DisLedger® - Distributed Concurrence Ledgers

www.DisLedger.com info@DisLedger.com

20 June, 2017

This whitepaper describes DisLedger® - Distributed Concurrence Ledgers (patent pending) an architecture for distributed ledgers tailored for financial institutions dealing in capital markets and payments. Concurrence is an alternative to seeking consensus in distributed ledger systems and does not utilize cryptocurrencies, Bitcoin, blockchains, or sidechains.

In current blockchains every transaction conducted by all of the members of a network are batched together and recorded in a single ledger. Other members on the system (not the actual parties to a transaction) must provide their approval for the transaction to be added to the ledger. Because numerous unrelated members have to give consent for a transaction, this type of architecture is called a consensus system. There are a few different protocols that blockchains use for consensus, but at the highest level they have the same effect. Parties that aren't involved in the transaction, and who are often one's direct competitors, must give their consent for you to conduct your transactions.

The blockchain and consensus protocols are artifacts of the Bitcoin system where their use made sense, but their continued use will keep blockchains from being implemented in some applications. Issues with consensus protocols center on four main areas: an organization is forced to rely on its direct competitors to process every business transaction; it is expensive to prove the non-repudiability of the system during a legal dispute; transaction processing times can't be guaranteed and the order of transactions can vary unpredictably due to system usage; and intelligence about the organization's business dealings are provided to its competitors in the network. Distributed concurrence ledgers are designed for situations where these issues aren't acceptable.

DisLedger® is a distributed concurrence ledger that provides more secure, faster and more scalable transaction processing than consensus blockchain systems. The same benefits of

immutable records, and regulatory transparency are provided, however the transactions are processed only by the actual counterparties involved and not by a consensus of the crowd.

Reliance on Competitors

Currently many organizations use clearinghouses or other services to assist in processing transactions but in these cases the outside parties are always trusted, impartial, and independent. Consensus based blockchains eliminate these impartial organizations and instead rely on a network of peers to validate and process transactions. One would expect the members of the blockchain network would all be direct competitors within an industry or asset class. An organization participating in a blockchain is forced to rely completely on its competitors to process its transactions in good faith without any manipulation, in order without frontrunning, and immediately without any delay. When transactions of such high values in such competitive industries are at stake, placing all of one's business deals in the hands of your competitors is unnecessarily risky.

In a distributed concurrence ledger the transaction processing is handled privately between only the actual counterparties to the transaction which eliminates any reliance on competitors.

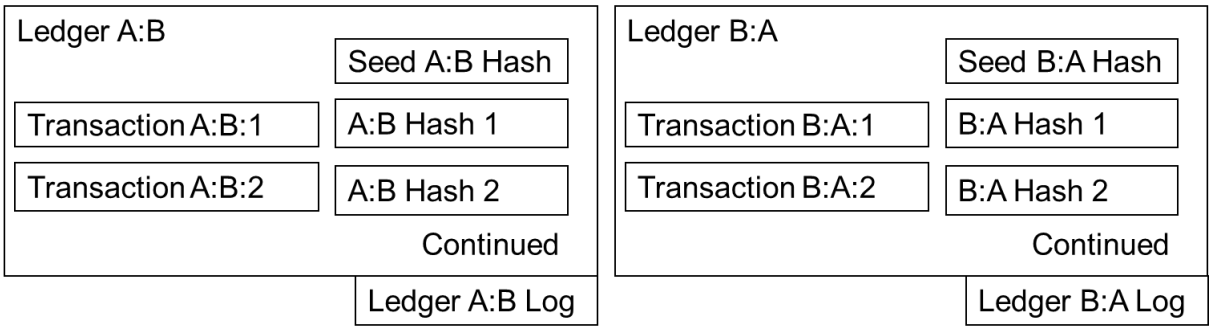
Non-Repudiable

The consensus protocols are both complex and imperfect, and can be manipulated causing improper processing, or the misordering and delaying of transactions. Because they are subject to attack and are processed completely outside of the control of the actual parties to a transaction they cannot be called irrefutable. When a dispute arises regarding a transaction in a blockchain one of the first defenses will be to argue the system was manipulated and that the transaction is not actually valid. Having a real world (off-chain asset) transaction represented on a blockchain does not guarantee meeting a burden of proof in informal dispute resolution, arbitration or litigation. It will be an unenviable position having to refute and prove that the incredibly complex system with no oversight or controlling body, that runs open source code, that was made up of competing organizations joining and leaving the network over time, and with different organizations actively validating or going inactive on a second by second basis, was not being manipulated at the time of the transaction and that the transaction was processed

