1 Introduction

Cryptocurrencies have several advantages to fiat currencies as a means of payment. They enable transfer of value that is much faster than a bank wire, at lower cost (especially for international payments), in a publicly auditable and secure manner, using a technology that is globally accessible so long as you have a smartphone. Further, cryptocurrencies can be programmed; allowing financial contracts, escrow, and insurance, all without intermediaries.

However, at the moment, there are several barriers to the mainstream adoption of cryptocurrencies as a means of payment. First, due to deterministic supply rules and unpredictable coin demand, successful coins[1] experience deflationary price instability. As a result, users rationally prefer to use them as a store of value rather than a medium of exchange. Second, even when people do wish to use price-volatile cryptocurrencies as a means of payment, they need to generate a private/public key pair to receive a payment, and enter in somebody's public key in order to send a payment. While these may seem small obstacles, experience has shown that small differences in user experience lead to large differences in usage outcomes.

For a cryptographic social payments system to prosper, sending a payment should be as easy as sending a text message, and the volatility of the currency should be minimal. We describe the Celo protocol, a protocol that addresses each of these issues. To address ease of sending payments, the Celo protocol introduces a cryptographic scheme that we call address-based encryption, in which participants verify a series of cell-phone number-to-public-key mappings, allowing users to then use their friends' cell phone numbers as public keys.

To address stability of value, the Celo protocol introduces an asset whose value is stabilized using a monetary policy with elastic supply rules, backed by a variable-value reserve. Further, it introduces a governance structure that allows the protocol to create a family of local, regional, and utility stable-value currencies, where the introduction of new successful stable-value coins to the family strengthens the stability characteristics of the existing coins.

Finally, the Celo protocol introduces a mobile block reward mechanism in which all users involved in transactions are also able to participate in verifications, creating a broad participant base and making block rewards more accessible to day-to-day users.

Together, these underpin a compelling social payments protocol.

2 Ease of Use through Lightweight Identity

An important obstacle for the mainstream adoption of cryptocurrencies as a means of payment is the lack of intuitive, decentralized public key infrastructures. As a result, in order to send a payment in today's decentralized systems, users must know the public key of the intended recipient (unless they are operating through a centralized gateway). And in order to receive a payment, a user must first set up a private/public keypair and broadcast it. It would be far easier to send a payment directly to an email address or phone number, and to be able to receive a payment without having to first set up a wallet.

Identity-based encryption [18] holds promise towards this end. In this scheme, when Alice wants to send an encrypted message to Bob at bob@company.com, she can simply use the public key string bob@company.com, without needing to obtain Bob's public key certificate. While a cryptocurrency system based on identity-based encryption would lead to a much more seamless user experience, both the original proposal and subsequent implementations [4, 6] are hindered by the fact that they require a trusted third party, called a private-key generator, to generate private keys. As a result, these schemes are less useful in open, permissionless systems.

[1] Academics, regulators, entrepreneurs and others use "coin" and "token" interchangeably to describe assets that function as a digital representation of value native to a distributed ledger. In this paper, we refer to 'digital assets,' 'coins,' 'cryptocurrencies' and 'tokens' with general interchangeability.