M2 Cash: A Digital Currency

ABSTRACT

M2cash ("M2") is a decentralized digital currency that will break the cycle of inevitability that occurs with almost every publicly mined cryptocurrency. Specifically, M2's mechanics prevent it from evolving to a state in which the wealthy and powerful dominate. Most cryptocurrency projects trigger technological arms races in which those with the most powerful mining tools, win. M2 changes the cryptocurrency mining landscape with Perpetual Individual Mining. Using public and personal nodes on a Distributed Proof of Activity (dPoA) blockchain, any person with connectivity and a mobile device capable of authenticating them to a dPoA blockchain can mine M2. The complete supply of M2 — 50 billion tokens — were minted to a smart contract on a Proof of Work blockchain. A Decentralized Supply and Pricing Oracle manages the token's supply and stability. Initialized with $50 million (USD) in liquidity, M2 is incorruptible; engineered to place people in a position of self-determination from which they can choose to participate in capitalism and commerce.

INTRODUCTION

According to the World Bank (2020), over 720 million people will be living in extreme poverty in 2021. Three factors that drive the current crisis — and extend its impact into the future — include the COVID19 pandemic (see Figure 1), the pandemic-associated global economic recession, armed conflict, and climate change.

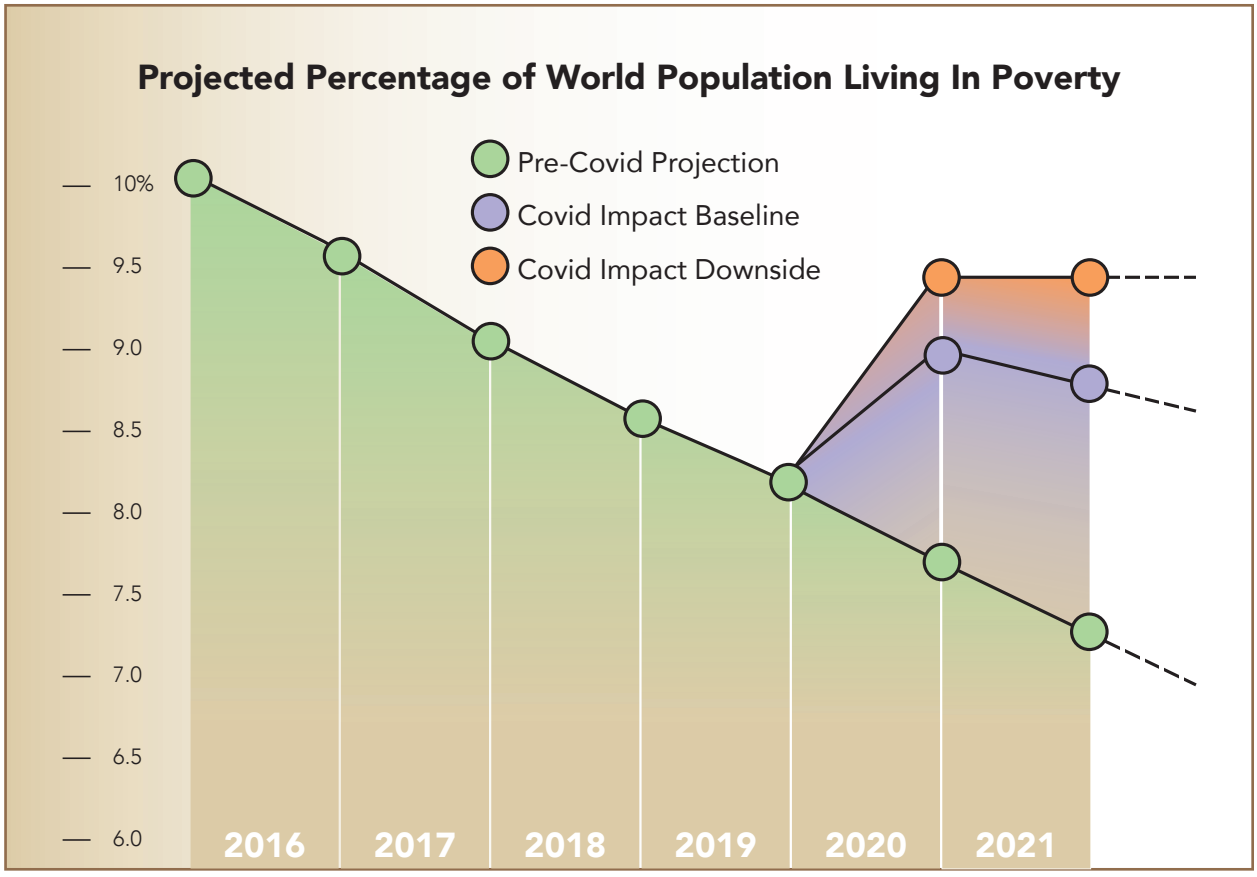

Figure 1: Impact of COVID-19 (two scenarios) on the proportion of global poverty, where the global extreme poverty rate is considered at US$1.90 per day (WorldBank 2020).

