PeopleMint: A Multi-Party Mining Protocol

v0.1

Kennedy Idialu (k@ellcrys.co)

01-09-2018

Abstract

In this paper, We discuss a protocol that allows network participants receive the native currency of a blockchain in exchange of real-world national banknotes and also leverage on this activity to increase the security of the network via an observer-based, chain monitoring mechanism. This system is meant to be used as a mining protocol of the Ellcrys Network and offers a fairer and inclusive miner community where users who possess specialised hardware and those who are not privileged enough to afford them can both benefit.

1 Introduction

In this section, I will discuss current coin generation and reward models used on existing public blockchains based on their consensus mechanism and why there is a need for alternatives that will offer a more egalitarian, accessible and inclusive coin distribution model.

1.1 Proof of Work (PoW)

In most blockchain systems, especially those based on Proof-of-Work (PoW) like Bitcoin[1], the distribution of the native coin happens via a repeating process involving the computation of cryptographic hashes in search of a given value that meets specific criteria. The participants who find these unique values are allocated newly created coins. This process is popularly known as "Mining", and it requires specialised hardware to keep the miners competitive. Many in the cryptocurrency industry widely criticise it because of the belief that it is an unworthy contributor to energy waste and ultimately damaging for the environment. Furthermore, the introduction of ASIC miners reduce miner inclusivity by centralising and delegating coin generation operation to corporations. As a result, mining increasingly became out of reach of most people.

1.2 Proof of Stake (PoS)

In Proof-of-Stake systems, the need to repeatedly compute random values that meet a set of criteria is not required. Instead, network participants who are interested in creating blocks stake some money (usually in the native coin) which is used as a security deposit to discourage bad behaviour. Upon the creation of a new block, the block creator is rewarded with some coins. This coin generation method outrightly eliminates users who are not able to afford the minimum staking amount. This will lead to a system that favours only the rich. Some PoS systems like Tezos[2], participants who are unable to meet the staking requirement have the ability to use their coin to vote delegates who would create blocks on their behalf and with the possibility of sharing the block rewards with them.

1.3 Hybrid PoW/PoS

Hybrid consensus system that successfully integrate features of both Proof-of-Work and Proof-of-Stake behaviours increase the number of participants who are eligible to benefit from the network coin creation process. An exciting example is Decred network, which allows PoW miners create blocks while PoS miners endorse those blocks. In this system, PoS miners stake money by purchasing a ticket which may be randomly selected from a pool to take part in the block endorsement process. Network participants who are unable to compete successfully on the PoW side may choose to purchase tickets and potentially be called upon to validate blocks and receive new coins as a reward. Hybrid consensus system offers a more inclusive and equatable coin distribution mechanism than Proof-of-Work system.

2 Hybrid PoW/PoS With Observers

It is widely accepted that the more people or entities dedicated to validating the state of the distributed ledger, the better and more secure the ledger and network will be. Researchers and developers continue to find approaches to increase network security and one of such explored approach is to enable mobile device owners to participate in the validation of the blockchain state. If this is achieved, it will greatly increase the security of a blockchain network by making attacks like 51% difficult to achieve as the attacker will be competing with potentially millions of mobile devices dedicated to the network.

Unfortunately, the resource requirement for synchronizing, validating and storing chain state makes this approach costly and impractical for most mobile devices. Projects like Electroneum[3] perform simulations of mining that do not offer the network any improvement to secure other than to distribute the native coins to as many people as possible.

In the rest of this paper, I will describe a combination of hybrid PoW/PoS consensus with the inclusion of additional network participants known as Banknote scanners and validators, who implicitly act as chain observers while performing their roles in the creation of new coins. Banknote scanners tag the hash of a given block to a banknote and send these banknotes to the network for validation. The tagged banknotes are picked up by validators who manually verify the identity of the tagged block along with other defining features. The process of

tagging and validating drives a system where banknotes providers and validators continuously vouch for blocks, thus, increasing block score and consequently the entire score of a branch. We believe this system will provide additional security and foster a more inclusive network where millions of people around the world can participate without much barrier.

