Preface

As the world becomes increasingly digital, cryptocurrency is a next natural step in the evolution of money. Pi is the first digital currency for everyday people, representing a major step forward in the adoption of cryptocurrency worldwide.

Our Mission: Build a cryptocurrency and smart contracts platform secured and operated by everyday people.

Our Vision: Build the world's most inclusive peer-to-peer marketplace, fueled by Pi, the world's most widely used cryptocurrency

DISCLAIMER for more advanced readers: Because Pi's mission is to be inclusive as possible, we're going to take this opportunity to introduce our blockchain newbies to the rabbit hole :)

Introduction: Why cryptocurrencies matter

Currently, our everyday financial transactions rely upon a trusted third party to maintain a record of transactions. For example, when you do a bank transaction, the banking system keeps a record & guarantees that the transaction is safe & reliable. Likewise, when Cindy transfers $5 to Steve using PayPal, PayPal maintains a central record of $5 dollars debited from Cindy's account and $5 credited to Steve's. Intermediaries like banks, PayPal, and other members of the current economic system play an important role in regulating the world's financial transactions.

However, the role of these trusted intermediaries also has limitations:

1. **Unfair value capture**. These intermediaries amass billions of dollars in wealth creation (PayPal market cap is ~$130B), but pass virtually nothing onto their *customers* - the everyday people on the ground, whose money drives a meaningful proportion of the global economy. More and more people are falling behind.
2. **Fees**. Banks and companies charge large fees for facilitating transactions. These fees often disproportionately impact lower-income populations who have the fewest alternatives.
3. **Censorship**. If a particular trusted intermediary decides that you should not be able to move your money, it can place restrictions on the movement of your money.
4. **Permissioned**. The trusted intermediary serves as a gatekeeper who can arbitrarily prevent anybody from being part of the network.
5. **Pseudonymous**. At a time when the issue of privacy is gaining greater urgency, these powerful gatekeepers can accidentally disclose -- or force you to disclose -- more financial information about yourself than you may want.

Bitcoin's "peer-to-peer electronic cash system," launched in 2009 by an anonymous programmer (or group) Satoshi Nakamoto, was a watershed moment for the freedom of money. For the first time in history, people could securely exchange value, without requiring a third party or trusted intermediary. Paying in Bitcoin meant that people like Steve and Cindy could pay each other directly, bypassing

institutional fees, obstructions and intrusions. Bitcoin was truly a currency without boundaries, powering and connecting a new global economy.

Introduction To Distributed Ledgers

Bitcoin achieved this historical feat by using *a distributed* record. While the current financial system relies on the traditional central record of truth, the Bitcoin record is maintained by a distributed community of “validators,” who access and update this public ledger. Imagine the Bitcoin protocol as a globally shared “Google Sheet” that contains a record of transactions, validated and maintained by this distributed community.

The breakthrough of Bitcoin (and general blockchain technology) is that, even though the record is maintained by a community, the technology enables them to always reach consensus on truthful transactions, insuring that cheaters cannot record false transactions or overtake the system. This technological advancement allows for the removal of the centralized intermediary, without compromising transactional financial security.

Benefits Of Distributed Ledgers

In addition to decentralization, bitcoin, or cryptocurrencies in general, share a few nice properties that make money smarter and safer, although different cryptocurrencies may be stronger in some properties and weaker in others, based on different implementations of their protocols. Cryptocurrencies are held in cryptographic wallets identified by a publicly accessible address, and is secured by a very strong privately held password, called the private key. This private key cryptographically signs transaction and is virtually impossible to create fraudulent signatures. This provides *security* and *unseizability*. Unlike traditional bank accounts that can be seized by government authorities, the cryptocurrency in your wallet can never be taken away by anyone without your private key. Cryptocurrencies are *censorship resistant* due to the decentralized nature because anyone can submit transactions to any computer in the network to get recorded and validated. Cryptocurrency transactions are *immutable* because each block of transactions represents a cryptographic proof (a hash) of all the previous blocks that existed before that. Once someone sends you money, they cannot steal back their payment to you (i.e., no bouncing checks in blockchain). Some of the cryptocurrencies can even support *atomic transactions.* “Smart contracts” built atop these cryptocurrencies do not merely rely on law for enforcement, but directly enforced through publicly auditable code, which make them *trustless* and can potentially get rid of middlemen in many businesses, e.g. Escrow for real estate.

Securing Distributed Ledgers (Mining)

One of challenges of maintaining a distributed record of transactions is security -- specifically, how to have an open and editable ledger while preventing fraudulent activity. To address this challenge, Bitcoin introduced a novel process called Mining (using the consensus algorithm “Proof of Work”) to determine who is “trusted” to make updates to the shared record of transactions.

