Saf-Send: Alternative banking solution

Safwan Salehjee [201324649]

201324649@student.uj.ac.za

Abstract. Our current banking system is limited with its reach in remote areas and it's not disaster proof. The research attempts to solve this problem by decentralizing banks. A model of social trust system is used to develop trust and use those channels to transfer fund via credit transfer techniques. This is based upon an ancient hawala based remittances system. The use of web based application is used to present an interface and an attempt to blockchain the transactions to make it temper proof.

Keywords: Remittances, Hawala, Block chain.

1 Introduction

The papers aims to present a problem with centralized banking, and proposes a modern-day implementation of the ancient hawala system practiced upon the silk route. In the introduction, problem is highlighted, my motivation for the research and method of solution. This is followed by a Literature Review in which is a summary of literature studies in related topics. The proposed solution model is discussed, followed by the implementation and the results. Finally, an analyses of the implementation is done followed by identification of further then a conclusion.

1.1 What is the problem?

Current banking solutions are based upon centralized institutions to carry out day to day services such as remittances, payments or transfers. These services are essential part of the economy, and personal lives of individuals. The absence of such services can have catastrophic consequences on the economy at large and at individual level.

A centralized institutional banking requires hefty investment to make remittance/payments possible. Thus, it makes them unlikely to invest in rural areas, in which business transactions are less. People located in rural areas would have to travel to access a basic need to banking.

The current method of banking is also vulnerable to natural disasters or manmade disasters such as war. If a bank in targeted then basic banking services are disabled in

the entire area. To avoid single point of failure, this paper purposes an alternative banking solution. It an effort to decentralize banking and facilitate entrepreneur in banking sector. The core functionality of which is remittance.

1.2 Motivation

If such a remittance is implemented it will give disadvantageous community a share in the banking industry. It will also encourage trade, especially in rural areas where banking was rare previously. It also encourages cultural interaction as it was previously proven in silk route as similar system was in place during the trade in silk route. The system can even operate in disastrous environment, which gives humanitarian work easy access to help trapped individuals.

The technology of Block chain is also an area which attracts my personal attention. Looking for further areas of its implementation has also been a reason for my choice of working for this solution.

1.3 Method of Solution

The solution attempts to replicate the ancient hawala system. However, it does not encourage further network, nor does it completely implement the ancient system. It would be merely a utility that can be used to cater such a system digitally. The role of the application will be supporting the system with record keeping.

The key to its success being correct flow of events. The technologies being used in a web based application (.net framework) and additional block chain data storage to make transactions temper proof.

2 Literature Review

2.1 Hawala system

The hawala system is an ancient remittance system to transfer funds. It is based upon social bonds and building trust. The system allows for transfer of funds without physically transferring funds. It is a result of the evolutions of how business along the silk route adapted to counter highway raids. The concept is illustrated in the figure below:

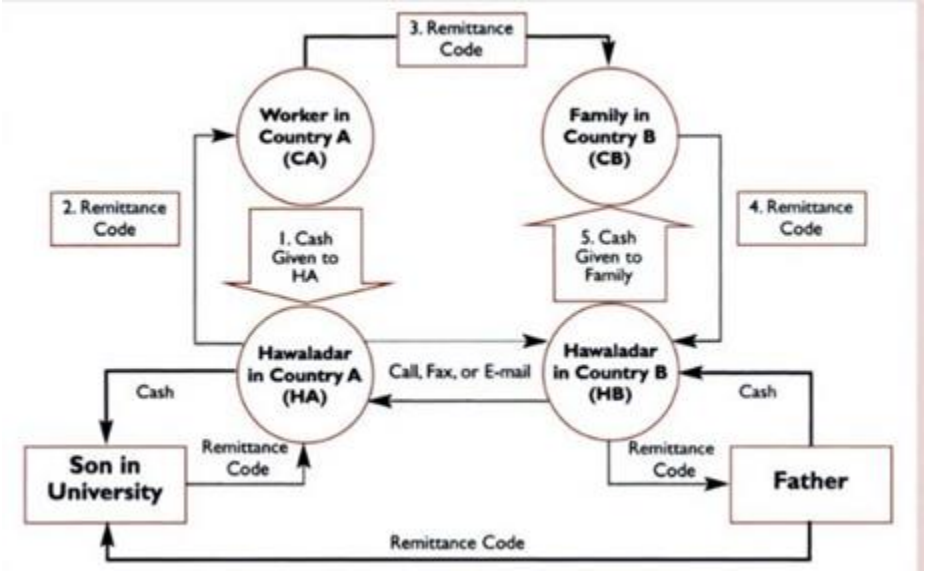

Fig. 1. Example of Hawala network [4]

The example above demonstrates how a hawala system is carried out. In this research we are trying to facilitate the communication between the two hawaladars. The calls/emails are to be replaced with the system called Saf-send. There will also be an attempt to blockchain the transaction.

2.2 Block chain

The paper has divided in three sections: Crypto hashing, Merkel Tree and finally the blockchain as a technology.

Hashing

Hashes are used to convert a string into another string with fix length. This is done using defined mathematical formulas. There are serval properties of a hash functions which makes it appropriate for it to be used in a cryptographic environment. The cryptographic element the hash function is one of the reasons of immutability of the block chain.

The Function should be fast as it is expected to generate a digest which is not expected to reversible like compression. The applications of hash functions also demanded robust responses. The hash had to be deterministic meaning that if the input has not changed then the hash should not be changed either ($F(x) = y$). However, if there is even a small change in the input message, the hash should be changed dramatically. This is to avoid the message to be guessed in

any way and so it protects the irreversibility of the hash function. The infeasibility of reversibility is a key property of the hash and it most important to prevent this in any of its application and this is known as Pre-image resistance. The Function should be designed in a way that it is extremely difficult to predict collisions. This is when two different messages have the same hash as pointed out in the figure above with the property of collision resistance. The hash function should also be such that once given a hash it's difficult to get another message with the same hash as the give hash (Hash (m1) = Hash (m2)). (Thomsen, 2008)

Merkle tree

A Merkle tree, which is also as the binary Hash tree, is used to store the blocks of the block chain. It has the responsibility of the integrity of the Blocks. The tree has existed from 1979 when it was patent by Ralph Merkle (RALPH, 1982). The tree is most famous for its usage in a peer-to-peer file sharing system and trust computing system. It checks if the blocks received are not damaged or altered.

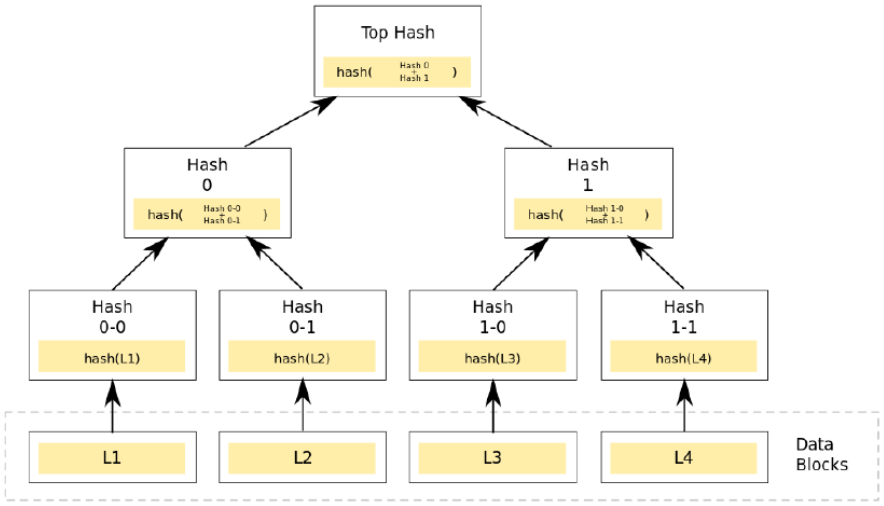

Fig. 2. Example of a Merkle tree

A Merkle tree's leaves are the actual data (Files, pictures, etc.) or the hashes of the data. The parents of these hashes are formed by hashing their children and this continuous until a single root node. This the case with Node 0, it is the result of the hash of hash 0-0 and hash 0-1(Hash 0 = hash (hash0-0 + hash 0-1)). The top hash is the end result which is the digital signature of the data and the order of that data.

