Abstract: In the 21st century, we live in a global economy where central banks continue to mismanage monetary policy, nearly two billion people don’t have access to financial services, and savers don’t see the majority of the profits made from their savings being lent out. With the development of cryptocurrencies and blockchain technology, we have the opportunity to completely rethink how our financial system works, and progress towards fixing these issues. However, less than one percent of the world’s population have adopted cryptocurrencies. Project Genesis proposes three new concepts that provide incentive to adopt cryptocurrencies and a framework to remove the dependency on traditional banking.

1. Ledger Analysis

For the past decade, blockchains have focused on rewarding validators for reaching consensus. This is commonly found in the two most popular consensus mechanisms, Proof-of-Work (PoW), used on networks like Bitcoin, and Proof-of-Stake (PoS), used by networks like Peercoin. The problem is that we haven’t developed a way to reward good behavior for users of cryptocurrency networks, rather than simply rewarding “miners” or “validators”.

In modern economies, it’s common for people to receive “cash back” rewards when they spend money with their credit cards [1]. This mechanism incentivizes engagement in economic behavior. Simply put, ledger analysis originates from the same concept.
**Ledger analysis** is a method of scanning a public ledger and rewarding users for specific behavior, without the need to know their identity or their reasoning for conducting such activity. This is done by defining which behaviors are beneficial for the network, creating an algorithm for scoring addresses based on those desired behaviors, and applying it to a set of data (blocks) that need to be reviewed in order to determine who deserves a reward for that given window of activity.

Let’s say Bob, Alice, and Jack are using XYZ network, and have engaged in a set of transactions indicated below that were published in the most recent block of the network. The network has applied ledger analysis into the protocol, and rewards are distributed to users based off of a simple algorithm:

\[
\text{User Score} = (\text{total spending value} \times 5) + (\text{total received value} \times 3)
\]

Transactions:

- Bob — sent 300 coins to —> Alice
- Jack — sent 50 coins to —> Bob
- Alice — sent 100 coins to —> Bob

If we apply our algorithm, Bob’s score would be 1,950, Alice’s would be 1,400, and Jack’s would be 250. This means that Bob was engaging in the most valuable economic behavior in the network for the given transaction set, which would lead to him either receiving a higher reward than the other participants or a higher chance of obtaining a reward compared to less active members. It depends on how the concept is implemented on the network.

Similar to how miners and stakers are given coins through block rewards as incentive for their behavior, any network that implements this technology can do the same for users, and it can be a great technique to incentivize early adoption, serving as a driving force to bring genuine adoption to the currency. The rewards can be derived from newly minted coins or fees collected on the network, similar to the rebates given in traditional cash back systems. It’s also important to note that the score isn’t what a user would receive in coins or tokens, rather, it’s a score used to compare participants level of economic activity against one another.

As a concept, ledger analysis is extremely flexible. Not only do networks have full flexibility to decide what economic behavior is beneficial, how rewards are distributed, and how much or how often rewards are given out, but they also get to apply specific game-theory mechanics to prevent people from abusing the system through false behavior (i.e. If users were simply rewarded for sending a crypto, they could ping-pong coins back and forth between two addresses and potentially receive rewards for fake economic behavior).

This technology can be used on public and private networks, however, it does require a transparent understanding of the transaction amount and type, depending on what the network wants to calculate.
2. **Peer-to-Peer Lending & P2P Pools**

It’s imperative that cryptocurrencies also provide functionality for **lending and borrowing peer-to-peer**, similar to how bitcoin allows users to transmit value between one another without the need of third parties. Along with this, we’ll need a better framework for money management. In doing so, we can guarantee access to capital across the world and the opportunity for users to potentially grow their own savings from the interest accrued on their loans. This can be done through smart contracts.

It is likely that most people will not want to conduct their own loans in a peer-to-peer nature, and rather, will depend on third parties to manage their money as they do with banks in today’s world. This can instead be done through **P2P pools**, where savers across the world can credit their money to a pool managed by a third party, and earn interest as the pool lends out crypto to individuals who they deem creditworthy. Similar to how miners on networks like bitcoin come together and combine their hashing power through online pools, users would combine their funds together and receive a fraction of the interest income generated by the pool.

![Peer-to-Peer Lending & P2P Pools Diagram](image)

This can all be done through a chain of smart contracts that deal with both sides of the transaction. Creditors and pools can agree on how long the pool will own the funds, what percentage of new income (interest payments) will be shared with the creditors, and much more. Borrowers and pools can agree as to what level of interest they’ll owe, as well as the loan’s payout schedule.

This results in an opportunity for competition to emerge in banking. No longer are a select few commercial banks the only gateways to capital. With potentially hundreds, if not thousands, of pools competing for creditors money, they’ll not only need to show consistent performance, all of which is transparent on the ledger, but they’ll have to keep costs low and offer more of the profits back to the original creditors.

This new framework of democratized lending and borrowing will revolutionize finance. Any group or individual will be able to become their own bank. And over time, a single individual or small team may build a vastly more intelligent and cost-efficient means of determining credit-worthy participants than the
archaic systems of the past, which will inevitably allow for smarter lending, as well as more profits going back to the creditors, thus creating true competition for traditional bankers.

This concept of peer-to-peer pools can be used for a variety of use cases outside of lending, including insurance, crowdfunding, and a variety of other industries that require funds to be pooled together.

3. Cooperative Addresses & Ecosystems

Most blockchains have focused heavily on providing a way for people to do transactions with one another in a peer-to-peer fashion. One big issue is that we haven’t provided a framework for businesses, organizations, non-profits, and communities to properly manage digital currencies and assets on blockchains. **Cooperative addresses** provide the ability to create a digital organization with its own governance model and methods of managing treasury funds. Ironically enough, one of the best use cases in need of cooperative addresses are cryptocurrency exchanges, such as Quadriga CX [2], an exchange where the CEO was the sole owner of the private keys to their digital assets.

Cooperative addresses would serve as an evolution from pre-existing technologies, such as multi-signature addresses [3] and decentralized autonomous organizations (DAOs) [4]. The difference between cooperative addresses and the two existing technologies is the addition of DAO-like functionality from within the address, rather than being involved with the entire protocol (i.e. Dash’s Treasury). They also allow for new participants to join and leave. At inception, a cooperative address is generated that grants specified participants the ability to use their private keys to vote on decisions or vote on treasury transactions, allowing for a group of people to come together and manage their funds in a cooperative manner.

If implemented, companies would be able to implement multi-sig requirements on withdrawals, rank certain addresses with more access to capital, establish limits on the amount of funds being transferred in a given window of time, and much more, all directly on-chain. Charitable groups could vote to grant funds to specific causes and online communities could vote for proposals to further development of shared efforts.

But most importantly, in an effort to liberate those who are either unbanked or choose not to trust central third parties with their funds, this technology allows for ecosystems.
Ecosystems are capital pools where vast groups of people can combine their funds together into a cooperative address, and establish a framework for how those funds can be used. This concept provides the ability to manage money without the need of a third party, and can be utilized for a wide range of use cases, such as insurance and crowdfunding. But in this paper, we focus on the biggest application; capital management.

In simple terms, they allow users to lend and borrow from one another, rather than a third party, allowing us to become our own community bank [5]. It holds resemblance to credit unions, where participants have say in how the business is run. The framework of any given ecosystem is highly customizable. They are permissioned by nature, meaning new participants must receive enough approval from existing members to join. Rules for any ecosystem are transparent on a block explorer, allowing users to know how much capital they’ll have access to at any given time, expectations on repayment periods and interest payments, and much more all before joining.

Once users have come together and formed an ecosystem, funds are combined into the ecosystem’s pool, where participants can go about borrowing funds from the pool and repaying the agreed upon amount on time. If participants borrow funds and pay them back consistently, likely bringing in new capital through interest payments, they not only can receive higher credit limits, but may receive a lower interest rate. If users don’t pay back on time with interest as agreed upon, they may be subject to removal from the ecosystem or lose their favorable credit limit and interest rate. This is determined through an ecosystem’s ranking algorithm, a way in which credit worthiness is generally determined. At its base level, ecosystems provide a way for a group of close individuals to manage capital together without needing much oversight on everyday borrowing. However, they can also provide means to settle larger transactions and even prevent bad actors from gaming the system.

For larger transactions, such as mortgage, auto, and student loans, ecosystem’s can require that borrowing requests that meet over certain levels of capital receive a certain amount of approval from stakeholders. Another means of checks and balances that can be utilized is known as “distribution periods”. With cryptocurrency being immutable, it’s important to offer the ability to lend fractions at a time for larger loans, so ecosystems can track if progress is being made. If they feel things aren’t moving accordingly,
participants can then opt-out from future distributions. A good example of this would be for small business loans. If the ecosystem analyzed that Bob wasn’t truly directing the money he received towards expanding his business, they could veto the next distribution, allocating the capital back to the pool. In order to prevent capital from being misused, ecosystems can restrict the flow of lent money to certain addresses. This is a great feature for student and auto loans, which are common forms of loans where the borrower is buying something from a specific entity, rather than multiple parties. And ultimately, individuals can opt-out of lending to specific participants or rankings. However, it goes both ways, meaning that any user who blacklists another won’t be able to borrow from their capital. This prevents malicious actors from being able to borrow capital from an ecosystem’s pool when they aren’t willing to put up their own for fellow users.

Ecosystems equally share reward and risk among active participants in each loan, meaning each user will receive their fair share of interest income or lose their portion of funds, as in some cases, ecosystems could face greater debt abandonment than interest payments. To combat non-creditworthy borrowers from getting away with not paying loans, ecosystems can communicate with one another, as companies currently do in modern markets [6]. One important fact to take into account is that identity has and always will play a role in applying for credit. In fact, the ecosystem model is built around it. So even in a world of endless public addresses, where someone may attempt to drop their previous borrowing history, the vast majority of ecosystems and P2P pools will require previous credit history before they accept new users. Identity information will be commonly exchanged as well, and doesn’t need to be stored or transmitted over a public ledger; rather, it can be done through third-party applications or self-sovereign identity systems as we use today. Users can also prove that addresses are their own by sending a small, specific amount of funds requested, similar to microtransfers which are commonly used by payment processors to validate ownership of a bank account. As most ecosystems will only accept people they commonly know, participants will think twice before they burn bridges with what could be their only available access to credit.

Conclusion: Programmable currency has provided a means of storing and transferring wealth that has never before been achievable. For the first time, money can have all the conveniences of payment systems, while also providing the ability to maintain sound monetary policy. It also provides us a profound opportunity to revolutionize how we incentivize participants and conduct financial transactions. With these properties, it is the fifth major evolution of money.

If you’d like to contribute, feel free to join us at the links below:
https://www.projectgenesisfoundation.org/
https://github.com/project-genesis-team
References:


