Network

WHITEPAPER

Mitthan Meena, Brad Miller, Mohit Bhargava

Rover Network Inc.

Table of Contents

Introduction **3**

Social Crypto 3

Monetary Issues of Developing nations 4

Introducing Rover Network **9**

Rover Consensus Agreement 9

1. DLT 9

2. Quantum Key Cryptography 9

3. Fault Tolerance 11

4. Associative Byzantine Agreement 12

4.1 Plenum Slices 12

5. Plenum Intersection 13

6. Associated Voting 14

6.1 Voting in Associative Byzantine Agreement System 14

6.2 Blocking Sets 14

6.3 Accepting and Confirming Statements 14

7 RCA 15

8 Current State of the entire system and Comparison 15

9 Conclusion 16

References **17**

Introduction

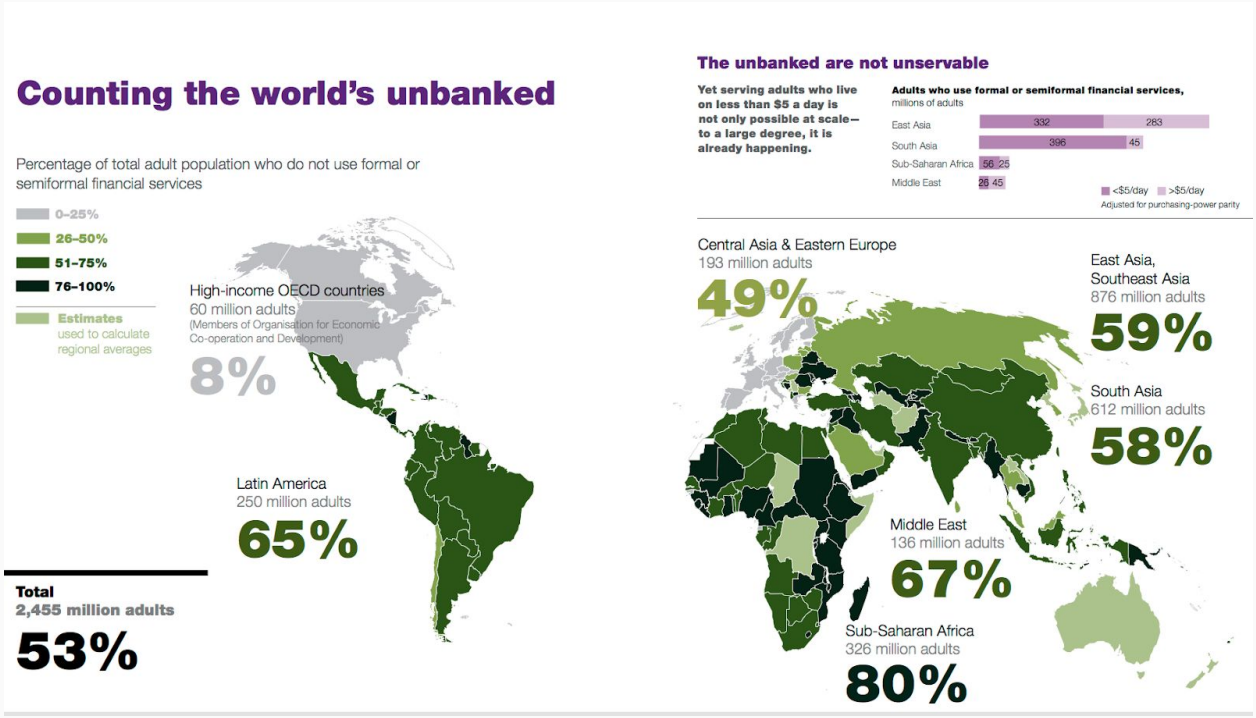
Social Crypto

In the crypto world today most companies are focused on two key metrics, technical development and the price of their tokens. We think there is a third component to consider, social responsibility, and we are proud there are a number of our crypto/blockchain competitors that agree with us and have demonstrated that in many ways. Many blockchain companies have taken the "direct route" and created foundations specifically to provide contributions for charities with coin donations or airdrops and there are blockchain and crypto companies that have been created just to service these charities as a specific industry. In this paper, attention will be brought to the "indirect route", exploring how certain aspects of the crypto world are also socially responsible just by providing our products and services for otherwise poorly served or even neglected global constituencies.

Servicing the "unbanked" population of the world has been a topic taken up by respected "think tanks" or public policy authorities for quite some time. A quick Google search brings up position papers by organizations like Accenture and The Brookings Institute that go back 15 years or more. The primary purpose of getting the unbanked into a banking relationship is to help these households build savings and improve their credit-risk profiles in order to lower their cost of payment services, eliminate a common source of personal stress and gain access to lower-cost sources of credit. Studies show that getting access to banking services can be the first step for the poor in lifting themselves from poverty and get them into the mainstream where they will have an opportunity for a better life with their families. This also benefits the overall population as the governments will have to dedicate fewer resources to the poor.

The strategy most often cited calls on banks and other financial institutions to open branches in the neighborhoods and communities where the poor reside. The United States Congress formally recognized this need for banking services for the poor in 1977 when they signed into law The Community Reinvestment Act (CRA) that insists that bank's service this population even if these branches are unprofitable and regulate their actions to insure compliance. Despite these regulatory efforts there are still today about 10 million unbanked households in the United States, or around 16 million residents.*****

Source: Mckinsey



Not surprisingly, a number of these people will most likely have mobile phones and and we think that might be the key to getting them into a banking relationship. But there will still be issues getting them banked via their mobile phone as banks charge monthly fees that are substantial to the point of disqualifying them from a meaningful banking relationship. In the aftermath of the Wells Fargo "fake account openings" scandal the relationship with US citizens and their banks is not one of trust at present. The perception today is that banks are more concerned with their profitability than helping people solve their financial challenges.

Not surprisingly the situation is worse in the less developed countries (LDCs) of the world where there are some 2 billion unbanked in the world today.** In high income OECD countries 94% of citizens have a bank account, in developing countries 54% have bank accounts and in the Middle East, the lowest in the world, only some 14% of the population have a bank account!

Monetary Issues of Developing Nations

In India today there are massive income equality issues, with the second greatest disparity between rich and poor where the top 1% have 58% of the wealth, and the top 10% have 81% of the wealth. These wealth disparities have gotten worse since 2000. The rich are getting richer and the poor are getting poorer due to a collapse in per capita food production and rural infrastructure deterioration, particularly power and road transportation. Market forces are said to

favor the urban areas over rural India. According to Oxfam India CEO Nisha Agrawal, "the growing divide undermines democracy and promotes corruption and cronyism."

India has made progress in the last several years in getting more of the unbanked banking as a result of their effort to get all citizens registered with India's Unique Identification Project known as "Aadhaar" (foundation in Hindi) which began in 2009. They use biometrics, fingerprints and iris scans for those that have no formal birth papers. Some 300 million new bank accounts have been opened since the project began, 180 million in the rural or semi urban areas where most of the unbanked reside. While there has been great progress, **50-60% of those that remain unbanked but have a mobile phone**, so that is where the effort must now be focused. Mobile banking costs make for a compelling business case. According to Citibank, the bank branch is 10 times more expensive than doing a transactions on a mobile phones. However, one problem remains; even if we get the unbanked a bank account through their mobile phone, bank fees are still quite expensive for the poor and can make a mobile banking account a non starter. It is thought that it will take another 20 years to open enough new bank branches in India to service the underserved locations. Banks still predominantly address their markets through brick and mortar branches and so they still have that high cost infrastructure when they deliver services to their mobile customers. It will be difficult for banks to compete with blockchain delivery systems and new internet or "virtual" banks that use them and have no physical presence.

Looking past India there are many other areas with large unbanked populations across the world, in Latin America 65% of the population do not have a bank account, 59% in East and Southeast Asia, 67% in the Mid East, and 58% in South Asia.

So the bottom line is that crypto currencies and the blockchain offer a more cost effective solution than the banking industry can offer including their mobile customers. The remaining unbanked need to get their banking done on the blockchain, where lower costs and fees will get them into a banking relationship and help them overcome poverty faster and in greater numbers, and the blockchain will be recognized as socially responsible in contributing to this economic transformation.

India also suffers from issues that other LDC's don't because of government actions that came into play in late 2016 and persist today. A large part of Indian commerce takes place in the cash economy where real estate and other large purchases for personal and business transactions are completed with cash in an effort to get around the goods and service tax which can be as high as 28%. This "parallel economy" or cash economy is said to represent around 20% of total GDP. It is thought that this "leaking wealth bucket" costs the government $200 billion a year in lost revenue.

Beyond trying to crack down on these untaxed transactions the Modi government cited corruption in general, the funding of terrorist organizations and counterfeit currency. The

government came up with an unusual solution. If people insist on getting around transaction taxes by making "all cash" transactions, then remove the higher denominations currency notes that are most frequently used to avoid these taxes. So in late 2016 they decided that they would eliminate the 500 and 1,000 rupee currency notes (about $7.50 and $15 USD today respectively). These bills, represented around 86% of the then existing currency in circulation. The thinking was that those large transactions would have to now be carried out with checks or with bank transfers that would make them trackable and thus taxable. The removal of these notes resulted in financial chaos as the transition to digital banking transactions failed to be adopted at a rate that could possibly offset the decline in cash transactions. The situation was also exacerbated by the fact that there ended up being a shortage of larger rupee notes because the central bank couldn't print new currency as fast enough to track the economy's growth rate, so the combination of two resulted in transaction velocity grinding to a fraction of the prior run rate. In the first month the lack of these large denomination notes resulted in stranding some 400,000 trucks as truck drivers had no small notes to pay for gas and other fees, including bribes. In addition ATMs across the country quickly ran out of cash, KC Chakrabarty, former deputy governor declared that the government had **"stopped market transactions for 70% of the economy."** The situation is so dire that wait times at banks can be as much as 12 hours with a maximum withdrawal of only $20 USD.

What if the Indian government had taken a different approach and addressed this black market by instead opening the market to crypto and the blockchain? Instead of banning the use of these high denomination notes they could do away with all paper currency and coins over time, so that every transaction would be done with a digital currency and would have a digital trail. They could create a new digital currency in short order and get it into circulation as fast as it could be downloaded! There have been calls for doing just this in a number of LDCs. Crypto can solve other issues as well. What about economies where inflation has plagued them for years such that it takes a wheelbarrow of paper currency to buy a bag of vegetables? Get rid of the wheelbarrow and replace it with a digital wallet (kept on their mobile phone) to keep their crypto money.

Banks in India with their relatively high cost structure charge minimum balances just like other places in the world so that they can rationalize (meaning not lose money) serving this market of poor people. Indian banks today require a minimum balance of 5,000 rupees ($73 USD) today, and dependent upon how low your balance falls relative to that minimum you will be charged a penalty fee of 100 rupees or 50 rupees (2% or 1%). With a mobile crypto offering and it's much lower cost structure the blockchain/crypto provider could afford to allow the poor to have accounts with no minimum and charge just a fraction of a rupee and make money.

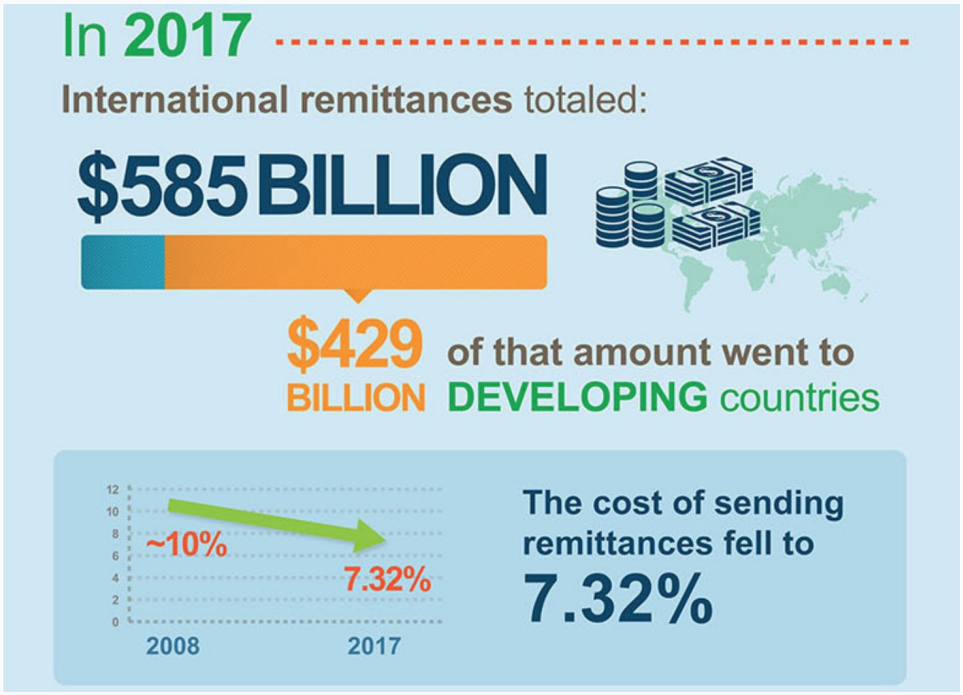
So a second socially responsible impact, you want to eliminate the ability to avoid a sales tax by paying with cash, then get rid of the cash! **Abolish your physical currency and you can**

resolve almost all corruption today, the funding of terrorist groups, currency counterfeiters, bribes of all description

All the things the Indian government was trying to do when they instituted their currency ban, were in the end made worse by neglecting to to promote digital currency transactions and bank accounts years ago.

Unfortunately corruption is not limited to India or even Southeast Asia. Transparency International has been publishing the Corruption Perception Index (CPI) since 1995, and in 2017 they rated 121 of 176 countries (69%) as having substantial corruption issues. It's our opinion that all of these countries that wish to try and attempt to curb corruption should take a serious look at adopting a digital currency, and because it's often government officials who benefit from the corruption, we fear there may not be many willing to consider it.

Let's move our focus to the "remittance market" where the blockchain can have another substantial financial impact. Remittance is when Indian nationals (all LDCs) send or remit money from where they are living back to relatives in India. We use India as an example because it is the largest remittance market, but this applies to all BRIC and LDC Countries. The much lower cost of living and income per capita of India relative to other western economies make India the largest remittance market in the world, whether the funds come from the US, Western Europe or Asia. If we look just at the US to India flow of funds, non resident Indians (NRI) sent $63 billion in 2017 from the US back home to India and paid about $3.5 billion to do that, around a 6% fee. If that money was instead sent from person to person on a blockchain those fee's would drop to a fraction of 1%, saving them about 90% of today's fee's, or well over $3 billion! Savings of that magnitude will have a social benefit for both remittance senders and recipients. Additionally instead of the money arriving in 2-7 days (standard for US banks) the funds will arrive in seconds! US banks and intermediaries, correspondent banks and currency exchange operators lose that income, but if they replace their current system with a blockchain themselves they can recoup some of their losses and get into the new payment system of the 21st century.



Source: World Bank

There are remittance markets in all the LDC's, and about 300 country corridors exist today, 35 are remittance "sending", and 99 remittance "receiving". The global average cost of sending remittances fell to 7.37% in 2015, down from 7.52% the prior year. According to the World Bank^^ Sub Saharan Africa has the most expensive remittance market with an average fee of 9.53% and South Asia has the cheapest fees at 5.43%. Banks are the most expensive remittance providers at a global average fee of 11.2%, money transfer brokers charge 6.2% and the post offices charge ***just*** 5.8% and not to mention the wire transfer fees regardless of the amount sent, those fees are especially onerous for the poor who often send small amounts! Remember that blockchain/crypto companies are talking about fees of around a quarter of 1% or lower.

Introducing Rover Network

The Rover Network a US start-up focused on enablement of private, permissioned blockchain solutions for the Enterprise. We offer customers ease, speed and scale of deployments built on the Rover Network platform with the use of our APIs and the support of our team of Blockchain specialists. Our vision is to help Enterprises of all sizes benefit from the security and efficiency of highly functional blockchains that can ensure trusted, timely transactions and authenticity of goods and services. We believe that money transfers should be as quick as a phone call or a WhatsApp message, not the 2-7 days it takes now to move money between the US and other foreign countries. In addition, we believe, the costs for global wire transfers can be reduced dramatically from an average fee of 6% to less than 1%.

Rover Consensus Agreement

This section represents DLT, Quantum Key Cryptography and an Associative Byzantine agreement (ABA) for internet-level consensus using a federally-hierarchical model. Below, we also uncover the findings of how the Rover Consensus Agreement is better than others in fault tolerant systems.

Currently most of the crypto world incorporates cryptographic functions that use Elliptical Curve Ed25519 for signing and it is found that it is quite difficult to recover enough of the secret key of a device performing EdDSA signatures. It is seen to have a single fault at the right time to be able to produce seemingly valid signature (even though the real signature by the actual secret key holder would not have the same value). This is an inherent weakness of the algorithms and cannot be avoided as long as the algorithms are generating their values through deterministic means. We present Quantum Key Cryptography here in addition to Ed25519 to enhance security at some point of time.

1. DLT

A Distributed Ledger Technology (DLT) is a database that is spread across multiple nodes (may be geographically distant). Each node replicates and saves a copy of ledger for its audit and authenticity. The groundbreaking reality in this ecosystem is that there is no central authority which needs to be considered as holding a master copy of the ledger. Updates to the ledger are independently carried out by each node by means of voting, consensus is reached once majority of the nodes agree on a given set of transactions. Distributed ledgers present a new paradigm for a way records are accumulated and communicated, and are poised to revolutionize the way individuals, firms and governments transact. This technology has also helped us to mitigate our dependence on banks, governments, lawyers, notaries and regulatory compliance officers.

2. Quantum Key Cryptography

This section covers the use of Quantum Key Cryptography along with the use of industry-standard public-key cryptography tools. Each transaction is currently signed by whomever sent it using the Ed25519 algorithm, which cryptographically proves that the sender was authorized to make the transaction. We thought to increase the security for the future and develop additional security features i.e. Quantum Key Cryptography when the other cryptographic keys may seem vulnerable when Quantum Computers come into existence. Conventional cryptosystems along with ENIGMA, DES or even RSA, are based on a combination of guesswork and arithmetic. Information idea indicates that conventional secret key cryptosystems can't be totally secure until the key is used only once and is at the least as long as the cleartext. The security of quantum cryptography is based on principles of essential physics, in contrast to assumptions about the sources available to a potential adversary.

This section describes the use of Bennett-Brassard (BB84) [1] quantum key distribution protocol as a case where the source and detector are under the limited control of an adversary. This evidence applies when both the source and the detector have small basis-based flaws, as is standard in sensible implementations of the protocol. The most important thing is the estimation of the generation price in some unique instances: resources that emit vulnerable coherent states, detectors with foundation-established efficiency, and misaligned resources and detectors. In traditional information principle and cryptography, it's taken for granted that virtual communications in principle can constantly be passively monitored or copied, even by means of someone ignorant of their meaning. However, whilst records are encoded in non-orthogonal quantum states, including single photons with polarization guidelines zero, forty five, ninety, and one hundred thirty five degrees, one obtains a communications channel whose transmissions in precept can not be examined or copied reliably by using an eavesdropper ignorant of sure key facts utilized in forming the transmission. The eavesdropper can't even benefit from partial records about the sort of transmission without altering it in a random and uncontrollable manner which will probably be detected by way of the channel's valid customers.

In quantum public key distribution, the quantum channel isn't directly used to send meaningful messages, but is instead used to transmit random bits between the users who share no common secret initially, in such a way that the users, by subsequent consultation over an ordinary non-quantum channel subject to passive eavesdropping, can tell with high probability whether the original quantum transmission has been disturbed in transit, as it would be by an eavesdropper. If the transmission has no longer been disturbed, they agree to apply these shared secret bits inside the famous (well-known) manner as a one-time pad to hide the meaning of next significant communications, or for other cryptographic packages requiring shared secret random statistics. If transmission has been disturbed, they discard it and attempt again, deferring any meaningful communications till they have succeeded in transmitting enough random bits via the quantum channel to function a one-time pad.

In more detail, a person ('Alice') chooses a random bit of string and a random sequence of polarization bases (rectilinear or diagonal). She then sends the other user ('Bob') a train of photons, each representing one bit of the string within the basis chosen for that bit function, a horizontal or 45 degree photon status for a binary 0 and a vertical or 135 degree photon standing

for a binary 1. As Bob receives the photons he comes to a decision, randomly for each photon and independently of Alice, whether or not to measure the photon's rectilinear polarization or its diagonal polarization, and translates the end result of the dimension as a binary 0 or 1. As explained in the previous section a random solution is produced and all facts lost whilst one attempts the rectilinear polarization of a diagonal photon, or vice versa. Thus Bob obtains significant records from only half of the photons he detects—the ones for which he guessed the precise polarization foundation.

Alice and Bob can therefore check for eavesdropping by way of publicly comparing a number of the bits on which they assume they ought to agree, though of course this sacrifices the secrecy of those bits. The bit positions used on this evaluation should be a random subset (say 1/3) of the correctly received bits, in order that eavesdropping on various photons is unlikely to break out detection. If all of the comparisons agree, Alice and Bob can conclude that the quantum transmission has been freed from tremendous eavesdropping, and those of the final bits that had been sent and acquired with the identical foundation additionally agree, and can effectively be used as a one-time pad for the next comfortable communications over the public channel. When this one-time pad is used up, the protocol is repeated to ship a new frame of random records over the quantum channel.

The following example illustrates the protocol.

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

3. Fault Tolerance

In almost all distributed systems there are 3 kind of issues that they have to deal with, namely faults, errors and failures. It is viable to say that the root cause of all is *fault*, wherever the problem starts, error is the result of that and failure is the final outcome. The ability of systems to keep functioning in a proper and desired manner even though there are partial faults occurring is termed as fault tolerant system. There could be some effect on the overall performance of the system, may be it might not be as good in performance as before but it will try to keep

functioning as usual. It is very challenging to develop a 100% fault tolerant system in distributed computing. There are two main reasons for the occurrence of a fault in a distributed system i.e. node failure - because of a hardware or a software & malicious errors caused by unauthorized access. In this work we will keep our focus to address the second issue.

4. Associative Byzantine Agreement

In this section we introduce the Associative Byzantine Agreement(ABA) model. ABA not only addresses the problem of updating the replicated state but also provides liveliness and availability throughout the participating entities. Nodes independently decide on what updates should be applied and avoid conflicting or incompatible states. We become aware of each update by means of a unique slot from which inter-update dependencies may be inferred. For example, slots may be consecutively numbered positions in a sequentially carried out log. The ABA system runs consensus that ensure nodes to agree on the contents of a slot.

A node n can effectively apply update x in slot j whilst it has competently carried out updates in all slots upon which j relies upon and, moreover, it believes all efficiently functioning nodes will ultimately agree on x for slot j. At this point, we are saying n has externalized x for slot j. The outside world can also react to the externalized values in irreversible ways but this node cannot later alter its thoughts when it has already externalized something. The most challenging part in such a system is that illicit parties can come and outnumber the well-behaved nodes. This associative model enjoys this safety by allowing each single node to choose its own group of trusted nodes on which it can rely on, we call this set as a plenum slice.

4.1 Plenum Slices

In protocols which use consensus mechanism, nodes swap messages declaring statements about slots. We count on such assertions that can't be solid, which can be assured if nodes are named by means of public key and that they digitally signed messages. When a node hears a enough set of nodes assert an assertion, it assumes no functioning node will ever contradict that declaration, we name that plenum slice. To allow progress within the face of node failures, a node may additionally have a couple of slices, some of which are enough to persuade it of a statement. At an excessive stage, then, an ABA device consists of a free confederation of nodes each of which has selected one or extra slices. An ABA is defined as a pair, comprising set of nodes and a plenum function.

A *plenum* is a set of nodes that can successfully reach agreement. Consensus mechanisms are taxonomically large and probably provide three key benefits that are: maintenance of group cohesion, enhancement of decision accuracy compared with lone individuals and improvement in decision speed. Here we are assuming of consensus in the same manner as animal groups, that are said to make consensus decisions when group members come to agree on the same option even partially if not unanimously. In the absence of centralized management, arriving at a consensus relies upon on neighborhood interactions in which every individual's chance of selecting an option will increase with the number of others already committed to that option. A plenum slice is a subset of a plenum which in particular convinces that particular node of agreement. It may be possible that the plenum slice is smaller than the plenum.

In ABA the membership and plenum must have some hierarchical order somehow maintained in spite of allowing open membership. We will walk over a simple example with a set of 4 nodes i.e. *n1, n2, n3* and *n4.* We illustrate how any of the node can elect their plenum slice.

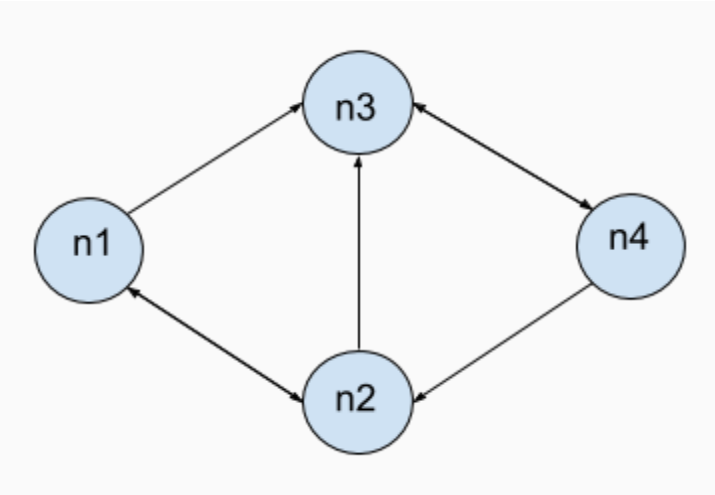


Fig 1 Different plenum slices

$$P(n1) = \{ n1, n2, n3 \}$$

$$P(n2) = \{ n1, n2, n3 \}$$

$$P(n3) = \{ n3, n4 \}$$

$$P(n4) = \{ n2, n3, n4 \}$$

In ABA we allow each node to choose it's trusted partners i.e. the plenum slice. By doing so we allow organic growth to the network by means of open membership. A traditional system, inclusive of PBFT [Castro and Liskov 1999], generally has $3f + 1$ nodes, any $2f + 1$ of which represent a plenum, f is the number of Byzantine Failures. System-extensive plenums consequently stand up from individual choices made via each node. Nodes may additionally pick out slices primarily based on arbitrary criteria which include reputation or financial arrangements. In some settings, no character node may additionally have whole knowledge of all nodes in the machine, but consensus should nonetheless be viable. Each node may have different tolerance numbers based on its selection of plenum.

5. Plenum Intersection

A protocol can assure agreement only if the plenum slices represented by using feature ***P*** satisfy a validity belongings we call that plenum intersection. An ABA relishes plenum intersection if any of the two plenums share at least one common node. A disarticulated plenum is more dangerous as an example where P permits two plenums $\{n1, n2,\}$ and $\{n3, n4\}$ that do not intersect. Disjoint plenums can independently agree on contradictory statements, undermining system-extensive agreement. When many plenums exist, plenum intersection fails if any of them do not intersect.

6. Associated Voting

This segment develops an associated balloting method that ABAS nodes can use to agree on a declaration. At a high stage, the process for agreeing on some statement *s* entails nodes exchanging sets of messages. First, nodes vote for s. Then, if the vote changed into a success, nodes confirm s, successfully holding a 2nd vote on the fact that the first vote succeeded.

From every node's perspective, the 2 rounds of messages divide agreement on a assertion s into three phases: unknown, standard, and confirmed. (This pattern dates back to 3pc [Skeen and Stonebraker 1983].) Initially, *s*'s popularity is completely unknown to a node *n*—sought to become actual, fake, or maybe stuck in a completely indeterminate nation. If the first vote succeeds, n may additionally come to simply accept s. No intact nodes ever take delivery of contradictory statements, so if n is intact and accepts s, then s can't be false.

6.1 Voting in Associative Byzantine Agreement System

A correct node in a Byzantine agreement system acts on a statement *s* handiest whilst it knows that other accurate nodes will by no means comply with statements contradicting *s*. Most protocols rent balloting for this purpose. Well-behaved nodes vote for a announcement *s* most effective if it's miles valid. Well-behaved nodes also in no way change their votes. Hence, in centralized Byzantine agreement, it is secure to just accept *s* if a plenum comprising a majority of nicely-behaved nodes has voted for it. We say a announcement *s* is endorsed once it has acquired the vital votes.

We also need to allow open membership by means of voting thus making the system associative and asynchronous. The most important aspect is to somehow ensure that the plenums intersect. Another implication of open membership is that nodes need to find out what constitutes a plenum as part of the vote casting technique.

6.2 Blocking Sets

In centralized consensus, liveness is either all or nothing asset of the system. Either a unanimously nicely-behaved plenum exists, otherwise ill-behaved nodes can prevent the working of the system by disallowing acceptance of new statements. In ABA, with the aid of comparison, liveness might also fluctuate throughout nodes.

6.3 Accepting and Confirming Statements

When an correct node *n* learns that it has endorsed a statement, it tells *n* that other intact nodes will not endorse contradictory statements. Although this condition is justifiable but we cannot make it mandatory for node *n* to accept statement *s*. The requirement for endorsing a statement is that the voting must have happened however some nodes may have voted for contradictory statements. If a node *n* is correct then no *n-blocking* set can consist of all corrupt nodes. In ABA node *n* accepts a statement *s* if it has never accepted a statement contradictory to *s*.

Unfortunately, for nodes to count on the reality of commonplace statements might yield sub-finest safety and liveness ensures in a associative consensus protocol.

Both obstacles of popular statements stem from complications when a set of intact nodes *N* votes in opposition to a statement *s* this is though encouraged. Particularly in light of ABA's non-uniform plenums, *S* may additionally prevent some intact node from ever endorsing *n*. To offer *n* a method of accepting *s* notwithstanding votes against it, the definition of accept has a 2d criterion based on *n-blocking* sets. But the second criterion is weaker than endorsement, offering no guarantees to corrupted nodes that revel in plenum intersection. The most important undertaking of disbursed consensus, whether centralized or not, is that a statement can get stuck in a completely indeterminate state than the system reaches settlement on it. Hence, a protocol has to know to not try and endorse externalized values at once.

7 RCA

The Rover Consensus Agreement is an implementation of associative Byzantine Agreement protocol. It is derived from the FBAS in which the optimal functions such as nomination and ballot voting are inherited. The nomination process in the protocol identifies the candidate values to be included in the slot. If run long sufficient, it in the end produces the same set of candidate values at each intact node, which means that nodes can combine the candidate values in a deterministic way to supply a single composite value for the slot. There are two huge caveats, but. First, nodes don't have any way of understanding while the nomination protocol has reached the point of convergence. Second, even after convergence, unwell-behaved nodes may be able to reset the nomination process a finite wide variety of times.

When nodes guess that the nomination protocol has converged, they execute the ballot protocol, which employs federated balloting to commit and abort ballots associated with composite values. When intact nodes comply with devote a ballot , the price related to the poll can be encouraged for the fit in question. When they agree to abort a poll, the ballot 's fee turns into irrelevant. If a ballot gets caught in a country in which one or greater intact nodes cannot dedicate or abort it, then nodes try once more with a better ballot , they associate the new ballot with the equal cost as the stuck one in case any node believes the stuck ballot became dedicated. Intuitively, safety consequences from making sure that all stuck and dedicated ballots are associated with the identical cost. Liveness follows from the fact that a stuck poll can be neutralized through moving to a better ballot.

8 Current State of the entire system and Comparison

As compared to other cryptocurrencies in the market we are already ahead in terms of transactions per second however we are working on supporting thousands of transactions in a second. Some of the key issues that we are trying to optimize include key signing, database optimizations and transaction submission. One experiment on key signing tells us that a typical SCSI disk performs speeds up to hundreds MB/s while SSD provides GB/s I/O, the key signing while using curve Ed25519 takes only 87548 cycles to sign a message. A quad-core 2.4GHz Westmere signs 109000 messages per second. Bitcoin or Ethereum blockchains cannot handle

even 10’s of transactions in a second but Rover blockchain can easily scale upto thousands of transactions in a second.

9 Conclusion

Byzantine agreement has long enabled peer to peer network to attain consensus with regulation, standard cryptography security and workability in designating faithful contributors. Recently, revolutionary notion of decentralized consensus has been instigated by Bitcoin which is leading to numerous modern network and research summons. Associative Byzantine agreement(ABA) is a prototype for accomplishing decentralized consensus while maintaining the conventional profits of Byzantine agreement (ABA). The key variation between ABA and prior Byzantine agreement systems is that ABA plenum from contributor's individual trust decisions, permitting an organic growth model which is similar to that of Internet. The Rover Consensus Agreement is an establishment for ABA that acquires minimal optimal safety against ill-behaved contributors. The key signing using Quantum Cryptography will allow the whole system to survive when the Quantum Computers come into existence thus we are keeping future interests in focus.

References

C. H. Bennett G. Brassard "Quantum cryptography: Public key distribution and coin tossing" Proceedings of IEEE International Conference on Computers Systems and Signal Processing Bangalore India pp. 175-179 1984.

Leslie Lamport. 1998. The Part-Time Parliament. 16, 2 (May 1998), 133–169.

Leslie Lamport. 2011a. Brief Announcement: Leaderless Byzantine Paxos. In *Proceedings of the 25th International Conference on Distributed Computing*. 141–142.

Leslie Lamport. 2011b. Byzantizing Paxos by Refinement. In *Proceedings of the 25th International Conference on Distributed Computing*. 211–224.

National Institute of Standards and Technology. 2012. *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publication 180-4.

http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

Jae Kwon. 2014. Tendermint: Consensus without Mining. (2014). http://tendermint.com/docs/tendermint.pdf

Marshall Pease, Robert Shostak, and Leslie Lamport. 1980. Reaching Agreement in the Presence of Faults.

Journal of the ACM 27, 2 (April 1980), 228–234.

Practical Byzantine Fault Tolerance: Miguel Castro & Barbara Liskov, Massachusetts Institute of Technology, (Feb 1999)