EDL Technical White Paper

Abstract

Electronic Dollar (or eDollar, Symbol: EDL) is a digital currency designed to be easily adopted for everyday use. Besides being fast, secure, and totally decentralized, it will always keep your balance secret, and the amounts, destiny or origin of your transactions, absolutely secured. You are the only responsible of the control of your funds, and nobody will ever trace your transfers unless you share your keys. All transactions in **eDollar** are **Ring Confidential Transactions (RingCT)**. By taking advantage of **Ring Signatures, eDollar** is able to ensure that transactions are not only untraceable, but have an optional measure of ambiguity that ensures that transactions cannot be tied back to an individual user or computer. Any concern about traceability is furthermore solved by **eDollar** by allowing the user to generate and publish different subaddress that belong to the same wallet in order to receive unlinkable payments. No observer can determine if any transactions were sent to a specific address or link two addresses together.

Introduction

When FIAT money, in the form of a paper bill or a metal coin, is used in any place of the world for any common transaction, there is no way to know who was the previous owner, nor what was the previous use, nor how much money have any of the giver or the receiver. When a paycheck or when Internet banking is used, then the bank -or "the trust"- can trace the origin of the funds, and the actual systems, will easily determine the path that the funds has followed even among different banks in different countries. Even worse, those trusts can usually be slow and expensive, and the system is by design made so it can always be determined the balance of any involved part, sometimes exposing the users safety to dishonest or controlling eyes.

With cryptocurrency introduction, the main objective is to safely allow commercial interchange in a trustless environment. Since the first successful commercial transaction, crypto currency has expanded and changed trying to adapt and fulfill user's requirements,

giving place to an growing number of different coins: Today, an overwhelming plethora of different, complicated -even unpronounceable coins and tokens- compete to get common users' attention while sometime scaring novice potential users, taking them away from knowing how easy and safe to use virtual assets can be.

To increase the expanding system's complexity, the goal of many projects, instead of willing to solve common user's needs, has simply turned into a way to raise funds, while copying the same limitations of the computational algorithms the cloned coins are derived from.

A simple, clear-and-easy-to-understand concept, integrating every aspect of safety, ease of use, transparency and anonymity, is the next obvious step both for evolution and widespread adoption of crypto currency:

Electronic Dollar (or eDollar) is

Decentralized

eDollar is decentralized, trustless cryptocurrency. The whole system is operated by peer-to-peer network. Transactions are confirmed by distributed consensus, and then recorded on the blockchain immutably.

Secure

Using the power of a distributed peer-to-peer consensus network, every transaction on the network is cryptographically secured. Wallet files are encrypted with a passphrase to ensure they are useless if stolen.

Private

All transactions in **eDollar** are Ring Confidential Transactions (RingCT) with minimum ring size of 4. The amount of any transaction is always hidden to the public, and because blocks cannot be analyzed, without the keys, no one can ever know where that money comes from.

Untraceable

By taking advantage of ring signatures, a special property of a certain type of cryptography, **eDollar** is able to ensure that transactions are not only untraceable, but have an optional

measure of ambiguity that ensures that transactions cannot be tied back to an individual user or computer.

ASIC resistant POW

Although no algorithm is ASIC-proof by design, developer team have a very active agenda to keep **EDL** continuously updated, so that ASIC will be never economically interesting, giving CPU/GPU miners the best opportunity to get the most profitable hashrates in order to protect our project concept of decentralization.

Smooth Emission

The **Cryptonote 2.0** algorithm adapted to **EDL** assures that block reward will decrease gradually. Subsequently, until an arbitrary decided by the community level is reached. Then the block reward will remain stable per minute indefinitely.

Background

"Bitcoin" has been a successful implementation of the concept of peer-to-peer electronic cash. The general public have come to appreciate the convenient combination of public transactions and proof-of-work as a trust model. Today, the user base of electronic cash is growing at a steady pace; customers are attracted to low fees and the anonymity provided by electronic cash and merchants value its predicted and decentralized emission. Bitcoin has effectively proved that electronic cash can be as simple as paper money and as convenient as credit cards.

But Bitcoin suffers from several deficiencies, some critical flaws that cannot be fixed rapidly deter Bitcoin's widespread propagation. In such inflexible models, it is more efficient to roll-out a new project rather than perpetually fix the original project.

Anonymity

The most important aspect of electronic cash. Privacy, as described by T. Okamoto and K. Ohta, "relationship between the user and his purchases must be untraceable by anyone", is a main criteria of ideal electronic cash. From their description, two properties define a fully anonymous electronic cash model:

Untraceability: for each incoming transaction all possible senders are equiprobable.

Unlinkability: for any two outgoing transactions it is impossible to prove they were sent to the same person.

Since all the transactions that take place between the network's participants are public, any transaction can be unambiguously traced to a unique origin and final recipient. A careful blockchain analysis may reveal a link between the users of the Bitcoin network and their transactions. A lot of hidden personal information can be extracted from the public database. Bitcoin's failure to satisfy the two properties outlined above leads us to conclude that it is not an anonymous electronic cash system. The same considerations applies to Ethereum network and its Tokens.