The block chain contains blocked chained together using the hash of the previous hash. Each Block, contains a set of transactions (which is the data of the application). The transactions are hashed using the Merkle tree hashing technique. Each of the transactions are hashed and that is the stored as the transaction ID. The Hashes are hashed

together in a binary way up until it reaches the root hashed. This hash is stored in the block header and is hashed again to be stored in the next block. (Becker, 2008)

The Merkle tree provides a cryptographic proof of the content in the block. If there has to be a small change in any of the content the change will be reflected up the tree up until the root hash. The hash will then have hashed different in the next block and the entire block chain will be changed. The Merkle tree is better than one hash of the transaction or a hash list because it also saves the

order of the transactions. If the order has to be changed, this will also reflect on the root hash of the Merkle tree. The order of the transaction are important in a banking and ledger context.

Blockchain

This section will look at the research paper Blockchain [1].The look on the disruptive technology is discussed in great simplicity and detail. The technology is described as disruptive in its nature meaning, it has potential in making changed in main stream industries.

There are many projects launched in many industries, but the most prominent impact it has made so far is the financial industry. The financial industries biggest product in this department is the bitcoin: A cryptographic currency and cash system which is decentralized. However other application is the same industry are the smart financial contracts, assets ownership records (like of blood diamonds, etc.), the elimination of intermediators in transactions. The intermediators go thru intense verifications between many intermediators to get the transaction verified. The process can take up days. Blockchain has the ability to authenticate the transaction with instant speeds. There are many organizations that are looking to solve this problem using block chain.

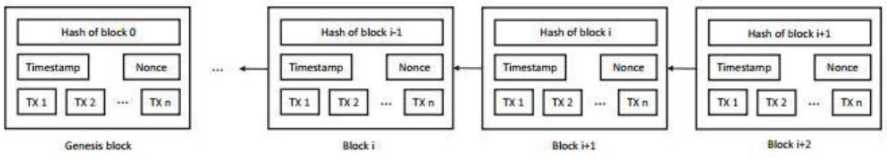

Fig. 3. Example of a Block Chain

The figure above is an example of a block chain. Every Block contains many transactions (TX 1-TX n) that were conducted, a timestamp of the compilation of the block, A Nonce which is random number that is responsible to verify the hash (of the block in the next block) and the hash of the previous block (parent block).

The transactions in the blocks are the actual data that is intended to be protected from any change. The timestamp is the time at which a block was made. This adds to the input in the hashes outcome as well as it tracks the creation of blocks as time passes. Meaningful data can be collected using the timestamp to predict resources required for the block chain and thus help with tackling scalability. The Nonce is a number which is mined to get a specific type of hash result. With the all the data now being constant, the nonce is variable. For example, the hash in a system is agreed to have the first 4 digits to be “0” of a 48-digit hash. Thus, after the nonce is generated for the first 4 digits

to be “0”. The next 44 digits will be variable for every block. Thus, a change in the constant data like one of the transaction, the timestamp or the previous hash will change the hash of the block and in most likeliness without the first four digits to have “0”. Thus, the nonce has to be re-mined to get a hash with the first 4 digits with four “0”. The hash of the previous block is the saved hash of the previous block. All the blocks have the hash of the previous block and this is one of the inputs to generate the hash of its own hash that will be saved in the next block. In this way all the nodes are heavily linked with each other and a small change in one of the blocks will change a lot in all the following blocks to come.