You can think of mining as a type of economic game that forces “Validators” to prove their merit when trying to add transactions to the record. To qualify, Validators must solve a series of complex computational puzzles. The Validator who solves the puzzle first is rewarded by being allowed to post the latest block of transactions. Posting the latest block of transactions allows Validators to “mine” a Block Reward - currently 12.5 bitcoin (or ~$40,000 at the time of writing).

This process is very secure, but it demands enormous computing power and energy consumption as users essentially “burn money” to solve the computational puzzle that earns them more Bitcoin. The burn-to-reward ratio is so punitive that it is always in Validators’ self-interest to post honest transactions to the Bitcoin record.

Problem: Centralization of power and money put 1st Generation Cryptocurrencies out of reach

In the early days of Bitcoin, when only a few people were working to validate transactions and mining the first blocks, anyone could earn 50 BTC by simply running Bitcoin mining software on their personal computer. As the currency began to gain in popularity, clever miners realized that they could earn more if they had more than one computer working to mine.

As Bitcoin continued to increase in value, entire companies began to spring up to mine. These companies developed specialized chips (“ASICs”) and constructed huge farms of servers using these ASIC chips to mine Bitcoin. The emergence of these enormous mining corporations, known drove the Bitcoin Gold Rush, making it very difficult for everyday people to contribute to the network and get rewarded. Their efforts also began consuming increasingly large amounts of computing energy, contributing to mounting environmental issues around the world.

The ease of mining Bitcoin and the subsequent rise of Bitcoin mining farms quickly produced a massive centralization of production power and wealth in Bitcoin’s network. To provide some context, 87% of all Bitcoins are now owned by 1% of their network, many of these coins were mined virtually free in their early days. As another example, Bitmain, one of Bitcoin’s biggest mining operations has earned billions in revenue and profits.

The centralization of power in Bitcoin’s network makes it very difficult and expensive for the average person. If you want to acquire Bitcoin, your easiest options are to:

1. Mine It Yourself. Just hook up the specialized hardware (here's a rig on Amazon, if you're interested!) and go to town. Just know that since you'll be competing against massive server farms from across the world, consuming as much energy as the country of Switzerland, you won't be able to mine much
2. Buy Bitcoin on an exchange. Today, you can buy Bitcoin at a unit price of $3,500 / coin at the time of writing (note: you can buy fractional amount of Bitcoin!) Of course, you would also be taking on substantial risk in doing so as the price of Bitcoin is quite volatile.

Bitcoin was the first to show how cryptocurrency could disrupt the current financial model, giving people the ability to make transactions without having a third party in the way. The increase in freedom, flexibility, and privacy continues to drive the inevitable march toward digital currencies as a new norm. Despite its benefits, Bitcoin's (likely unintended) concentration of money and power present a meaningful barrier to mainstream adoption. As Pi's core team has conducted research to try to understand why people are reluctant to enter the cryptocurrency space. People consistently cited the risk of investing/mining as a key barrier to entry.

Solution: Pi - Enabling mining on mobile phones

After identifying these key barriers to adoption, the Pi Core Team set out to find a way that would allow everyday people to mine (or earn cryptocurrency rewards for validating transactions on a distributed record of transactions). As a refresher, one of the major challenges that arises with maintaining a distributed record of transactions is ensuring that updates to this open record are not fraudulent. While Bitcoin's process for updating its record is proven (burning energy / money to prove trustworthiness), it is not very user (or planet!) friendly. For Pi, we introduced the additional design requirement of employing a consensus algorithm that would also be extremely user friendly and ideally enable mining on personal computers and mobile phones.

In comparing existing consensus algorithms (the process that records transactions into a distributed ledger), the Stellar Consensus Protocol emerges as the leading candidate to enable user-friendly, mobile-first mining. Stellar Consensus Protocol (SCP) was architected by David Mazières a professor of Computer Science at Stanford who also serves as Chief Scientist at the Stellar Development Foundation. SCP uses a novel mechanism called Federated Byzantine Agreements to ensure that updates to a distributed ledger are accurate and trustworthy. SCP is also deployed in practice through the Stellar blockchain that has been operating since 2015.

A Simplified Introduction To Consensus Algorithms

Before jumping to introducing the Pi consensus algorithm, it helps to have a simple explanation on what a consensus algorithm does for a blockchain and the types of consensus algorithms that today's blockchain protocols generally use, e.g. Bitcoin and SCP. This section is explicitly written in a oversimplified manner for the sake of clarity, and is not complete. For higher accuracy, see the section *Adaptations to SCP* below and read the stellar consensus protocol paper.

