# 20 April 2022
# Block Chain Alternative

## 1. Introduction

Block chain is a technology to support a distributed database. There is no single party responsible for the database. Instead, the database is "distributed" to the participants (also called validators) who collectively agree on the version of the database that is supposed to be "correct".

## 2. Bitcoin

Bitcoin is a cryptocurrency that is based on the block chain concept.

There is a fixed number of bitcoins created at the start. A small number of bitcoin is given to the miners who validate the database and are able to solve a complex mathematical puzzle. The process is called "mining". The validators are called "minors".

Solving the mathematical puzzle consumes tremendous amount of energy. As a result, the bitcoin platform is energy intensive.

Other cryptocurrency platforms do away with the "mining" approach, but they do not get the degree of attention as bitcoin.

Bitcoin has appreciated several tens of thousand times in value since its inception. As the number of bitcoin is limited, the enormous sums of money used to purchase the bitcoin cause the value to rise. It is like a Ponzi scheme.

## 3. Alternative to block chain

I wish to suggest an alternative approach to the block chain technology to manage cryptocurrencies.

The primary concept of block chain is that it is "decentralized" and is not under the control of any single party.

My alternative approach is to have a central database that is managed by a certain party, but the database is validated daily by several approved auditors who have access to the daily account balances and transactions.

It is not possible for the database operator to manipulate the data. If hackers hack the database and alter some account balances, the differences will be detected the following day and investigated.

It is possible to have the auditing to be carried out at shorter intervals, if there is a need to do so.

Although the account balances are available to the auditors, the identity of the account holder is not accessible to the auditors.

## 4. Summary

In summary, my “block chain alternative” approach allows the account holders to have confidence that the database is not subject to manipulation by the database operator or by hackers, and is transparently audited by several auditors.

In annex 1, I describe the approach to be used to audit the database.

Tan Kin Lian
kinlian@gmail.com
65 8168545

# Annex 1

# Block Chain Alternative

## 1. Introduction

I develop a proof of concept website for an alternative to blockchain in ensuring the integrity of the database.

At the end of each day, it downloads the data of the opening and closing balance of each account and the transactions for the day.

The data is sent to the appointed auditor(s).

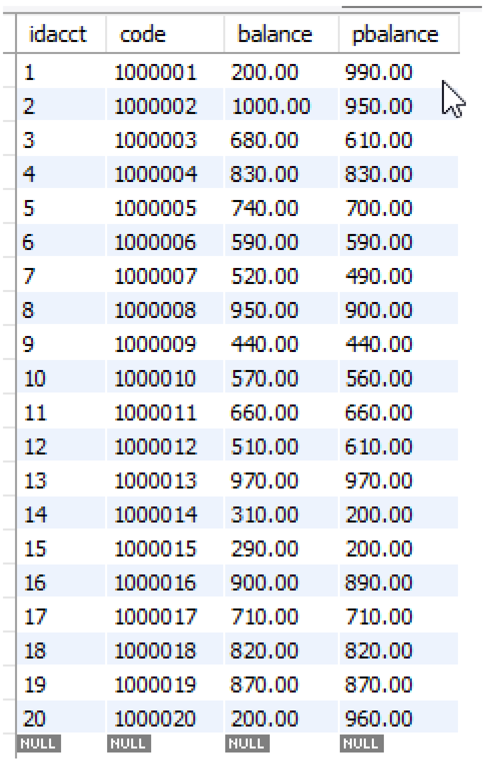
The auditor can check the transactions against the opening and closing balances, and identifies the accounts that do not reconcile.

The error could be due to unauthorized alternation of the account balance or to errors in the processing of the transactions.

