块时候都要查询几百万的账户;

3) 在一个实际的金融系统,建块必须是高速的.建块高速,建的块也多,而每次建块都要查询链上代码并且加以执行,执行完下一块才能开始建[34].这就变成很难的任务.

金融链上代码需求:

1) 链上代码必须考虑长时间的合约,因为这是市场的需求;
2) 建块必须是高速的,因为这也是市场的需求;
3) 链上代码必须经过软件工程分析、测试、验证通过,例如使用形式化方法、仿真等方式;
4) 链上代码必须经过法律上的验证.

根据以上的需求,本文提出下列原则:

- 原则 A:一个功能可以写在应用系统中或者链上代码里,在绝大多数的环境,尽量在应用系统中解决;
- 原则 B:绝大多数的链上代码都应该不需要查询就能够被发现需要执行;
- 原则 C:每个账户的链上代码都只能够处理自己的账户或是少数相关的账户;
- 原则 D:大多数的链上代码都能够迅速地完成;
- 原则 E:长时间的链上代码,可以存中间的数据在中间的区块中.

所以,链上代码要有局部性(partial)、地方性(localized)、限时性(limited time span)、针对性(specific)才能实用.例如,这段代码只与某个账号有关系、每天下午 5 点执行、仅限制某些交易.在央视的微电影系统里,所有的点击、交易都不使用链上代码,但是分账使用链上代码.因为大部分的点击不需要分账,大部分情况下,链上代码不会被执行,所以符合原则 A.每次分账都是因为点击才产生的,因而每次建块不需要查询哪一个账户的链上代码需要执行,只有被点击的账户需要查询链上代码是否需要执行,这就符合原则 B.分账符合原则 C,也符合原则 D.原则 E 指出,长时间的链上代码要有一个复杂的机制来处理,例如,另外有一个区块链来存链上代码出的中间数据.

## 4 总结与展望

本文从区块链构成要素、应用特征开始,讨论区块链需求,包括一致性需求、软件设计需求、可扩展性需求、数据库需求和链上代码需求.在此基础上设计了北航链的体系架构.首次提出了开放式区块链连接器 OBCC,并实现了 Java 版的区块链连接器——JBCC.该 JBCC 已经支持多个区块链的应用系统的开发,具有开发周期短、可扩展性高、运行速度快的特点.为使区块链能够应用于金融业,介绍了由作者提出的双链模型,即 ABC 和 TBC.满足通信量庞大,快速响应、账户信息隐私的需要.本文讨论了链上代码面临法律合法性、代码可信性、执行安全性和外部信息共识等许多问题.

**References**:

[1] 国家密码管理局公告(第 23 号).2012. http://www.oscca.gov.cn/News/201204/News_1229.htm
[2] Ed25519: High-speed high-security signatures. http://ed25519.cr.yp.to
[3] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems (TOPLAS), 1982,4(3):382−401. [doi: 10.1145/357172.357176]
[4] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proc. of the USENIX Association. 1999. 173−186.
[5] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
[6] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012.
[7] Ethereum Whitepaper. https://github.com/ethereum/wiki/wiki/White-Paper
[8] Bitcoin traffic bulletin. http://hashingit.com/analysis/34-bitcoin-traffic-bulletin
[9] Bitcoin traffic bulletin (redux). http://hashingit.com/analysis/44-bitcoin-traffic-bulletin-redux
[10] 蔡维德,赵梓皓,张弛,郁莲.英国央行数字货币 RSCoin 探讨.金融电子化,2016,(10):78−81.
[11] Hyperledger whitepaper-wg. https://wiki.hyperledger.org/groups/whitepaper/whitepaper-wg

[12] UK Government Chief Scientific Adviser. Distributed ledger technology: Beyond block chain, UK government office for science. 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[13] Veena P, Ahluwalia G, Panikkar S. An Economy of Things—A Visionary Architecture and Monetization of Devices with Blockchain. IBM Inter Connect, 2016.