Improvement in mobile phone technology is facilitating access to the internet. GSMA estimates that 67% or 5.27 billion people currently have a mobile device and that by 2022, 5 billion will have access to the internet (see Figure 2). Significant growth is expected in emerging markets such as Sub-Saharan Africa, Asia Pacific, and Greater China.

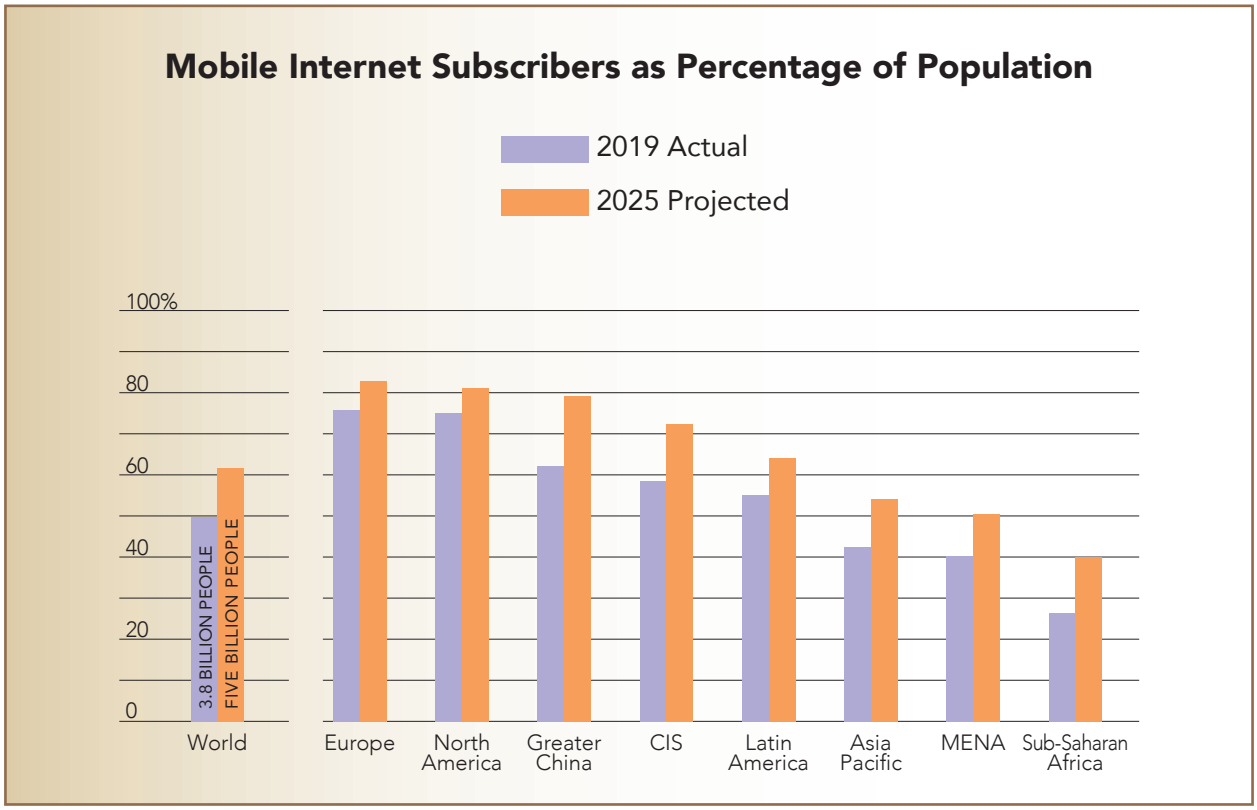

Figure 2: Mobile Internet Access (Stryjak, 2020)

Attempts to facilitate access to finance through cryptocurrencies have had limited success. While the largest cryptocurrencies have succeeded in creating great stores of value, they have been unable to prevent the transfer of wealth and power to the domain of banks, governments, and other highly capitalized organizations.