## 2. Data

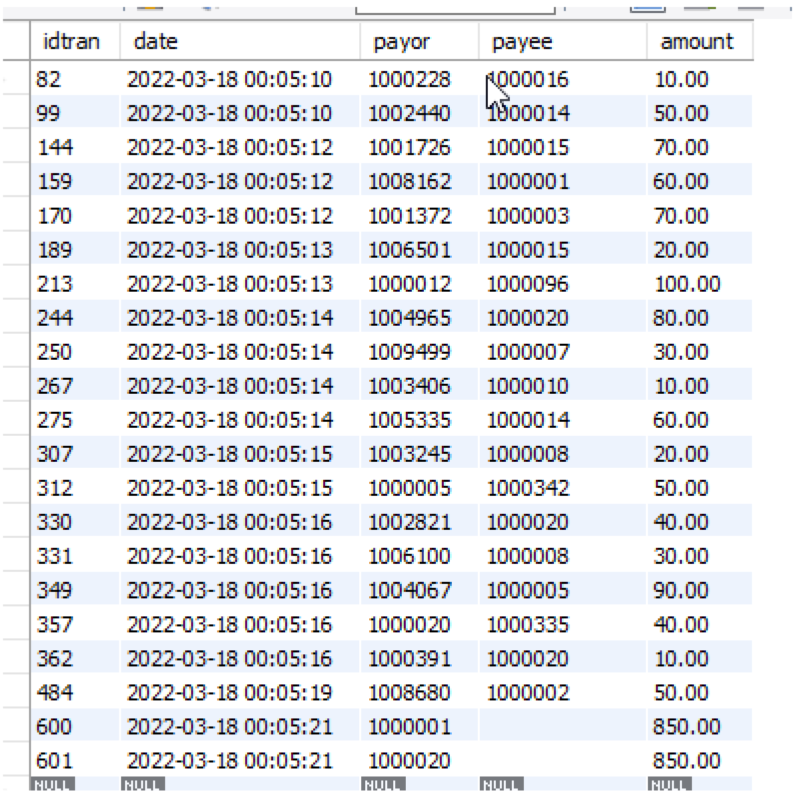
This table shows the transactions and balances for 18 March 2022. I have extracted only the data for the first 200 accounts.

### 2.1 Account balances



| idacct | code | balance | pbalance |
|---|---|---|---|
| 1 | 1000001 | 200.00 | 990.00 |
| 2 | 1000002 | 1000.00 | 950.00 |
| 3 | 1000003 | 680.00 | 610.00 |
| 4 | 1000004 | 830.00 | 830.00 |
| 5 | 1000005 | 740.00 | 700.00 |
| 6 | 1000006 | 590.00 | 590.00 |
| 7 | 1000007 | 520.00 | 490.00 |
| 8 | 1000008 | 950.00 | 900.00 |
| 9 | 1000009 | 440.00 | 440.00 |
| 10 | 1000010 | 570.00 | 560.00 |
| 11 | 1000011 | 660.00 | 660.00 |
| 12 | 1000012 | 510.00 | 610.00 |
| 13 | 1000013 | 970.00 | 970.00 |
| 14 | 1000014 | 310.00 | 200.00 |
| 15 | 1000015 | 290.00 | 200.00 |
| 16 | 1000016 | 900.00 | 890.00 |
| 17 | 1000017 | 710.00 | 710.00 |
| 18 | 1000018 | 820.00 | 820.00 |
| 19 | 1000019 | 870.00 | 870.00 |
| 20 | 1000020 | 200.00 | 960.00 |
| NULL | NULL | NULL | NULL |