2.1 Network Participants

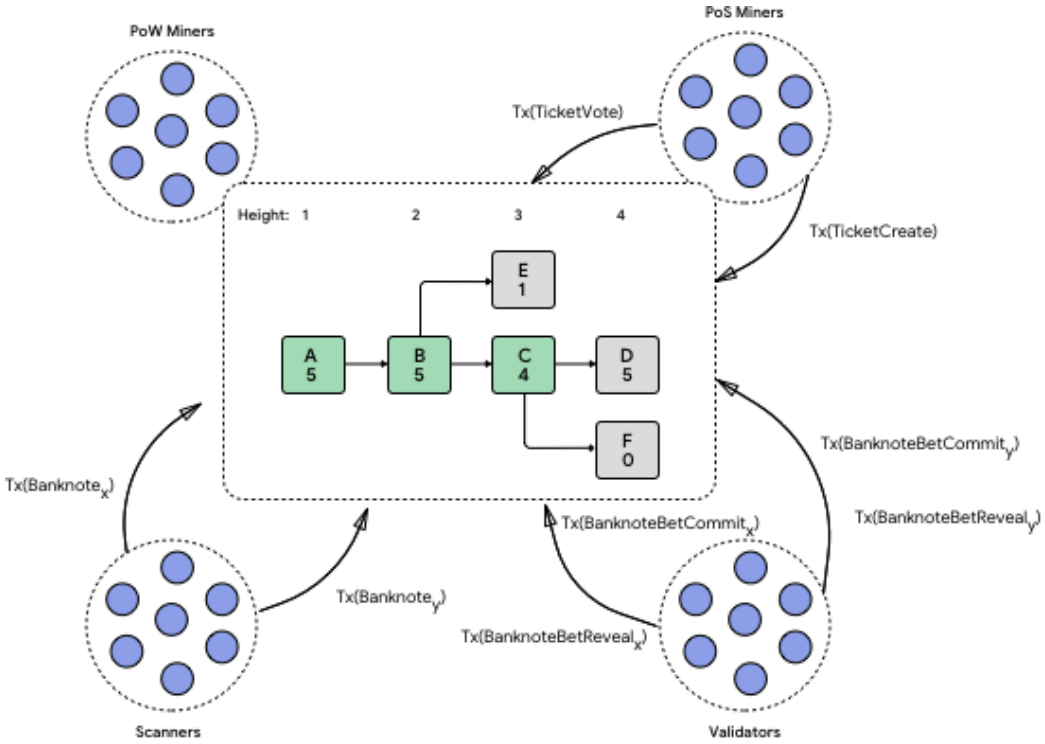

Figure 1: Network Participants

Figure 1 describes a network of 4 participants namely Proof-of-Work miners, Proof-of-Stake miners, Banknote Scanners and Banknote validators. PoW miners are responsible for proposing new blocks. PoS miners endorse proposed blocks by voting for blocks they have confirmed to be valid under the consensus rule they follow. Banknote

scanners provide the resource that is required to generate new coins which is used to incentivise other participants. This resource is a national banknote; an asset that is valuable and requires work to acquire. Banknote scanners provide this asset to the network in attempts to exchange for new coins after it undergoes and passes validations. Banknote validators are responsible for validating the correctness of a banknote. They do this by manually verifying attributes of the banknote and betting on the outcome of their validation.

2.2 Miners (PoW & PoS)

Proof-of-Work and Proof-of-Stake participants are classified as Miners. These are people or organizations who provide hardware and compute capabilities and form the network of computers that make up the system. They can also act as validators, endorsing blocks produced through Proof-of-Work processes. Miners in Bitcoin and other PoW systems earn reward for solving a computationally hard problem after which they broadcast a block containing the solution and a transaction that allocates their reward to the rest of the network. This system encourages competition between participants and forces them to seek more powerful and expensive mining equipments in hopes of outcompeting other miners. While this leads to an increased overall mining hash rate and network security, the wealth generated will be distributed unevenly, thus, creating a system that is centralized and reserved for the wealthy individuals and organizations.