Absent from the cryptocurrency landscape has been an equalizing opportunity within which individuals could mine an exchangeable digital currency to improve their lives - and do so without access to a centralized exchange or a financial institution.

M2 is a decentralized digital currency initially backed by the liquidity in its central bank on the Ethereum blockchain and redeemable at the current market rate. The notable elements of M2 include the following:

- No centralized company or organization controls M2.
- M2 is not pegged to fiat currency.
- M2 can be mined as a result of specific user activity on a mobile app.
- While M2 is mined on a dPoA blockchain, the token can exist on any blockchain.
- M2 will function as a digital currency, regardless of how it is used, moved, and or exchanged.
- 100% of M2 will be placed in an Automated Market Maker and there will be zero pre-mining.

M2 DEPLOYMENT

In mid-2021, $50 million (USD) and the entire supply of 50 billion M2 tokens were placed into an Automated Market Maker ("AMM") bonding curve in an Ethereum smart contract. No further tokens can be minted, and no keys exist to modify this decision. Any person or smart contract with access to the AMM on the Ethereum blockchain can trade this ERC20 token. M2 can be acquired or redeemed at its calculated price from an AMM smart contract that serves as its decentralized central bank. The token price is updated after every trade as a function of changing reserves in the curve.

DECENTRALIZED CENTRAL BANK MANAGEMENT

To facilitate M2 price discovery, an AMM uses its bonding curve's liquidity and spreads it along a token price/supply curve using a mathematical formula to create a virtual order book (see Figure 3).

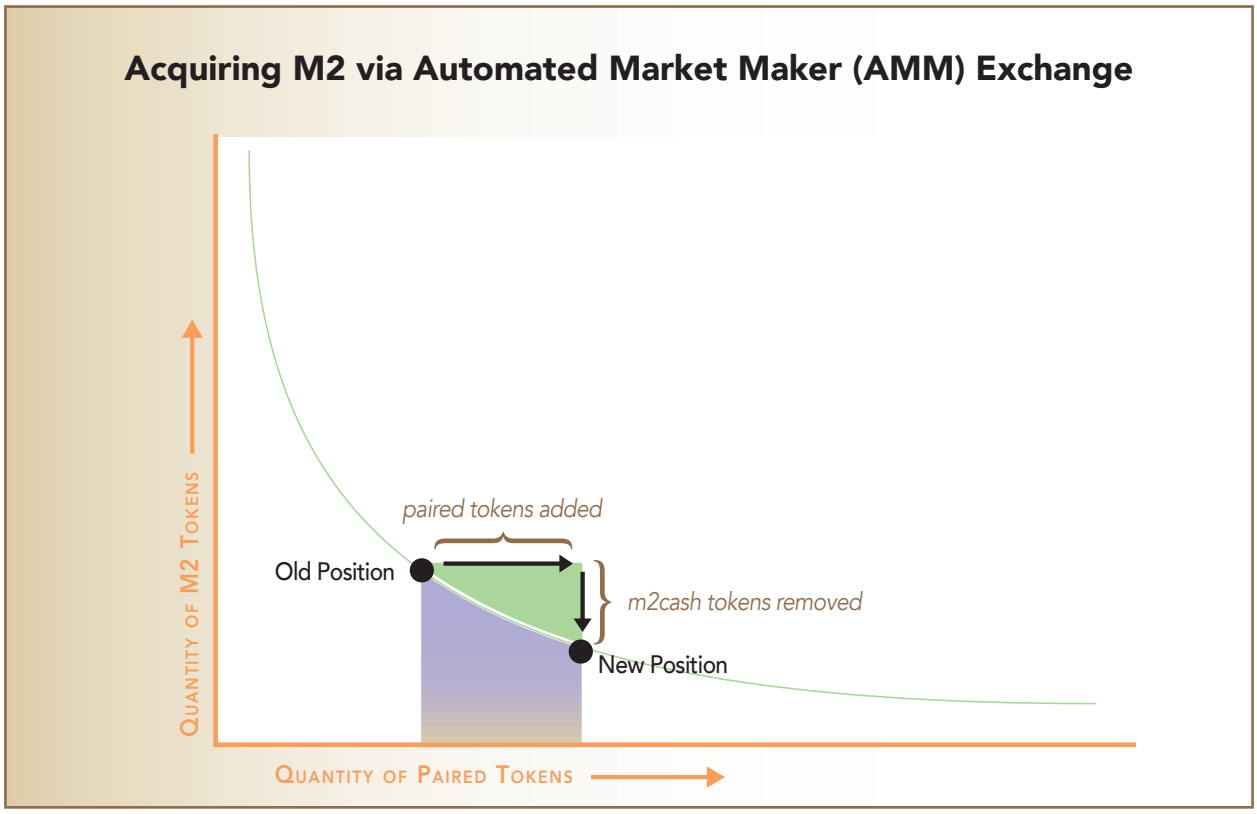

Figure 3: M2 AMM Bonding Curve

When a token is purchased from the M2 smart contract, the AMM will increase the price of the next token. When a token is sold into the M2 smart contract, the AMM will decrease the price of the next token. The AMM holds assets whose price is measured by its reserves.

The AMM's pricing function maps the assets' quantities in reserves to their marginal price. Holding M2's reserve on the blockchain is essential in building trust for the token - as every stakeholder can verify it. The M2 bonding curve holds M2 and the PE coin - which secures the distributed proof of activity blockchain.

DECENTRALIZED SUPPLY & PRICING ORACLE

The Decentralized Supply and Pricing Oracle ("dSPO") and the AMM bonding curve manage the supply of M2 and support its stability. An excess of M2 tokens in the liquidity pool (LP) implies limited demand for the token; consequently, when M2's LP token process is executed (please see "The Mechanic" below for details), the number of M2 tokens extracted from the curve will increase. Conversely, when there is high demand for M2, the number of LP tokens extracted will decrease. The dSPO and AMM stabilize the value of M2 by adjusting the availability of the token's supply to meet demand. This methodology is known as the M2 Mechanic.

THE AMM AND THE CONSTANT PRODUCT FORMULA

A Liquidity Pool token ("LP Token") is created when two tokens are "merged" or paired to establish a liquidity pool. The AMM for M2's LP Token uses a Constant Product Formula (X*Y=K). This formula describes the relationship between the two tokens, as illustrated in Figure 3 above. In a liquidity pool, each LP token contains proportionally equal amounts of M2 and its paired token from a value perspective.

Using the Constant Product Formula as a guide, each LP token has a value of K in which X would equal the value of M2 and Y would equal the value of the paired token. So after a point at which a large volume of M2 has been purchased and removed from the curve, the LP tokens would contain proportionally less M2 (X) than the paired token (Y); the product (from a value perspective) of these (K) would be the same value as it was before the purchase took place.

When M2 tokens are swapped (i.e., removed or purchased) from the AMM bonding curve ("the curve") by virtue of a trade, an equivalent amount in value must be replaced in the curve by its paired token. The converse occurs upon the sale of M2 into the liquidity pool wherein an equivalent value of the paired token is removed to offset the addition of M2 into the curve.

THE M2 MECHANIC

The M2 Mechanic (the "Mechanic") is a decentralized process that can be executed only once every 24 hours. The Mechanic is executed by calling a contract by any user on the Ethereum blockchain. The Mechanic runs only when called; it is an entirely decentralized, democratic element of M2.

When called, the Mechanic will execute the following seven tasks:

1. Extract 0.1428% of the LP Tokens from the pool in their current "concentrations" of M2 and its paired token.
2. Split the LP Token into its atomic parts (i.e., M2 and its paired token).
3. Send 50% of the M2 tokens to a burn contract (i.e., sent to an unrecoverable address on the blockchain).
4. Send 50% of the M2 tokens to a mining contract for perpetual individual mining.
5. Swap 50% of the paired token for M2 at current market prices.
6. Combine the newly swapped M2 and the remaining paired tokens into an LP token and insert it back into the M2 liquidity pool.
7. Reward any "remnant tokens" that can't be paired to the re-inserted LP to the entity or individual that executed the Mechanic.

BALANCING SUPPLY AND DEMAND WITH THE M2 MECHANIC

If the M2 LP Token composition contains fewer M2 than its paired token, fewer individual M2 tokens will be burned and allocated to mining by the Mechanic. The Mechanic interprets this condition as an indication of greater market demand for M2. If the LP contains more M2 than its paired token, more individual M2 tokens will be burned and allocated to mining by the Mechanic. The Mechanic interprets this condition as an indication of lower market demand for M2 and reduces its supply accordingly. These results — in conditions of either excess or limited M2 supply — are M2's de facto mining emission rate.