## 2.2 Transactions

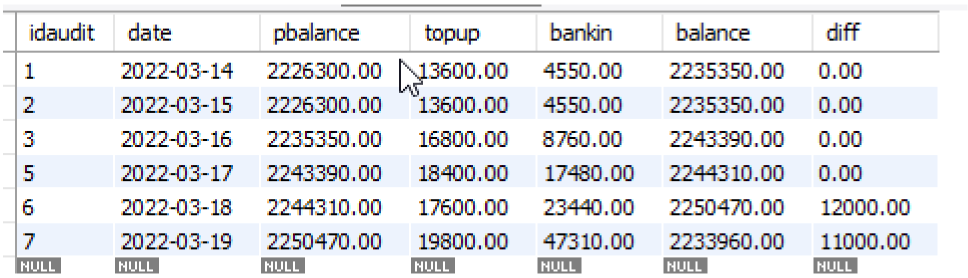


| idtran | date | payor | payee | amount |
|---|---|---|---|---|
| 82 | 2022-03-18 00:05:10 | 1000228 | 1000016 | 10.00 |
| 99 | 2022-03-18 00:05:10 | 1002440 | 1000014 | 50.00 |
| 144 | 2022-03-18 00:05:12 | 1001726 | 1000015 | 70.00 |
| 159 | 2022-03-18 00:05:12 | 1008162 | 1000001 | 60.00 |
| 170 | 2022-03-18 00:05:12 | 1001372 | 1000003 | 70.00 |
| 189 | 2022-03-18 00:05:13 | 1006501 | 1000015 | 20.00 |
| 213 | 2022-03-18 00:05:13 | 1000012 | 1000096 | 100.00 |
| 244 | 2022-03-18 00:05:14 | 1004965 | 1000020 | 80.00 |
| 250 | 2022-03-18 00:05:14 | 1009499 | 1000007 | 30.00 |
| 267 | 2022-03-18 00:05:14 | 1003406 | 1000010 | 10.00 |
| 275 | 2022-03-18 00:05:14 | 1005335 | 1000014 | 60.00 |
| 307 | 2022-03-18 00:05:15 | 1003245 | 1000008 | 20.00 |
| 312 | 2022-03-18 00:05:15 | 1000005 | 1000342 | 50.00 |
| 330 | 2022-03-18 00:05:16 | 1002821 | 1000020 | 40.00 |
| 331 | 2022-03-18 00:05:16 | 1006100 | 1000008 | 30.00 |
| 349 | 2022-03-18 00:05:16 | 1004067 | 1000005 | 90.00 |
| 357 | 2022-03-18 00:05:16 | 1000020 | 1000335 | 40.00 |
| 362 | 2022-03-18 00:05:16 | 1000391 | 1000020 | 10.00 |
| 484 | 2022-03-18 00:05:19 | 1008680 | 1000002 | 50.00 |
| 600 | 2022-03-18 00:05:21 | 1000001 |  | 850.00 |
| 601 | 2022-03-18 00:05:21 | 1000020 |  | 850.00 |
| NULL | NULL | NULL | NULL | NULL |

## 2.3 Daily Summary

Here is the summary of the balances and transactions for the entire database for the past few days.

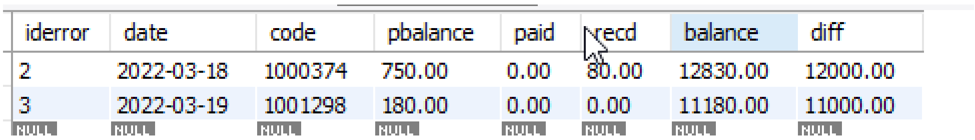
It shows a difference for the latest two days.
Note – I have deliberately altered the account balance, to see if the audit script is able to identify the account.



| idaudit | date | pbalance | topup | bankin | balance | diff |
|---|---|---|---|---|---|---|
| 1 | 2022-03-14 | 2226300.00 | 13600.00 | 4550.00 | 2235350.00 | 0.00 |
| 2 | 2022-03-15 | 2226300.00 | 13600.00 | 4550.00 | 2235350.00 | 0.00 |
| 3 | 2022-03-16 | 2235350.00 | 16800.00 | 8760.00 | 2243390.00 | 0.00 |
| 5 | 2022-03-17 | 2243390.00 | 18400.00 | 17480.00 | 2244310.00 | 0.00 |
| 6 | 2022-03-18 | 2244310.00 | 17600.00 | 23440.00 | 2250470.00 | 12000.00 |
| 7 | 2022-03-19 | 2250470.00 | 19800.00 | 47310.00 | 2233960.00 | 11000.00 |
| NULL | NULL | NULL | NULL | NULL | NULL | NULL |

## 2.4 Error in specific accounts

The audit script has identified the specific accounts that have the difference, i.e. the balance has been fraudulently altered.



| iderror | date | code | pbalance | paid | recd | balance | diff |
|---|---|---|---|---|---|---|---|
| 2 | 2022-03-18 | 1000374 | 750.00 | 0.00 | 80.00 | 12830.00 | 12000.00 |
| 3 | 2022-03-19 | 1001298 | 180.00 | 0.00 | 0.00 | 11180.00 | 11000.00 |
| NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL |

This audit script is run in the primary database. This is the primary check.

The data files are sent to the auditor(s) who are able to run their own script to validate all the accounts. This is a secondary check.

Tan Kin Lian

kinlian@gmail.com
81685845