With PeopleMint, miners do not have monopoly over network reward as the resources that is used to produce rewards are provided by a different class of network participants who scan and validate banknotes. Contrary to the norm in Bitcoin-like systems where the miner rewards themselves, miners must collect banknotes up to a maximum amount before their blocks are accepted by the rest of the network and the resulting block reward shared between them and any other participants. Without the other participants, creating and validating banknotes, a miner cannot generate new coins and any reward will be through transaction fees.

2.3 Banknote Scanners

Banknote scanners are people who send images of national banknotes to be processed, included in blocks and generate new coins. As described in figure 1, they send ***TxBanknote*** transaction which contains a banknote that is tagged with the last 12 characters of the current tip block. There are millions of people across the world who have access to currency notes that may be supported and have never been processed by the Ellcrys network. These people can provide the system with this resource and become an essential category of users who work to ensure security by providing the supply of currency notes that generates the incentives while also acting as observers by implicitly voting for a block and preventing miners from going against consensus rules by refusing to tag blocks created by untrusted miners.

Scanners cannot re-scan banknotes that have been previously processed and indexed. The currency notes they provide, are passed through a scanning protocol that provides a deterministic, effort-driven scanning procedure that standardises the way banknotes are scanned and offers economic difficulties to make abuse costly.

2.4 Banknote Validators

Banknote validators are participants who depend on the actions of banknote scanners to fulfil their obligations to the network. Their primary activity is to fetch banknotes, endorse and predict the validity of the notes. There are two stages of validation:

- **Pre-Validation (a.k.a Vouching):** In this stage, validators (a.k.a Vouchers) verify and endorse banknotes that are in the transaction pool. They assert the correctness of the serial, denomination, currency code, tagged block hash and encode this information into a ***TxVouch*** transaction. After $^2/_3$ of N required ***TxVouch*** transactions are received for a banknote, Miner must create a ***TxVouchedBanknote*** which includes the ***TxBanknote*** transaction and the received ***TxVouch*** transactions, broadcast it and add to the block they will mine.

- **Pre-Validation Using Machine Learning (Alternative):** An alternative to the user-driven pre-validation stage is the use of machine learning to detect banknote details. The use of Machine Learning to aid validation has the advantage of automating the validation process, eliminating the need for vouchers and the incentives they need to function. However, supporting more banknotes will require more time and resources.
- **Validation:** After the ***TxBanknote*** is added to a block, the final validation begins. Similar to the pre-validation stage, the validator (a.k.a bettor) verifies the correctness of serial, denomination, currency code, tagged block hash and endorses it by sending ***TxBanknoteBetCommit*** transaction containing the details in an encrypted form and subsequently a ***TxBanknoteBetReveal*** transaction to reveal the votes for collation and reward disbursement.

During these stages, the validators are required to stake some amount of coins on every vouch or vote they make on a banknote as a "*proof of truth*" which will be returned to them if they rightly predict the validity in the direction of the majority. Bettors who failed to predict in the course of the majority lose their stake to the winning majority.

The purpose of the pre-validation phase is to identify the banknote, collect necessary information and confirm that required properties are in place. Validators help provide information that is used to construct a fingerprint for a given note. It is similar to a Captcha we all know and hate except this comes with network incentives.

The validation stage randomly selects N number of ***TxBanknoteBetReveal*** to reduce the ability of attackers to create fake identities, coordinate and vote for their notes. At the pre-validation stage, it is possible for the note owners to generate Sybil identities to vouch for their banknotes, but they will be unable to do so when the banknote is already in a block and ready to be voted on in the main validation phase since votes will be selected randomly.

3 Scanning

In this section, We will discuss the procedure and rules that should be followed by scanners to produce a valid digital representation of a

banknote that can be processed and validated initially by miners and finally by banknote validators/bettors.

3.1 Introduction

The scanning protocol dictates a set of steps to be carried out by people who intend to exchange banknotes for the native coin. These banknotes act as raw materials for creating new coins, providing the block rewards shared between the block creator, block endorsers, validators/bettors and any other future network participants. Without the introduction of new banknotes into the system, new coins are not created, and the network will be unable to incentivize participants. People around the world send currency notes and hope that validators find their submission acceptable. However, naively asking people to send still images exposes the network to the following attacks:

3.2 Counterfeit & Image Manipulation

The most obvious problem is the issue of counterfeit. The likelihood of people feeding the network with banknotes that have been counterfeited or manipulated using image editing software is high. Manipulation using image editing tools is cheap; The attacker only needs to change the serial of one banknote many times. However, the process of counterfeiting currency notes is not cheap or a zero cost operation. We believe that with the right scanning and economic model, we will be able to replicate the cost constraints that existing counterfeiting enterprises face and make it costly for them to move their business to the Ellcrys network. We have identified some of the cost factors experienced by these organisations and way by which we can replicate them:

- **Physical Cost:** Counterfeiters are in the business of creating fake currencies in their physical, tangible form. They invest in infrastructure that enables them to reach their goals. Their expenditure includes rent, raw materials, vehicles, printers, electricity and other equipment. Like manufacturing business, they incur production costs.
- **Transportation Cost:** After the production of counterfeited currencies, the counterfeiters move them from their hidden location

to the distributor, the end-users and other people in the supply chain. Transporting this product is very risky to them and comes at a cost.

- **Workforce:** Counterfeiters employ labourers who possess varying skill sets that are required to produce quality counterfeits. They include but not limited to designers, printers, cutters to artists. These people receive monetary payments for the services they render.
- **Competition:** They also contend with their competitors concerning the quality of the product they distribute. Like regular, legal businesses, they will be willing to spend on improving the quality of their product to guarantee their ability to compete, retain and acquire new customers.
- **Time:** Producing quality counterfeit notes takes a lot of care and time. The process is so delicate that every detail of a real currency must be carefully and skillfully replicated. The more time expended, the more the risk and financial requirement.
- **Uncertainty:** Regardless of all the care and financial investment put into the production of fake currencies; Counterfeiters and people in this line of work are never always guaranteed a return on their investment. Their distribution pipeline may be unexpected compromised. Their production location could are raided at any time. One or two employers might be arrested or just become unavailable.

As described above, even counterfeiters incur some cost that makes the production of counterfeit currency notes costly in a similar way the acquisition of an original banknote by ordinary users requires cost which is the expense of energy or the offering of skill to a person, employer or organisation. Nobody should be able to receive the native coin without giving something of value. The scanning protocol must make sure that the cost factors described above are in place to a reasonable extent.

3.3 Replicating Cost Factors

In this section, We discuss ways to replicate the cost factors described in subsection 3.2 ins such a way that will provide have similar difficulties built into the protocol.

3.3.1 Physical Cost

To support physical cost, we must be able to force the use of material-based, tangible currency notes as opposed to static versions of a currency that may have been created or modified in an image editing software. If the tangibility proof is made mandatory, then it will be costly to set up farms dedicated to mass producing or scanning banknotes. These are the proposed methods to enforce tangibility:

- **Fixed-Length Video Format:** The first step is to require banknotes to be sent to the network encoded in a fixed-length video format. It is more difficult to cleanly and unnoticeably modify a video than it is to alter a still image.
- **Hashstamping:** The video scanning procedure must integrate a mechanism that requires work to be carried out as "proof of work" mechanism. We propose that scanners must flip the front and back of the banknote and proceed to write the last 12 characters of the hash of the most recent block on the note using a pencil or any other writing tool that does not permanently deface the banknote. The scanning ritual must be done within a fixed amount of time (e.g. 15 seconds). Writing the last 12 characters of a recent block's hash servers to (1) Force the video to expire after a number of blocks have been confirmed (2) Prevent stockpiling of videos create days ago (3) Used as an implicit means of voting for a block and consequently used to decide the value of a branch over another (fork choice algorithm).

3.3.2 Transportation Cost

Counterfeiters will continue to incur the transportation cost of moving materials used to create fake banknotes because they will continue to distribute their counterfeit notes to maximise their profit. Also, they will also pay network transaction fees to transfer the banknotes to the network like regular users. There will be competition between them and other scanners. They are more likely to increase transaction fees to gain more priority over other scanners. Measures must be put in place to prevent an unfair fee market by normalising scanning fees such that good scanners are not edged out due to their inability to pay higher transaction fees.