The first block is known as the genesis block. The genesis block contains the hash of its self. The block chain is then extended with the addition of a new block. The new block contains the hash of the previous block and the current transactions. Similarly, the chain continuous, thus the chain contains the ledger of all the transactions of the past. The chain is spread across various nodes in the network. All the individual nodes are alerted of the transactions. The individual then generates the nonce and the hashes individually. The Consensus is then reached if all the nodes in the network have reached the same conclusion. If there has to be an attempt to change a transaction in one of the blocks, not only do the attacker has to change all the nonce in the rest of the chain of that specific node but the attacker has to do the same changes in all the rest of the nodes. The majority of the nodes in the network will be taken to be the authentic chain. As long as the attacker does not have the majority of the nodes in the network, the network will be safe. This is known as the 51% attack.

Smart Contracts has been given life since the introduction of block chain. A smart contract aims to replace the banks, lawyers and other third-party institutions that very used to establish trust. Block chain has replaced trust from humans to mathematics. The block chain is to be trusted by market which is transparent, secure and cost-effective. The most prominent example of such application is the Ethereum.

There are many applications identified and implemented in the financial and non-financial sector. In the financial world the block chain is making a dominate impact. The creation of bitcoin: a cryptocurrency, is the biggest application of block chain. This in it of itself is a powerful concept and shows the strength of the tech world. There are many applications in the insurance security, trading, and settlements like block stream, etc. Non-financial successful applications have also been implemented: Storj (a decentralized storage), Blockverify (an Anti-counterfeit solution), Imogen heap (Managing music right ownerships and royalties), Namecoin (an internet protocol to decentralize domain name servers instead of governments and co-operations) and many more.

3 Solution Model

3.1 Web Application

The solution will be a web based application. The technologies used is VB and SQL server.

3.2 Users

There will be two users to the system: Hawaladar(teller) and an admin. The Hawaladar will use the app for record purposes. This includes keeping track of his/her transactions requested, the transactions that are expected of him/her and his/her debt and credit upon other hawaladars. The idea of an admin is for it to be used by either the government or any nonprofit organizations. The admin will have a broader view of general hawala transaction network. He/she will be able to see various trust levels of the network. This is to help use the information in times of disaster to send funds.

3.3 Home Page

After a registered user will log in. The most important page is the home page. The home page will have three sections:

1. Network Users

This section will have all the users that are already networked. This means that they have already been proved that they are socially connected. The section will show all necessary details regarding the specific fellow

2. Pending transactions

This section will be transaction sent by other hawaladars to the logged in User. The user will have the option to complete the transaction once the money is received by the receiver.

3. New Network Request

This section includes all the invites that the logged in user have received by other hawaladars. The user must provide the correct password by each user and they can then establish the network.

3.4 Networking

Hawaladar will have the option to expand their network. However, they can only expand their network via social means and not thru this application. Thus, it means the users must meet in person or thru other methods. They would share their User Ids and create a unique password to establish their network. One user will invite the other with the unique password and the other will accept the invite with the correct password. This method will insure the hawaladars are socially connected.

3.5 Transactions

The transaction will be carried out in two steps: Send and Receive. One Hawaladar will send a request to the receiver hawaladar. He/she will state the amount and the description of the receiver. The hawaladar at the receiver end, will wait for the amount to be collected by the receiver. There after the receiver hawaladar will update the transaction request as completed. Then process is stored as a completed transaction and calculation are done to update credits and profit share between the hawaladars.

3.6 Trust

A trust level is calculated between from the activities of the hawaladars. The trust levels are stored but not shared with the hawaladars. This is kept for the admin report.

3.7 Trust Report

The trust Report contains the trust levels of the hawaladars. This may have practical usage depending upon the situation. For example, in disaster situation the government and the NGO could use such a report to send money in areas where there are no banking services available.