PERPETUAL INDIVIDUAL MINING

The DPoA mining of M2 means that only biometrically authenticated individual miners on mobile devices can mine M2. No identifying photographic information is stored by the mobile app, only biometric markers sufficient to prove the user's unique identity. The M2 mining scheme will always be bottom-up in its methodology. "Bottom-up" refers to establishing mining equity in which only individual miners on mobile phones can mine M2 - one human transaction at a time.

Contrast this with the "top-down" mining on Proof-of-Work (POW) blockchains such as Bitcoin and Ethereum. Under POW, miners must consume large amounts of energy to solve increasingly complex cryptographic calculations in order to be rewarded. This increasing complexity requires increasingly high computer processing power; creating a mining ecosystem with high economic barriers to entry. In the "top down" world, only those with access to the fastest computing power can play; eliminating most of the world's population from participating in the financial benefits of mining these cryptocurrencies.

M2's bottom-up approach specifies how the token will be mined on a dPOA blockchain. M2's mining approach is called Perpetual Individual Mining (or "PIM"). PIM is the dPOA consensus mining protocol that uses a non-custodial digital wallet on a mobile phone using a dramatically smaller carbon footprint than its peers on POW blockchains. PIM will commence when price discovery of the token first reaches (USD) $0.10.

In order to be rewarded with M2, an individual must interact with the mining application on their mobile phone. If a user were to miss just one day of activity, that deficit would dramatically impact their M2 yield.

M2's mining protocol enforces a uniform daily limit on individual mining activity. M2's mining mechanics have been engineered to provide moderate mining rewards to individual miners at levels that would be unattractive to the industrial-scale mining ecosystems that exist today for cryptocurrencies such as Bitcoin.

M2 features a "minimalistic algorithmic mining" approach, enabling beneficiaries in the most economically distressed regions of the world an opportunity in participate in cryptocurrency ownership and exchange (i.e., The 50 Lesser Developed and Lower Income countries as classified by the United Nations and World Bank, respectively). M2's activity-based mining approach — using a quantitative behavior formula to reward miners — ensures that the mining rate of M2 will be dynamic and be utilized by those who need it the most.

M2 mining will be a reflection of the Human Hash Rate (HHR) driven by the Market Price (MP) and a constant "equilibrium" M2 Reward (M2R). The HHR is the relative measure of difficulty it would take to yield M2R.

The relationship between the variables is MP*HHR=M2R, implying that when M2R is constant

- As MP increases, the HHR will decrease.
- As MP decreases, the HHR will increase.

The time and effort required to mine M2 will incent only those who need M2's mining rewards to participate. As the price of M2 changes so will the HHR, ensuring that those that need M2R will dedicate their energies to yield M2R. Consequently, when the HHR decreases, more miners — those who feel that they need the rewards of M2 — will be motivated to participate, thereby increasing the pool of miners. Conversely, when the HHR increases, some miners will be discouraged to participate in M2 mining, thereby decreasing the pool of miners.

It's anticipated that the equilibrium M2 Reward level will not be established until mining is used by a significant portion of the target mining cohort. Additionally, the M2R is anticipated to exist within a range (or confidence interval).

CONCLUSION

M2 miners will be responsible for bringing this digital currency into circulation; earning a seat at the table with access to a method with which they will finally be able to participate in the financial ecosystem. Contrast this with Bitcoin; which circulates very little, and is acquired from miners who can afford mining rigs that cost over 5x the Gross National Income of the Low-Income Countries in which the majority of M2 miners will reside.

Bitcoin succeeded in becoming an independent, highly sought-after store of value, but it failed to deliver its vision of a "purely peer-to-peer version of electronic cash." M2 empowers independent economies via PIM on mobile devices, producing capital backed by the most valuable asset on the planet: human activity.

REFERENCES

World Bank. 2020. Poverty and Shared Prosperity 2020: Reversals of Fortune. https://openknowledge.worldbank.org/handle/10986/34496

Stryjak, J. 2020. The Mobile Economy 2020. https://data.gsmaintelligence.com/research/research/research-2020/the-mobile-economy-2020

Cryptopedia. 2021. What Is an Automated Market Maker (AMM)? https://www.gemini.com/cryptopedia/amm-what-are-automated-market-makers

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

World Bank. 2020, World Bank Country and Lending Groups, https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups