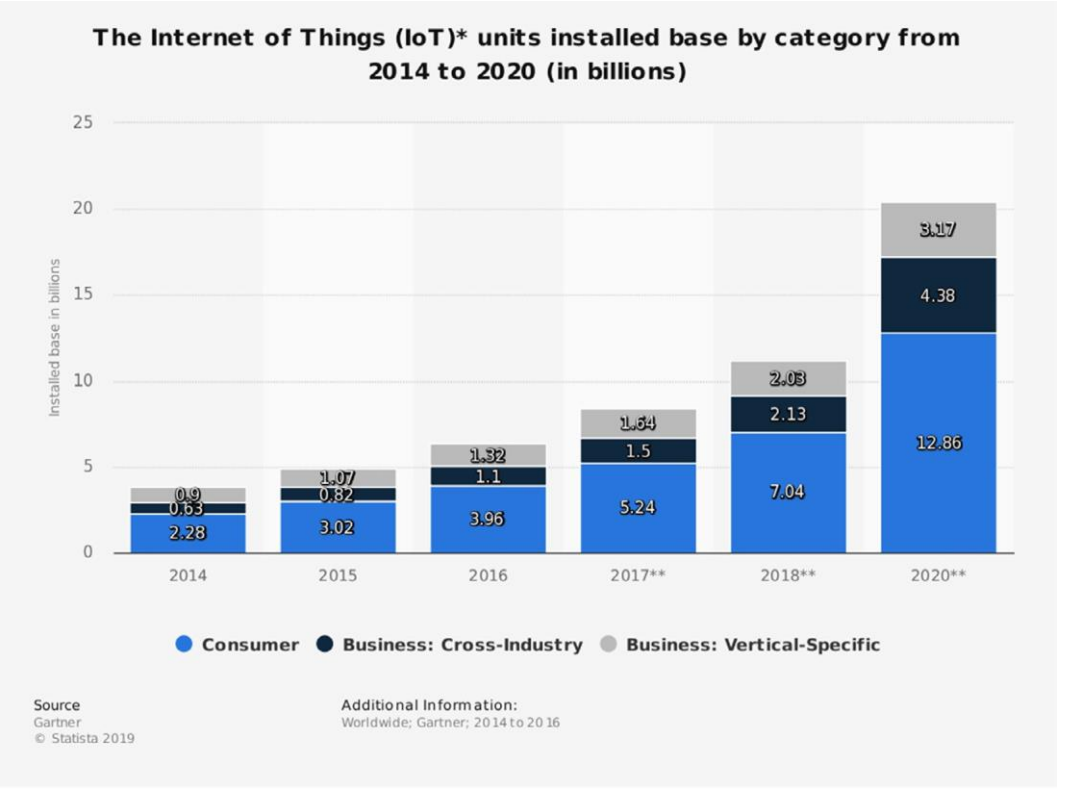

Fig. 3. The growth curve for IoT devices. The expected number of IoT devices in 2020 is roughly 20 billion.
Source: https://www.statista.com/statistics/370350/internet- of- things- installed- base- by-category/ (accessible by creating a free account on statistica.com).

สิ่งนี้ทำให้การเชื่อมต่ออุปกรณ์ IoT เข้ากับเครือข่ายเหล่านี้เป็นเรื่องน่าสนใจสำหรับการใช้งานใหม่ ๆ [40,41]. ข้อมูลจำเพาะทางเทคนิคของเครือข่าย 5G สามารถพบได้ในบทความสำรวจ[42]. เครือข่าย 5G ควรให้อัตราข้อมูลสูงสุด 1 Gbps สำหรับผู้ใช้มือถือและ 10 Gbps สำหรับผู้ใช้ที่อยู่กับที่ [43,44].ความพร้อมใช้งานของความเร็วเครือข่ายดังกล่าวจะช่วยให้แง่มุมของบล็อกเชน เช่นฉันทามติแบบกระจายทำงานได้อย่างมีประสิทธิภาพ

3.3. *Cloud computing and web services* การประมวลผลแบบคลาวด์และบริการบนเว็บ

การเติบโตอย่างรวดเร็วของคลาวด์คอมพิวติ้งและบริการบนเว็บทำให้ความจำเป็นในการประมวลผลของคอมพิวเตอร์ในไซต์ลดลงอย่างมาก แม้ว่าการจัดเก็บและการประมวลผลข้อมูลทั่วไปจะมีให้บริการมาหลายปีแล้ว แต่เมื่อไม่นานมานี้มีการนำเสนอพิเศษสำหรับบล็อกเชนออกสู่ตลาด. ตัวอย่างเช่น Amazon Web Services นำเสนอ blockchain เป็นบริการที่มีการจัดการเต็มรูปแบบ[45], และนี่เป็นการเปิดทิศทางใหม่ในการรวมอุปกรณ์ IoT เข้ากับบริการบล็อกเชน [46].

4. **Emerging applications** การใช้งานที่เกิดขึ้นใหม่

ในส่วนนี้เรากล่าวถึงแอพพลิเคชั่นที่เกิดขึ้นใหม่ที่สำคัญสามอย่าง ซึ่งประกอบด้วยการดูแลสุขภาพ ซัพพลายเชนและกริดพลังงานอัจฉริยะ.

4.1. *Focus application #1: healthcare*

ในด้านการดูแลสุขภาพเราพิจารณากรณีการใช้งานบางกรณีที่คาดว่าการประยุกต์ใช้ IoT และเทคโนโลยีบล็อกเชนจะส่งผลดีในระยะสั้น.

4.1.1. Using RFID and barcodes to tag medical devices การใช้ RFID และบาร์โค้ดเพื่อติดแท็กอุปกรณ์ทางการแพทย์

FDA กำหนดให้มีการระบุอุปกรณ์เฉพาะ (UDI) สำหรับอุปกรณ์ทางการแพทย์. เราสามารถสร้างสมาร์ทโค้ดได้โดยมีเซ็นเซอร์ RFID ฝังอยู่ในฉลากบาร์โค้ด. โรงพยาบาลสามารถใช้เซ็นเซอร์ RFID เพื่อติดตามทรัพย์สินทางการแพทย์ได้อย่างง่ายดาย. อุตสาหกรรมอุปกรณ์ทางการแพทย์กำลังสำรวจโซลูชันที่ใช้เครือข่าย RFID ทั่วโลกในการระบุสินทรัพย์ แผนผังที่ใช้ RFID และบาร์โค้ดกับอุปกรณ์ IoT เช่น Raspberry Pi จะแสดงในรูปแบบ Fig. 4 ชุดอุปกรณ์นี้สามารถใช้เป็นรากฐานสำหรับโซลูชันบล็อกเชนสำหรับการติดตามทรัพย์สินที่เชื่อถือได้และไม่เปลี่ยนรูป มีคำถามเปิดอยู่มากมายในพื้นที่เทคโนโลยีสารสนเทศสำหรับการดูแลสุขภาพรวมถึงการได้มาและการใช้ข้อมูลไบโอเมตริกซ์เพื่อระบุตัวผู้ป่วย [47]

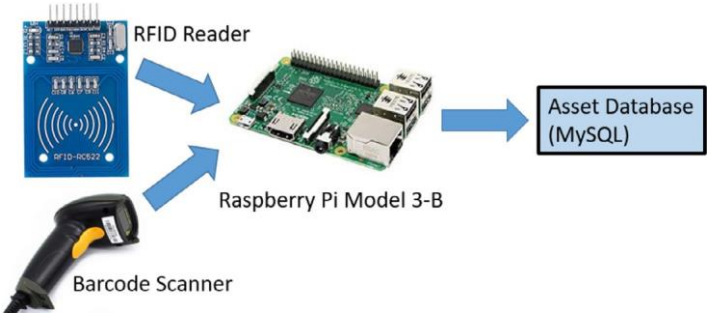

Fig. 4. Using RFID readers and barcode scanners attached to an IoT device (Raspberry Pi). This can be used for device tagging in medical supply chains and for asset tracking in hospitals.

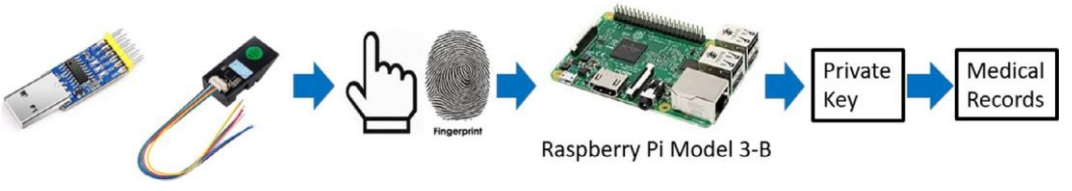

Fig. 5. Biometric information (e.g. a fingerprint) can be used to access patient records.

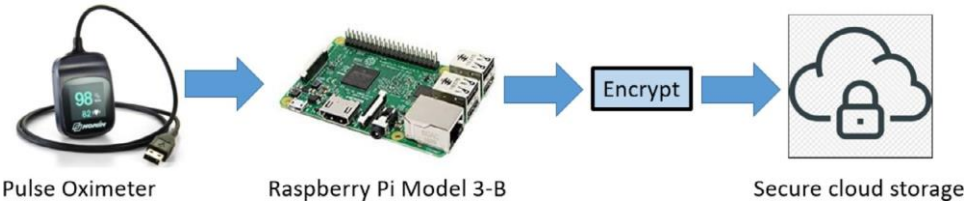

Fig. 6. A pulse oximeter (e.g. Nonin or Contex CMS-50F) which provides USB and/or Bluetooth connectivity can be connected to an IoT device like the Raspberry Pi. This allows patient data to be directly stored on a computer without human intervention.

การรักษาความเป็นส่วนตัวของผู้ป่วยภายในองค์กรและการแบ่งปันบันทึกผู้ป่วยอย่างปลอดภัยในหลายองค์กร[48] . การปกป้องข้อมูลผู้ป่วยในระบบไอทีหลายระบบทำให้เกิดความท้าทายด้านความปลอดภัยหลายประการ ดังนั้นจุดตัดของความปลอดภัยในโลกไซเบอร์ข้อมูลผู้ป่วยและอุปกรณ์ทางการแพทย์จึงเป็นพยานถึงการเติบโตอย่างมีนัยสำคัญ[49,50] . Blockchain กำลังถูกเสนอให้เป็นเทคโนโลยีสำหรับการแบ่งปันข้อมูลผู้ป่วยในขณะที่ยังคงรักษาความเป็นส่วนตัว[51] .

4.1.2. Using patient biometrics for identification การใช้ไบโอเมตริกของผู้ป่วยเพื่อระบุตัวตน

ปัจจุบันโรงพยาบาลส่วนใหญ่ระบุผู้ป่วยตามชื่อและวันเกิด. ทำให้เกิดปัญหาเพิ่มขึ้นเนื่องจากผู้ป่วยหลายรายอาจมีชื่อและวันเกิดเหมือนกัน.เมื่อเร็ว ๆ นี้ รายงาน The Wall Street Journal [47] ที่อยู่ในระบบการดูแลสุขภาพของรัฐเท็กซัส,“ ตอนนี้มี Maria Garcias 2833 คน โดย 528 คนมีวันเดือนปีเกิดเดียวกัน”เนื่องจากไม่มีแนวทางที่เป็นมาตรฐานระดับประเทศสำหรับปัญหานี้ในสหรัฐอเมริกา โรงพยาบาลบางแห่งหันมาใช้ไบโอเมตริกเพื่อเป็นแนวทางแก้ปัญหา เป็นไปได้มากที่จะติดเครื่องอ่านลายนิ้วมือเข้ากับ Raspberry-PI ลายนิ้วมือที่สแกนสามารถแปลงเป็นคีย์ส่วนตัวเพื่อเข้าถึงเวชระเบียนดังที่แสดงใน Fig. 5 .

4.1.3. Using sensors to measure patient vitals การใช้เซ็นเซอร์เพื่อวัดความมีชีวิตชีวาของผู้ป่วย

นอกจากนี้โดยปกติแล้ว Vitals ของผู้ป่วยยังคงถูกวัดโดยอุปกรณ์แบบสแตนด์อะโลนโดยไม่ต้องเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ใด ๆ ตัวอย่างเช่นความสูงน้ำหนักความดันโลหิตระดับน้ำตาลในเลือดและ oximeter โดยทั่วไปมนุษย์จะป้อนการอ่านลงในคอมพิวเตอร์

รายการเหล่านี้อาจเกิดจากข้อผิดพลาดของมนุษย์ซึ่งยังคงเกิดขึ้น[47] . การใช้อุปกรณ์ IoT ราคาไม่แพงจึงค่อนข้างเป็นไปได้ที่จะป้อนข้อมูลนี้ลงในเวชระเบียนของผู้ป่วยโดยอัตโนมัติดังที่แสดงใน Fig. 6 . Vitals ของผู้ป่วยสามารถเป็นส่วนหนึ่งของ blockchain ที่ประกอบเป็นบันทึกสุขภาพอิเล็กทรอนิกส์ของผู้ป่วย[52] . นอกจากนี้ยังสามารถใช้ร่วมกับข้อมูลไบโอเมตริกซ์ของผู้ป่วยสำหรับการเข้ารหัสแบบ end-to-end [52] , ซึ่งเป็นแนวป้องกันการโจมตีทางไซเบอร์ที่กำหนดเป้าหมายบันทึกสุขภาพอิเล็กทรอนิกส์.

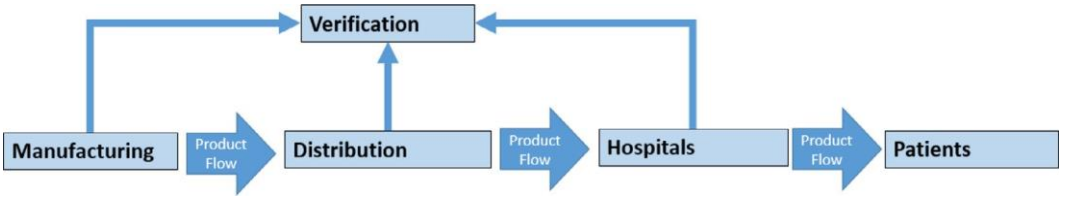

Fig. 7. Product flow in a pharmaceutical supply chain. The end-to-end verification prevents the entry of counterfeits and illegal products.

4.2. Focus application #2: supply chain

อุตสาหกรรมการเดินเรือมีการนำเทคโนโลยีดิจิทัลมาใช้อย่างช้าๆรวมถึงการประมวลผลข้อมูลทางเว็บ[53] . มีอุปสรรคหลายประการรวมถึงความจำเป็นในการได้รับช่องว่างด้านกฎระเบียบหลายประการเมื่อสินค้าเคลื่อนย้ายข้ามพรมแดน[54] . ช่องว่างเหล่านี้ส่วนใหญ่ใช้เอกสารและค่าใช้จ่ายจะอยู่ที่ประมาณ 15–50% ของค่าขนส่งทั้งหมด[54] . มีข้อดีที่ชัดเจนที่จะได้รับจากการเพิ่มประสิทธิภาพห่วงโซ่อุปทานทั่วโลกรวมถึงการจัดการสินค้าคงคลังที่ดีขึ้นความแม่นยำในการคำนวณเวลานำสินค้าที่ดีขึ้นและการปฏิบัติตามคำสั่งซื้อที่รวดเร็วขึ้น. ข้อดีที่นำเสนอโดยเทคโนโลยีบล็อกเชนทำให้เกิดแรงผลักดันที่สำคัญต่อการเปลี่ยนแปลงทางดิจิทัลของอุตสาหกรรมการเดินเรือ สัญญาหลายฉบับยังคงดำเนินการโดยผู้ปฏิบัติงานที่เป็นมนุษย์ซึ่งนำไปสู่ข้อผิดพลาด สามารถจัดการสัญญาได้อย่างชาญฉลาดขึ้นด้วยการตรวจสอบข้อมูลอัตโนมัติที่ป้อนลงในแบบฟอร์มเมื่อตู้คอนเทนเนอร์เคลื่อนผ่านพื้นที่หักบัญชีศุลกากรหลายแห่ง[55] . Blockchain เป็นรากฐานสำหรับการจัดการเอกสารการจัดส่งที่เชื่อถือ

ได้ซึ่งนำไปสู่ความจริงเวอร์ชันเดียวและเส้นทางที่ไม่เปลี่ยนรูปซึ่งสามารถตรวจสอบได้ทันที สิ่งสำคัญคือต้องได้รับข้อมูลเกี่ยวกับสถานะของการจัดส่งและสภาพของวัตถุที่จัดส่งระหว่างการขนส่ง. การใช้อุปกรณ์ IoT เช่นเซ็นเซอร์อุณหภูมิภายในตู้สินค้าและกล้องสำหรับการขนส่งสามารถให้เส้นทางการตรวจสอบที่พิสูจน์ว่าเนื้อหาได้รับการจัดการอย่างเหมาะสม อุปกรณ์ IoT จะสร้างข้อมูลโดยอัตโนมัติในช่วงเวลาปกติและสามารถเพิ่มลงในบล็อกเชนที่ต้องการได้