The CryptoNote Technology

Untraceable Transactions

CryptoNote proposes a scheme of fully anonymous transactions satisfying both ***untraceability*** and ***unlinkability*** conditions. An important feature of **CryptoNote** is its autonomy: the sender is not required to cooperate with other users or a trusted third party to make his transactions; hence each participant produces a cover traffic independently.

The new scheme relies on the cryptographic primitive called a group signature. First presented by D. Chaum and E. van Heyst, it allows a user to sign his message on behalf of the group of users. After signing the message the user provides the keys of all the users of his group. A verifier can proof that the real signer is one member of the group, but cannot exclusively identify the signer.

The actual version is called a **Ring Signature**, introduced by Rivest et al, that is *an autonomous scheme without Group Manager nor anonymity revocation.* A similar cryptographic construction is also known as a ad-hoc group signature. It emphasizes the arbitrary group formation, whereas group/ring signature schemes rather imply a fixed set of members.

For the most part, **CryptoNote** solution is based on the work “Traceable ring signature” by E. Fujisaki and K. Suzuki, and is called a one-time ring signature, stressing the user’s capability to produce only one valid signature under his private key. The public key may appear in many foreign verifying sets and the private key can be used for generating a unique anonymous signature.

In the model used by Bitcoin and Ethereum, a user possesses one **FIRST** unique key that is **private** (used to sign and send funds) and **SECOND** unique key that is **public** (used to receive the funds). In CryptoNote model a sender generates a one-time public key based on the recipient’s address and some random data. In this sense, an incoming transaction for the same recipient is sent to a public key and only the recipient can redeem his funds using his unique private key and spend the funds using a ring signature. A **THIRD** different key, the unique **"VIEW key"** is used to display a transaction in the public ledger explorer, showing only a single given transaction while hiding all other transactions sent to the same recipient address. Without this **VIEW key**, no one can see the amount sent, thus keeping ownership and actual spending, completely anonymous.

Unlinkable payments

Classic Bitcoin and Ethereum addresses, once published become an unambiguous identifier for incoming and outgoing payments, linking them together, tying to the sender’s or the recipient’s address, and publicly displaying the transaction amount, forever. If someone wants to receive an “untied” transaction, he should convey his address to the sender by a private channel and never use the same address again. If he wants to receive different transactions which cannot be proven to belong to the same owner he should generate all the different addresses and never publish them in his own pseudonym.

Cryptonote solves this situation allowing a user to publish a single address and receive unlinkable payments. No observer can determine if any transactions were sent to a specific address or link two addresses together.

One-time ring signatures

A protocol based on one-time ring signatures allows users to achieve unconditional unlinkability. Ordinary types of cryptographic signatures permit to trace transactions to their

respective senders and receivers. **Cryptonote** solution to this deficiency lies in using a different signature type than those currently used in electronic cash systems. The idea behind the protocol is fairly simple: a user produces a signature which can be checked by a set of public keys rather than a unique public key. The identity of the signer is indistinguishable from the identities of the other users whose public keys are in the same set.

Privacy within **Cryptonight 2.0** transactions is achieved by three primary constructions: **Ring Signatures**, **One-Time Keys**, and **Amount Commitments**. The use of **Ring Signatures** ensures that an attacker cannot determine the actual input public key used in the transaction, as it is obscured by the presence of randomly chosen input public keys.

One-Time Keys are generated using transaction parameters and the recipient's published wallet address, and are intended to make it impossible for anyone but the recipient to identify the destination of transactions or spend the resulting funds.

Amount Commitments use homomorphic properties to guarantee that while a third party is not able to determine the amount of a transaction output, it can prove that the transaction inputs and outputs are balanced. When combined with a range proof to ensure that the output is within a defined and valid range, commitments mask transaction amounts while avoiding misuse by a malicious spender.

A different issue not addressed by these three privacy guards is that of recipient addresses. A user may wish to receive funds into a wallet for personal donations, but also wish to receive funds for purchase from his business. If the user is conscious of his privacy, he may not wish to use the same wallet address, since this links his personal and business online presence to the same individual. An obvious solution for him is to create two wallets and publish the addresses separately, one to his personal blog and the other to his business site. But this means that he must scan each transaction twice to determine the wallet it was sent to.

By using **eDollar**'s **Cryptonote 2.0** practical implementation, a user can generate and publish different and unlinkable addresses in a way that does not adversely affect computations applied to incoming transactions: a subaddress scheme which allows him to produce as many addresses as he wishes and distribute them freely in any way he needs. All these subaddresses coexist within the same wallet, under the absolute and sole control of the user,

and cannot publicly be linked to each other. And as the computations required scale in constant time with the number of subaddresses during incoming transactions, then there is no additional computational complexity overloading the system nor putting in risk the anonymity of the wallet itself.

eDollar is the first successful practical implementation of both one-time ring signature scheme and wallet subaddresses.

References

1. https://cryptonote.org/whitepaper.pdf
2. https://lab.getmonero.org/pubs/MRL-0005.pdf
3. https://lab.getmonero.org/pubs/MRL-0006.pdf