香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

Towards Searchable and Verifiable Blockchain

PI : **Prof. XU Jianliang**

Funding Scheme: **General Research Fund**
Project Ref. No.: **12201018**
Amount Awarded (to HKBU): **HK$693,000**
Project Period: **Jan 2019 - Dec 2019**

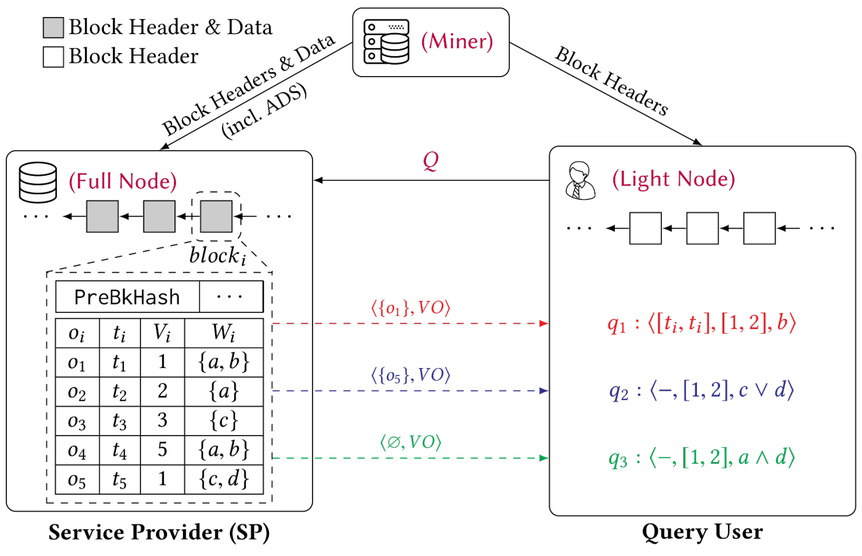
OBJECTIVES

1. To design a framework for blockchain to alleviate the storage and computing costs of the user and support verifiable Boolean range queries to guarantee the results' integrity.
2. To design an efficient index structure that supports range queries with integrity assurance in a hybrid-storage blockchain framework.

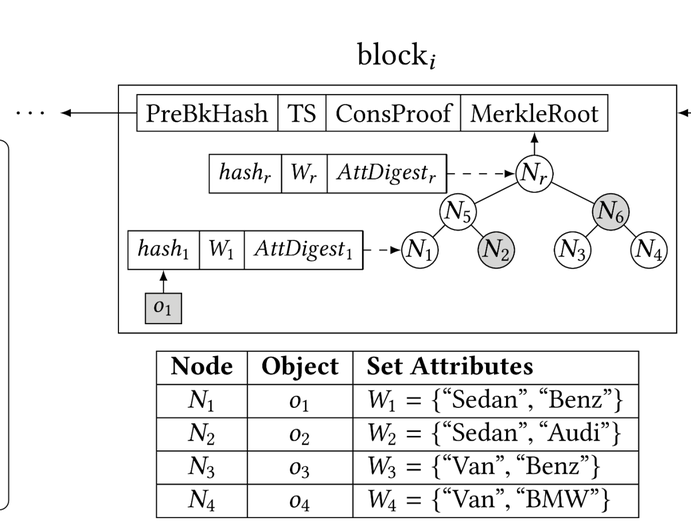
HIGHLIGHTS

vChain: Enabling Verifiable Boolean Range Queries over Blockchain Databases

- Investigate the verifiable query processing over blockchain databases.
- To support verifiable Boolean range queries, propose an *accumulator-based authenticated data structure* that enables dynamic aggregation over arbitrary query attributes.
- Design two new indexes to further aggregate intra-block and inter-block records for efficient query verification.
- Develop an inverted prefix tree structure to accelerate the processing of a large number of subscription queries simultaneously.

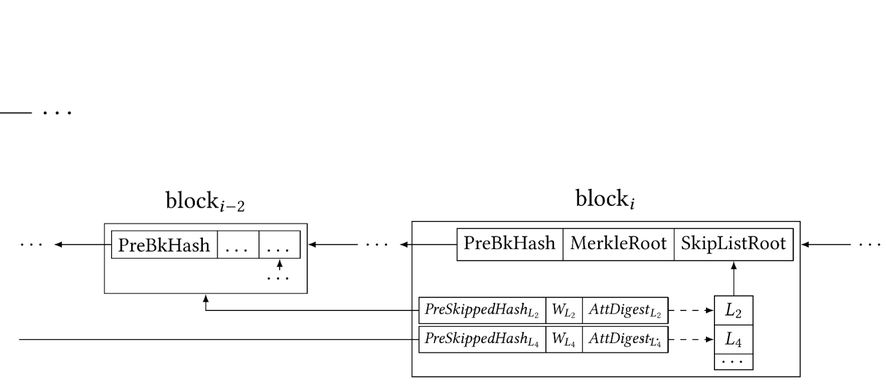


System Model of vChain



Node	Object	Set Attributes
N_1	o_1	W_1 = {"Sedan", "Benz"}
N_2	o_2	W_2 = {"Sedan", "Audi"}
N_3	o_3	W_3 = {"Van", "Benz"}
N_4	o_4	W_4 = {"Van", "BMW"}

