These crypto lunatics know nothing about money, banking finance, monetary policy. They have zero financial literacy. And they pretend to reinvent money. A solution to a problem that doesn't exist. And a solution that is the return to the Stone Age of barter.
BLOCKCHAIN AND FIAT DIGITAL CURRENCY: THE FIRST STEP

Kang Chen
Computer Science and Technology
Tsinghua University
What’s in Blockchain?

Excel operations (represented as logs)

What is smart contract?

VBA program (run everywhere)
OUTLINES

• The Banking System
• Fiat Digital Currency
• Considerations
• Architecture: Tow Levels
• Discussion
THE CURRENT BANKING SYSTEM

• Different countries seem to have different banking system.
• Each country tends to have a central bank like agency.
• Governments have their department(s) to manage the banking system.
  • Central Bank.
  • Federal Reserve System.
WHY BANKING SYSTEM?

- Regulation

  - Why?
  - fraud prevention
  - anti-money laundering
  - anti-terrorism
  - anti-usury lending
  - deposit insurance
  - Important for financial healthy
  - A long history for protecting
  - None can be achieved by the current public blockchain based digital currency.
BANKING SYSTEM IN CHINA

- Two Levels of Banking System
- Central Bank and Commercial Bank
NOTE-ISSUING

• Based on some reasons (hopefully not at will), central bank (or maybe central government) wants to print some money.

• The money will be put to some accounts in the commercial banks.

• Then the money can be considered as running into liquidity.
M0, M1, M2

- M0: Cash, the money outside the banking system
- M1: M0 + Demand Deposit
- M2: M2 + Time Deposit
CBDC: CENTRAL BANK DIGITAL CURRENCY

• Why?
  • Actually, I don’t know why.
  • For maintaining the cash system, the government needs to spend about billion Yuan every year. If all digitalized, big save of cost.
  • Related to the third party payment. All your payment information can be collected by third party. CBDC wants to avoid such third party involvement.
  • And also related to deposit reserve.
CBDC: CENTRAL BANK DIGITAL CURRENCY

• Somewhat, it should exactly look like cash. It will be better to have the capability of offline payment.
  • Can we do offline payment? (Special hardware, replay attacks, secure monotonic counter).

• Payment system avoiding third-part. Unified payment. (no third-party to collect information, accessible to all payees.)

• Regulatable.

• Used for M0. M1, M2 are well supported by banking system (accounts).

• Maybe programmable money.
TWO LEVELS OF CBDC

Top Level
related to deposit reserve

Bottom Level
High performance payment system

Central Bank
Commercial Banks
Personal Company
DEPOSIT RESERVE

• Deposit Reserve: the money pool that belongs to a commercial bank but can not be used. The money in the pool is regulated by the central bank. And the ratio of the money in the pool to all the deposit is adjusted by the central bank. (usually 10%~20%). Why? control the leverage.

• Contract between the central bank to all the commercial banks.
TOP LEVEL: INSIDE BANKING SYSTEM
Central Bank keeps tracking the CBDC inside the banking system.
**TOP LEVEL: ACCOUNTING SYSTEM FROM CENTRAL BANK**

- Central Bank keeps tracking the CBDC inside the banking system

<table>
<thead>
<tr>
<th>Central Bank</th>
<th>CBDC Tracking</th>
<th>Banking System</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reclaim CBDC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>中央银行数字货币系统</td>
<td>管控审批</td>
<td>接收回笼通知</td>
</tr>
<tr>
<td>商业银行数字货	系统</td>
<td>提交CBDC</td>
<td>发起存款准备金调增</td>
</tr>
<tr>
<td>中央银行会计核算系统</td>
<td>回笼作废CBDC</td>
<td>通知回笼成功</td>
</tr>
<tr>
<td></td>
<td></td>
<td>其他发行基金至存款准备金</td>
</tr>
</tbody>
</table>
TOP LEVEL: ACCOUNTING SYSTEM FROM CENTRAL BANK

Transfer CBDC

<table>
<thead>
<tr>
<th>商业银行A数字货币系统</th>
<th>发起CBDC转移请求</th>
<th>银行库接收CBDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>商业银行B数字货币系统</td>
<td>银行库接收CBDC</td>
<td></td>
</tr>
<tr>
<td>中央银行数字货币系统</td>
<td>作废来源CBDC</td>
<td>生成去向CBDC</td>
</tr>
</tbody>
</table>
TECHNOLOGIES USED IN TOP LEVEL

