Preface

Cryptocurrency is the next natural step in the evolution of money as the world becomes increasingly digital. Pomo is a digital currency project that paved the way for the penetration and adoption of cryptocurrencies in people's daily lives and represents an important step forward in this field.

Our Mission

Building a cryptocurrency and smart contracts platform secured and operated by ordinary people.

Our Vision

Building the world's most comprehensive peer-to-peer marketplace powered by Pomo, the world's most participating cryptocurrency.

DISCLAIMER for advanced readers: As Pomo’s mission is to be as inclusive as possible, we will use this opportunity to introduce blockchain newbies to this complex structure.

Introduction: Why are cryptocurrencies important?

In the current system, our daily financial transactions are dependent on a trusted third party keeping track of those transactions. For example, when you make a bank transaction, the banking system keeps a record and guarantees that the transaction is safe and reliable. Similarly, when Efe transfers 5 USD to Arda using PayPal; PayPal maintains a central record of 5 USD debited to Efe's account and 5 USD deposited to Arda's account. All intermediaries like banks, PayPal, and other members of the current economic system play an important role in regulating the world's financial transactions.

However, these reliable brokers have some limitations:

- Unfair Valuation: These brokers accumulate billions of dollars in assets (PayPal's market cap is approximately $130 billion), but they transfer almost nothing to the people whose money drives a significant portion of the global economy and forms the base - their customers. More and more people are getting poorer day by day.
- Fees: Banks and companies charge large fees for handling financial transactions. These wages disproportionately affect the low-income population, who often have the fewest alternatives.
- Censorship: If a certain trusted broker decides that you shouldn't move your money, they can place restrictions on the movement of your money.
- Authorization: The trusted agent serves as a controller that can arbitrarily prevent anyone from being part of the network.
- Pseudonym: At a time when the privacy issue becomes more important, these powerful controllers can/may accidentally or forcibly disclose more of your financial information than you would like.

Introduction to Distributed Ledgers

Bitcoin achieved this historical feat using a distributed record. While the current financial system relies on the traditional and centralized record of truth, the Bitcoin record is maintained by a distributed community of "verifiers" who access and update this ledger.

You can think of the Bitcoin protocol as a globally shared “Google Excel Spreadsheet” containing a record of transactions approved and maintained by this distributed community.

The groundbreaking point of Bitcoin (and blockchain technology in general); This technology ensures that the community always reaches consensus on the correct transactions, ensuring that even if the registration is provided by a community, cheaters cannot register false transactions or hijack the system. This technological development allows the removal of central intermediaries without compromising the security of financial transactions.

Benefits of Distributed Ledgers

Besides decentralization, bitcoin, or cryptocurrencies in general, share many features that make money smarter and more secure, although stronger in some features and weaker in others, depending on the different implementations of their protocols.

Cryptocurrencies are kept in cryptographic wallets identified by a publicly accessible address and protected by a very strong, personal password called a private key. This private key cryptographically signs the transaction. Creating fraudulent signatures is nearly impossible. It prevents seizure and provides security.

Unlike traditional bank accounts, which can be confiscated by government officials, your wallet cannot be taken by anyone without your private key. Cryptocurrencies are resistant to censorship thanks to decentralization, as anyone can send transactions to any computer on the network for registration and confirmation. Cryptocurrency transactions cannot be changed because each block of transactions represents an encrypted proof (providing) of all previous blocks that previously existed.

When someone sends you money, they can't steal their payment back (i.e. no bounced checks on the blockchain). Some cryptocurrencies may even support atomic transactions. “Smart contracts” built on top of cryptocurrencies do not simply rely on rules to be enforced but are directly enforced via publicly auditable codes that make the rules unreliable and potentially enable many businesses to get rid of intermediaries (e.g. escrow account for real estate).

Securing Distributed Ledgers (Mining)

One of the challenges of keeping a distributed record of transactions is security – specifically, how to have a clear and editable ledger while preventing fraudulent activity. To address this challenge, Bitcoin has launched a new process called Mining, using the Proof of Work (POW) consensus algorithm to determine who is “trusted” to update the shared transaction record.

You can think of mining as a kind of economic game that forces “validators” to prove their rights while trying to add transactions to the record (to the blockchain). These validators must solve a series of complex computational puzzles in order to be selected. The validator who solves the puzzle first is rewarded by being allowed to publish the latest block of transactions. Publishing the latest block of transactions allows validators to mine a Block Reward that is currently (14/03/2019) 12.5 bitcoins (or ~$40,000).
This process is very safe, but it takes enormous computing power and energy consumption (aka burning money) to solve the computational puzzles that earn Bitcoin. The conversion rate of burnt money to reward is so punishing that it is always in miners' best interest to enter honest transactions in the Bitcoin record.

Problem: Centralization of power and money makes 1st generation cryptocurrencies inaccessible

In the early days of Bitcoin, where only a few people worked to confirm transactions and mine the first blocks, anyone could earn 50 BTC by running Bitcoin mining software on their personal computers. As the currency began to gain popularity, clever miners realized that they could earn more if they had multiple computers to mine. As the value of Bitcoin continued to increase, all companies began to take an interest in mining. These companies developed customized chips (ASIC) and built huge server farms to mine Bitcoin with these ASIC chips.

Bitcoin – The emergence of these huge mining firms that created the gold rush phenomenon has made it very difficult for ordinary people to contribute to the network and be rewarded. All these efforts began to consume more and more computational energy and contributed to the increase of environmental problems in the world.

The ease of Bitcoin mining and the subsequent increase in mining farms has resulted in a rapid and massive centralization of productive power and wealth in the Bitcoin network. For example, currently, only 1% of the Bitcoin network owns 87% of all Bitcoins, most of which were mined almost for free in their early days.

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

1. Dig Yourself. To do this, simply install and run special hardware! Of course, while doing this, know that you will not be able to mine many Bitcoins as you will be competing against large server farms all over the world that consume as much energy as the country of Switzerland. You will have to give your all!

2. Buy Bitcoin on an exchange. Today, at the time of this writing, you can own 1 Bitcoin at a unit price of $3,500. (note: you can buy Bitcoin in fractions!) Of course, you also take a significant risk in doing so because the price of Bitcoin is highly volatile.

Bitcoin was the first attempt to show how cryptocurrency could disrupt the current financial model by giving people the ability to conduct financial transactions without a third party. The rise in freedom, flexibility, and privacy continues to drive the inevitable transition towards the new norm, digital currencies. Despite its benefits, Bitcoin's (possibly involuntary) distribution of money and power remains a serious obstacle to its widespread adoption. Pomo's core team conducted research to understand why people were reluctant to enter the cryptocurrency space. People have consistently shown that the main barrier to entry is investment/mining risk.

Solution: Pomo - Making mining possible on mobile phones

After identifying these key barriers to adoption, the Pomo Core Team began looking for a way that would allow ordinary people to mine (i.e. earn cryptocurrency rewards for verifying transactions in a distributed transaction record). Here's a reminder: One of the biggest challenges in keeping a distributed record of transactions is ensuring that updates to this open record are not fraudulent. While Bitcoin's process of updating records is proven (burning energy/money to prove credibility), this method is not user (or planet!) friendly. For the Pomo, we have outlined the additional design needs of using a consensus algorithm that will enable mining on PCs and mobile phones while also being extremely user-friendly.