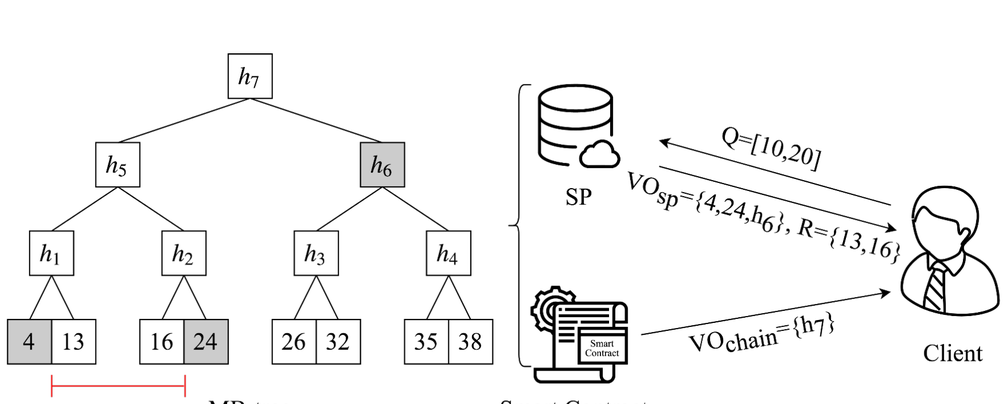
Batch Verification: Intra-Block Index



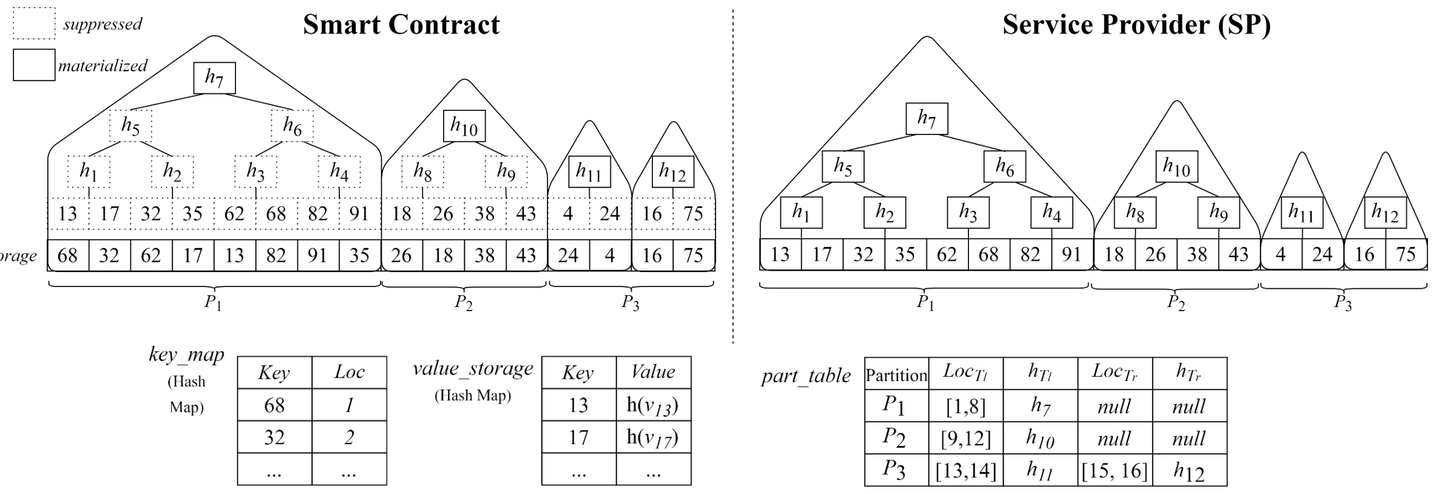
Batch Verification: Inter-Block Index

GEM²-Tree: A Gas-Efficient Structure for Authenticated Range Queries in Blockchain

- Study the authenticated range queries in the hybrid-storage blockchain.
- Leverage the blockchain smart contract and the Service Provider to both maintain the authenticated data structure.
- Design an authenticated data structure GEM²-Tree that can be efficiently maintained by the blockchain in terms of gas cost.
- Propose an optimized structure GEM²*-Tree to further reduce the maintenance cost without sacrificing much the query performance.



Authenticated Query Framework in Hybrid-Storage Blockchain



key_map (Hash Map)

Key	Loc
68	*1*
32	*2*
...	...

value_storage (Hash Map)

Key	Value
13	h(v_{13})
17	h(v_{17})
...	...

part_table

Partition	Loc_{T_l}	h_{T_l}	Loc_{T_r}	h_{T_r}
P_1	[1,8]	h_7	*null*	*null*
P_2	[9,12]	h_{10}	*null*	*null*
P_3	[13,14]	h_{11}	[15, 16]	h_{12}

Overall Structure of GEM²-Tree with Hybrid Storage

SELECTED PUBLICATIONS

1. C. Xu, C. Zhang, and J. Xu. "vChain: Enabling Verifiable Boolean Range Queries over Blockchain Databases." Proc. the ACM SIGMOD International Conference on Management of Data (SIGMOD '19), Amsterdam, Netherlands, 2019.
2. C. Zhang, C. Xu, J. Xu, Y. Tang, and B. Choi. "GEM²-Tree: A Gas-Efficient Structure for Authenticated Range Queries in Blockchain." Proc. the 35th IEEE International Conference on Data Engineering (ICDE '19), Macau SAR, China, 2019.