3.3.3 Workforce Cost

Counterfeiters and people who may create farms dedicated to scanning banknotes will need to invest more into their operations to accommodate more human scanners and will require more space if they need to increase capacity, thus, further re-enforcing the physical cost of scanning mentioned in subsubsection 3.3.1.

3.3.4 Competition Cost

The fact that the network is open to millions of people around the world with very little or no barrier, counterfeiters and scanning farms may find that they are unable to outcompete conventional scanners. The normalisation of fees will also work to create a levelled network. Counterfeiters may prefer to continue with their original business model.

3.3.5 Time & Uncertainty Cost

Counterfeiters will not instantly get coins successfully exchanged for an excellently produced banknote. Blockchain networks typically require rewards to reach a certain maturity period before they are spendable. During this time, the coin may gain or lose value. If there is a loss of coin value, the counterfeiter may have spent more to produce the banknotes that resulted in the low-value reward. Furthermore, they are subjected to scrutiny by the validators whom they are unable to control and may have their scanned notes rejected.

3.4 Stockpiling

Stockpiling is the act of collecting and storing a pre-scanned banknote to be exchanged at a later date, possibly at a time when the price of the coin is high. People who stockpile many notes may have the ability to plan and significantly affect the market and economics of the network within a short time and at little cost to them. By tagging each banknote with the last 12 characters of a new block's hash, We force pre-scanned banknotes to expire after a fixed number of block confirmations (e.g. After six blocks starting from the tagged block). This process is called **"hashstamping"**

3.5 Selection Bias

Selection bias describes a situation where scanners begin to centralise towards a single or small sets of banknotes that they believe will have a better network exchange rate; Network exchange rate determines how much Ellies are exchangeable for a currency note. The number of ELL exchanged for USD banknote will be different from that of EUR. Additionally, miners may also begin to censor banknotes that do not fall within a given set of banknote types that have certain qualities. If this is allowed to happen, then scanners in countries with low-valued banknotes will be practically disenfranchised.

An approach to solving this is to deny miners and banknote validators the ability to select banknotes. The protocol should randomly select a set of notes that are eligible for scanning during a given epoch. Random selection of currency type forces scanners and validators to work within the selected choices. It also provides a property that encourages scarcity and alternates coin generation between regions/countries. If professional scanning becomes an occupation, people would have to acquire banknotes from a different region to be able to participant in coin generation.

4 Banknote Selection

In this section, We will describe the selection procedure employed by miners for selecting banknotes. It is important for this selection process to promote the following properties:

- **Censorship-Resistance:** This requires everyone to have a fair chance to exchange their banknotes for the native coin. If scanners and miners can decide what notes are worth processing/validating, then thousands across the world will be unfairly denied the chance to participate.
- **Liveness:** Liveness means the network continues to progress even when blocks do not contain banknotes. In such a case, miners will have to rely only on fees as their reward since block generation does not result in the creation of new coins.
- **Scarcity:** Excessive creation of new coins will significantly reduce the value of existing coins in circulation. We must provide constraints to reduces inflation to the existing monetary base.