[14] McConaghy T, Marques R, Müller A, De Jonghe D, McConaghy TT, McMullen G, Henderson R, Bellemare S, Granzotto A. BigchainDB: A Scalable Blockchain Database. 2016.

[15] Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895, 2015.

[16] 蔡维德,罗佳.浅析私有区块链技术.2016. http://sanwen8.cn/p/1efjDL3.html

[17] Tsai WT, Blower R, Zhu Y, Yu L. A system view of financial blockchains. Service-oriented System Engineering, 2016. 450−457. [doi: 10.1109/SOSE.2016.66]

[18] Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proc. of the 1st Int'l Conf. on P2P'01. IEEE, 2001. 101−102. [doi: 10.1109/P2P.2001.990434]

[19] Bandara HMND, Jayasumana AP. Collaborative applications over peer-to-peer systems—Challenges and solutions. Peer-to-Peer Networking and Applications, 2013,6(3):257−276. [doi: 10.1007/s12083-012-0157-3]

[20] 蔡维德.以系统观念来看区块链.2016. http://finance.sina.com.cn/money/bank/bank_hydt/2016-08-23/doc-ifxvcsrm2277962.shtml

[21] Nomura Research Institute, Ltd. NRI to conduct proof of concept for applying blockchain technology to banking. 2015. https://www.nri.com/global/news/2015/151216_1.aspx.2015

[22] Pinna A, Ruttenberg W. Distributed Ledger Technologies in Securities Post-Trading. 2016.

[23] 郁莲,邓恩艳.区块链技术.中国计算机学会通讯,2017,13(5):10−15.

[24] Haerder T, Reuter A. Principles of transaction-oriented database recovery. ACM Computing Surveys (CSUR), 1983,15(4):287−317. [doi: 10.1145/289.291]

[25] Gray J. The transaction concept: Virtues and limitations, 1981,81:144−154.

[26] Gray J, Reuter A. Transaction Processing: Concepts and Techniques. Elsevier, 1992.

[27] Brewer E. Towards robust towards robust distributed systems. In: Proc. of the 19th ACM Symp. on Principles of Distributed Computing. 2000. [doi: 10.1145/343477.343502]

[28] Gilbert S, Lynch N. Brewer's conjecture and the feasibility of consistent. In: Proc. of the Available, Partition-Tolerant Web Services. 2015.

[29] Kung HT, Robinson JT. On optimistic methods for concurrency control. ACM Trans. on Database Systems, 1981,6(2):213−226. [doi: 10.1145/319566.319567]

[30] Bernstein PA, Goodman N. Multiversion concurrency control—Theory and algorithms. ACM Trans. on Database Systems 1983, 8(4):465−483. [doi: 10.1145/319996.319998]

[31] Delmolino K, Arnett M, Kosba A, Shi E. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. Berlin, Heidelberg: Springer-Verlag, 2016. 79−94. [doi: 10.1007/978-3-662-53357-4_6]

[32] Thomas S, Schwartz E. Smart oracles: A simple, powerful approach to smart contracts. 2014. https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts

[33] Hazard J, Hardjono T. CommonAccord: Towards a foundation for smart contracts in future blockchains. In: Proc. of the Blockchains and the Web: W3C Workshop on Distributed Ledgers on the Web. 2016.

[34] Yu L, Tsai WT, Li GN, Yao YF, Hu CJ. Smart-Contract Execution with Concurrent Block Building. In: Proc. of the 10th IEEE Int'l Symp. on Service-Oriented System Engineering, 2016.

**蔡维德**(1958－),男,四川庐县人,博士,教授,博士生导师,主要研究领域为区块链技术,软件工程,分布式系统,云计算与大数据.

**郁莲**(1963－),女,博士,副教授,主要研究领域为分布式计算,形式化方法,区块链技术,软件分析与验证.

**王荣**(1988－),男,硕士,主要研究领域为区块链,机器学习.

**刘娜**(1984－),女,讲师,主要研究领域为区块链,移动数据库.

**邓恩艳**(1972－),女,主要研究领域为区块链,软件工程.