accurately. They will also have to prove that from the time of the transaction to the current date the system has not been manipulated in any way, that every subsequent change to the blockchain was accurate, and that the record of the transaction has not been altered. While it may be possible to prove eventually, due to the complexity of the system proving all of this will be very costly for every disputed transaction. Significant cost will be expended by the parties to the transaction as well as all of the other members of the blockchain whose transactions are intermingled and were part of the consensus protocol. Validity of the consensus protocols and of transactions conducted using these protocols has not been challenged in court. But they certainly will be challenged at great expense to all involved including all of the unrelated parties in the network that will be embroiled in each dispute or litigation in the future.

In a distributed concurrence ledger transactions between counterparties are recorded with proof of the parties' agreement that each transaction is accurate, complete and valid; and that the entire ledger is accurate every time a ledger is updated with a new transaction. The evidence that the parties agree is documented repeatedly, cryptographically secured, and validated continuously. A shared counterparty ledger that is private and accessible only by the parties involved is created. The counterparty ledger holds each individual transaction that occurs between those counterparties.

Figure 1- Counterparty ledgers held by corresponding organizations A & B



As the ledger is held and accessible only by the counterparties, only the parties can add to the ledger, and identical updates must be executed by each party keeping the counterparty ledgers perfectly equal. This allows rapid processing of individual transactions, each cryptographically secured and immutable, while still providing transparency for auditing and regulatory

compliance access as required. No third parties are involved in the transaction, it is processed solely under the control of the parties involved, and a clear simple, evidentiary trail of the transactions is provided for dispute resolution. The non-repudiable ledgers provide a clear chain of title, which is easily proven with built-in documentary evidence.

Processing Speed and Order

Blockchains utilize a single ledger that is replicated and redundantly processed by all the members of a network. This single ledger batches all of the transactions from all the members within the network into one block. Consequently over time the file of every transaction can become large and unwieldy to transmit and process. Transactions are aggregated into blocks of unrelated transactions gathered from all members of the system for periodic processing which also delays execution and transaction settlement. The massive, but unnecessary, redundancy requires computer processing and data storage of large amounts of transactions to which the organization is not a party with direct impact on IT, electrical and cooling expenses.

In distributed concurrence ledgers the parties only process and store the transactions in which they are involved and do so rapidly and in sequential order without chance for frontrunning.

Business Intelligence

Information, such as which counterparties are conducting transactions, at what volume, with what frequency, etc., is sensitive and the sharing of it in blockchain systems provides valuable intelligence to one's competitors.

Distributed concurrence ledgers hold transactions between counterparties privately in a counterparty ledger not shared in monolithic blockchain. There is a counterparty ledger within the organization's Prime Ledger for each party with whom the account may conduct transactions.

The counterparty ledger is small, efficient, and records each individual transaction separately so no outside party gains insight into deal flow. This allows for rapid, deterministic processing at the individual transaction level as opposed to periodic processing of commingled transactions in a blockchain system. The ability to manage, partition and archive counterparty ledgers are simple

tools to keep the system sustainable over time that aren't available to monolithic blockchains. Transparency is still provided for compliance, however it can be tailored to provide access to only the appropriate counterparty ledgers under the regulator's purview and not offer universal access to the organization's entire workings.

Overview of Concurrence Ledger Processing

In any distributed ledger transactions can come from any traditional business function and in any asset class. It isn't critical to the ledger whether they are system generated, or manually entered, all digital or electronic scans of paper transactions. Using concurrence multiparty transactions are handled by the same process but for simplicity this description uses just two parties and skips some trivial details.