4 Implementation

4.1 Tools

Visual Studio 2017 community
The Program will be written in Visual Basic on Visual Studio. The IDE presents with various tools to cater for such development. Web application will be based upon Web forum template provided by Visual Studio. The IDE also provides various components for web interaction with user. Additionally, bootstrap will be used to give the web application a modern appearance.

SQL Server
SQL server will be a primary database. All the data will be stored on the SQL server. The block chain will only be used to store the transactions. Visual Studio provides SQL server which can also be connected to the Web application.

Bootswatch
Bootswatch will be used to make the Web application more interactive. The colors, panels, buttons and various other components of the web application will be delegated to styling sheeting provided by Bootswatch.

VIS.js
vis.js is java script library that will be draw various reports. The reports will be used to show various trust levels between the tellers. Network graphs may be used to show trust levels between users.

4.2 Database Changes

Blockchain was the initial database to be used to store user data and interaction between teller. This was later changes to a SQL server. The reason was to illustrate the idea of such a remittance on SQL server and later change it to a block chain database. Block chain implementation was not achieved as time resource was limited.

4.3 Storage Approach

Hawala system is a debt transfer system. Thus, user will not a single amount stored rather different debt and credit upon each network teller. Thus, a method to keep track of all the credit/debit was to use a network table to store each debt.

The approach was to set the inviter as the dominant figure over invitee. In the network table, the inviter is teller A and invitee is Teller B. The column of “Credit” represented what teller B has credit over teller A. Example, if Teller A has requested to send R100 through teller B then the credit will get update with a sum of R100.

This approach was tricky as it required to check which user is making a transaction request and who is delivering the cash. Based upon the transaction the credit would be updated. Another problem was to show in the home page credit details of tellers based upon which user is logged in. if the user ID was stored in as teller A then credit should be showed as is, but if the logged in user’s Id is stored in Teller B then the credit had to be negated.

5 Results

A system with fully functioning remittance system was created. The remittance system was based upon ancient hawala system. The credit transfer system was fully operational with trust rewards functionality. The networking of the system was also based upon hawala system.

Networking

Every user had the ability to invite. In the hawala system, remittance is only done with someone who is socially connected. Thus, every user had to provide the username of the invitee and a pass key that both users would share via their social connection. The invitee would respond to the invitation with the pass key.

Credit Calculation

Since this remittance is debt transfer system, credit/debit calculation was a key aspect of this system. These had to be adjusted upon every transaction. Example, if User A transfers R1000 through User B. User B has R1000 credit upon User A. Later, if User B transfer R500 through User A, User B still has R500 credit upon User A.

6 Critique / Analysis

Trust Calculation

My approach of trust calculation could be improved. The current system only took number of transactions to determine the trust levels. There could be various elements in the system that can be used to determine the trust.

Trust is a social phenomenon. If special study of sociology is done on this system to find out when the trust of two individuals are at their highest and lowest using the input of the system. An expert opinion of predicting trust would sharpen prediction and bring the trust level closer to the truth.

Block Chain Implementation

The implementation did not include blockchain. Implementation of blockchain is a reasonable approach to make transactions temper proof. Temper proof transaction can be useful to present it as evidence in times of dispute. The evidence may also be to the standard of being accept in the courts of law.

7 Conclusion

This paper purposes an alternative banking solution. It is based upon an ancient hawala system which was discussed in the paper. The paper aims to make a practical demonstration of the concept using a web based application. The application included networking of the tellers and then fully implemented remittance system.

This paper proposes for further research in trust monitoring based on user activity and interaction. Along with trust monitoring, the implementation of a block chain as a

References

1.Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Business & Information Systems Engineering. 59, 183-187 (2017).

2.Becker, G.: Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Seminararbeit Ruhr-Universit¨at Bochum (2017).

3.Gauravaram, P., Kelsey, J., Knudsen, L., Thomsen, S.: On hash functions using checksums. International Journal of Information Security. 9, 137-151 (2009).

4.Hawala: How it Works. Africa Research Bulletin: Economic, Financial and Technical Series. 45, 17780C-17780C (2008).