THE UNIVERSITY OF HONG KONG 香港大學
faculty of architecture 建築學院

iLab @ HKURBANlab
the urban big data lab

華中科技大學
土木工程与力学学院
SCHOOL OF CIVIL ENGINEERING & MECHANICS

第六届工程管理前沿暑期学校 暨
土木工程全国优秀大学生云端夏令营
华中科技大学 土木工程与力学学院

Blockchain for Smart Construction

23 July 2020
Wuhan, China

Frank Xue
Assistant Professor
iLab, REC, HKU, HK SAR

Outline

1. Construction: Distributed collaboration
2. Blockchain: Distributed trustworthy database
3. Two cases

0.1 HKU iLab: The urban big data hub

- iLab 实验室
  - Director: Prof. Wilson Lu
  - Urban big data hub at Faculty of Architecture, HKU
  - multi-dimensional and multi-disciplinary *urban big data* collection, storage, analysis, and presentation to inform decision-making in urban development
  - Focusing on information technology (IT)
    - *Building Information Modeling* (BIM)
    - *Geographical Information System* (GIS)
    - *Global Navigation Satellite System* (GNSS)
    - *Urban Remote Sensing* (URS)
    - *Internet of Things* (IoT)
    - Blockchain (BC/DLT)

iLab @ HKURBANlab the urban big data lab

iLabHKU

fac.arch.hku.hk/iLab

2020 New Year dinner

0.2 About myself

- A mixed background 背景
  - BEng in Automation, CAUC — 2004
  - MSc in Computer Science, CAUC — 2007
    - Advisor: Prof. W Fan
  - PhD in System Engineering, HKPU — 2012
  - PDF/RAP/AP in Construction IT — 2016
- Research interests 方向
  - Urban sensing and computing
  - Automation/IT in construction
  - Applied operations research, ML, etc.
- Homepage: QR code for new updates

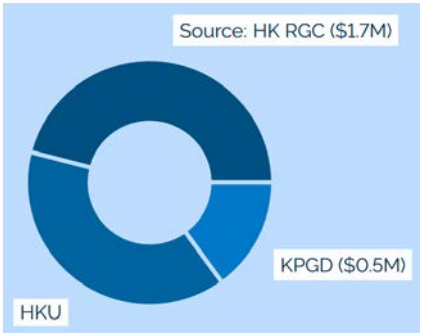
- Engineering
  - ISE, CEM, EIE
- Computer Science
  - AI, OR, ML
- Economics
  - SCM

Homepage (free full-text)

0.2 My research projects

- On-going 在研
  - PI: HK RGC GRF/ECS (17201717, 17200218, 27200520), HKU-Tsinghua SPF (20300083), HKU (102009917, 201811159177, 201910159238)
  - Co-PI: Key R&D Guangdong (2019B010151001), HKU PTF (102009741)
  - Co-I: NSFC (71671156), NSSFC (17ZDA062), HK SPPR (S2018.A8.010.18S), HK ECF (111/2019)
- Completed 完成
  - PI: HKU (201702159013, 201711159016)
  - Co-I: NSFC (60472123), HK PPR (2018.A8.078.18D)
- Job vacancy (2 openings)
  - PhD, HK$200,000~350,000/year
  - RA, transferable to PhD (vision, rigor, & performance)

- Keywords
  - BIM/CIM
  - 3D point cloud
  - Derivative-free optimization
  - Urban semantics



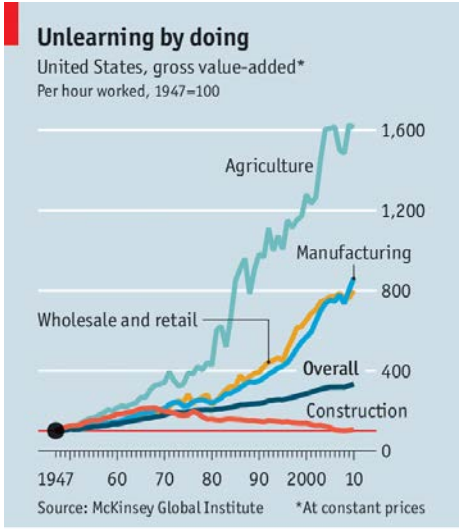
Sponsors of projects as PI/Co-PI

Section 1

CONSTRUCTION:
DISTRIBUTED COLLABORATION

1.1 Smart construction

- Construction is known as a "backward industry"
  - Low productivity, labor-intensive (*v.s.* aging workers)
  - Fatality, occupational hazards, management (*e.g.*, cost overrun)
- A consensus of global research institutes (e.g., Harty et al., 2007)
  - Effective (productive, automatic, age friendly) and efficient (safer, profitable, on-time, sustainable) industry
- Construction smartization with new *Information Tech.*
  - Computing power
  - New devices
    - RFID, LiDAR, GPS, UAV, smart phones…
  - New technologies
    - BIM, GIS, CV, VR/AR, blockchain, …

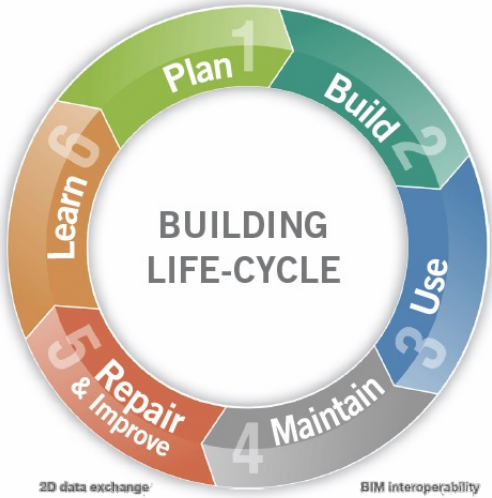


USA's gross value-added by sectors
source: economist.com

Recent advances in IT

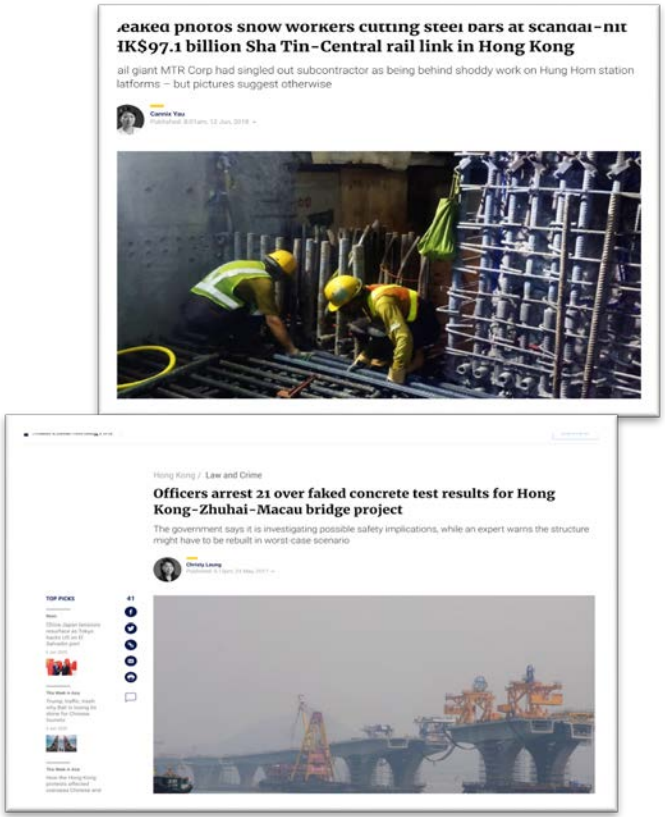
1.1 The distributed collaboration to smartize

- Multi-stage construction life cycle
  - Architectural design
  - Engineering design
  - Construction
  - Operation & maintenance
  - Demolition
- Many stakeholders
  - Even more decision makers, professionals
  - Teaming → Coordination→ Collaboration
- Distributed collaboration
  - Spatially and Temporally
  - Semi-controlled working environment



1.2 What if collaboration fails?

- Undermined project quality
- Overrun project period
- Harmed peers' benefits
- Even scandals
  - 2018: Faked screwing of steel bars into couplers, by cutting them shorter for an illusion
  - 2017: Faked concrete test results for Hong Kong-Zhuhai-Macau bridge project
- Because, in the project organization
  - Conflicts of interest exist as always
  - Physically distributed, hard to manage
  - The culture encourages covering small problems up



Two recent scandals in Hong Kong (Source: SCMP)

Section 2

BLOCKCHAIN: DISTRIBUTED TRUSTWORTHY DATABASE

2.1 What is a blockchain?

- Blockchain **区块链**
  - Linked-list-like incremental Block data storage systems
    - Saved distributed, identically on each "node"
    - Verified by "miners" for rejecting Attack
    - Each "solved" Block becomes immutable
  - Less related to Bitcoin **比特币**, Ethereum **以太坊**, ….
  - By generation
    - Blockchain 1.0; 2.0; 3.0; 4.0 (?) ...
- Three old components "wine" in any blockchain "bottle"

Sect. 2.2 ▣ Consensus mechanisms (1990s) **新瓶旧酒？鸡尾酒?**

Sect. 3.1 ▣ Distributed storage (1970s)

Sect. 3.2 ▣ Cryptographic tools (1990s) / smart contract (1990s)

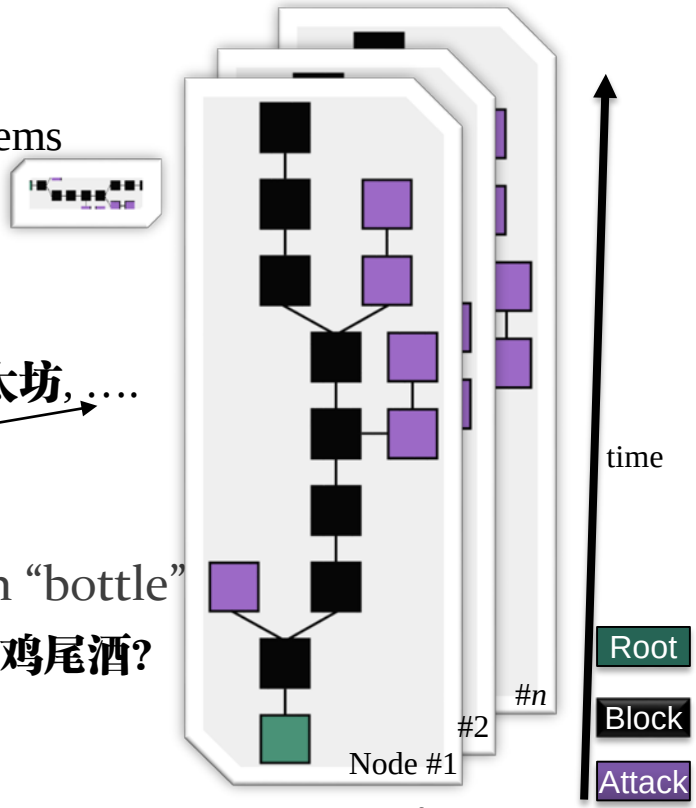


Diagram of a blockchain (miners hidden)

2.2 PoW consensus: Invented against Email spam

- Email spam, junk email
  - Appeared in early 1990s
  - 90+% world emails were spam by 2014
  - Reason 1: Spamming cost ~ 0;
  - Reason 2: Assuming-people-are-good Email protocols
- Dwork & Naor (1992): 'Proof of computational efforts'

计算量证明

  - "If I don't know you and you want to send me a message, then you must prove that you spent, say, ten seconds of CPU time, just for me and just for this message." (Dwork et al. 2003)
- Jakobsson & Juels (1999): 'Proof of work'

工作量证明

  - Where a prover demonstrates to a verifier that he has expended a certain level of computational effort in a specific time interval

2.2 PoW consensus: On hard-to-solve, easy-to-check math problems

- Sudoku puzzle
  - Each column, each row, and each of the nine 3×3 grids
    - All nine digits (1-9)
  - Hard to solve, easy to check
  - Nondeterministic Polynomial time-Complete (NPC) when $n > 3$
- And Max clique, Boolean satisfiability, Subset sum, …
  - NPC
- And, e.g., hashcash PoW (Back 1997; 2002)
  - PUBLIC: $H()$, k
    - *k: difficulty*
  - MINT: solving = $O(2^k)$ complexity
  - VALUE: checking = $O(k)$ complexity

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

PUBLIC:	hash function $\mathcal{H}(\cdot)$ with output size k bits
$\mathcal{T} \leftarrow \text{MINT}(s, w)$	**find** $x \in_R \{0,1\}^\star$ **st** $\mathcal{H}(s\|\|x) \overset{\text{left}}{=}_w 0^k$ **return** (s, x)
$\mathcal{V} \leftarrow \text{VALUE}(\mathcal{T})$	$\mathcal{H}(s\|\|x) \overset{\text{left}}{=}_v 0^k$ **return** v

2.2 PoW consensus: How it works

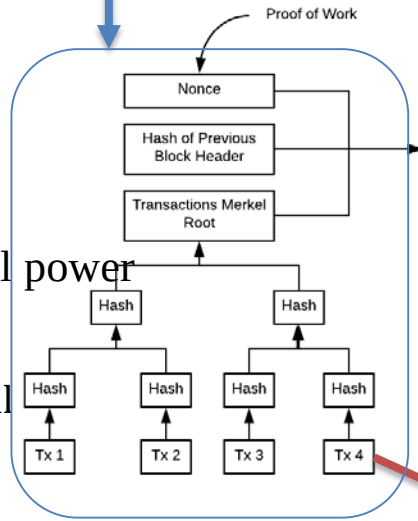
- Proof of work (PoW) 工作量证明
  - A class of consensus
  - Sender / prover / miner side
    - Hard to solve (e.g., Soduko, hashing, …)
  - Server / verifier / node side
    - Easy to check
- Examples
  1. Hashcash PoW (Back 1997; 2002)
     - X-Hashcash: 1:52:380119:calvin@comics.net:::9B760005E92F0DAE
     - $ echo -n 1:52:380119:calvin@comics.net:::9B760005E92F0DAE | openssl sha1

       $ **00000000000000**756af69e2ffbdb930261873cd71 (✓ correct; 13 hex (52 binary) 0s in <1us)
  2. Email attaches a key to the Sudoku's initialized by sender + content + Email time

2.3 Nakamoto (2008)'s Bitcoin (Blockchain 1.0)

- Bitcoin is a typical application of BC
- Immutable
  - 1 block = many transactions
  - 1 trans = 1 sender + 1 receiver + amount
- Anonymous
  - Hash "wallets"
- Secure (and expensive)
  - ~ 125EH/s (1.2 $\times 10^{20}$ H/s) computational power
  - ~100TWh/year
    - 2 × Google, 4 × Ireland, or US$10B bill
- Decentralized (pseudo?)
  - But, > 65% in China, > 35% in Xinjiang (Gogo 2020)

Number	Hash	Time	Transactions	Total BTC	Size (kB)
356987	141a6f95b2...	2015-05-18 13:28:14	1714	17353.00313324	749.227
356986	13cff723ec...	2015-05-18 13:11:53	2114	23805.24520712	749.204
356985	1128aa2601...	2015-05-18 12:27:49	594	6119.90095486	392.306
356984	140b0f27b9...	2015-05-18 12:20:14	1087	7849.33374079	544.102
356983	d1ea5bc1c7...	2015-05-18 12:08:01	830	7799.27270534	455.006
356982	76634b52be...	2015-05-18 11:58:42	221	1706.08443753	152.745



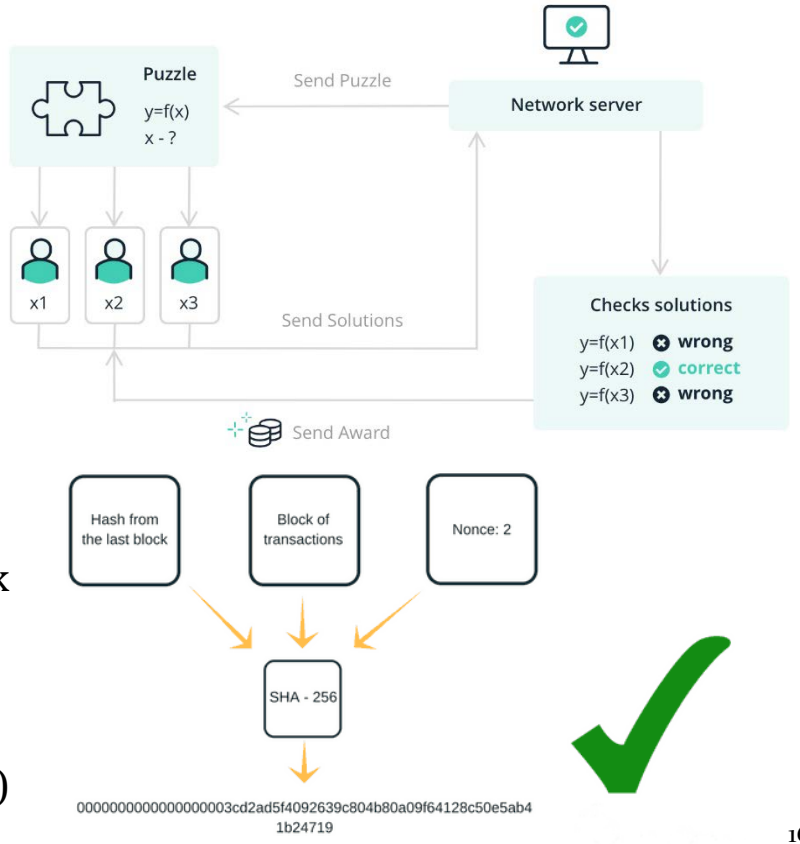
Cryptographic Hash Function such as SHA-256 → **Hash with Difficulty Target**

LATEST TRANSACTIONS

1isA21Xgj7Uw	1l62Tqm53p5	0.011
1BOB13hEMr4...	1ANNA8c1x37...	3.000 BTC
1r6q8G84Kt51...	1b93lJfV2aQ2...	12.345 BTC
1s62Tqn53p9...	1p12qo29w83...	0.639 BTC
1bF90Se24Tiu...	1k430f2jGG5s...	0.730 BTC
1eb4He3kL2o1...	1pASdmG34G...	0.067 BTC
17aS3nef3l7er...	1S4nf7a947lh...	15.230 BTC

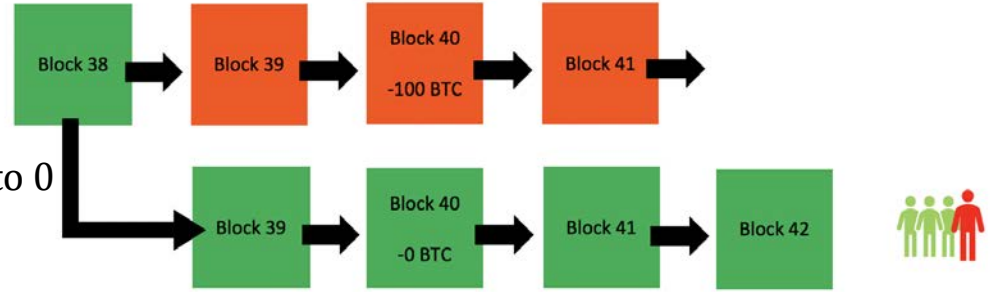
2.3 Bitcoin's consensus: Hashcoin PoW

- A "miner" is a prover
  - Solves the hashcash PoW
    - Data content = trans + hash pointer
    - Return 'nonce' to server
  - Receives reward as BTC
- Server / validator
  - Collects and packs transactions
  - Opens a puzzle for millions of machines
    - Flexible difficulty: every 10 mins per block
  - Awards the winner with 6.25 BTC (now)
- The ledger (> 200 GB now)
  - Live on millions of devices (Space redundant)



2.3 PoW's cons: 51% attack and more

- A malicious miner
  - Tries to modify transactions
    - E.g., change his/her -100 BTC to 0
    - (by US$1M goods for free)
  - Can succeed if > 50% computing power
- Other cons
  - Competitiveness between miners
    - Root cause of 51% attack
    - Too much energy cost
  - 21 million hard cap BTC
  - Easy coins before 2010
    - 97% bitcoins were held by 4% of addresses
    - Regardless of those unregistered

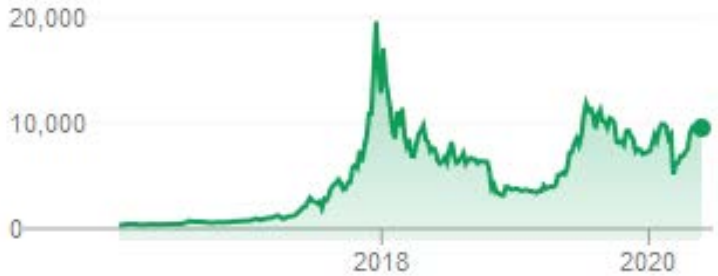


PoW 51% Attack Cost

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash
Bitcoin	BTC	$123.38 B	SHA-256	33,511 PH/s	*$582,622*	2%
Ethereum	ETH	$52.58 B	Ethash	216 TH/s	*$364,099*	3%
Bitcoin Cash	BCH	$15.79 B	SHA-256	4,013 PH/s	*$69,773*	13%
Litecoin	LTC	$6.47 B	Scrypt	309 TH/s	*$65,298*	7%
Monero	XMR	$2.51 B	CryptoNightV7	370 MH/s	*$20,048*	14%
Dash	DASH	$2.39 B	X11	2 PH/s	*$17,106*	27%
Ethereum Classic	ETC	$1.50 B	Ethash	6 TH/s	*$10,344*	89%
Bytecoin	BCN	$986.84 M	CryptoNight	164 MH/s	$637	219%
Zcash	ZEC	$933.60 M	Equihash	458 MH/s	*$50,028*	24%

2.4 Blockchain as a distributed trustworthy technology

- Some characteristics meet smart construction requirements
  - Immutability
  - Distributedness
  - Transparency
  - Security
- Blockchain is not equal to “crypto-currency” (not currency)
  - Good medium of exchange ✓
  - Poor store of value ✗
    - See the right picture
  - Inappropriate unit of account ✗
    - Countless new ‘coins’ (> 5,000 now)



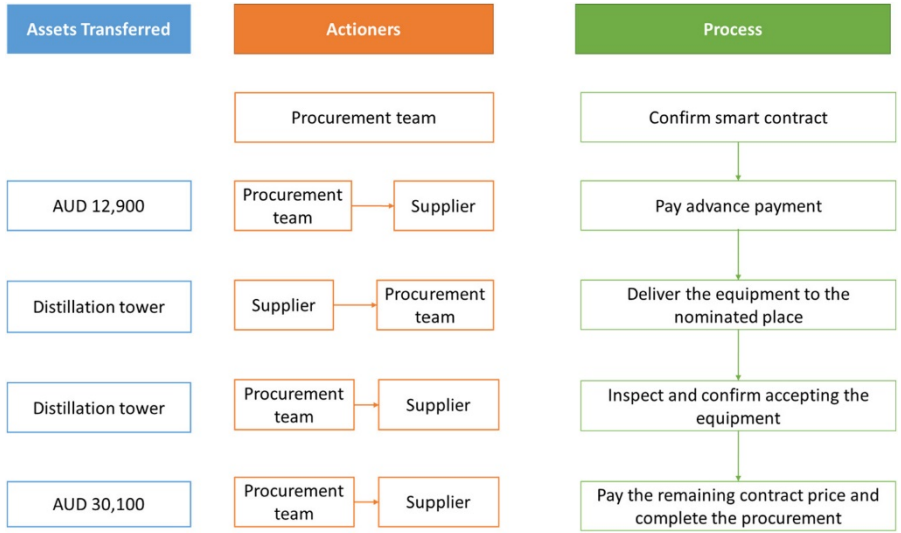
Bitcoin price

Section 3

TWO CASES

3.1 Case 1: Blockchaining supply chain (Yang et al. 2020)

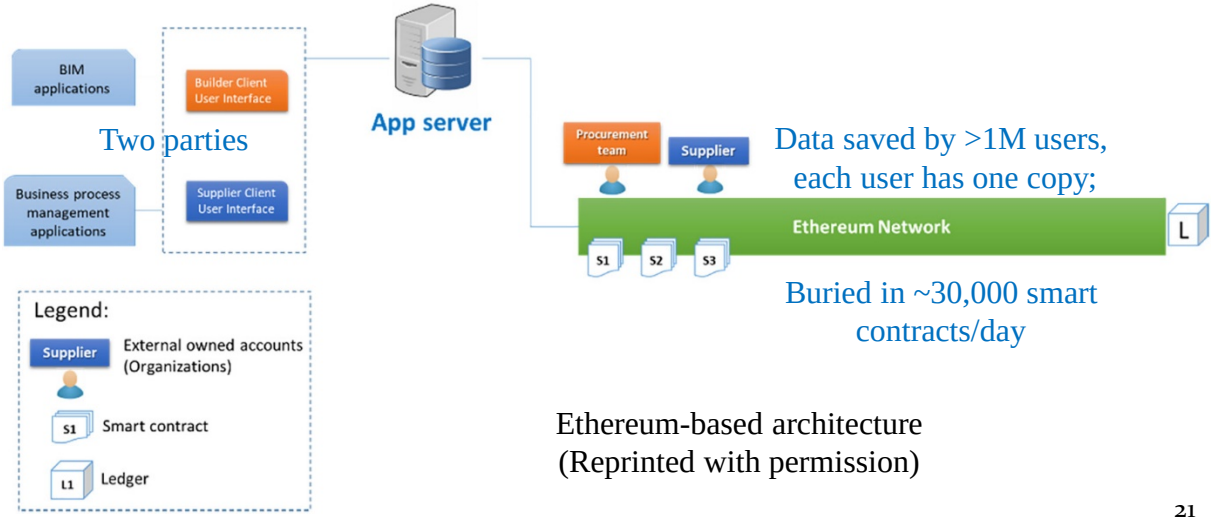
- Construction supply chain
  - Multi-stakeholder, distributed
  - Having possible trust/compliance problems
  - Involving payment, quality assurance
- Yang et al.'s (2020) example
  - Purchasing a distillation tower
  - In five steps
- Objective
  - Blockchaining the procurement
    - E.g., "pay AU$ 30,100"
  - On Ethereum (Blockchain 2.0)



Processing of purchasing construction equipment
(Reprinted with permission)

3.1 Data storage: From two parties to >1 million

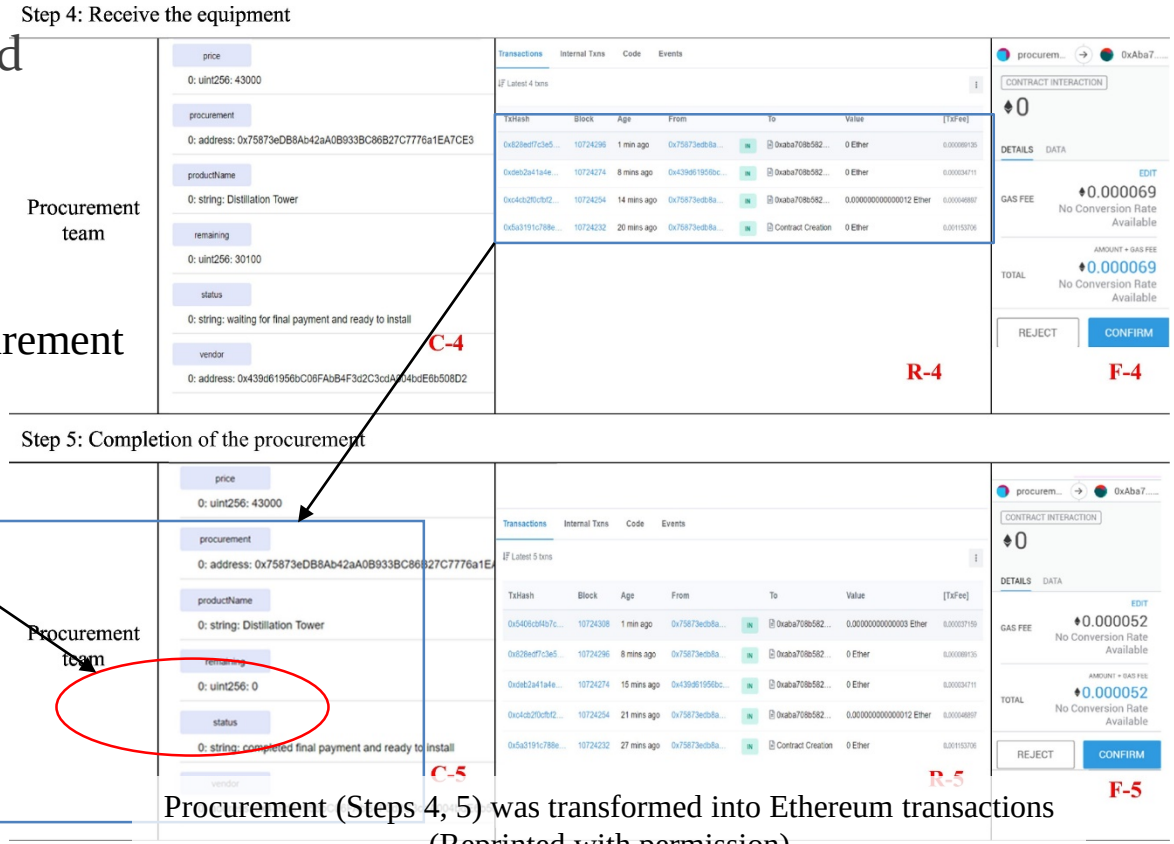
- Smart contact
  - Modeled in “App server”
  - A “World state” computer in a Ethereum “virtual machine”
- Data in the application layer (top left)
  - Two parties
  - 6 world states, 5 steps
- In Ethereum layer
  - > 1M user (data copies)
  - ~ 30,000 similar smart contracts per day



Ethereum-based architecture
(Reprinted with permission)