When the parties want to process a transaction they each conduct their own cryptographic hash on the contents of their version of the transaction data which results in a transaction hash. If the parties both are using complete and accurate data to conduct the hash operation then the resulting transaction hash calculated by one party will be the same as the transaction hash arrived at independently by the other party. By comparing the transaction hashes the two parties agree that the data concerning the transaction is identical. So at the time of the transaction both parties provide digitally signed Transaction Concurrence that the other party's record of the individual transaction is accurate and agreement has been reached. If the transaction hashes are not equal then there is a problem with one of the counterparty's version of the data that is immediately recognized; agreement between the parties does not take place; no contractual obligation or other transaction progress occurs; and the transaction cannot be processed until appropriate remedies are made to bring the two versions of the transaction data into alignment.

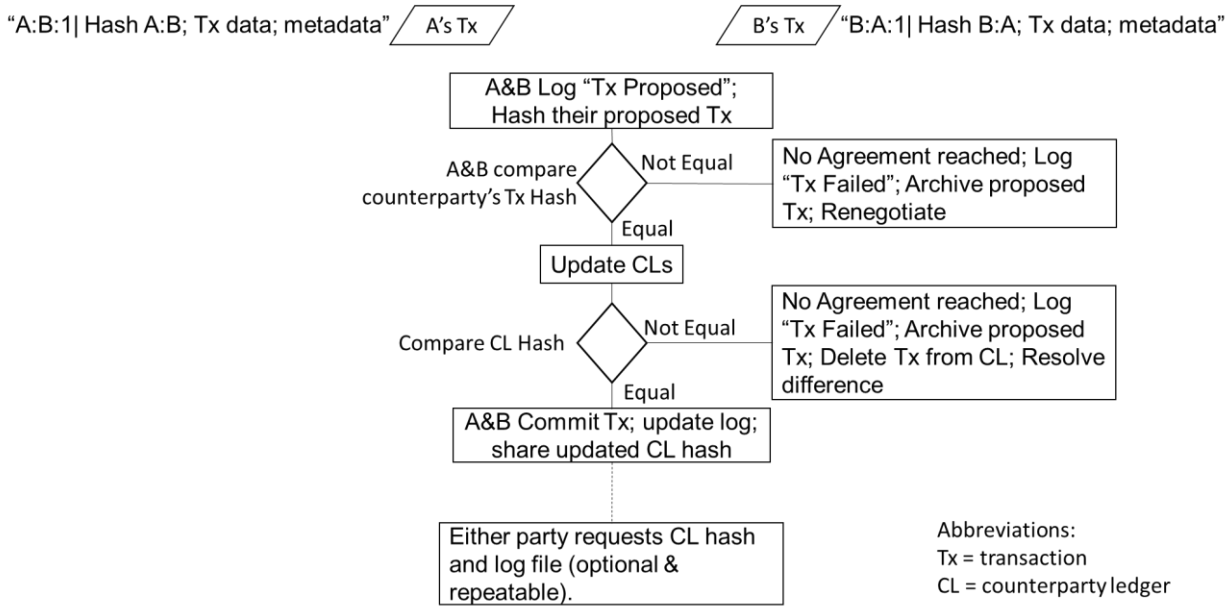
Upon agreement that the individual transaction record is correct by both parties a hash of the counterparty ledger updated with that latest transaction is conducted by each party. This counterparty ledger hash is then provided to the other party for comparison. If accurate records have been kept and the transaction is updated properly, both counterparties will have an identical counterparty ledger and the cryptographic hash of one party's ledger will be identical to a cryptographic hash of the other party's ledger. If both counterparty ledger hashes are equal then

this second concurrence, Chain Concurrence, irrefutably proves that not only is the latest transaction accurate but that the chain of all of the records on the counterparty ledger dating from the creation of the ledger to the latest transaction are accurate. Chain Concurrence provides non-repudiable proof of accurate recordkeeping also known as a clear chain of title. If the counterparty ledger hashes are not equal then there is a problem with updating one of the counterparty's ledgers and the problem can be resolved. Since the update to the counterparty ledgers wasn't successful; agreement between the parties did not take place; no contractual obligation is created and effectively the transaction fails.