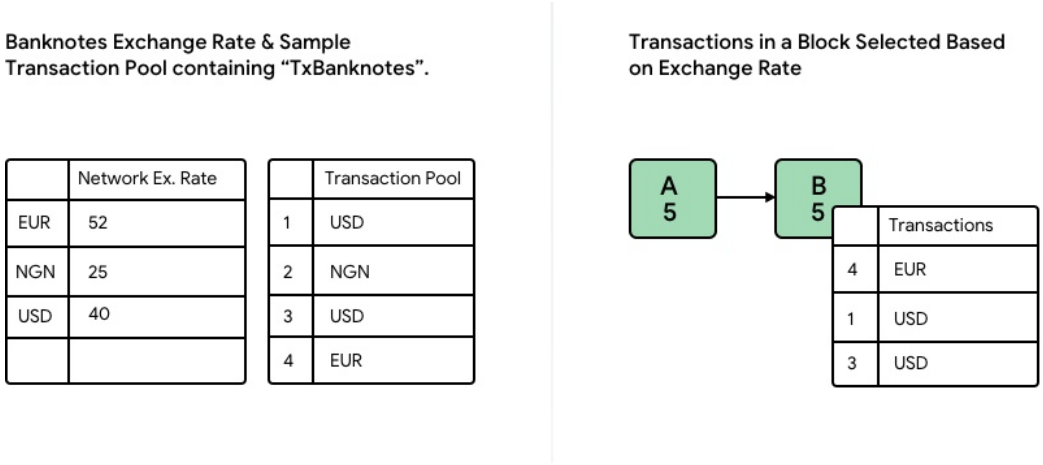

Figure 2: Selection Bias: Banknotes of higher exchange value are preferred

On the left of Fig 2, We are presented with a set of ***TxBanknote*** transactions in a transaction pool and their ELL exchange rate. On the right, We show transactions that were selected and included in a block **B**. Due to the difference in the real-world value of currencies, miners are incentive to select only transactions that will result in higher revenue. In the illustration, these currencies are **EUR** and **USD**. Lower-valued currencies will only be considered when a coin reward limit is introduced, and only lower-valued banknotes are sufficient to reach the limit without exceeding it.

4.1 Random Banknote Selection

Miners follow an unpredictable but deterministic algorithm to select N currency types that can be accepted and processed in blocks created over a given epoch. They use the hash of the current block to seed a pseudo-random number generator and subsequently fetch more banknote types by extending the seed with the byte equivalent of the last selected currency type id. Figure 3 describes the selection algorithm in Go programming language. The process is repeated at the beginning of a new epoch.

4.1.1 Benefits of Random Banknote Selection

These are some of the benefits of derived from selecting banknotes types randomly.

- The Miners, Scanners and Validators ability to censor banknotes transactions based on exchange rate value is reduced as they have no control over what sets of banknotes are valid per epoch.
- Fair opportunity for citizens within the jurisdictions of the selected currency types to exchange their notes.
- Makes banknote stockpiling much more difficult as scanners are unable to predict which banknotes will be eligible.
- Regulation of scanners population; The number of people able to scan will be randomly regulated.

```go
package main

import (
    "fmt"
    "math/big"
    "math/rand"
)

// currencyCode is a list of supported currency types.
var currencyCode = []string{"USD", "NGN", "EUR", "RAND", "GBP"}

func main() {
    var lastBlockHash = []byte("0xa28dq8sajdhge8hbgd8a")
    var seed = append([]byte{}, lastBlockHash...)
    var r = rand.New(rand.NewSource(makeSource(seed)))

    var selected = []string{}
    for len(selected) < 3 {
        index := r.Intn(len(currencyCode))
        curCode := currencyCode[index]
        selected = append(selected, curCode)

        // Extend the seed deterministically
        // by appending the bytes equivalent
        // of the selected currency code.
        seed = append(seed, []byte(curCode)...)

        // Update the PRNG seed
        r.Seed(makeSource(seed))
    }

    // Output: [EUR USD RAND]
    fmt.Println(selected)
}

func makeSource(src []byte) int64 {
    return new(big.Int).SetBytes(src).Int64()
}
```

Figure 3: Random Selection Algorithm

5 Network Exchange Rate

The network exchange rate determines how much native coin is exchangeable for a given banknote type. For instance, how much will ELL be exchanged for 1 USD? This information will typically be hard-coded into the client allowing all nodes to perform same exchange calculations. Similar to Bitcoin, We can reduce exchange rates over time to produce the same effect of halving rewards over time.

6 Conclusion

This paper introduced a mining protocol that can be used to create a more equitable reward system for a distributed system. However, it is incomplete as there is a need for further study, particularly on incentives alignment and security. We are actively looking at this issues and will release updated versions of these document in the future.

References

[1] **Bitcoin** The decentralized digital currency http://bitcoin.org/bitcoin.pdf

[2] **Liquid Proof-of-Stake** https://medium.com/tezos/liquid-proof-of-stake-aec2f7ef1da7

[3] **Electroneum Mobile Mining** https://electroneum101.com/how-to-mine-electroneum-with-a-mobile-phone/