3.1 ETH transactions under the hood

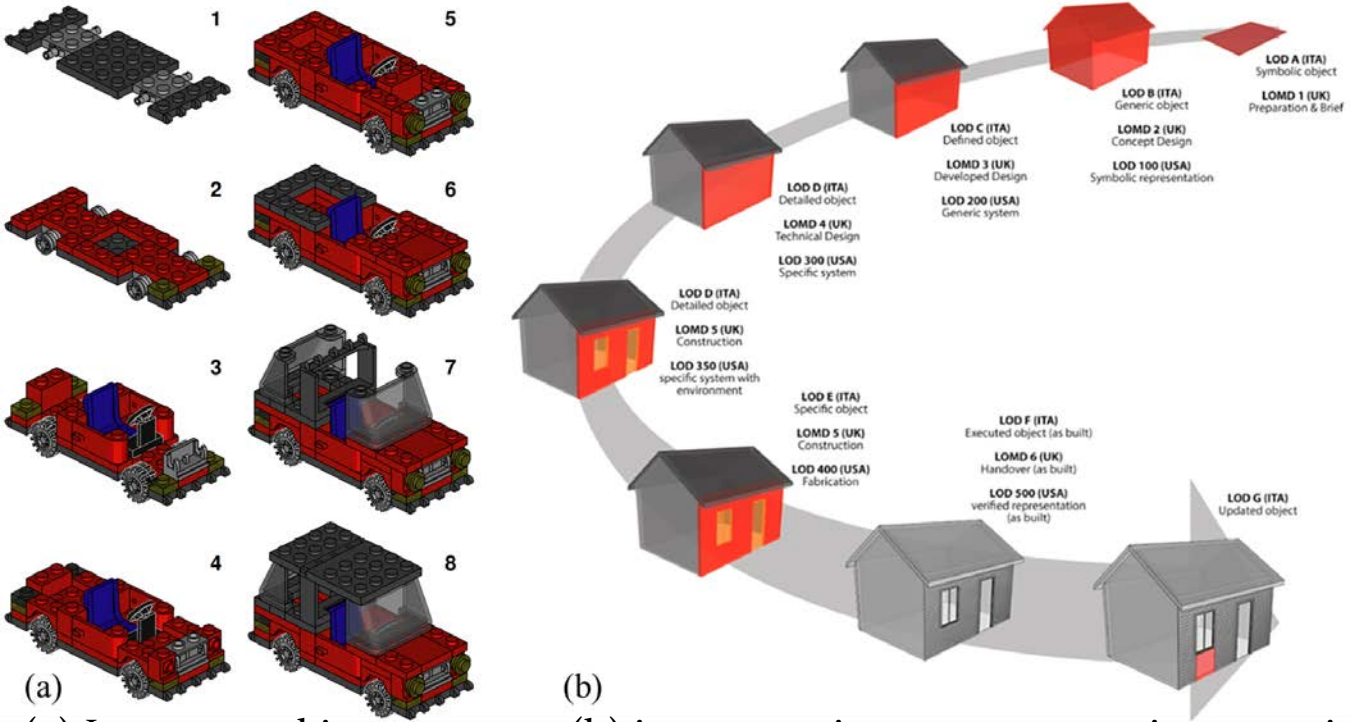
- Each step is transformed
  - To a ETH transactions
- ETH's Transaction fee
  - ~HK$0.1 / step
  - ~HK$0.5 for each procurement
- Note:
  - Payment was offline



Procurement (Steps 4, 5) was transformed into Ethereum transactions (Reprinted with permission)

3.2 Case 2: Blockchaining BIM changes (Xue & Lu, 2020)

- Rome wasn't built in a day; so wasn't BIM.



(a) Incremental in geometry, (b) in geometric + non-geometric semantics (Ellis 2019)

3.2 Semantic differential transaction of local BIM

- IFC (Industry Foundation Classes)
  - The best open BIM standard
  - STEP (Standard for the Exchange of Product Data) format
  - Clear, [hardly] readable
  - But massive, involving many random global IDs
- Our in-house program for the semantic difference tra

procedure compute_SDT
input: ifc_0, ifc_1 // IFC changed between t_0 and t_1

1 $\sigma_0 \leftarrow$ semantic_interoperability (ifc_0); // To call "semantic interoperability"
2 $\sigma_1 \leftarrow$ semantic_interoperability (ifc_1);
3 $\sigma^* \leftarrow \sigma_0 \cap \sigma_1$; // The intersection (unchanged) tree
4 $\sigma_{0c} \leftarrow \sigma_0 - \sigma^*$; // To purge the unchanged instances
5 $\sigma_{1c} \leftarrow \sigma_1 - \sigma^*$;
6 $\Delta_\sigma \leftarrow$ tree_diff (σ_{0c}, σ_{1c}); // Difference between changed objects
7 **return** Δ_σ

(Xue & Lu 2020)

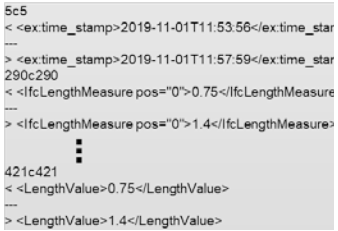
Example IFC

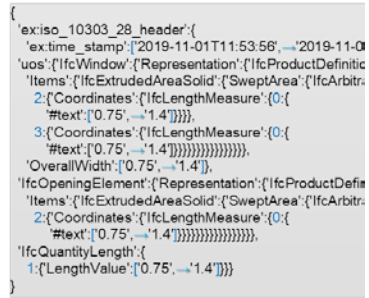
```
ISO-10303-21;
HEADER;
FILE_DESCRIPTION(('ViewDefinition [CoordinationView, …);
FILE_NAME('example.ifc','2008-08-01T21:53:56',('Architect…);
FILE_SCHEMA(('IFC2X3'));
ENDSEC;
DATA;
#1=IFCOWNERHISTORY(#84,#71,$,.ADDED.,$,$,$,1217620436);
#2=IFCAXIS2PLACEMENT3D(#11,#4,#8);
#3=IFCCARTESIANPOINT((0.0,0.0));
#4=IFCDIRECTION((0.0,0.0,1.0));
#5=IFCGEOMETRICREPRESENTATIONCONTEXT($,'Model',3,1.0E-5,#75,$);
#6=IFCWALLSTANDARDCASE('3yB2YO$MX4xv5uCqZZG05x',#1,'Wall …);
#7=IFCWINDOW('0LV8Pid0X3IA3fLVDPidY',#1,'Window xyz',’…);
#8=IFCDIRECTION((1.0,0.0,0.0));
#9=IFCOPENINGELEMENT('2LcE70iQb51PEZynawyvuT',#1,'Opening …);
#10=IFCCARTESIANPOINT((0.75,0.0));
#11=IFCCARTESIANPOINT((0.0,0.0,0.0));
#12=IFCCARTESIANPOINT((0.0,0.3));
#13=IFCORGANIZATION($,'TNO','TNO Building Innovation',$,$);
#14=IFCPROPERTYSINGLEVALUE('AcousticRating','AcousticRating',…);
#15=IFCPROPERTYSINGLEVALUE('Reference','Reference',IFCTEXT(''),$);
#16=IFCPROPERTYSINGLEVALUE('FireRating','FireRating',IFCTEXT(''),$);
#17=IFCPROPERTYSINGLEVALUE('IsExternal','IsExternal',IFCBOOLEAN(.T.),$);
#18=IFCPROPERTYSINGLEVALUE('ThermalTransmittance',…);
#19=IFCQUANTITYLENGTH('Height','Height',$,1.4);
#20=IFCQUANTITYLENGTH('Width','Width',$,0.75);
#21=IFCLOCALPLACEMENT($,#2);
#22=IFCBUILDING('0yf_M5JZv9QQXly4dq_zvI',#1,'Sample Building',…);
#23=IFCBUILDINGSTOREY('0C87kaqBXF$xpGmTZ7zxN$',#1,…);
#24=IFCLOCALPLACEMENT(#21,#2);
…
END-ISO-10303-21;
```

3.2 SDT tests

- Changing a window's size

Input	Item	Line-by-line file comparison	The proposed SDT
IFC (7.4KB each)	Size (KB)	1.00	0.36
	Time (s)	0.041	0.003
	SH?*	×	✓
	Output	6 changed lines:	4 changed properties:
IFCXML (32.9KB each)	Size (KB)	0.56	0.89
	Time (s)	0.042	0.012
	SH?*	×	✓
	Output	6 changed lines:	6 changed properties:

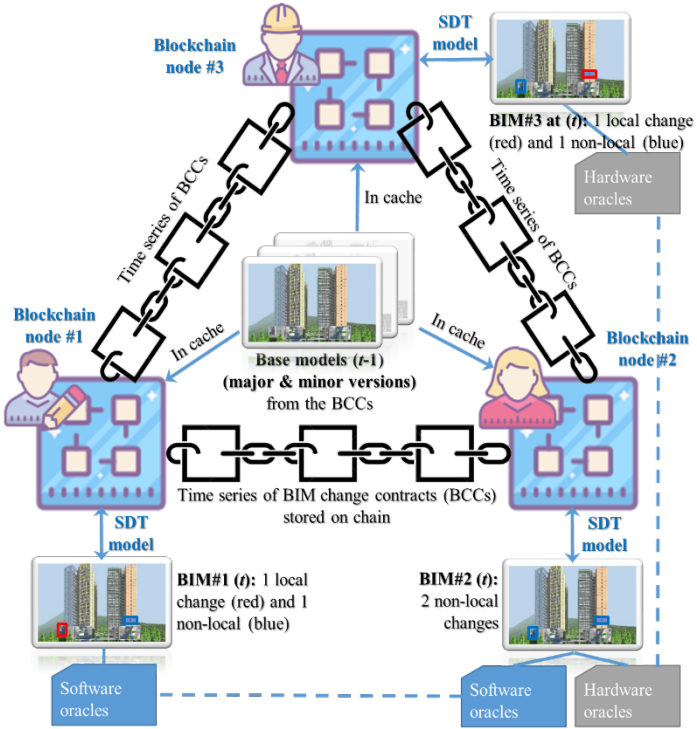




*: With semantic hierarchies?

3.2 BIM change contract as a smart contract

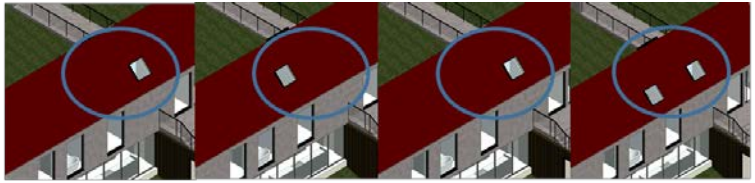
- BIM change contract (BCC)
  - BCC_t: All BIM changes at time t
    - $BCC_i = \bigoplus_n \sigma_i$
    - Note: $\bigoplus$ is the simplest operation for proof-of-concept
  - A BIM can be created from the model at t - 1 and changes at t
    - $ifc_t = ifc_{t-1} + BCC_t$.
  - BIM at any time can be recovered from base BIM and the chained BCCs
    - $ifc_t = ifc_0 + \Sigma_t\, BCC_i$.
- Data storage
  - Permissioned nodes, not public

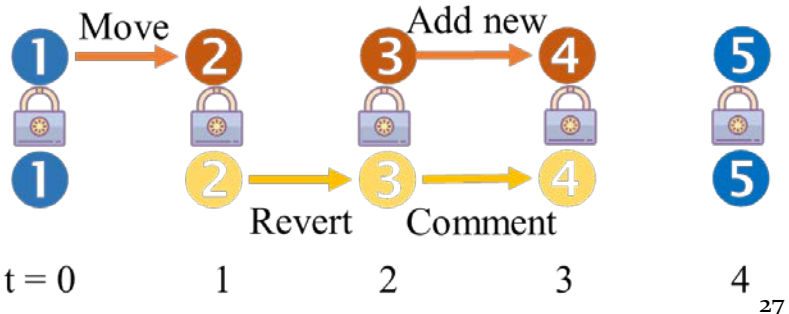


Permissioned blockchain architecture
(Reprinted with permission)

3.2 Another test case

- Autodesk Revit 2018's sample BIM (a modern villa, 27.4 MB in IFC)
- Sequential / simultaneous roof window changes
  - By two BIM users, from t = 0 to 4
  - $t_2 \rightarrow t_3$: Simultaneous changes by two users

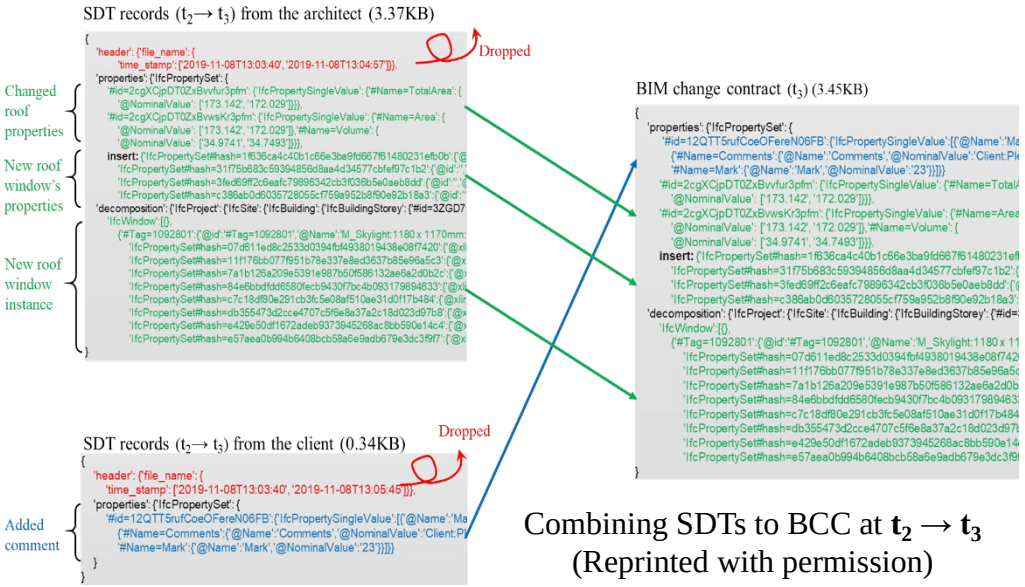




A test case
(Reprinted with permission)

3.2 SDT/BCC tests

- $t_2 \rightarrow t_3$
  - User A: Added a roof window
    - σ_A = top left block
  - User B: Added text comments to another window
    - σ_B = bottom left block
- BCC as the conflict-free merge
  - BCC = right block
- BCC is efficient (<0.02%)
  - 3.37KB out of 27.4MB IFC
  - Good for blockchaining

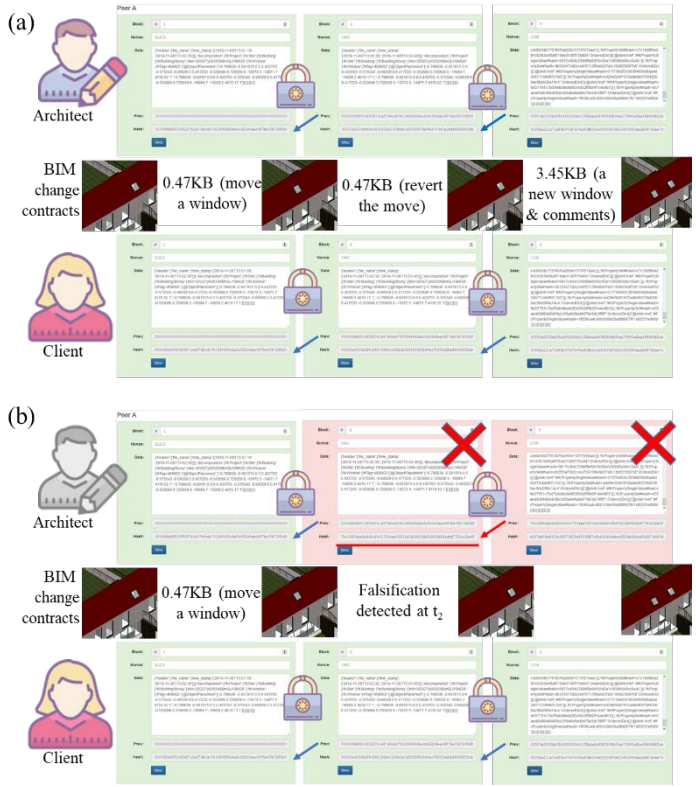


Combining SDTs to BCC at $\mathbf{t_2 \rightarrow t_3}$
(Reprinted with permission)

Input	Change	Line-by-line file comparison Size (KB) (lines)	Time (s)*	SH?#	The proposed BCC/SDT Size (KB)	Interop. time (s)*	SDT time (s)*	SH?#
IFC (27.4MB each)	$t_2 \rightarrow t_3$ (Arch.)	54,700 (533,923)	0.789	×	3.45	6.681	0.463	✓
	$t_2 \rightarrow t_3$ (Client)	53,900 (514,192)	0.756	×				

3.2 Blockchained BIM changes

- On a simplest blockchain
  - Web-based
  - Easy nonce
  - Visualized blocks
    - Green = verified; red = wrong / hacked
- BIM was immutable from
  - claiming false authorships,
  - destroying evidence, or
  - being hacked, etc.



3.3 Discussion

- Existing blockchain applications for smart construction
  - Works, e.g., blockchaining SCM and BIM changes
  - but preliminary and infantile
- The characteristics of blockchain are appropriate for construction
  - Immutability, transparency, security (e.g., data loss)
- Challenges ahead
  - Culture, regulation, governance
  - Cost and efficiency (e.g., not widely used to fight spams)
  - Security (e.g., business secrets, privacy)
  - Understanding and acceptance

References

- Back A. (1997). Hashcash. http://www.cypherspace.org/hashcash/
- Back A. (2002). Hashcash—A Denial of Service Counter-Measure. http://www.hashcash.org/hashcash.pdf
- Brambilla, G., Amoretti, M., & Zanichelli, F. (2016). Using blockchain for peer-to-peer proof-of-location. *arXiv preprint arXiv:1607.00174*.
- Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. In *Annual International Cryptology Conference* (pp. 139-147). Springer, Berlin, Heidelberg.
- Dwork, C., Goldberg, A., & Naor, M. (2003). On memory-bound functions for fighting spam. In *Annual International Cryptology Conference* (pp. 426-444). Springer, Berlin, Heidelberg.
- Ellis, M. (2019, July 12). *Level of Detail or Development: LOD in BIM*. Retrieved November 6, 2019, from REBIM: https://rebim.io/level-of-detail-or-development-lod-in-bim/
- Harty, C., Goodier, C. I., Soetanto, R., Austin, S., Dainty, A. R., & Price, A. D. (2007). The futures of construction: a critical review of construction future studies. Construction Management and Economics, 25(5), 477-493
- Gogo, J. (2020). 65% of Global Bitcoin Hashrate Concentrated in China, Blockchain News, https://news.bitcoin.com/65-of-global-bitcoin-hashrate-concentrated-in-china/
- Jakobsson, M., & Juels, A. (1999). Proofs of work and bread pudding protocols. In *Secure information networks* (pp. 258-272). Springer, Boston, MA.
- Xu, J., Chen, K., Zetkulic, A. E., Xue, F., Lu, W., & Niu, Y. (2019). Pervasive sensing technologies for facility management: A critical review. *Facilities*.
- Xue, F., & Lu, W. (2020). A semantic differential transaction approach to minimizing information redundancy for BIM and blockchain integration. *Automation in Construction*, *118*, 103270.
- Xue, F., Guo, H., & Lu, W. (2020). Digital twinning construction objects: Lessons learned from pose estimation methods. In *The Joint Conference ICCCBE and CIB W78 2020*.
- Xue, J., Shen, G.Q., Yang, R.J., Wu, H., Li, X., Lin, X., & Xue, F. (2020). Mapping the knowledge domain of stakeholder perspective studies in construction projects: A bibliometric approach. *International Journal of Project Management 38* (6), 313-326.
- Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., ... & Chen, S. (2020). Public and private blockchain in construction business process and information integration. *Automation in Construction*, *118*, 103276.

If you want to go fast, go alone.
If you want to go far, go together.
— *African proverb*

Q&A