A blockchain is a fault-tolerant distributed system that aims to totally order a list of blocks of transactions. Fault-tolerant distributed systems is an area of computer science that has been studied for many decades. They are called distributed systems because they do not have a centralized server but instead they are composed of a decentralized list of computers (called *nodes* or *peers*) that need to come to a consensus as to what is the content and total ordering of blocks. They are also called fault-tolerant because they can tolerate a certain degree of faulty nodes into the system (e.g. up to 33% of nodes can be faulty and the overall system continues to operate normally).

There are two broad categories of consensus algorithms: The ones that elect a node as the leader who produces the next block, and the ones where there is no explicit leader but all nodes come to a consensus of what the next block is after exchanging votes by sending computer messages to each other. (Strictly speaking the last sentence contains multiple inaccuracies, but it helps us explain the broad strokes.)

Bitcoin uses the first type of consensus algorithm: All bitcoin nodes are competing against each other in solving a cryptographic puzzle. Because the solution is found randomly, essentially the node that finds the solution first, by chance, is elected the leader of the round who produces the next block. This algorithm is called “Proof of work” and results in a lot of energy consumption.

A Simplified Introduction To Stellar Consensus Protocol

Pi uses the other type of consensus algorithms and is based on the Stellar Consensus Protocol (SCP) and an algorithm called Federated Byzantine Agreement (FBA). Such algorithms don’t have energy waste but they require exchanging many network messages in order for the nodes to come to “consensus” on what the next block should be. Each node can independently determine if a transaction is valid or not, e.g. authority of making the transition and double spending, based on the cryptographic signature and the transaction history. However, for a network of computers to agree on which transactions to record in a block and the order of these transactions and blocks, they need to message each other and have multiple rounds of voting to come to consensus. Intuitively, such messages from different computers in the network about which block is the next would look like the following: “I *propose* we all vote for block A to be next”; “I *vote* for block A to be the next block”; “I *confirm* that the majority of the nodes I trust also voted for block A”, from which the consensus algorithm enables this node to conclude that “A is the next block; and there could be no block other than A as the next block”; Even though the above voting steps seem a lot, the internet is adequately fast and these messages are lightweight, thus such consensus algorithms are more lightweight than Bitcoin’s proof of work. One major representative of such algorithms is called Byzantine Fault Tolerance (BFT). Several of the top blockchains today are based on variants of BFT, such as NEO and Ripple.

One major criticism of BFT is that it has a centralization point: because voting is involved, the set of nodes participating in the voting “quorum” are centrally determined by the creator of the system in its beginning. The contribution of FBA is that, instead of having one centrally determined quorum, each node sets their own “quorum slices”, which will in turn form different quorums. New nodes can join the network in a decentralized way: they declare the nodes that they trust and convince other nodes to trust them, but they don’t have to convince any central authority.

SCP is one instantiation of FBA. Instead of burning energy like in Bitcoin's proof of work consensus algorithm, SCP nodes secure the shared record by vouching for other nodes in the network as trustworthy. Each node in the network builds a quorum slice, consisting of other nodes in the network that they deem to be trustworthy. Quorums are formed based on its members quorum slices, and a validator will only accept new transactions if and only if a proportion of nodes in their quorums will also accept the transaction. As validators across the network construct their quorums, these quorums help nodes to reach consensus about transactions with guarantee on security. You can learn more about the Stellar Consensus Protocol by watching this short, 7 min explanation video or checking out this technical summary of SCP.

Pi's Adaptations to Stellar Consensus Protocol (SCP)

Pi's consensus algorithm builds atop SCP. SCP has been formally proven [Mazieres 2015] and is currently implemented within the Stellar Network. Unlike Stellar Network consisting mostly of companies and institutions (e.g., IBM) as nodes, Pi intends to allow devices of individuals to contribute on the protocol level and get rewarded, including mobile phones, laptops and computers. Below is an introduction on how Pi applies SCP to enabling mining by individuals.

There are four roles Pi users can play, as Pi miners. Namely:

- **Pioneer**. A user of the Pi mobile app who is simply confirming that they are not a "robot" on a daily basis. This user validates their presence every time they sign in to the app. They can also open the app to request transactions (e.g. make a payment in Pi to another Pioneer)
- **Contributor**. A user of the Pi mobile app who is contributing by providing a list of pioneers he or she knows and trusts. In aggregate, Pi contributors will build a global trust graph.
- **Ambassador**. A user of the Pi mobile app who is introducing other users into Pi network.
- **Node**. A user who is a pioneer, a contributor using the Pi mobile app, and is also running the Pi node software on their desktop or laptop computer. The Pi node software is the software that runs the core SCP algorithm, taking into account the trust graph information provided by the Contributors.

A user can play more than one of the above roles. All roles are necessary, thus all roles are rewarded with newly minted Pi on a daily basis as long as they participated and contributed during that given day. In the loose definition of a "miner" being a user who receives newly minted currency as a reward for contributions, all four roles are considered to be Pi miners. We define"mining" more broadly than its traditional meaning equated to executing proof of work consensus algorithm as in Bitcoin or Ethereum.

First of all, we need to emphasize that the Pi Node software has not been released yet. So this section is offered more as an architectural design and as a request to solicit comments from the technical community. This software will be fully open source and it will also heavily depend on stellar-core which is also open source software, available here. This means that anyone in the community will be able to read, comment and propose improvements on it. Below are the Pi proposed changes to SCP to enable mining by individual devices.

Nodes

For readability, we define as a *correctly connected node* to be what the SCP paper refers to as an *intact node*. Also, for readability, we define as the *main Pi network* to be the set of all intact nodes in the Pi network. The main task of each Node is to be configured to be correctly connected to the main Pi network. Intuitively, a node being incorrectly connected to the main network is similar to a Bitcoin node not being connected to the main bitcoin network.

In SCP's terms, for a node to get correctly connected means that this node must chose a "quorum slice" such that all resulting quorums that include this node intersect with the existing network's quorums. More precisely, a node vn+1 is correctly connected to a main network N of n already correctly connected nodes (v1, v2, …, vn) if the resulting system N' of n+1 nodes (v1, v2, …, vn+1) enjoys quorum intersection. In other words, N' enjoys quorum intersection iff any two of its quorums share a node. -- i.e., for all quorums U1 and U2, $U1 \cap U2 \neq \emptyset$.

The main contribution of Pi over the existing Stellar consensus deployment is that it introduces the concept of a trust graph provided by the Pi Contributors as information that can be used by the Pi nodes when they are setting up their configurations to connect to the main Pi network.

When picking their quorum slices, these Nodes must take into consideration the trust graph provided by the Contributors, including their own security circle. To assist in this decision, we intend to provide auxiliary graph analysis software to assist users running Nodes to make as informed decisions as possible. This software's daily output will include:

- a ranked list of nodes ordered by their distance from the current node in the trust graph; a ranked list of nodes based a pagerank analysis of nodes in the trust graph
- a list of nodes reported by the community as faulty in any way a list of new nodes seeking to join the network
- a list of most recent articles from the web on the keyword "misbehaving Pi nodes" and other related keywords; a visual representation of Nodes comprising the Pi network similar to what is shown in StellarBeat Quorum monitor [source code]
- a quorum explorer similar to QuorumExplorer.com [source code]
- a simulation tool like the one in StellarBeat Quorum monitor that shows the expected resulting impacts to this nodes' connectivity to the Pi network when the current node's configuration changes.

An interesting research problem for future work is to develop algorithms that can take into consideration the trust graph and suggest each node an optimal configuration, or even set that configuration automatically. On the first deployment of the Pi Network, while users running Nodes can update their Node configuration at any time, they will be prompted to confirm their configurations daily and asked to update them if they see fit.

Mobile app users

When a Pioneer needs to confirm that a given transaction has been executed (e.g. that they have received Pi) they open the mobile app. At that point, the mobile app connects to one or more Nodes to inquire if the transaction has been recorded on the ledger and also to get the most recent block number

and hash value of that block. If that Pioneer is also running a Node the mobile app connects to that Pioneer's own node. If the Pioneer is not running a node, then the app connects to multiple nodes and to cross check this information. Pioneers will have the ability select which nodes they want their apps to connect to. But to make it simple for most users, the app should have a reasonable default set of nodes, e.g. a number of nodes closest to the user based on the trust graph, along with a random selection of nodes high in pagerank. We ask for your feedback on how the default set of nodes for mobile Pioneers should be selected.

Mining rewards

A beautiful property of the SCP algorithm is that it is more generic than a blockchain. It coordinates consensus across a distributed system of Nodes. This means that the same core algorithm is not only used every few seconds to record new transactions in new blocks, but also it can be used to periodically run more complex computations. For example, once a week, the stellar network is using it to compute inflation on the stellar network and allocate the newly minted tokens proportionally to all stellar coin holders (Stellar's coin is called lumens). In a similar manner, the Pi network employs SCP once a day to compute the network-wide new Pi distribution across all Pi miners (pioneers, contributors, ambassadors, nodes) who actively participated in any given day. In other words, Pi mining rewards are computed only once daily and not on every block of the blockchain.

For comparison Bitcoin allocates mining rewards on every block and it give all of the reward to the miner who was lucky enough to be able to solve a computationally intensive randomized task. This reward in Bitcoin currently 12.5 Bitcoin (~$40K) is given to only one miner every 10 minutes. This makes it extremely unlikely for any given miner to ever get rewards. As a solution to that, bitcoin miners are getting organized in centralized mining pools, which all contribute processing power, increasing the likelihood of getting rewards, and eventually sharing proportionally those rewards. Mining pools are not only points of centralization, but also their operators get cuts reducing the amount going to individual miners. In Pi, there is no need for mining pools, since once a day everyone who contributed get a meritocratic distribution of new Pi.

Transaction fees

Similar to Bitcoin transactions, fees are optional in the Pi network. Each block has a certain limit of how many transactions can be included in it. When there is no backlog of transactions, transactions tend to be free. But if there are more transactions, nodes order them by fee, with highest-fee-transactions at the top and pick only the top transactions to be included in the produced blocks. This makes it an open market. Implementation: Fees are proportionally split among Nodes once a day. On every block, the fee of each transaction is transferred into a temporary wallet from where in the end of the day it is distributed to the active miners of the day. This wallet has an unknown private key. Transactions in and out of that wallet are forced by the protocol itself under the consensus of all nodes in the same way the consensus also mints new Pi every day.

Limitations and future work

SCP has been extensively tested for several years as part of the Stellar Network, which at the time of this writing is the ninth largest cryptocurrency in the world. This gives us a quite large degree of

confidence in it. One ambition of the Pi project is to scale the number of nodes in the Pi network to be larger than the number of nodes in the Stellar network to allow more everyday users to participate in the core consensus algorithm. Increasing the number of nodes, will inevitably increase the number of network messages that must be exchanged between them. Even though these messages are much smaller than an image or a youtube video, and the Internet today can reliably transfer videos quickly, the number of messages necessary increases with the number of participating nodes, which can become bottleneck to the speed of reaching consensus. This will ultimately slow down the rate, at which new blocks and new transactions are recorded in the network. Thankfully, Stellar is currently much faster than Bitcoin. At the moment, Stellar is calibrated to produce a new block every 3 to 5 seconds, being able to support thousands of transactions per second. By comparison, Bitcoin produces a new block every 10 minutes. Moreover, due to Bitcoin's lack in the safety guarantee, Bitcoin's blockchain in rare occasions can be overwritten within the first hour. This means that a user of Bitcoin must wait about 1 hour before they can be sure that a transaction is considered final. SCP guarantees safety, which means after 3-5 seconds one is certain about a transaction. So even with the potential scalability bottleneck, Pi expects to achieve transaction finality faster than Bitcoin and possibly slower than Stellar, and process more transactions per second than Bitcoin and possibly fewer than Stellar.

While scalability of SCP is still an open research problem. There are multiple promising ways one could speed things up. One possible scalability solution is bloXroute. BloXroute proposes a blockchain distribution network (BDN) that utilizes a global network of servers optimized for network performance. While each BDN is centrally controlled by one organization, they offer a provably neutral message passing acceleration. I.e. BDNs can only serve all nodes fairly without discrimination as messages are encrypted. This means the BDN does not know where messages come from, where they go, or what is inside. This way Pi nodes can have two message passing routes: A fast one through BDN, which is expected to be reliable most of the time, and its original peer-to-peer message passing interface that is fully decentralized and reliable but is slower. The intuition of this idea is vaguely similar to caching: The cache is place where a computer can access data very quickly, speeding the average computation, but it is not guaranteed to always have every needed piece of information. When the cache misses, the computer is slowed down but nothing catastrophic happens. Another solution can be using secure acknowledgment of multicast messages in open Peer-to-Peer networks [Nicolosi and Mazieres 2004] to speed up message propagation among peers.

Pi Economic Model: Balancing Scarcity and Access

Pros and cons of 1st Generation Economic Models

One of Bitcoin's most impressive innovations is its marriage of distributed systems with economic game theory.

Pros

Fixed Supply

Bitcoin's economic model is simple. *There will only ever be 21 million Bitcoin in existence*. This number is set in code. With only 21M to circulate among 7.5B people around the world, there is not enough Bitcoin to go around. This scarcity is one of most important drivers of Bitcoin's value.

Decreasing Block Reward

Bitcoin' distribution scheme, pictured below, further enforces this sense of scarcity. The Bitcoin block mining reward halves every 210,000 blocks (approximately every ~4 years.) In its early days, the Bitcoin block reward was 50 coins. Now, the reward is 12.5, and will further decrease to 6.25 coins in May 2020. Bitcoin's decreasing rate of distribution means that, even as awareness of the currency grows, there is less to actually mine.

Cons

Inverted Means Uneven

Bitcoin's inverted distribution model (less people earning more in the beginning, and more people earn less today) is one of the primary contributors to its uneven distribution. With so much Bitcoin in the hands of a few early adopters, new miners are "burning" more energy for less bitcoin.

Hoarding Inhibits Use As A Medium Of Exchange

Although Bitcoin was released as a "peer to peer electronic cash" system, the relative scarcity of Bitcoin has impeded Bitcoin's goal of serving as a medium exchange. Bitcoin's scarcity has led to its perception as a form of "digital gold" or a digital store of value. The result of this perception is that many Bitcoin holders are unwilling to spend Bitcoin on day-to-day expenses.

The Pi Economic Model

Pi, on the other hand, seeks to strike a balance between creating a sense of scarcity for Pi, while still ensuring that a large amount does not accumulate into a very small number of hands. We want to make sure our users earn more Pi as they make contributions to the network. Pi's goal is to build an economic model that is sophisticated enough to achieve and balance these priorities while remaining intuitive enough for people to use.

Pi's economic model design requirements:

- **Simple**: Build an intuitive and transparent model

- **Fair distribution**: Give a critical mass of the world's population access to Pi
- **Scarcity**: Create a sense of scarcity to sustain Pi's price over time
- **Meritocratic earning**: Reward contributions to build and sustain the network

Pi - Token Supply

Token Emission Policy

1. Total Max Supply = M + R + D
    1. M = total mining rewards
    2. R = total referral rewards
    3. D = total developer rewards

1. M = $\int$ f(P) dx where f is a logarithmically declining function
    1. P = Population number (e.g., 1st person to join, 2nd person to join, etc.)

1. R = r * M
    1. r = referral rate (50% total or 25% for both referrer and referee)

1. D = t * (M + R)
2. t = developer reward rate (25%)

M - Mining Supply (Based on fixed mining supply minted per person)

In contrast to Bitcoin which created a fixed supply of coins for the entire global population, Pi creates a fixed supply of Pi *for each person that joins the network up to the first 100 Million participants.* In other words, for each person that joins the Pi Network, a fixed amount of Pi is pre-minted. This supply is then released over the lifetime of that member based on their level of engagement and contribution to network security. The supply is released using an exponentially decreasing function similar to Bitcoin's over the member's lifetime.

R - Referral Supply (Based on fixed referral reward minted per person and shared b/w referrer and referee)

In order for a currency to have value, it must be widely distributed. To incentivize this goal, the protocol also generates a fixed amount of Pi that serves as a referral bonus for both the referrer and the referee (or both parent and offspring :) This shared pool can be mined by both parties over their lifetime - when both parties are actively mining. Both referrer and referee are able to draw upon this pool in order to avoid exploitative models where referrers are able to "prey" on their referees. The referral bonus serves as a network-level incentive to grow the Pi Network while also incentivizing engagement among members in actively securing the network.

D - Developer Reward Supply (Additional Pi minted to support ongoing development)

Pi will fund its ongoing development with a "Developer Reward" that is minted alongside each coin that is minted for mining and referrals. Traditionally, cryptocurrency protocols have minted a fixed amount of supply that is immediately placed into treasury. Because Pi's total supply is dependent on the

number of members in the network, Pi progressively mints its developer reward as the network scales. The progressive minting of Pi's developer reward is meant to align the incentives of Pi's contributors with the overall health of the network.

f is a logarithmically decreasing function - early members earn more

While Pi seeks to avoid extreme concentrations of wealth, the network also seeks to reward earlier members and their contributions with a relatively larger share of Pi. When networks such as Pi are in their early days, they tend to provide a lower utility to participants. For example, imagine having the very first telephone in the world. It would be a great technological innovation but not extremely useful. However, as more people acquire telephones, each telephone holder gets more utility out of the network. In order to reward people that come to the network early, Pi's individual mining reward and referral rewards decrease as a function of the number of people in the network. In other words, there is a certain amount of Pi that is reserved for each "slot" in the Pi Network.

Utility: Pooling and monetizing our time online

Today, everyone is sitting on a veritable treasure trove of untapped resources. Each of us spend hours day on our phones. While on our phones, each of our views, posts or clicks creates extraordinary profits for large corporations. At Pi, we believe that people have the right to capture value created from their resources.

We all know that we can do more together than we can alone. On today's web, massive corporations like Google, Amazon, Facebook have immense leverage against individual consumers. As a result, they are able to capture the lionshare of value created by individual consumers on the web. Pi levels the playing field by allowing its members to pool their collective resources so they can get a share of the value that they create.

The graphic below is the Pi Stack, where we see particularly promising opportunities for helping our members capture value. Below, we go into each of these areas in more detail.

Introducing the Pi Stack - Unleashing underutilized resources

Pi Ledger And Shared Trust Graph - Scaling Trust Across The Web

One of the biggest challenges on the internet is knowing who to trust. Today, we rely on the rating systems of providers such as Amazon, eBay, Yelp, to know who we can transact with on the internet. Despite the fact that we, customers, do the hard work of rating and reviewing our peers, these internet intermediaries capture the lionshare of the value created this work.

Pi's consensus algorithm, described above, creates a native trust layer that scales trust on the web without intermediaries. While the value of just one individual's Security Circle is small, the aggregate of our individual security circles build a global "trust graph" that help people understand who on the Pi Network can be trusted. The Pi Network's global trust graph will facilitate transactions between strangers that would not have otherwise been possible. Pi's native currency, in turn, allows everyone who contributes to the security of the network to capture a share of the value they have helped create.

Pi's Attention Marketplace - Bartering Unutilized Attention And Time

Pi allows its members to pool their collective attention to create an attention market much more valuable than any individual's attention alone. The first application built on this layer will be a *scarce social media channel* currently hosted on the home screen of the application. You can think of the *scarce social media channel* as Instagram with one global post at a time. Pioneers can wager Pi to engage the attention of other members of the network, by sharing content (e.g., text, images, videos) or asking questions that seek to tap into the collective wisdom of the community. On the Pi Network, everyone has the opportunity to be an influencer or to tap into the wisdom of the crowd. To date, Pi's Core Team has been using this channel to poll the community's opinion on design choices for Pi (e.g. the community voted on the design and colors of the Pi logo.) We have received many valuable responses and feedback from the community on the project. One possible future direction is to open the attention market for any Pioneer to use Pi to post their content, while expanding the number of channels hosted on the Pi Network.

In addition to bartering attention with their peers, Pioneers may also opt into bartering with companies that are seeking their attention. The average American sees between 4,000 and 10,000 ads a day. Companies fight for our attention and pay tremendous amounts of money for it. But we, the customers, receive no value from these transactions. In Pi's attention marketplace, companies seeking to reach Pioneers will have to compensate their audience in Pi. Pi's advertising marketplace will be strictly opt-in only and will provide an opportunity for Pioneers to monetize one of their greatest untapped resources: their attention.

Pi's Barter Marketplace - Build Your Personal Virtual Storefront

In addition to contributing trust and attention to the Pi Network, we expect Pioneers to be able to contribute their unique skills and services in the future. Pi's mobile application will also serve as a Point of Sales where Pi's members can offer their untapped goods and services via a "virtual storefront" to other members of the Pi Network. For example, a member offer up an underutilized room in their apartment for rent to other members on the Pi Network. In addition to real assets, members of the Pi Network will also be able to offer skills and services via their virtual storefronts. For example, a member of the Pi Network could offer their programming or design skills on the Pi marketplace. Overtime, the value of Pi will be supported by a growing basket of goods and services.

Pi's Decentralized App Store - Lowering The Barrier Of Entry For Creators

The Pi Network's shared currency, trust graph, and marketplace will be the soil for a broader ecosystem of decentralized applications. Today, anyone that wants to start an application needs to bootstrap its technical infrastructure and community from scratch. Pi's decentralized applications store will allow Dapp developers to leverage Pi's existing infrastructure as well as the shared resources of the community and users. Entrepreneurs and developers can propose new Dapps to the community with requests for access to the network's shared resources. Pi will also build its Dapps with some degree of interoperability so that Dapps are able to reference data, assets, and processes in other decentralized applications.

Governance - Cryptocurrency for and by the people

Challenges w/ 1st Generation Governance models

Trust is the foundation of any successful monetary system. One of the most important factors engendering trust is *governance*, or the process by which changes are implemented to the protocol over time. Despite its importance, governance is often one of the most overlooked aspects of cryptoeconomic systems.

First generation networks such as Bitcoin largely avoided formal (or "on-chain") governance mechanisms in favor of informal (or "off-chain") mechanisms arising from a combination of role and incentive design. By most measures, Bitcoin's governance mechanisms has been quite successful, allowing the protocol to grow dramatically in scale and value since its inception. However, there have also been some challenges. The economic concentration of Bitcoin has led to a concentration of political power. The result is that everyday people can get caught in the middle of destructive battles between massive holders of Bitcoin. One of the most recent examples of this challenge has been the ongoing battle between Bitcoin and Bitcoin Cash. These civil wars can end in a fork where or where the blockchain. For token holders, hard forks are inflationary and can threaten the value of their holdings.