Ndraha et al. [56] ทบทวนความท้าทายเฉพาะในอุตสาหกรรมซัพพลายเชนที่เกี่ยวข้องกับการดูแลรักษาอุณหภูมิที่เหมาะสมในห่วงโซ่อุปทานอาหาร. Even small temperature variations of a few degrees centigrade, where the container temperature is either higher or lower than the recommended temperature can result in spoilage of the transported food, or greatly reduce its expected shelf life. Both types of variations have been observed by Nunes et al. [57] , where cold-sensitive fruits were transported too cold, and heat-sensitive produce were transported too warm. This results in a wastage of at least 50% of the products [56] . In many cases, the basic problem is that the food supply chain operators are unaware of these temperature fluctuations and unable to react appropriately [58] . Lunden et al. [58] also estimated the duration over which the temperatures were out of range, and found that for nearly 50% of the cases, the temperature was more than 3 °C for at least 30 min. Suggested solutions in the literature include temperature management control by using IoT sensors, RFID tags, and wireless sensor networks [59] . The use of blockchains offers a tamper-resistant way of capturing deviations from a desired time-temperature profile. Such deviations can be added to the blockchain as they occur, which avoids the need to continuously store sensor data. This is an example of the use of intelligence at the edge-of-the-network, which can be implemented with a few simple rules. The receiver of the container is notified of any such deviations, and the transporter is not able to conceal this information or tamper with it. With further sophistication, including utilizing training data to infer such rules, this scenario provides a path to connect artificial intelligence with blockchain technologies, as analyzed by Dinh and Thai [60] .

Even with these sensor measurements, it may be possible to thwart the monitoring system by altering the associations between the container, what it contains, and the measurements being recorded. For instance, the temperature sensor may be tracking temperature deviations in an empty container. Hence, we need a mechanism to verify that all the measurements are obtained from the true object we wish to monitor. This mechanism is discussed in the next paragraph concerning the establishment of provenance and avoidance of counterfeits.

Establishing provenance and a rightful chain of ownership is important for costly goods such as diamonds or critical items such as medicines. Traditionally, the ownership and authenticity have been established through paper certificates, which can be misplaced or tampered with. Blockchain based solutions are now available for diamonds [61] . A crucial aspect of establishing provenance is to bind the physical item to its metadata, including authenticity and certificates of origin. In the case of diamonds, this is achieved by creating a set of physical features (forty in the solution reported in [61]) of an individual diamond and adding it to the blockchain. An ideal solution would be one where the object is physically inscribed with an immutable identification, which is then merged with its metadata. However, this is not possible for a wide range of objects, including diamonds. The next best solution appears to be one where physical features of the objects are measured and computed. IoT devices are well suited to perform these measurements and compute the required features. For instance, IoT devices such as cameras and barcode scanners can verify packaging information and the integrity of package seals during the shipment and movement of medical drugs [62] . The envisioned workflow is shown in Fig. 7 . This could be an enabling technology [63] to achieve the goals of the recently introduced European Union Falsified Medicines directive, which is aimed at curbing the rise of falsified medicines entering the supply chain [64] .

A recent emerging application area is the use of blockchain technology to manage food supply chains. This helps identify sources of potential contamination so that corrective action can be applied quickly, especially in the case of food borne illnesses such as e-coli outbreaks [65] . Recent efforts include the research in [33,66] and the pilot study being conducted by Walmart [67] .

4.3. Focus application #3: smart energy grids

There is considerable interest in green and renewable energy sources today, including bio-fuels, hydroelectric, solar, and wind energy [68] . Due to encouragement from government policies, including tax rebates, solar panel installation has seen significant growth in states such as California in the USA. This has resulted in individual homeowners contributing electricity generated from solar panels into the larger electric grid [69] . However, in many cases, they may not receive the monetary compensation they expect, either in terms of the price per kilowatt-hour, or may be burdened by regulatory issues [70] . This has created the impetus for a peer-to-peer electricity trading arrangement, which is based on free market principles. An example is the Brooklyn microgrid (www.brooklyn.energy), which is a community-powered microgrid. Though this is in very early stages, key components include the use of IoT devices for metering, and the use of blockchain for conduct- ing transactions. The blockchain aspect of this project involves the management of contracts, and dynamically determining pricing according to the contracts. The creation of such microgrids can be especially useful for developing countries, where many locations do not have well established centralized power grids [71] . Such peer-to-peer energy producing and trading systems are growing in the world, with installations in the USA, Germany, and Australia [71] .

From an IoT device point of view, an enabling technology is the smart electric meter [72] . There are many types of smart meters available, as reviewed in [73] , and include minimum functionality smart meters, smart meters with in-home display and smart meters with a demand-control unit. Mengelkamp et al. [74] provide the architecture and technical specifications behind the Brooklyn microgrid. A pilot installation and test have revealed that blockchain combined with smart metering is able to connect all the market participants in the microgrid, and provide an operational platform. It is well-known that the pricing of energy is subject to hourly fluctuations depending on demand and supply [75] . The availability of a local energy market implies that participants have a choice of using the local grid when its price is lower than that of the external grid [74] . Furthermore, they even

have the option to support the local grid and local renewable energy suppliers by paying a higher price. Hence, the availability of IoT-blockchain solutions can have significant socio-economic impact, and result in profits that stay within local communities.

Major external grid companies such as Con Edison in the New York region are planning to move their services to a distributed system model in the future [76] . One of planned components includes information sharing through an advanced metering infrastructure. This planned activity is similar to the work on the microgrid, due to the distributed nature of the transactions. Nevertheless, the energy sector seems to be challenging to penetrate due to stricter regulations. In comparison, it is easier to implement and experiment with enterprise blockchain applications such as the supply chain. The technology field is still in the early phase of testing out pilots in many promising application areas.

5. Common challenges

In this section, we review common challenges that apply to the three focus areas we selected earlier. These challanges are explored in detail in the following subsections.

5.1. Cybersecurity considerations

Significant research has been conducted on end-to-end encryption in sensor networks [77] . An interesting recent de- velopment in network communications is an increasing demand for end-to-end encryption driven by consumers, and their implementation by corporations. For instance, WhatsApp began end-to-end encryption of user messages only in 2016 [78] . Furthermore, other options are also available, including organizations such as Let's Encrypt (https://letsencrypt.org) which serves as a free, automated, and open certificate authority. It is important for communications between devices to be secure and protected. By using massive investments in physical infrastructure, many of the leading technology companies such as Apple, Facebook and Google are able to provide such end-to-end encryption services. However it is still challenging for inde- pendent software developers and startups to provide such capabilities in native applications. Nevertheless, negligence, when it comes to security, is still widely pervasive, and is exacerbated by the increasing number of devices potentially affected by new vulnerabilities.

The Verizon Data Breach Reports regularly disclose that negligence in applying security patches is a big contributing factor in cyberattacks. For instance, Grimes observes that "The Verizon Data Breach Report 2016 revealed that out of all detected exploits, most came from vulnerabilities dating to 2007. Vulnerabilities dating to 2003 still account for a large por- tion of hacks of Microsoft software. We're not talking about being a little late with patching. We're talking about persistent neglect." The Verizon Data Breach Report from 2018 [79] confirms this observation, and shows that cybercriminals continue to exploit known vulnerabilities. The Verizon Report [79] notes that "Some companies are failing to take the most basic of security measures— like keeping anti-virus software up to date." Though it is possible that a cloud service provider like Amazon could be up-to-date in applying security patches to their servers, the sheer number of IoT devices makes patching an enormous challenge. In a recent cyberattack, multiple machines including IoT devices were recruited in a coordinated fashion to create bot-nets [80] , which were then used in the Dyn Distributed Denial of Service (DDoS) attack.

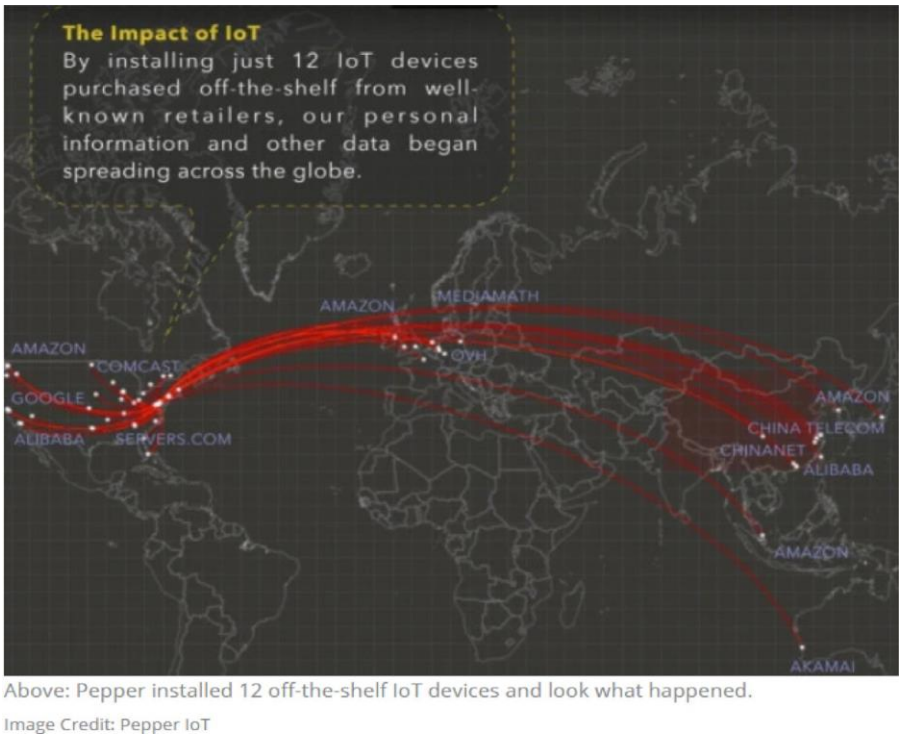

Fig. 8. A recent article [39] highlights the unintended spread of personal information through IoT devices. Many of these IoT devices are insecure the moment they are installed. Since this poses security problems worldwide, it is imperative for each nation to secure its own cyberspace. (Figure reproduced with permission from Pepper IoT).

Given the low cost of the IoT devices that are being deployed, it is important for cryptography toolkits used in encryption and decryption to be democratized and made widely available. End-to-end encryption is by nature decentralized and does not require any infrastructure. The primary used encryption schemes are publicly well known and studied (e.g. RSA). With the judicious use of public and private keys, it is possible to attenuate the effect of potential cyberattacks. There are open- source cryptography toolkits being made available, along with guidelines for their usage (e.g. by virgilsecurity.com).

Fig. 8 shows how easily personal information can inadvertently be spread through consumer smart-home embedded devices. Consumers purchase embedded devices from retailers, and immediately connect them to the public internet. This results in several anomalies and unexplained communications, as observed by a testing agency, Dark Cubed [39] . Thus, simply operating these devices leads to a distribution of personal data. When we consider that the expected number of IoT devices will be 20 billion by 2020 (Source: Gartner), this presents great concern to the security community. The 5G rollout occurring in 2019 will only accelerate the adoption of IoT devices. So much so that the government of Japan has announced their intent to hack into their citizens' IoT devices to warn them of vulnerabilities before the 2020 Olympics in Tokyo [81] .

People are already using multiple IoT devices including smartphones, fitness trackers, smart watches, and smart home appliances. This increases the number of security exposures per person. Phishing attacks are ubiquitous and occur on a daily basis, affecting all users of these devices. User privacy can be breached in totally unexpected ways, with a disturbing example offered by a fitness tracker app used by US Army personnel that revealed the location of secret army bases [82] . This story illustrates how using IoT devices such as a cellphone can result in unexpected security issues.

It is relatively easy to fix such a problem once it has been discovered. However, the preferred route is to prevent these incidents in the first place. One way to work towards prevention is to inculcate a "security mindset" in the users of these technologies. Users need to understand the mechanisms and ploys used by attackers, so they can stay alert and watchful. Educating the current generation of students at universities would be a great starting point, especially for students in STEM and engineering fields who can grasp the technicalities behind cyber-attacks. Accordingly, we have developed instructional material for detailed hands-on exercises for students in the area of cyber-security for embedded devices [83–86] .

5.2. Computation and storage

Though the computational capabilities of IoT devices are increasing, it is still computationally intensive for such a device to participate as a node capable of adding a transaction to a blockchain. Current estimates are that it takes several minutes to add a block to bitcoin. Though permissioned blockchains can be used to speed up the addition of a new block, it is still difficult to add blocks at the speed with which IoT data can be generated. Similarly, the storage requirements will increase rapidly if additional metadata needs to be stored along with the IoT sensor data. Hence, viable solutions will require

Fig. 9. The Movidius neural compute stick is a low-power and small form factor device that can implement deep neural network algorithms for signal processing and image recognition. Here, a Movidius compute stick costing $75 it is shown attached to a USB port of a Raspberry Pi Model 3-B that costs $35.

chunking of the data, or the identification of markers such as deviations from expected thresholds. In order to perform such processing, more computational power is required for the IoT or edge-of-network devices.

Though the IoT device itself may not have the required computational power, add-on devices that provide specialized processing capabilities are increasingly becoming available. For instance, the Intel Movidius neural compute stick, shown in Fig. 9 implements deep neural networks in hardware, which can be used for tasks such as filtering and object detection [87] . An IoT temperature sensor can be configured to report only significant temperature deviations from an acceptable range. Similarly, an IoT camera can report only the number of people it detects, rather than the images of the people themselves. This can be integrated with the blockchain for video surveillance applications in smart cities [88] .

There are increasing numbers of instances where IoT devices like the Raspberry Pi are being used for process control applications in industrial manufacturing settings. For instance, Sony recently reported a 30% improvement in its processes by using about 60 Raspberry Pis in a manufacturing plant [89] . The low cost of these devices encourages more experimentation, as a potential failure does not involve excessive capital expenditures.

5.3. Granularity of transactions

By the granularity of a transaction, we refer to the resolution of the physical quantity that is metered and noted. For instance, in the realm of smart meters, we would like to determine whether we pay for the usage of 1 W at a time, especially if we are buying the power from suppliers that may constantly change. These are the types of details that need to be captured in the contracts. This also has implications for how frequently the blockchain ledgers will need to be updated, and whether it makes practical sense in a given domain. Also, given that such transactions need to be replicated across multiple nodes in the network, this could quickly snowball into irrelevant data being propagated and stored. It may be necessary to apply processing at the edge-of-the-network by using filters or rules. For instance, in the supply chain use case we considered earlier, the temperature can be stored only at pre-determined intervals, or if there is a deviation beyond a specified range.

Such edge-of-the-network intelligence is being utilized in the array-of-things project at the Argonne National Laboratory, where cameras at traffic intersections only count the number of pedestrians without storing pictures of individual pedestri- ans [90] .

5.4. Trust

Trust is another issue related to granularity. At what level should the party delivering the service be trusted? And at what level should the ability of the recipient of the service to pay for it be trusted? For instance, if the service provider in an electric grid wants to be to be paid for every watt of energy as and when it is delivered, then that may impose an unnecessary burden on the system. Interestingly, Amazon Web Services requires a credit card to be on file for customers who use their services, so that they are guaranteed payment.

Another issue is that there is it is difficult to establish true validation of the transaction. For instance, a service provider could transmit 10 W of power, and the receiver may record only 9 W. How does one resolve this collision? It is important for the meters need to be calibrated. We need an independent way of evaluating the amount of electricity transmitted and received. All the players in the ecosystem need to trust that. Furthermore, there could be the potential for fake devices, or it may prove very difficult to verify that a device functions exactly as specified. For instance, the evaluation of Huawei 5G equipment has proven to be very challenging, even for the security agencies of the leading powers in the world [36,91]. Hence there is room for significant innovation in the space of IoT sensors.

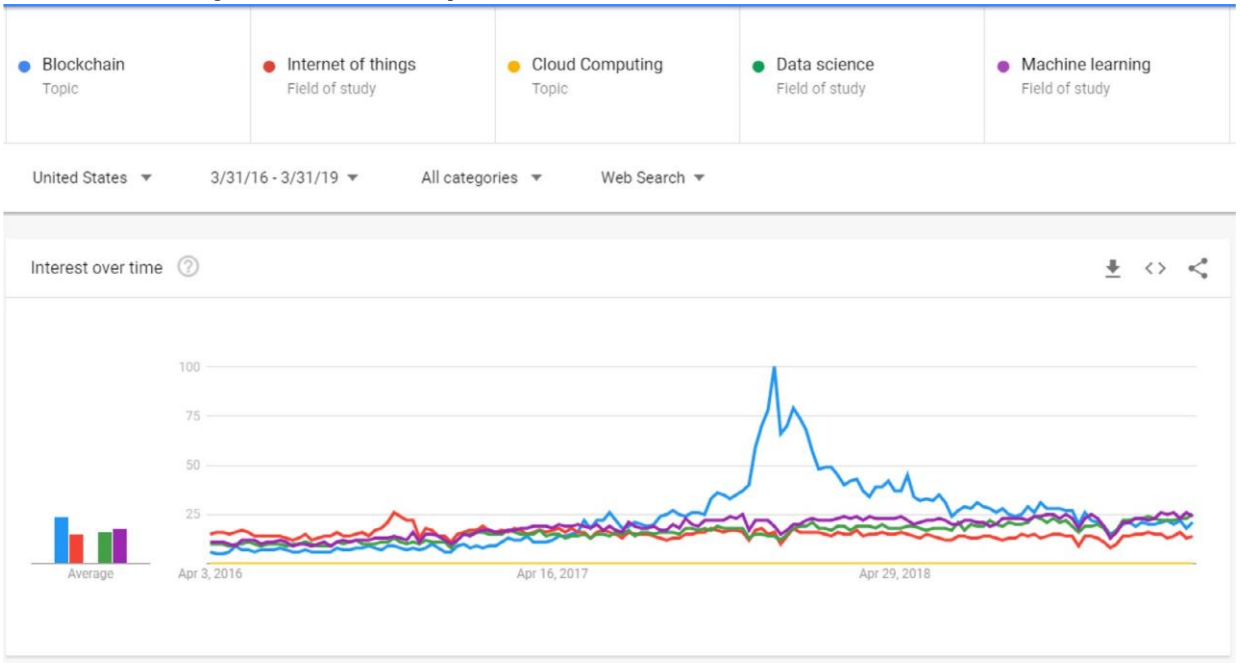

Fig. 10. This figure shows the trends in google searches for the different topics including blockchain, and internet of things. The other topics such as cloud computing, data science and machine learning are used to gauge the interest in other popular areas in the field of computing today. A 3-year window is used for the comparison. (Data source: Google Trends, (https://www.google.com/trends).

These issues indicate that there may be room for rating agencies to provide information about trust. This is similar to the use of ratings for sellers and buyers in online marketplaces such as eBay [92] , or that of bond credit rating agencies such as Moody's [93] . In summary, the resolution of trust is outside the ecosystem of the blockchain. For instance the sending and receiving of a certain amount of bitcoin is guaranteed, but not the service that it may represent.

5.5. Privacy

With IoT sensors such as cameras being used to monitor traffic and pedestrians in cities, it is important for the privacy of citizens to be protected. Though law enforcement agencies may have such cameras, public service organizations such as the Robert Woods Johnson Foundation are funding efforts to monitor traffic and pedestrian flow. This leads to a better understanding of urban efficiencies, and an improvement in public health due to increased pedestrian safety and activity [94] . The technology being used is designed to protect privacy by only storing extracted features from the images, such as pedestrian counts at different times of the day. In the interest of making such data available to the public through an "open data" principle [18,95–101] , this data can be stored in a public blockchain. This not only makes the data accessible, but also elevates the level of public trust, as the data is immutable.

5.6. Jumpstarting the ecosystem

There are very few peer reviewed research publications that present the status of current blockchain projects in the industry. As a consequence, we have to rely on reports by consulting and marketing firms. A recent Forrester report claims that 90 percent of blockchain pilots will fail [102] . Similar observations were made in a Computerworld article [103] about the lack of successful blockchain projects, and also the lack of data about the status of these projects. The overwhelming consensus seems to be to proceed with caution, as there are many more unknowns and kinks, both actual and potential. Fig. 10 illustrates the steep relative decline in interest in blockchain, though this is only through the metric of Google searches. Nevertheless, the current interest appears to be comparable with other emerging technologies such as machine learning and data science, which are seeing widespread adoption and business penetration. In contrast, the technology of cloud computing is quite mature, and it is accompanied by a relatively low number of searches for this topic. A more detailed comparison would examine the trends in the publications of research papers in these areas, which may be a lagging indicator of the more widespread searches in Fig. 10 .

These trends, and the sense of caution developing around blockchain indicate that the ecosystem needs to be jumpstarted with a few successful pilots, which would encourage further investment and research in this area. More fundamental research needs to be conducted, including that along the lines discussed in this paper on different applications of blockchain, and use cases with intersecting areas such as IoT and machine learning.

5.7. Education and workforce training

In addition to the projected shortage of STEM (Science, Technology, Engineering, Mathematics) professionals in the USA [104] , there is an even more acute shortage of professionals in areas such as cybersecurity [105] and blockchain. The rapid growth of these new technologies creates challenges from the academic and teaching viewpoint, as there is a widening gap between what the students learn in traditional courses and the cutting edge of industrial technologies. Students in the USA are already dropping from STEM majors at a high rate, and this widening gap is likely to exacerbate the problem. This necessitates rapid changes to existing curricula, and the adoption of new pedagogical techniques.

Furthermore, there is a severe lack of instructional material that offers an integrated view of emerging technologies such as the internet-of-things [12] , cloud computing [106] , security [107] , cryptography [108] , and blockchain [109] . Though there are individual books in these areas [108,109] , they may not be suitable at the undergraduate level. Publishers are experiencing declining revenues [110] and may not be interested in creating textbook material in fast-changing fields.

An interesting development is the creation of new courses on MOOC (massively open online course) platforms such as Coursera and EdX [111] . Just in 2018 the demand for course materials in areas such as blockchain and cryptocurrency was so high that *undergraduate* students in University of California Berkeley offered a course entitled "Blockchain Fundamentals", on EdX.org in [111] .

The National Security Agency in the USA has been funding efforts to develop educational materials in the areas sur- rounding cybersecurity [105] and cryptography. Rao et al. started using the Raspberry-Pi to develop new course material based on embedded systems, IoT and cybersecurity [84–86] . The introduction of hands-on laboratory exercises was found to significantly improve student interest, and engagement. A set of lab exercises to understand blockchain uses in IoT devices was introduced recently. These exercises help students to develop a "security mindset", which is important in the world of cybersecurity [112] .

6. Open issues and future directions

The current status of blockchain in IoT resembles the classic chicken-and-egg problem. Companies and individuals will not use blockchain unless there is demonstrated value and an obvious return-on-investment. However, it is difficult to gen- erate value unless a sufficient number of applications are deployed, and economies of scale have been established.

This indicates that a necessary milestone is that successful pilot projects are executed. Some areas where this is close to happening is the accounting sector and retail applications. Walmart and IBM have reported that their food supply chain project will exit the pilot phase in 2019 [67] .

A challenge with deploying blockchain in the energy sector through decentralized smart meters is government regulation. The developers of this technology may not be able to seamlessly scale and deploy this technology worldwide, as regulations vary from country to country. Furthermore, energy transfer across international borders such as through an electric grid is also highly regulated. For this reason, many blockchain startups in the field of energy are struggling to establish a viable business model [71,74] .

The promise of decentralized solutions to transactive energy are likely to be realized in the longer term, after a five- year timeframe. This is because energy companies like ConEdison are first tackling lower complexity problems such as automating internal business processes, and working with ESCOs (Energy supply companies) to integrate them seamlessly into the energy supply chain. There is a more attractive return-on-investment and shorter term viability for such projects. In addition, data exchange and privacy issues need to be resolved.

Enterprise blockchain is a potentially easier application of blockchain and IoT. The tracking of inventory is an important problem. RFID tags have become popular in this space, and constitute an enabling technology [33] . Some RFID tags are passive. It is possible to use active tags that can

communicate with a server or peers and disclose the contents of a package. Maersk Shipping is using blockchain for managing shipping of containers [54] .

The issue of a private (or permissioned) versus public blockchain is important. Early adopters in the energy sectors are finding out that a public blockchain (based on ether) is too expensive as a mechanism to pay for contracts. Hence, many entities are using private implementations of ether so that they can control transaction costs [113] . Another potential solution is to use intranets, as details for data sharing on public blockchains have yet to be worked out [114] . Hence, it is easier to start with deployments on intranets first.

In the energy sector, the energy grid is actually private, as users need to be registered to connect to the grid. Hence a private structure is appropriate for the energy grid. Furthermore, there are different latency expectations for applications running at different portions of the energy grid. At the edge of the grid, transactions may need to be very fast. For instance, negotiations may need to be conducted rapidly before a fuse is blown. However, the speed of transactions between two substations could be slower as larger loads may not fluctuate as quickly. This implies that one can utilize two separate blockchains with different latency requirements. These ideas need to be implemented and tested out, which necessitates a significant amount of experimentation in real marketplaces.

Finally, a gray zone is that of legal enforcement of blockchain contracts. The legal framework needs to be expanded to handle use cases based on blockchains, and this is a very new area [115] . The speed of technological advancement in this area has been very fast, and the existing contract laws have not kept pace. This requires the cultivation of experts conversant both with the capabilities of blockchain and an understanding of the legal world. Hence, we need a regulatory sandbox for business model development.

One of the implications of a blockchain enabled ecosystem is that accounting ledgers may need to be held on indefinitely. In the case of IoT devices, this requires the accounting data to be offloaded from the IoT device to local or remote servers. Some open questions are: at what level of detail should this data be collected and stored, and at what temporal frequency (e.g. every millisecond, or second, or minute, or hour)? Though storage costs are shrinking rapidly, the solution providers need to determine where and when this data is stored.

One relevant technology in this context is that of fog networks [22] , where the multitude of devices in a connected home pool their storage and computation resources together. There is a significant amount of unused storage and computation on many IoT devices, including laptops, refrigerators, personal assistants such as Alexa, and cell-phones within a home. If the capabilities within these devices are harnessed in a coordinated fashion, the limitation of a single device can be overcome.

Another aspect to keep in mind is that processing power, storage and memory size are all increasing according to Moore's law. So a solution that is not possible with today's devices may become viable in the longer term. The underlying technology can be developed and tested, and widespread deployment could possibly take a decade or more. This is a common theme in the development of technologies such as the internet, which took a long time to develop, but exploded once it started seeing wider adoption.

The granularity of IoT device participation in the blockchain is an important design issue. For instance, should a smart thermostat be directly connected to the energy grid, or should it communicate data to a centralized server in the base- ment of a home? The home server can then participate in blockchain transactions with other homes or the utility ser- vice provider. This shows that total decentralization may not be necessary, where every single IoT device participates in transactions.

The recent cyberattack [116] on IoT devices demonstrates the vulnerability of these devices. There are various levels at which the IoT devices can be compromised, from totally disabling them to rigging them so false data is provided. For in- stance, a thermostat can be hacked to provide wrong temperature values, which then has an adverse effect on the energy grid. Hence there are many physical variables that are measured by IoT devices that are not part of the blockchain environ- ment. This is a compromised situation that is outside end-to-end encryption channels or the security provided by blockchain transactions.

Similarly, the trust that exists when you provided an expected service to another party is outside the scope of blockchain transactions. The blockchain cannot verify that you actually provided the service that meets a service level agreement. This is especially true in more complex transactions that may involve human labor.

The extraction of commercial value from the data generated by IoT devices has proven to be challenging. GE had high expectations of creating a predictive analytics platform that utilized data from industrial IoT devices [54,117] . This did not materialize as envisioned, and the reasons are complex, ranging from the core technical challenges to make this happen to marketing issues. This has resulted in a scaling back of expectations and an extension of the time horizon. As a result, GE is focusing on specific use cases rather than trying to build a generic platform. This case study is relevant to the broad issues discussed in the current paper, as a cautious approach is likely to be used by the early adopters.

In the area of logistics and supply chain management, Kersten et al. [118] note that logistics companies, especially the smaller and medium sized companies have very limited expertise in blockchains. Though companies such as Cargosmart [55] are creating specialized offerings to fill this void, the larger logistics and shipping companies are reluctant to experiment with newer technologies [53] .

It is possible to establish provenance for expensive items like diamonds by using IoT devices to measure a wide range of object features. The cost of the IoT devices can be justified in such a business solution. However, the use of IoT devices in containers for perishable food items may take longer to get established. Even though IoT devices and sensors are getting cheaper, retailers are constantly cutting costs and will be reluctant to utilize solutions without demonstrable cost savings
[119] .

7. Conclusion

The number of IoT devices has increased greatly, and is accompanied by increases in processing power and 5G network- ing speeds. Since it is becoming difficult to have centralized computational models in this environment, we are witnessing a shift to decentralized models. There are additional requirements that users seek, including privacy, trust, and immutability of stored information. These requirements can be met with blockchain technology. The intersection of IoT with blockchain provides potential solution paths to existing problems with smart contracts, where

the boundaries of cyber physical systems need to be better defined. IoT sensors can verify information contained in smart contract clauses by providing continuous measurements from the physical world. We examined three specific scenarios consisting of healthcare applications, sup- ply chain applications and smart energy applications. In each of these scenarios we highlighted the interplay between IoT devices and the blockchain. We also outlined several existing problems that need careful research. By advancing such research, we expect that fruitful progress can be made in realizing the full potential of the confluence of IoT with blockchain technology.

Conflict of interest statement

The authors indicate that they have no conflicts of interest.

References

[1] A. Al-Fuqaha , M. Guizani , M. Mohammadi , M. Aledhari , M. Ayyash , Internet of Things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (2015) 2347–2376 .

[2] (2018). MIT Technology Review: The Blockchain Issue. Available: https://www.technologyreview.com/magazine/2018/05/ . [3] L. Mearian. (2018). IoT Could be the Killer App for Blockchain.

[4] H. Subramanian , Decentralized blockchain-based electronic marketplaces, Commun. ACM 61 (2018) 78–84 .

[5] G.W. Peters , E. Panayi , Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money, Banking Beyond Banks and Money, Springer, 2016, pp. 239–278 .

[6] A. Tapscott , D. Tapscott , How blockchain is changing finance, Harvard Business Review 1.9 (2017) 2–5 .

[7] K. Christidis , M. Devetsikiotis , Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303 .

[8] P. De Filippi, The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies, 2016.

[9] M. Conoscenti , A. Vetro , J.C. De Martin , Blockchain for the Internet of Things: a systematic literature review, in: Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1–6 .

[10] T.M. Fernández-Caramés , P. Fraga-Lamas , A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001 .

[11] Internet of things in 2020: a roadmap for the future, INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in Co-operation with the RFID Working Group of the European Technology Platform on Smart Systems Integration (EPOSS), 5 September, 2008.

[12] L. Atzori , A. Iera , G. Morabito , The internet of things: a survey, Comput. Netw. 54 (2010) 2787–2805 .

[13] M. Lee , J. Hwang , H. Yoe , Agricultural production system based on ioT, in: Proceedings of the 2013 IEEE 16th International Conference on Computa- tional Science and Engineering (CSE), 2013, pp. 833–837 .

[14] G. Zhang , C. Li , Y. Zhang , C. Xing , J. Yang , SemanMedical: a kind of semantic medical monitoring system model based on the IoT sensors, in: Proceed- ings of the 2012 IEEE 14th International Conference One-health Networking, Applications and Services (Healthcom), 2012, pp. 238–243 .

[15] C. Perera , A. Zaslavsky , P. Christen , D. Georgakopoulos , Sensing as a service model for smart cities supported by internet of things, Trans. Emerg. Telecommun. Technol. 25 (2014) 81–93 .

[16] J.-c. Zhao , J.-f. Zhang , Y. Feng , J.-x. Guo , The study and application of the IOT technology in agriculture, in: Proceedings of the 2010 3rd IEEE Interna- tional Conference on Computer Science and Information Technology (ICCSIT), 2010, pp. 462–465 .

[17] A. Zanella , N. Bui , A. Castellani , L. Vangelista , M. Zorzi , Internet of things for smart cities, IEEE Internet Things J. 1 (2014) 22–32 .

[18] B. Ahlgren , M. Hidell , E.C.-H. Ngai , Internet of things for smart cities: interoperability and open data, IEEE Internet Comput. 20.6 (2016) 52–56 .

[19] Y. Mehmood , F. Ahmad , I. Yaqoob , A. Adnane , M. Imran , S. Guizani , Internet-of-things-based smart cities: recent advances and challenges, IEEE Com- mun. Mag. 55 (2017) 16–24 .

[20] A. Botta , W. De Donato , V. Persico , A. Pescapé, Integration of cloud computing and internet of things: a survey, Futur. Gener. Comput. Syst. 56 (2016) 684–700 .

[21] R. Jacobson. (July 1). 2.5 Quintillion Bytes of Data Created Every Day. How Does CPG & Retail Manage It? 2013.

[22] H. Zhang , Y. Xiao , S. Bu , D. Niyato , F.R. Yu , Z. Han , Computing resource allocation in three-tier IoT fog networks: a joint optimization approach combining stackelberg game and matching, IEEE Internet Things J. 4 (2017) 1204–1215 .

[23] (2018). *Array of Things* .

[24] S. Jernigan , S. Ransbotham , D. Kiron , Data Sharing and Analytics Drive Success with IOT, MIT Sloan Management Review, 2016 .

[25] R.L. Jacob , C. Catlett , P. Beckman , R. Sankaran , Early results from the array of things, in: Proceedings of the AGU Fall Meeting Abstracts, 2017 .

[26] C. Perera , A. Zaslavsky , P. Christen , D. Georgakopoulos , Context aware computing for the internet of things: a survey, IEEE Commun. Surv. Tutor. 16 (2014) 414–454 .

[27] MIT Technology Review Editors, Explainer: What is a blockchain? MIT Technology Review, 2018 https://www.technologyreview.com/s/610833/ explainer- what- is- a-blockchain/ .

[28] S. Nakamoto, Bitcoin: Aa Peer-To-Peer Electronic Cash System, 2008.

[29] Z. Zheng , S. Xie , H.-N. Dai , X. Chen , H. Wang , Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (2018) 352–375 .

[30] A . Kosba , A . Miller , E. Shi , Z. Wen , C. Papamanthou , Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: Pro- ceedings of the 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 839–858 .

[31] F.-Y. Wang , The emergence of intelligent enterprises: from CPS to CPSS, IEEE Intell. Syst. 25 (2010) 85–88 .

[32] K.R. Özyılmaz , A. Yurdakul , Integrating low-power iot devices to a blockchain-based infrastructure: work-in-progress, in: Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion, 2017, p. 13 .

[33] F. Tian , An agri-food supply chain traceability system for china based on RFID & blockchain technology, in: Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), 2016, pp. 1–6 .

[34] P. Brody , V. Pureswaran , Device Democracy: Saving the Future of the Internet of Things, IBM, September 2014 .

[35] M. Durovic , A. Janssen , The formation of Blockchain-based smart contracts in the light of contract law, Eur. Rev. Private Law 26 (2018) 753–771 .

[36] A. Satariano , Huawei Security 'Defects' are Found by British Authorities, New York Times, 2019 .

[37] D. Cimilluca , D. Mattioli , T. Gryta , GE Puts Digital Assets on the Block, Wall Street Journal, 2018 .

[38] D. Tokar , Three Recommendations for GE's Newly Formed Industrial IoT Software Company, Forbes, 2018 .

[39] D. Takahashi. (2019) Smart Devices aren't so Bright When it Comes to Security. Available: https://venturebeat.com/2019/01/29/ pepper- iot- smart- devices- arent- so- bright-when- it- comes- to- security/ .

[40] G.A. Akpakwu , B.J. Silva , G.P. Hancke , A.M. Abu-Mahfouz , A survey on 5G networks for the Internet of Things: communication technologies and challenges, IEEE Access 6 (2018) 3619–3647 .

[41] S. Li , L. Da Xu , S. Zhao , 5G Internet of Things: a survey, J. Ind. Inf. Integr. 10 (2018) 1–9 .

[42] M. Agiwal , A. Roy , N. Saxena , Next generation 5G wireless networks: a comprehensive survey, IEEE Commun. Surv. Tutor. 18 (2016) 1617–1655 .

[43] I. Chih-Lin , S. Han , Z. Xu , Q. Sun , Z. Pan , 5G: rethink mobile communications for 2020 + , Philos. Trans. R. Soc. A: Math. Phys. Eng. Sci. 374 (2016) 20140432 .

[44] E.J. Oughton , Z. Frias , The cost, coverage and rollout implications of 5G infrastructure in britain, Telecommun. Policy 42 (2018) 636–652 .

[45] Blockchain on AWS: Eeasily Build Scalable Blockchain and Ledger Solutions. 2019. Available: https://aws.amazon.com/blockchain/ .

[46] M. Samaniego , R. Deters , Hosting virtual IoT resources on edge-hosts with blockchain, in: Proceedings of the 2016 IEEE International Conference on Computer and Information Technology (CIT), 2016, pp. 116–119 .

[47] B. Gormley , Hospitals Turn to Biometrics to Identify Patients, Wall Street Journal, 2019 .

[48] M. Li , S. Yu , Y. Zheng , K. Ren , W. Lou , Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst. 24 (2013) 131–143 .
[49] K. Fu , J. Blum , Inside risks controlling for cybersecurity risks of medical device software, Commun. ACM 56 (10) (2013) 35–37 .
[50] E.D. Perakslis , M. Stanley , A cybersecurity primer for translational research, Sci. Transl. Med. 8 (2016) 322ps2 .
[51] N. Kshetri , Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (2017) 1027–1038 .
[52] D. Augot , H. Chabanne , T. Chenevier , W. George , L. Lambert , A user-centric system for verified identities on the bitcoin blockchain, Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2017, pp. 390–407 . [53] E. Samwel , Redefining e-commerce, Contain. Int. 41 (2008) 63–64 .
[54] N. Hackius , M. Petersen , Blockchain in logistics and supply chain: trick or treat? in: Proceedings of the Hamburg International Conference of Logistics (HICL), 2017, pp. 3–18 .
[55] Cargosmart, CargoSmart Launches Blockchain Initiative to Simplify Shipment Documentation Processes, Global Newswire, 2018 .
[56] N. Ndraha , H.-I. Hsiao , J. Vlajic , M.-F. Yang , H.-T.V. Lin , Time-temperature abuse in the food cold chain: review of issues, challenges, and recommen- dations, Food Control 89 (2018) 12–21 .
[57] M.C.N. Nunes , J.P. Emond , M. Rauth , S. Dea , K.V. Chau , Environmental conditions encountered during typical consumer retail display affect fruit and vegetable quality and waste, Postharvest Biol. Technol. 51 (2009) 232–241 .
[58] J. Lundén , V. Vanhanen , T. Myllymäki , E. Laamanen , K. Kotilainen , K. Hemminki , Temperature control efficacy of retail refrigeration equipment, Food Control 45 (2014) 109–114 .
[59] K.P. Koutsoumanis , M. Gougouli , Use of time temperature integrators in food safety management, Trends Food Sci. Technol. 43 (2015) 236–244 .
[60] T.N. Dinh , M.T. Thai , Ai and blockchain: a disruptive integration, Computer 51 (2018) 48–53 .
[61] N. Lomas, Everledger is Using Blockchain to Combat Fraud, Starting with Diamonds, URL: https://techcrunch.com/2015/06/29/everledger , 2015.
[62] T. Bocek , B.B. Rodrigues , T. Strasser , B. Stiller , Blockchains everywhere-a use-case of blockchains in the pharma supply-chain, in: Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 772–777 .
[63] N. Alzahrani , N. Bulusu , Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain, in: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, 2018, pp. 30–35 .
[64] S. Houlton , Tackling the problem of falsified medicines in the UK, Prescriber 29 (2018) 33–35 .
[65] S. Luna , V. Krishnasamy , L. Saw , L. Smith , J. Wagner , J. Weigand , et al. , Outbreak of E. coli O157: H7 infections associated with exposure to animal manure in a rural community—Arizona and Utah, June–July 2017, Morb. Mortal. Wkly. Rep. 67 (2018) 659 .
[66] M.P. Caro , M.S. Ali , M. Vecchio , R. Giaffreda , Blockchain-based traceability in agri-food supply chain management: a practical implementation, in: Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), 2018, pp. 1–4 .
[67] B. Tan , J. Yan , S. Chen , X. Liu , The impact of blockchain on food supply chain: the case of walmart, in: Proceedings of the International Conference on Smart Blockchain, 2018, pp. 167–177 .
[68] E.S. Shuba , D. Kifle , Microalgae to biofuels: 'promising' alternative and renewable energy, review, Renew. Sustain. Energy Rev. 81 (2018) 743–755 .
[69] T. von Wirth , L. Gislason , R. Seidl , Distributed energy systems on a neighborhood scale: reviewing drivers of and barriers to social acceptance, Renew. Sustain. Energy Rev. 82 (2018) 2618–2628 .
[70] M. Muro and D. Saha. Rooftop Solar: Nnet Metering is a Net Benefit [Online]. 2017. Available: https://www.brookings.edu/research/ rooftop- solar- net- metering- is- a- net-benefit/ .
[71] D. Cardwell , Solar Experiment Lets Neighbors Trade Energy Among Themselves, New York Times, 2017 .
[72] S. Blumsack , A. Fernandez , Ready or not, here comes the smart grid!, Energy 37 (2012) 61–68 .
[73] E. Andrey , J. Morelli , Design of a smart meter techno-economic model for electric utilities in Ontario, in: Proceedings of the 2010 IEEE Electrical Power & Energy Conference, 2010, pp. 1–7 .
[74] E. Mengelkamp , J. Gärttner , K. Rock , S. Kessler , L. Orsini , C. Weinhardt , Designing microgrid energy markets: a case study: the brooklyn microgrid, Appl. Energy 210 (2018) 870–880 .
[75] A. Ghasemi , H. Shayeghi , M. Moradzadeh , M. Nooshyar , A novel hybrid algorithm for electricity price and load forecasting in smart grids with demand-side management, Appl. Energy 177 (2016) 40–59 .
[76] (2018). Distributed System Platform. Available: https://www.coned.com/en/our- energy- future/our- energy- projects/distribution- system- platform .
[77] Y. Sang , H. Shen , Y. Inoguchi , Y. Tan , N. Xiong , Secure data aggregation in wireless sensor networks: a survey, in: Proceedings of the Seventh Interna- tional Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT'06, 2006, pp. 315–320 .
[78] K. Ermoshina , F. Musiani , H. Halpin , End-to-end encrypted messaging protocols: an overview, in: Proceedings of the International Conference on Internet Science, 2016, pp. 244–254 .
[79] (2018). Verizon 2018 Data Breach Investigations Report. Available: https://enterprise.verizon.com/resources/reports/dbir/ .
[80] B. Rashidi , C. Fung , E. Bertino , A collaborative DDoS defence framework using network function virtualization, IEEE Trans. Inf. Forensics Secur. 12 (2017) 2483–2497 .
[81] C. Cimpanu, Japanese Government Plans to Hack Into citizens' IoT Devices, Zdnet, 2019 zdnet.com .
[82] A. Hern , Fitness Tracking App Strava gives Away Location of Secret US Army Bases, The Guardian, 2018 .
[83] A.R. Rao , R. Dave , Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications, in: Proceedings of the IEEE Integrated STEM Education Conference, Princeton, NJ, 2019 .
[84] A.R. Rao , D. Clarke , N. Mohammed , Creating an anchor hands-on cybersecurity course using the raspberry pi, in: Proceedings of the Colloquium for Information Systems Security Education (CISSE), New Orleans, 2018 .
[85] A.R. Rao , D. Clarke , D. Yeskepalli , M.-R. Mallu , Teaching cybersecurity concepts through Internet-of-things applications based on the raspberry pi, in: Proceedings of the Colloquium for Information Systems Security Education (CISSE), New Orleans, 2018 .
[86] A.R. Rao , D. Clarke , M. Bhadiyadra , S. Phadke , Development of an embedded system course to teach the Internet-of-Things, in: Proceedings of the IEEE STEM Education Conference, ISEC, Princeton, 2018, pp. 154–160 .
[87] M.H. Ionica , D. Gregg , The movidius myriad architecture's potential for scientific computing, IEEE Micro 35 (2015) 6–14 .
[88] P. Gallo , S. Pongnumkul , U.Q. Nguyen , BlockSee: blockchain for IoT video surveillance in smart cities, in: Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2018, pp. 1–6 .
[89] P. Olson , How Sony Sped up a Factory with These Tiny, $35 Computers, Forbes, 2019 .
[90] C.E. Catlett , P.H. Beckman , R. Sankaran , K.K. Galvin , Array of things: a scientific research instrument in the public way: platform design and early lessons learned, in: Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering, 2017, pp. 26–33 . [91] B. Pancevski , S. Germano , In Rebuke to U.S., Germany Considers Letting Huawei, Wall Street Journal, 2019 .
[92] D. Gregg , M. Parthasarathy , Factors affecting the long-term survival of eBay ventures: a longitudinal study, Small Bus. Econ. 49 (2017) 405–419 .
[93] M. Adelino , I. Cunha , M.A. Ferreira , The economic effects of public financing: evidence from municipal bond ratings recalibration, Rev. Financ. Stud. 30 (2017) 3223–3268 .
[94] (2018). Technology for Healthy Communities. Available: http://www.communityhealthtech.org/pilots .
[95] S. Baack , Datafication and empowerment: how the open data movement re-articulates notions of democracy, participation, and journalism, Big Data Soc. 2 (2015) 1–11 .
[96] R. Kitchin , The Data revolution: Big data, Open data, Data Infrastructures and Their Consequences, Sage, 2014 .
[97] E.G. Martin , N. Helbig , N.R. Shah , Liberating data to transform health care: New York's open data experience, JAMA 311 (2014) 2481–2482 .
[98] T. Davies , F. Perini , Researching the emerging impacts of open data: revisiting the ODDC conceptual framework, J. Community Inform. 12 (2016) 148–178 .
[99] T. Jetzek , The Sustainable Value of Open Government Data: Uncovering the Generative Mechanisms of Open Data Through a Mixed Methods Approach, Copenhagen Business School, Institut for IT-LedelseDepartment of IT Management, 2015 .
[100] P. Conradie , S. Choenni , On the barriers for local government releasing open data, Gov. Inf. Q. 31 (2014) S10–S17 .
[101] G. Boulton , M. Rawlins , P. Vallance , M. Walport , Science as a public enterprise: the case for open data, Lancet 377 (2011) 1633–1635 .
[102] O. Kharif, Blockchain, Once Seen as a Corporate Cure-All, Suffers Slowdown, in Bloomberg.com, ed, 2018.

[103] L. Mearian. (2018) Blockchain: WWhat's it Good For? Absolutely Nothing, Report Finds. Computerworld. Available: https://www.computerworld.com/article/3324359/blockchain- what- s- it- good- for- absolutely- nothing- report- finds.html .
[104] (2016). *US Department of Education* , https://innovation.ed.gov/files/2016/09/AIR-STEM2026 _ Report _ 2016.pdf .
[105] Cybersecurity Workforce Education - CNAP Initiatives, Developing Hands-on Exercises for Secure Embedded System Design & Security Data An- alytics for Computing and Engineering Students Number H98230- I 7- I -032, National Security Agency, 2017 CNAP-CAE CNAP-CAE2017 Grant# H98230-17-1-0321 .
[106] M. Armbrust , A. Fox , R. Griffith , A.D. Joseph , R. Katz , A. Konwinski , et al. , A view of cloud computing, Commun. ACM 53 (2010) 50–58 . [107] P.W. Singer , A. Friedman , Cybersecurity: What Everyone Needs to Know, Oxford University Press, 2014 .
[108] Y. Lindell , J. Katz , Introduction to Modern Cryptography, Chapman and Hall/CRC, 2014 .
[109] M. Swan , Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc, 2015 .
[110] C. Straumsheim. (2017) Is 'Inclusive Access' the Future for Publishers? Available: https://www.insidehighered.com/news/2017/01/31/ textbook- publishers- contemplate-inclusive- access- business- model- future .
[111] L. Mearian. (2018) UC Berkeley Puts Blockchain Training Online; Thousands Sign Up. *Computerworld* . Available: https://www.computerworld.com/article/3282791/blockchain/uc-berkeley-puts-blockchain-training-online-thousands-sign-up.html .
[112] S. Hooshangi , R. Weiss , J. Cappos , Can the security mindset make students better testers? in: Proceedings of the 46th ACM Technical Symposium on Computer Science Education, 2015, pp. 404–409 .
[113] W. Li , A. Sforzin , S. Fedorov , G.O. Karame , Towards scalable and private industrial blockchains, in: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017, pp. 9–14 .
[114] M. Ferguson , Preparing for a Blockchain Future, 60, MIT Sloan Management Review, 2018, pp. 1–4 .
[115] G. Governatori , F. Idelberger , Z. Milosevic , R. Riveret , G. Sartor , X. Xu , On legal contracts, imperative and declarative smart contracts, and blockchain systems, Artif. Intell. Law 26 (2018) 377–409 .
[116] K. Bhardwaj , J.C. Miranda , A. Gavrilovska , Towards IoT-DDoS prevention using edge computing, in: Proceedings of the USENIX Workshop on Hot Topics in Edge Computing (HotEdge 18), 2018 .
[117] K. Moskvitch , When machinery chats [Connections industrial IOT], Eng. Technol. 12 (2017) 68–70 .
[118] W. Kersten , M. Seiter , B. von See , N. Hackius , T. Maurer , Trends and Strategies in Logistics and Supply Chain Management–Digital Transformation Opportunities, BVL International, 2017 .
[119] M. Hingley , A. Lindgreen , D.B. Grant , C. Kane , Using fourth-party logistics management to improve horizontal collaboration among grocery retailers, Supply Chain Manag. Int. J. 16 (2011) 316–327 .