Available online at http://www.mecs-press.net/ijeme

Distributed Ledger Management for an Organization using Blockchains

Mrs. Dipti Pawade[a], Mr. Sagar Jape[b], Mr. Rahul Balasubramanian[b], Mr. Mihir Kulkarni[b], Ms. Avani Sakhapara[a]

[a] Assistant Professor, K. J. Somaiya College of Engineering, Department of IT, Mumbai, Maharashtra, India
[b] Student, K. J. Somaiya College of Engineering, Department of IT, Mumbai, Maharashtra, India

Abstract

In the financial systems of the modern era, trust has always been a missing entity; concentrations of power and trust have given birth to numerous breakdowns. To resolve the problems at this end, the paper attempts for a solution using Blockchains, a data structure that allows for the creation of cryptically secured distributed tamperproof ledgers. The paper discusses the data structure and further disserts on the case study in consideration.

Index Terms: Blockchain, Distributed Database, Merkle Hash, Ledger.

1. Introduction

Post the 2008 financial crisis, the world came to some sparkling revelations in the world of finance, business, economics and politics [1]. One of the fundamental ones of those was the failure of the trust system in banking. The fall of the giants like Lehman Brothers [2] and the cessation of the Fannie Maes and Freddie Macs [3] of the world simply eroded the concept that 'banks can be trusted with public money'. The crisis warrants the question: how can trust be reborn into financial systems? How can organizations manage decentralized ledgers? How can power be redistributed among stakeholders in an equable proportion?

The answer to the question has been tried out in the past in different ways (stakeholder collaborations, boards of directors, fiduciary systems, audits, etc.) however all of them have resulted in major or minor failures. At the advent of this era of data, the data structure named 'blockchains' [4,5] comes out as a promise worthy attempt

* Corresponding author.
E-mail address: diptipawade@somaiya.edu

at solving the question of trust. The architecture which powers the Bitcoin [6,7], world's first public currency can also be used to create applications which distribute trust within organizations.

This paper attempts to discuss such methods and approaches of using blockchains to create trust and invigorate resilience within systems at large. Starting with a detailed review of technology, the paper discusses lateral experimentations with blockchains over the world, and further majorly focuses on our efforts to implement blockchains at an asset management firm based out of Mumbai, India (Sacred Capital Pvt. Ltd.: https://sacred.capital/) using a case based approach. The paper concludes with propositions for future implementations within our scope in the current development project underway.

2. Blockchain as a Data Structure and its Associated Merits

As a prerequisite to understand the applications of the blockchain technology, it shall be necessary to divulge on the technical aspects of how this technology works at the bottom layer. Blockchains are basically a set of interconnected distributed ledgers [8]. In case of the distributed system; connecting and managing heterogeneous system may create issues while maintaining the data [9]. But blockchain ensures that retroactive tampering will not occur within the datasets. This feature is facilitated as a fundamental characteristic of the data structure itself. For this purpose, the blockchain works on the system of blocks: a fixed size collection of transaction entries. As the time progresses, multiple blocks start getting added to the blockchain subject to their validated verification. A set of nodes called miners connected in a peer-to-peer network possess a copy of all the blocks right from the genesis block (first block in the chain). Transactions are broadcasted on the network for miners to pick up.

Now, the blockchain is different from distributed databases and other technologies due to its mining feature: the competitive problem solving that happens within the miners network. In principle, the blockchain technology comes with the fundamental proposition that the miners shall act as entities which will validate the transactions and write them to the blocks. To validate a particular block, miners will have to solve a cryptographic hash generation problem, which shall require enormous computing power to compute. Once the hash is generated by a particular miner (winner of the time-bound challenge to compute the hash), the particular block gets added to the blockchain [10,11].

The chain of blocks is maintained as follows: with the transactions of any block to be mined, the hash code of the previous block is also added to the current block. This ensures continuity in the chain and also ensures that any attempts at tampering previously added blocks results in the whole chain being altered. This process can be illustrated by using the original proposed model of blockchain for implementation of Bitcoin, the world's first public cryptocurrency[12]. Mining is a computationally intensive task governed by mining algorithms that are dictated by the system stakeholders and miners. Such algorithms can dictate the rate at which blocks get added on to the blockchain and thereby are extremely important towards the security of the entire chain. The chain that has the largest amount of computational effort put into its creation is considered to be the trusted chain.

Working of the blockchain as a data structure can be further understood by studying the basic model of Ethereum, a distributed blockchain service provider[13]. Following points should explain the information flow in the system.

- Transactions are broadcasted over the network of peer miners and users of the system.
- Miners pick up the transaction and compile them into blocks.
- Along with the transaction sets to be added, the miners add a particular Nonce (one time random variable to avoid replay attacks in the system and to ensure time-stamping) and the Merkle root of the transaction block (which is essentially a hash tree made upon concatenating hashes as the tree moves upward).
- Miners encrypt the block based on the cryptographic function used. The rules for proper hash generation are previously defined as a function of stakeholder and security objective.

- All miners update their ledgers as per the latest block added. The block to be added is a result of the problem solving competition that happens within the miners.

The blockchain technology application is highly useful for distributed applications [14]. Some of its core strengths lie in the fact that since the entire architecture is distributed in real-time, data does not accumulate at a particular node. Hence, there is no source of high power centricity in the system, and hence all sources are equal, resulting in the reduction of vulnerability in case of a system attack. This also ensures that trust is distributed in the system since all the miners are equal stakeholders of the data in question [15]. Any one node does not have the power to control the data of the system, this decentralizes power and maintains trust. Moreover, since the block to be added to the blockchain is a function of the hash mining competition, only legitimate users who want to propagate authentic transactions within the system will be willing to invest into computer resources enormously required for the hash computations. This ensures that an attacker will not be able to attack the system since he will have to overcome the resource ability of all the ethical miners in the question, which is pragmatically impossible. Hence, the system is tamper-proof, decentralized and robust on trust and data integrity [16].

2.1. Types of Blockchain and Specific Usages

Based on the various applications of blockchain technology since its inception, the following are the types of blockchains that can be generalized [17]:

- Public Blockchains: A public blockchain is a blockchain which is readable and writable to all the participants in the system, wherein all the participants can expect to see their transactions get validated and added in the blockchain if they are at all legitimate. For such a blockchain, the consensus building process is public and the number of miners in the system is large enough. These blockchains are trustworthy due to their cryptonomics − a combination of economic incentives and cryptographic problem solving using mechanisms like the 'proof of work concept', following an axiom that the level to which a particular entity can have an influence in the consensus process is directly proportional to the spectrum of economic as well as computational power they can bear. These blockchains are fully decentralized in nature.
- Consortium Blockchains: A consortium blockchain is where the consensus process is monitored by a pre-selected group of nodes or miners. As an example, say a consortium of 15 banks maintains an interbank ledger, in which for every transaction to be valid a block will require a minimum verification clearance by 10 banks. Such blockchains can divulge the details of the ledger on a limited basis, as per the requirement and liabilities of the stakeholders and participants. These blockchains are partially decentralized in nature.
- Fully Private Blockchains: A fully private blockchain is a closed chain, where the write permissions are kept with a limited set of people within an institution. Read permissions may be public or restricted to an arbitrary extent. Such blockchains are maintained for a specific organizational purpose, and public audit of such ledgers is desired.

3. Past Studies and Experimentations on Blockchains

Blockchains is a relatively new technology, and hence experimentation is underway. The only one biggest and foremost application of Blockchain technology - The Bitcoin - is widely and publicly accepted. Rest all are in the nascent stage and more on them will emerge in the subsequent future. However, the research studies and experimentations done till date offer an interesting viewpoint on the suitability and versatility of blockchains to facilitate trust and resilience in financial and non-financial applications.

A study by Barclays, UK highlights the various opportunities blockchains presents to the world of finance [7]. Right from facilitating e-cash and currency models, blockchains can be further extended to maintain banking ledgers for loans, investment banking, etc [18]. They can also be used to the sequential logs of commodity trading - Everledger, for example, is a proposed model to track all the diamond trades taking place in the history. A report by the Office of the Chief Scientific Adviser, UK Government [19] also points out at the applications of blockchains outside the world of finance; its applications to something as diverse as governance models. For example, democratic election processes can be made public over blockchains to create one of the most secure voting records ever.

An analytical report at UC Berkeley points out at the various experimentations and implementations of blockchain technology till date [20]. Some of them are as follows:

- NASDAQ implementing blockchains for its Private Equity exchange.
- Everledger creating ledgers for diamond trading.
- Stampery is an organization enabling stamping of documents through blockchains.
- IBM in partnership with Samsung has developed a platform ADEPT (Autonomous Decentralized Peer to Peer Telemetry) that uses elements of blockchain design to build a distributed network of the devices- a decentralized Internet of Things (IoT).

Such experimentations and studies provide conclusive insights and further guidance to apply blockchains to the specific case being studied in this paper.

4. Distributed Autonomous Organization using Blockchains: A Case Study Approach

In this section, we shall primarily highlight the findings which came across in the implementation of blockchain ledgers with Sacred Capital Pvt Ltd, an asset advisory practice based out of Mumbai. The implementation of blockchain ledgers aimed at transforming Sacred Capital, converting it into a distributed autonomous organization in the coming years, wherein the client engagements, client interactions, data analytics and bookkeeping happens through a blockchain backend.

4.1. Problem Case

Sacred Capital Pvt Ltd is a registered investment advisory (RIA) licensed under the Securities Exchange Board of India (SEBI). They help people to curate their assets and nurture their investments in a healthy manner. The clientele ranges from individuals, proprietary firms, companies, startups, angel investors, etc. Its primary functions are as follows:

- Serve as a fiduciary and provide advice to clients in an unbiased manner, without any predetermined affinity to any particular asset class or investment scheme whatsoever.
- Evaluate clients for their asset mappings, cash-flows and investment objective analysis to prescribe recommendations as per their requirements and suitabilities.
- Help clients like startups and small scale enterprises find angel investors within the network, thereby facilitating a budding investor-investee relationship.
- Build in-house research on various asset classes ranging from stocks, mutual funds, bonds to real estates, private equity, etc.
- Maintain a web portal system for every client to see his portfolio, with dashboards notifying the latest updates and recommendations as per market activities.
- Algorithmically evaluate the clients on basis of their engagability, investor discipline, etc. to judge them for their potential to receive privileged benefits within the Sacred Capital Ecosystem (e.g. the startups

with the best score on the above criteria will receive seed funding from the best investors in the circle).

4.2. Objectives for Solution Design: Functionality Review

In the above case, it shall be useful to examine the objectives a proposed blockchains based solution must achieve in terms of functionalities. Accordingly, a distributed autonomous organization approach could be designed by keeping the following aspects in consideration:

- The system must ensure to collect data from the existing Customer Relationship Management (CRM) and Data management systems at Sacred Capital. Such data can be collected at time instants by dynamic querying or can be pre-downloaded through a data staging process.
- The data can relate to multiple things and can be used to evaluate clients on a number of parameters. Data types can vary right from the frequency of logins a user makes on the platform (say, for determining the engagement of the client) to his portfolio excel sheets (say, for determining the risk taking the potential of a client).
- The data must be filtered and analyzed according to a predetermined algorithm which mathematically derives the potential of a client. Such potential can be recorded as a function of a score in unit values assigned to every client.
- The determined score and other data can be pushed on to the blockchain. This secures the score assignment for every client and ensures that such a client assessment system is free from judgmental or prejudicial error.

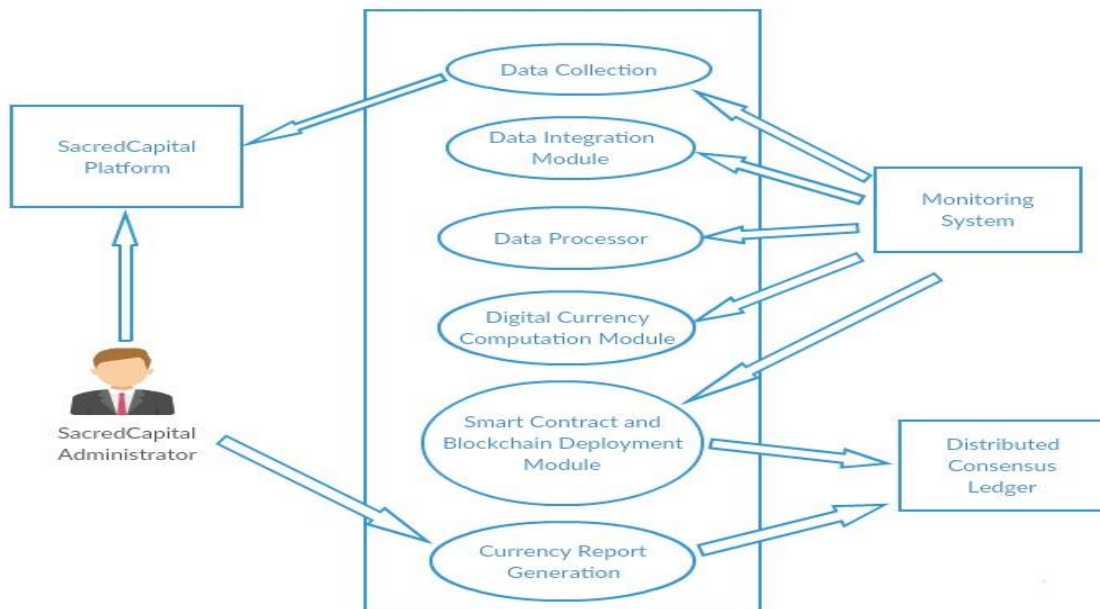Fig. 1 gives a pictorial representation of Use case diagram for our system.

Fig.1. Use Case Diagram

4.3. System overview and Discussion

Since the creation of a public blockchain is an expensive task, and such a privately created blockchain might not be necessarily effective due to the absence of the proof of work concept, we propose to outsource the blockchain functionality to Ethereum- a worldwide blockchain service provider. Ethereum lets clients use their blockchain facility by the means of smart contracts. The smart contract is a programmable code unit, results of which can be pushed on to the blockchain. We have integrated Ethereum Wallet using the smart contract to keep a record of the cryptocurrency balance with each client node of the system. The interface shall be primarily inherent, with interactions happening through the smart contract deployed on the Mix IDE. The system architecture and data flow sequence in the system are given in Fig. 2 and Fig. 3 respectively. Basically, our web based application fetches the client portfolio, perform preprocessing, apply the currency calculation algorithm on it and store that value on blockchain and finally generate the report. The user can query the blockchain to get the currency holding report.

```
                    ┌─────────────────────────────┐
                    │    Sacred Capital Platform   │
                    └─────────────────────────────┘
                                  │
                                  │  Fetch Customer ledger
                                  ▼
             ┌──────────────────────────────────────────┐
             │    Digital Currency Computation Unit      │
             │ (Algorithmically determine Currency Units │
             │             to be assigned)               │
             └──────────────────────────────────────────┘
                                  │
                                  ▼
                    ┌─────────────────────────────┐
                    │        Smart Contract        │
                    └─────────────────────────────┘
                                  │
                                  ▼
             ┌──────────────────────────────────────────┐
             │              Mining Process               │
             │ (Mine data following proof of work        │
             │              protocol)                    │
             └──────────────────────────────────────────┘
                                  │
                                  ▼
                    ┌─────────────────────────────┐
                    │        Genesis Block         │
                    └─────────────────────────────┘
                                  │
                                  ▼
             ┌──────────────────────────────────────────┐
             │                Report Gen                 │
             │ (Mine data following proof of work        │
             │              protocol)  eration           │
             └──────────────────────────────────────────┘
                                  │ ▲
                                  ▼ │
                    ┌─────────────────────────────┐
                    │      Report Access Model     │
                    └─────────────────────────────┘
```
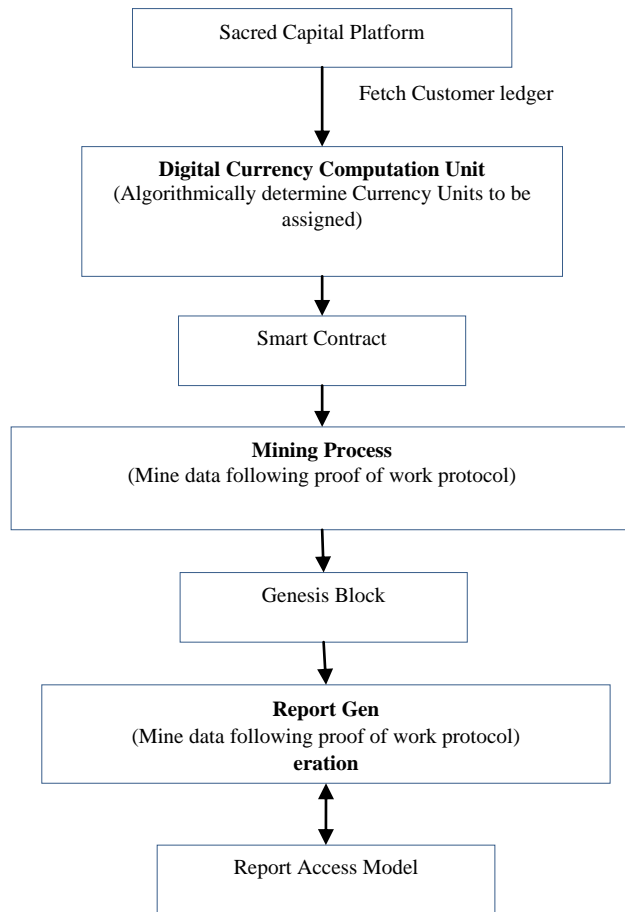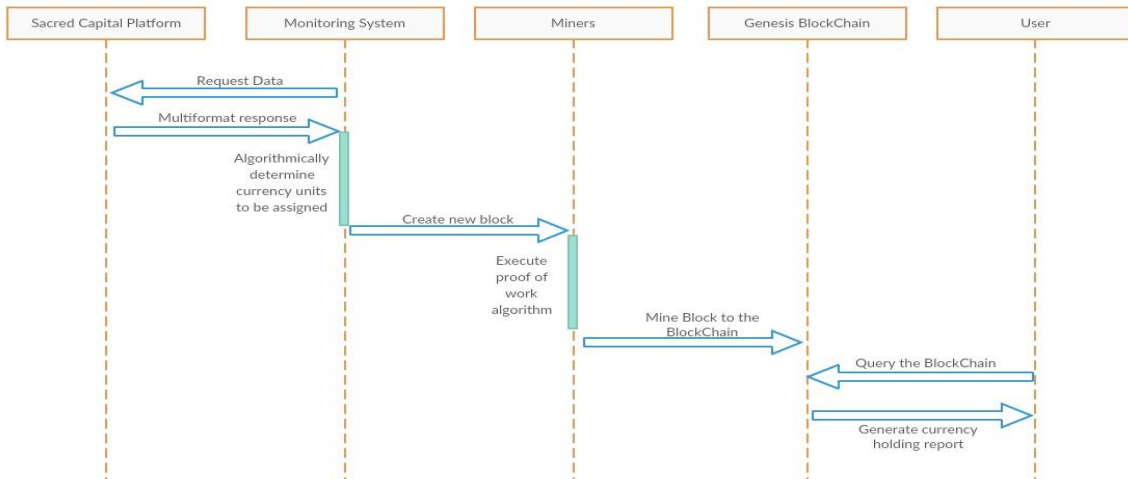
Fig.2. Architecture Diagram

Fig.3. Sequence Diagram

The detailed working of the system is as follows:

- Step 1: The blockchain ledger system queries data by sending systematic HTTP protocol requests to the Sacred Capital IT system. The system responds with the required data in a structured JSON format.
- Step 2: The received JSON format is an excel-type portfolio shown in Fig. 4 which map entailing all assets and cashflow details for a particular client. In this step, the task is to pick out the selective parameters (for example amount invested in each asset class, etc) and then feed them to the currency determination algorithm mentioned in the subsequent.

			Currency	Return	Risk	Fungibility	Maturity
6	Current Portfolio						
7	Fixed Income		62,16,636	Currency	Return	Risk	Fungibility	Maturity
8	ULIP	2,20,000			Fixed	Monitoring	Fungible	Long
9	Insurance	2,27,380		INR	Fixed	Monitoring	Not Substitutable	Long
10	PPF/EPF	15,84,592		INR	Fixed	Monitoring	Fungible	Long
11	Mutual Funds(Debt)	5,60,000			Fixed	Monitoring	Fungible	Short
12	Deposits/Loans	13,35,847		INR	Fixed	Monitoring	Fungible	Short
13	Loans	5,00,000			Fixed	Monitoring	Not Substitutable	Short
14	FDs	10,00,000			Fixed	Monitoring	Fungible	Short
15	Traded Bonds	7,45,817		INR	Fixed	Monitoring	Fungible	Long
16	NCD/Debentures	25,000			Fixed	Monitoring	Fungible	Short
17	Post Office	18,000			Fixed	Monitoring	Fungible	Long
18	Equity		8,20,254		Return	Risk	Fungibility	
19	Mutual Funds(Equity)	-			Variable	Monitoring	Fungible	
20	Large Cap Holdings in MF's	2,50,000						
21	Mid Cap Holdings in MF's	8,76,000						
22	Stocks	4,41,397		INR	Variable	Monitoring	Fungible	
23	Large Cap Holdings in Stocks	4,41,397						
24	Mid Cap Holdings in Stocks							
25	International Stocks	2,78,858		USD	Variable	Monitoring	Fungible	
26	Private Equity	1,00,000			Variable	Engaged	Not Substitutable	
27	Real Estate		80,00,000		Return	Risk	Fungibility	
28	Cuttack	80,00,000		INR	Variable	Monitoring	Fungible	

Fig.4. Client Portfolio

- Step 3: This step calculates the currency units to be allocated to each client. This algorithm can be exemplified as follows:

3.1: The algorithm considers two parameters which define the structure of a particular client in the system. In this example, let us consider two parameters such as 'Risk Appetite' and 'Fungibility'

3.2:   Risk Appetite can be calculated as the percentage of equity (higher-risk) assets in the portfolio. The fungibility refers to the interchangeable units present in the portfolio. For example in the sample portfolio shown in fig. 4, fixed deposits, bond, debt, and equity mutual funds are considered as fungible while issuance and private equities are non-substitutable.

3.3:   Each asset class has its own preference in calculating each of this parameter. This preference is decided by allotting a multiplier (y) to each asset class (x).

3.4:   The parametric value can then be calculated (in a generalized manner) using formula (1):

$$(\text{parametric value}) = \sum_{k=0}^{n} x_k y_k \tag{1}$$

Where x,y is an individual asset class and its corresponding multiplier and (n) is the total number of assets in a client's portfolio

- Step 4: The calculated currency units per client are structured as key value pairs, with the name of the client referred as the key, while the currency units referred as the value. These values are then passed to the smart contract on the backend, which has been called by the scripts running on the frontend.
- Step 5: The blockchain peer service network then deploys the transactions to the main blockchain and the mining process starts. As soon as the mining is complete, the transaction data gets appended to the longest blockchain in the peer network. Fig. 5 shows the mined blocks each having a unique ID. Once this is done, the mined blocks generate a report from the backend blockchain interface. This one report then serves as the total repository of blockchain execution details. The web modules can access this file and read it to get the data on the blockchain. The blockchain is used to store the mapping of the currency values in real time.
- Step 6: Clients and the administrator can then query the blockchain as per the demand to fetch the details for the currency allocations pertaining to the clients in the system.
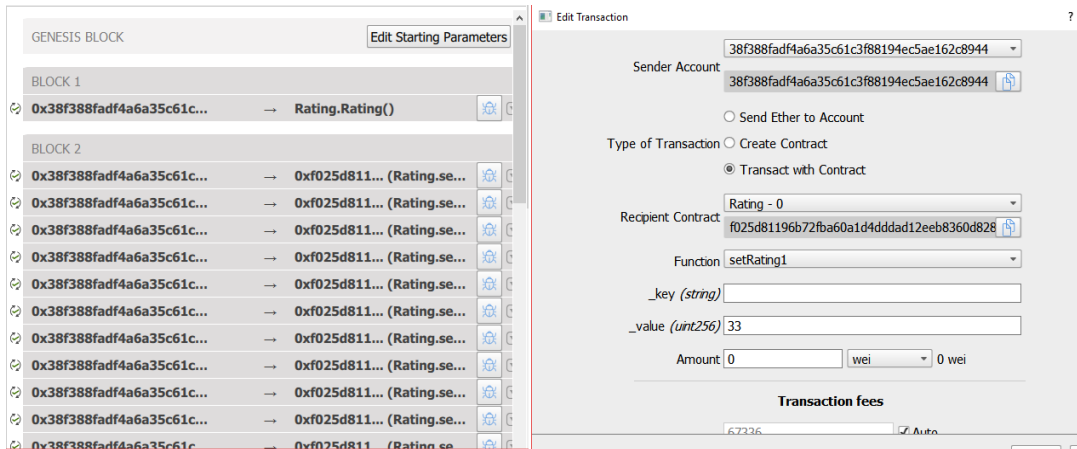

Fig.5. Block mining on Ethereum IDE

Fig.6 shows how the final currency allocation details per client are served by the system. From the security point of view, we have taken dummy names of client and worked on the actual portfolio. This crypto currency will be onwards used to determine the worthiness of particular client. Rather than just categorizing the client based on the amount held by them, the cryptocurrency is calculated by considering factors like 'risk appetite'

and 'asset fungibility' which will be helpful to get clear notion about the value of the client. This will be useful to have the better understanding about the nature of the client and will provide a good base to plan the further business strategies. As a result, the trust in a system can be improved as decision won't be based on human influence. Lack of human being as a central certifier for predicting the value of customer speed up the overall process. Also, the ledger is maintained in a distributed manner based on consequence and is secure and available all the time.

Fig.6. Final Currency Allocation Details per Client

5. Result Analysis

In the current basic prototype, the "sacred capital dollar" (currency calculated by proposed system) is a currency aims at autonomously valuing clients in the ecosystem, as a function of their portfolios. In a post financial crisis world, resilience has emerged as the key parameter for valuing a portfolio's worth across asset management functions. However, post financial crisis, several lucrative investment opportunities, and sophisticated financial products have also emerged, thus creating higher expectations for returns. Hence in such scenario, ideal portfolios are those which exhibit high risk as a function of stronger exposure to equity linked assets, while simultaneously maintaining high fungibility of assets. Higher fungibility ensures greater resistance and resilience, while high risk ensures availability of premium return over the risk free rate. Our algorithm thus calculates the currency and the worthiness to be associated with each client as a computation of risk and fungibility parameters which are input to a weighted average, as per the systemic weights associated to each asset class. For discussion, we have considered the portfolio of nine clients. Table 1 represents the risk and fungibility parameter values for each client and associated Currency allotted to them. The Fig. 7 depicts the relationship in currency allocated vis-a-vis risk and fungibility parameters.

Table 1. An example of a table

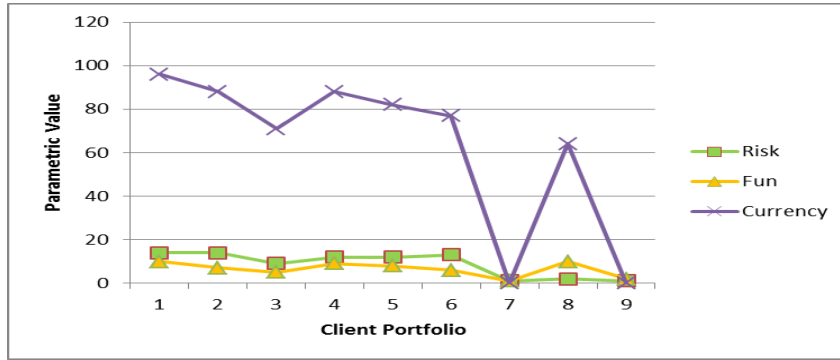| Client	Risk	Fungibility	Currency Allotted by Our System
1	14	10	96
2	14	7	88
3	9	5	71
4	12	9	88
5	12	8	82
6	13	6	77
7	1	1	0
8	2	10	64
9	1	2	0

Fig.7. Relationship Between Currency Allotted to the Risk and Fungibility

As it can be seen from Table 1, client 1 and Client 2 has the portfolios having higher risk appetite and higher fungibility will be most valued in the system, and hence will be allocated maximum currency. Hence, though Client 1 and Client 2 have same risk appetites, Client 1 has higher fungibility, and hence is allocated higher currency values. The client 3 and Client 4 has the portfolios which show higher risk appetite, with increased fungibility, are valued more than those portfolios which exhibit lower risk appetite with lower fungibility. This ensures that the system encourages high risk, high return portfolios while enabling better resilience through the higher fungibility parameter. The client 7 and Client 8- the portfolios with lower risk appetite but higher fungibility are valued higher than portfolios with both low risk appetite and low fungibility. This ensures that the system values those portfolios which exhibit higher transactions, even in assets with lower returns.

Thus through our experimental results, we have observed that implementation of our blockchain based system in an organization for ledger management outcomes in following advantages:

- Distribution and Robustness: The system has a backend designed on a server that runs blockchain algorithm through its vast network of interlinked distributed databases. This fulfills the requirements of robustness and integrity in ledger computations.
- Anonymity: The blockchain backend runs on cryptographic verification and hence does not divulge any details of credentials of the client.
- Computation: The design supports the blockchain service to compute the currency determination algorithm on the backend itself, and then save the values into the blocks of the blockchain. Hence, the system does not bear the load for a separate platform for currency determination.
- Client-Server Model: Helps the client front end to query values as and when required, while a distributed blockchain service integrated with the client service model helps to keep the currency determination intact with the current transaction record.
- Three Layer Architecture: Front End, Middleware, and Backend help to keep the system demystified and fulfill all the requirements.

6. Conclusion and Future Scope

In the current status of the development work, the above said considerations have been implemented. A successful stage one prototype has been established, in which the system communicates with the pre-existing IT infrastructure through APIs; the currency scores are determined in the Ethereum IDE and are pushed to the Ethereum Blockchain subsequently. The current currency determination algorithm takes only financial data into consideration. It is a typical weighted averaging methodology, that takes into account the current portfolio assets and allocations of any client, thereby determining the worthiness of the portfolio in terms of the 'risk

appetite' and 'asset fungibility'.

Since the project is in the nascent stage, the functionalities of the prototype have been kept minimal on purpose to ensure progressive scaling without any compromise on security and resilience of the application. However, in the near future, we aim at attempting some of the below enlisted progressions:

- Integrating the blockchain ledgers and the current information systems at Sacred Capital into a single web based entity.
- Expanding the penetration of the currency determination algorithm to extend to parameters beyond financial data and include other data types like frequency of client logins, client-advisor communication analysis, etc. Such varied data types will increase the spectrum of client analysis.
- To make the system fully real time - i.e. currency scores must fluctuate according to real time assets prices and stock market quotes at any instant.
- To include data visualization for generating insightful reports on currency scores of clients, recent activities of clients, etc.

In the above proposed manner, we aim at invigorating trust and resilience once again in financial systems. The blockchain technology and its applications present us with an efficacious paradigm that can be nurtured in the days to come.

References

[1]   John, M, "The financial crisis in the US: key events, causes and responses", House of Commons Library, 2009. Available at: http://www.parliament.uk

[2]   Zadinamin, Amirsaleh, "The Bankruptcy of Lehman Brothers: Causes of Failure & Recommendations Going Forward", Social Science Research, August 2013, DOI: 10.2139/ssrn.2016892.

[3]   W. Scott Frame, Andreas Fuster, Joseph Tracy, and James Vickery, "The Rescue of Fannie Mae and Freddie Mac", Federal Reserve Bank of New York Staff Reports, no. 719, March 2015

[4]   Simon, T., "Blockchain: Understanding the Potential. Barclays Bank PLC",2015.

[5]   Nicola Dimitri, "The Blockchain Technology: Some Theory and Applications" Working Paper No. 2017/03, Maastricht School of Management, 2017.

[6]   Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., "Bitcoin and Cryptocurrency Technologies", Princeton University Press, 2016.

[7]   J. Bonneau et al, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in 36th IEEE Symposium on Security and Privacy, May 18-20, 2015.

[8]   San Jose, Puerto Rico "Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay," 19th International Conference on Financial Cryptography and Data Security 2015, January 26–30, 2015.

[9]   Tarek S. Sobh, Medhat Fakhry,"Evaluating Web Services Functionality and Performance", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.5, pp.18-27, 2014. DOI: 10.5815/ijitcs.2014.05.03.

[10]   Haber, S., & Stornetta, W.S., "Secure names for bit-strings", in Proceedings of the 4th ACM Conference on Computer and Communications Security. Pp 28-35, 1997.

[11]   Massias, H., Avila, X.S., & Quisquater, J.J., "Design of a secure timestamping service with minimal trust requirements", In 20th Symposium on Information Theory in the Benelux, 1999.

[12]   Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008. Available at http://bitcoin.org/bitcoin.pdf.

[13]   Zanzu, "Ethereum block architecture", 2016. Available at: http://ethereum.stackexchange.com/questions/268/ethereum-block-architecture. [Accessed: 13- Feb- 2017].

[14]   Peter Evans-Greenwood, Robert Hillard, Ian Harper, Peter Williams," Bitcoin, Blockchain & distributed

ledgers: Caught between promise and reality", Deloitte, Australia, 2016. Available at: https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf

[15] El Defrawy, Karim, and Joshua Lampkins, "Founding Digital Currency on Secure Computation," CCS '14: Proceedings of ACM SIGSAC Conference on Computer and Communications Security, March 2014, pp. 1–14.

[16] Arpita Nayak, Kaustubh Dutta, "Blockchain: The Perfect Data Protection Tool" in proceedings of International Conference on Intelligent Computing and Control (I2C2), 2017, Coimbatore, India, 23-24 June 2017, DOI: 10.1109/I2C2.2017.8321932

[17] David, S., Harvey, L., Vimi, G., Alexander, S., Stephen, M., Tyler, W., "What is blockchain? Blockchain Enigma. Paradox. Opportunity", Deloitte, 2016.

[18] J. Leon Zhao, Shaokun Fan and Jiaqi Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue", Financial Innovation 2016, 2:28 DOI 10.1186/s40854-016-0049-2, 2016.

[19] Government Office for Science, The Rt Hon Matt Hancock MP, Ed Vaizey., "Distributed Ledger Technology: beyond blockchain", Press Release, 2016.

[20] Crosby, M., "Blockchain Technology: Beyond Bitcoin", Sutardja Centre for Entrepreneurship & Technology, UC Berkeley, 2015.

Authors' Profiles

Dipti Yogesh Pawade received B.E. degree in Computer Science and Engineering from Sant Gadge Baba University in 2009 and M.E. degree in Embedded System and Computing from G. H. Raisoni College of Engineering, Nagpur in 2012. Since 2012 she is an Assistant Professor in the Department of Information Technology at K J Somaiya College of Engineering, Vidyavihar, Mumbai. Her interest includes Machine learning, Web Security, and Web Application Development.

Sagar Jape is is an Information Technology graduate from the K J Somaiya College of Engineering,Mumbai and now working as a software developer at Oracle Financial Services Software. Programming has always been his key area of interest. He has secure 100% in Oracle Certified Professional Java SE Programmer(OCPJP) thus facilitated a better understanding of programming thus enabling implementation of efficient logical algorithms in various domains. Technologies such as blockchain technology, cryptography and machine learning have fascinated him.

A technologist at heart and also by profession, Rahul holds a Bachelor's degree in Information Technology. The concepts of big data and analytics and blockchains have always intrigued him and he is currently exploring the big data world. He has always been mesmerised by the volumes of information that can be extracted from seemingly unimportant data if processed the right way. As a passionate programmer he always looks forward to the challenges that enablers of monstrous computations in the big data have to face. He firmly believes that the more information we are able to extract out of these systems, the better prepared we are for the future.

Mihir Kulkarni is an Information Technology graduate from the K J Somaiya College of Engineering,Mumbai and has been working as a technology management consultant with several global banks and insurance companies. Across his graduate years, he has worked with several organizations, building projects across the domains of blockchain and distributed autonomous applications. His recent interest spans throughout disruptive agile infrastructures used in investment banking and asset management verticals; peculiarly, his study is focused on applications of blockchain decentralized networks towards enablement of new age resilient products in finance verticals like global trade ecosystems, financial markets, insurance and retail banking.

Avani Sakhapara received B.E. degree in Information Technology from Thakur College of Engineering and Technology, Mumbai University and M.E degree in Computer Engineering from K.J. Somaiya College of Engineering, Mumbai University. Since 2009 she is an Assistant Professor in the Department of Information Technology at K.J. Somaiya College of Engineering, Vidyavihar, Mumbai. Her interest includes Information Security, Machine Learning, Natural Language Processing and Web Application Development.