These two concurrences ensure that the ledgers between counterparties are kept identical because the current transaction being processed and the historical chain of transactions from the beginning of the system must be identical or a transaction cannot be processed and the ledger cannot be altered. However each time a transaction is processed successfully and the counterparty ledger is updated a new counterparty ledger hash is agreed to by the parties. When the next transaction is conducted the hash of the counterparty ledger becomes part of the transaction to be processed which creates the chain of title.

A log of these sequential counterparty ledger hashes and all transactions attempted is maintained by both parties. At any time a party can request that their counterparty verify the corresponding counterparty hash. This periodic check provides ongoing proof of concurrence between the parties of the entire chain of transactions between them. Hashes can be repeatedly verified and the continued concurrence documented over time as evidence of the accuracy of the ledger. If in the future a counterparty ledger is claimed to have been altered by one party without concurrence by the other party the log will provide evidence of which system was correct and disputes can easily be resolved.

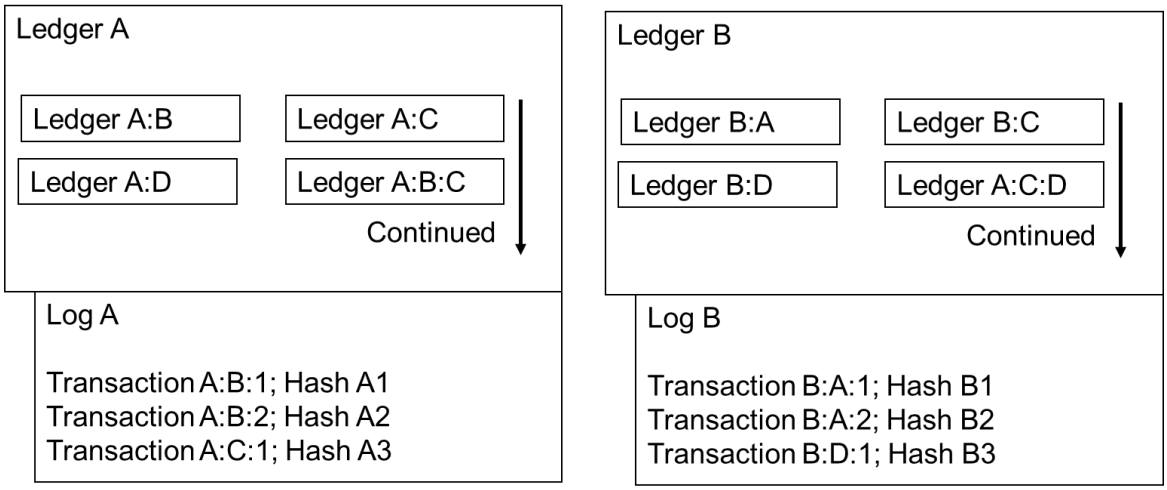
Figure 2- Concurrence ledger processing



Aggregation into the Prime Ledger

DisLedger® counterparty ledgers maintain the record of transactions with a single trading partner. To provide an accounting of the entire asset base of the organization each counterparty ledger is added to the Prime Ledger. By aggregating all of the positions from each counterparty ledger the organization maintains a real time view of its assets; settlement can occur on a gross basis or it can netted with support for ad hoc, intraday, and daily netting. The Prime Ledger allows for a separation of the high speed trading with counterparties from the holistic reporting on the organization's total asset base. The aggregation of positions provides the ability to use the assets in the underlying transactions for lending and collateral as is required in capital markets.

Figure 3- Prime ledgers for A & B holding multiple counterparty ledgers



Takeaway

The concurrence architecture will have a significant impact on the future of distributed ledgers. It is not a solution for every problem but organizations considering activity in the blockchain space should review this approach to see if it might be a better fit for their problems.

Blockchain is best suited for provenance type systems (land title, artwork, etc.) where providing visibility is a main goal and the long latency of transaction processing is not important. DisLedger® is tailored for high speed, transactional systems (capital markets settlement and payments processing) where privacy is important and transaction speed is critical.

Organizations looking for more information on adopting this architecture can contact us to continue the discussion: info@DisLedger.com