- Blockchain? Maybe yes
- Synchronized Database
- PKI
- MIS system
- Marketing Platform (Interbank Offer Transaction, interbank lending and borrowing)
- BigData analysis tools (small data?)
BOTTOM LEVEL: THE PAYMENT SYSTEM

• The payment system is more crucial.
• Payment service for end users.
• Requirement?
  • Controllable Anonymity (Controllable?)
  • Programmable Money
  • Payment across multiple management domain (inter banks, interchange between banks and third-parties)
• High Performance (Scale-out Performance)
• High Availability
END USER: May support billions of users – Need very high performance. Tens of thousands of transactions per second.

Complex and sometimes contradict requirements: anonymity vs. regulation.

Compatible to the current banking system. Even need to support the third party payment system.

Programmable: like colored coin, for supporting dApps. (Need to support complete computation power?)
BUILD PAYMENT SYSTEM USING BLOCKCHAIN?

• Performance?
  • Throughput: 7TPS for BTC, 30TPS for Ethereum
  • Latency: 10 minutes for BTC, several minutes for Ethereum
  • Can be built fast (Hybrid Consensus, Algorand, Spectre, Phantom, Conflex). What about storage?
  • Off-chain payment: like lightening network. But, why you need to build payment path?

• Regulation
  • Public blockchains are born to be non-regulatable.
  • Central Bank needs to know the cash flow. But not for third party or commercial banks.

• Currently may not be suitable for CBDC.
AVOIDING USING ACCOUNT SYSTEM

• Teller may know the purchase information. Even the bank does not want to know.
• Similar like the current banking system, third party payment.
• Payment information known to the providers.
• Not like cash.
• But how?
  • Using UTXO. (Unspent Transaction Out). Borrow from BitCoin. At least pseudo anonymous.
  • Exist some other forms that avoid using account names.
  • May use Zero Knowledge prove. (Complex, and you still need to consider regulation.)
UTXO

A → A ¥5000
A → A ¥2000
A → A ¥3000

A → B ¥2000
B → A ¥3000
C → A ¥2000

B → A ¥5000
A → D ¥5000
C → A ¥3000

B → A ¥2000
C → A ¥2000
D → A ¥3000
A → E ¥3000
A → D ¥3000
HIGH PERFORMANCE: SCALE OUT

• BlockChain not scalable. More machines, slower.
• We have solutions in traditional distributed system. Sharding!
PROGRAMMABLE MONEY

• Using either filters or smart contracts.
• Filters: the transaction can have attached information about what kind of filters before spending the money. The filters will be an additional criteria to check before making the payment valid.
• Smart Contracts: the money will be sent to a smart contract (maybe multiple smart contracts). Without global state and generalized blockchain (operation logs), smart contracts are not used. (May support in future.)
APPLICATIONS OF PROGRAMMABLE MONEY

- Only staff, professors and students can have meals in dining halls in a university.
- You can issue some special money tagged with additional information (like issued by the administrator of the university). And then, the POS machine can only accept such kind of money.
- Support from the infrastructure. Define the general interface of filters and with the mechanism of running the filter.
HIGH AVAILABILITY

• Replicated state machine for each shard or separate voting for each transaction.
• In the form of blockchain or just transaction database.
• The ledger is merely used for deciding whether double spending happens or not.
• Broadcast transactions and then decide. Only one proposer (only the user) can issue the transaction. Greatly simplify the protocol.
REGULATION

• Sometimes, you still need to match the pseudo name to real name for regulation.

• Still, filters can be used to make some (simple) regulations like “If you transfer over 100,000, you should show your ID card.”

• More regulation can be performed by using big data analysis. A big data platform may need to build to collect data and make analysis.
OTHER ISSUES?

• Replacement for UTXO? It is possible. But you still need to get sender and receiver for regulations.

• Blockchain? Shardded blockchain may be OK. RSM like blockchain will face the storage problem. (Suppose we have enough performance.) like RSCoin. However, blocks are actually not needed.

• Hardware assisted encryption/decryption may be needed.
THANKS

Q&A