Pi's Governance Model - a two-phase plan

In an article challenging the merits of on-chain governance, Vlad Zamfir, one of Ethereum's core developers, argues that blockchain governance "*is not an abstract design problem. It's an applied social problem.*" One of Vlad's key points is that it is very difficult to design governance systems "a priori" or before observations of the particular challenges arising from a specific political system. One historical example is in the founding of the United States. The first experiment with democracy in the United States, the Articles of Confederation, failed after an eight-year experiment. The Founding Fathers of the United States were then able to draw upon the lessons of the Article of Confederation to craft the the Constitution - a much more successful experiment.

To build an enduring governance model, Pi will pursue a two-phase plan.

Provisional Governance Model (< 5M Members)

Until the network hits a critical mass of 5M members, Pi will operate under a provisional governance model. This model will most closely resemble “off-chain” governance models currently employed by protocols like Bitcoin and Ethereum, with Pi’s Core Team playing an important role in guiding the development of the protocol. However,, Pi’s Core Team will still rely heavily on the input of the community. The Pi mobile application itself is where Pi’s core team has been soliciting community input and engaging with Pioneers. Pi embraces community critiques and suggestions, which is implemented by the open-for-comments features of Pi’s landing page, FAQs and white paper. Whenever people browse these materials on Pi’s websites, they can submit comment on a specific section right there to ask for questions and make suggestions. Offline Pioneer meetups that Pi’s core team have been organizing will also be an important channel for community input.

Additionally, Pi’s Core Team will develop more formal governance mechanics. One potential governance system is liquid democracy. In liquid democracy, every Pioneer will have the ability to either vote on an issue directly or to delegate their vote to another member of the network. Liquid democracy would allow for both broad and efficient membership from Pi’s community.

Pi’s “Constitutional Convention” (> 5M Members)

Upon hitting 5M members, a provisional committee will be formed based on previous contributions to the Pi Network. This committee will be responsible for soliciting and proposing suggestions from and to the wider community. It will also organize a series of on- and offline conversations where Pi’s members will be able to weigh on Pi’s long-term constitution. Given Pi’s global user base, the Pi Network will conduct these conventions at multiple locations across the world to ensure accessibility. In addition to hosting in-person conventions, Pi will also use its mobile application as a platform for allowing Pi’s member to participate in the process remotely. Whether in-person or online, Pi’s community members will have the ability to participate in the crafting Pi’s long-term governance structure.

Roadmap / Deployment plan

Phase 1 - Design, Distribution, Trust Graph Bootstrap.

The Pi server is operating as a faucet emulating the behavior of the decentralized system as it will function once its live. During this phase improvements in the user experience and behavior are possible and relatively easy to make compared to the stable phase of the main net. All minting of coins to users will be migrated to the live net once it launches. In other words, the livenet will pre-mint in its genesis block all account holder balances generated during Phase 1, and continue operating just like the current

system but fully decentralized. Pi is not listed on exchanges during this phase and it is impossible to “buy” Pi with any other currency.

Phase 2 - Testnet

Before we launch the main net, the Node software will be deployed on a test net. The test net will use the same exact trust graph as the main net but on a testing Pi coin. Pi core team will host several nodes on the test net, but will encourage more Pioneers to start their own nodes on the testnet. In fact, in order for any node to join the main net, they are advised to begin on the testnet. The test net will be run in parallel to the Pi emulator in phase one, and periodically, e.g. daily, the results from both systems will be compared to catch the gaps and misses of the test net, which will allow Pi developers to propose and implement fixes. After a thorough concurrent run of both systems, testnet will reach a state where its results consistently match the emulator’s. At that time when the community feels its ready, Pi will migrate to the next phase.

Phase 3 - Mainnet

When the community feels the software is ready for production, and it has been thoroughly tested on the testnet, the official mainnet of the Pi network will be launched. An important detail is that, in the transition into the mainnet, only accounts validated to belong to distinct real individuals will be honored. After this point, the faucet and Pi network emulator of Phase 1 will be shut down and the system will continue on its own forever. Future updates to the protocol will be contributed by the Pi developer community and Pi’s core team, and will be proposed by the committee. Their implementation and deployment will depend on nodes updating the mining software just like any other blockchains. No central authority will be controlling the currency and it will be fully decentralized. Balances of fake users or duplicate users will be discarded. This is the phase when Pi can be connected to exchanges and be exchanged for other currencies.