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 untraceable and cannot be tied back to an individual user or computer. By default, 10,000 different* ***subaddresses*** *that belong to the same wallet can be generated in order to receive unlinkable payments. No observer can determine what transaction was sent to a specific address nor link two addresses together.* ***eDollar*** *wallet takes advantage of linked subaddresses to perform secured off-chain atomic private transactions which funds are consolidated on the* ***eDollar*** *Blockchain before being use again, in order to prevent double expend.*

DISCLAIMER: Anyone may use, reproduce or distribute without permission any material in this white paper for non-commercial and educational use (i.e., other than for a fee or for commercial purposes) provided that the original source and the applicable copyright notice are cited. This eDollar Technical White Paper is for information purposes only. eDollar.cash guarantees the accuracy of or the conclusions reached in this white paper, only while used within eDollar.cash approved and recommended software implementations. This white paper is provided "as is". eDollar.cash does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights. eDollar.cash and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. In no event will eDollar.cash or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.

Introduction

When FIAT money, in the form of a paper bill or a metal coin, is used in any place 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 easily determine the path that the funds followed among different banks in different countries. Even worse, those trusts are slow and expensive, and the system is by design made so it can always know the balance of any involved part, exposing the users safety to dishonest or controlling eyes.

With cryptocurrency introduction, the main objective was to safely allow commercial interchange in a trustless environment. Cryptocurrency 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 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 complexity, the goal of many projects has simply turned into a way to raise funds, copying the 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, anonymity and scalability, 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**, **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, 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 proposal of the concept of peer-to-peer electronic currency. The general public have come to appreciate the convenient combination of public transactions as a trust model. Bitcoin has effectively proved that electronic currency can be as simple as paper money and as convenient as credit cards. However, it suffers from critical flaws that cannot be fixed rapidly, detering Bitcoin's propagation. In such inflexible models, it is more efficient to roll-out a new project rather than perpetually fix the original project. These flaws are:

Anonymity

Should be the most important aspect of electronic cash. Privacy, defined by T. Okamoto and K. Ohta, as the "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.

When using Bitcoin, 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 network and their transactions. A lot of hidden personal information can be extracted from the public ledger 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 all of its Tokens.

Scalability

Refers to the limits on the amount of transactions the bitcoin network can process during a timeframe. It is related to the fact that records (known as blocks) in the bitcoin Blockchain are limited in size and frequency. Bitcoin's blocks contain the transactions on the bitcoin network with a transaction processing capacity limited by the average block creation time of 10 minutes and a block size. These jointly constrain the network's throughput. The maximum transaction processing capacity is estimated between 3.3 and 7 transactions per second. That is extremely slow compared to the amount of cash transactions per second that can occur in a single crowded market of any city.

eDollar CryptoNote Based Technology

Untraceable Transactions

In the model used by Bitcoin and Ethereum, a user possesses one **FIRST** unique key that is **private** (used to **SPEND,** sign and send funds) and **SECOND** unique key that is **public** (used to **RECEIVE** the funds, and the becomes openly linked to the public key of the sender). In **CryptoNote** model, a **THIRD** different key, owned by the receiver, is the unique **"VIEW"** key, that must be used in combination with the public key in order to display a transaction in the public ledger explorer, and when used with the transaction hash, will show only a single given record while hiding all other sent to the same recipient address. Without this **VIEW key/Transaction Hash** pair, no one can see the amount sent, thus keeping ownership and actual spending, completely anonymous.

When a sender generates a transaction, his Wallet creates a one-time public key based on the recipient’s address and some random data. 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 then spend the funds when needed. This new scheme relies on the cryptographic primitive called "group signature", first presented by D. Chaum and E. van Heyst, where a verifier can proof that the real sender is one member of a 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*. 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 Wallet 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.

Unlinkable payments

Once published, classic Bitcoin and Ethereum addresses, become an unambiguous identifier for incoming and outgoing payments, tying up the sender’s and the recipient’s public addresses, and displaying the transaction amount in the public ledger, 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 each time and never publish them in with his own name or pseudonym.

Cryptonote solves this situation allowing a user to publish and receive unlinkable payments with a subaddress that is unlinkable to his main address. 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** 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. Thus, **eDollar** becomes the first successful practical implementation of both one-time ring signature scheme and wallet subaddresses.

Scalability Pulse and Scalability Pulse Nodes

The Bitcoin adoption has been slowed down for the transactions-per-second bottleneck. This is due to several technical limitations which involve Internet connection bandwidth, nodes, CPU´s, block size, Blockchain algorithm, etc. However, there is an enormous amount of Bitcoin transactions actually occurring off-chain. Speculative markets run bots that perform several hundred off-chain trades per second. These transactions are happening in every and each of the cryptocurrency trades that multiply all over the world, allowing a big scale trade of coins, but not the trade of coins for goods or services, which was meant to be the original Bitcoin objective. Only when the funds are moved from one exchange to another, or sent to/from a personal wallet, the transactions are registered in the Blockchain.

eDollar has an unique feature that allows off-chain private transactions. Every **eDollar** Atomic Unit, named ePenny now on, exists in two different, excluding states: **Non-Cash or Inactive Cash State (ICS)** and **Cash Currency State (CCS)**.

- **ICS:** When the coin is in its **Non-Cash State**, it can be stored, used and normally traded on the **eDollar** Blockchain as every other crypto that uses the CN algorithm, taking the all the above mentioned advantages inherent to **EDL** implementation.
- **CCS:** When the coin is **Cash-Currency State**, it can be tradable between two offline wallets. The binary code of every single **ePenny** is a fixed size block of code composed by two intimately linked parts, a **head** holding the intrinsic binary information that defines itself as a cryptocurrency, and a "**tale"** consisting of an allocated, fixed amount of bytes that are cryptographically modified with every transaction to accommodate a coherent sequence of up to 3 hashes or short-history.
- The first hash is generated when the coin is transferred from the Blockchain to the **ePenny Active Wallet (PAW)** using an encrypted routine that explodes the advantage of the subaddresses inherent to the CN algorithm. With each interchange where the **ePenny** is involved up to 2 subsequent hashes, are added to the **"tale"**.

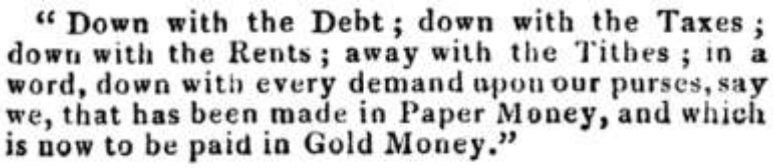
Once an **ePenny** has reached the limit of 3 hashes, it has to be consolidated -sent back to the Blockchain- in order to be tradable again and prevent double spend.

- In this model, every hash will remain attached to the Atomic Unit until being consolidated on the **eDollar** Blockchain, which occurs when the network is available, or upon the last owner request. During the atomic unit consolidation phase -or Block creation- the **"tale"** of hashes is cleared and removed from every **ePenny**, and the cycle (**Scability Pulse**) of this fungible Atomic Unit can then be repeated again.
- These off-chain transactions render a **"tale"** or short sequence of hashes, that can be assumed as a limited **Intra-Coin-Ledger (ICL)** which relies on the two involved peers mutual trust. It is intended for everyday face-to-face expenses, such as tipping and paying for goods and services, allowing fast interchange of the intrinsic value of the coin instead of delaying futile operations through a complex cryptographic process. The amount of hashes is *initially* limited to just a couple of transactions, in order to prevent double-spend of funds.
- The desired **eDollar** amount is transferred from the chain to the **ePenny Active Wallet (PAW)** using the main wallet address, and then it can be freely traded as **cash-currency** by an lightning fast, two-party agreement, peer-to-peer instant atomic trade, only limited by the speed of the communication protocol between the two devices running the wallets (USB, Bluetooth, Wi-Fi, NFC).
- Each involved wallet must be registered and activated in the **eDollar** network to perform off-chain operations under a common handshaking protocol, where the integrity of the wallets is cross-checked before the interchange occurs, acting as a micronode that progressively changes the hash "tale" of the traded coins, both in the giver and in the receiver sides.
- The Wallet registration process is a one-time quick and easy process, costing only one **ePenny**, which hash is used as a seed, together with the main **eDollar** address of the wallet being registered, to create the **Activation Hash**. The conversion from the **Inactive Cash State (ICS)** to the **Cash Currency State (CCS)** is instantaneous, and consumes the same resources/fees as every in-chain transaction.
- The reverse process involves the reinsertion of the coins in **CCS,** from the last wallet that received it to the Blockchain in order to perform the consensus that will confirm the first and the last hashes (that belongs to the last owner of the coin being

registered in the Blockchain). This way every participating node scrutinizes the sequence of hashes to create a **Ring CT** with the use of the intermediate hashes, and then removes all the **"tale"** before confirming the transaction and generating the corresponding Block. Only then, the **ePenny** is ready for another cycle or **Pulse**.

- In a larger scale solution, a local off-chain node with a special **Scalability Pulse Internal Node (SPIN)** running on it, can be securely registered and set up to serve a **Private Electronic Trade Site (PETS)**. This site can be conceptualized as the off-chain ledger within an Intranet, WiFi/Bluetooth private network in a Theme-Park, Resort, Cruise (or a Ferry Boat), international agricultural fair, private auction, Casino, a professional meeting with a hundred booths, or even the most demanding and challenging site: a city market. Here, every seller participating in the **PETS** will register one or more of his receiving addresses in the **SPIN**. And when a customer enters the **PETS** is allowed to register one of his multiple wallet addresses linked to his main account, and a single use view-key. Then, by using his **ePenny Active Wallet**, a the potential customer would lock an amount of his funds (which is the maximum of what he can freely spend into this **PETS)**. When the seller or the customer leave the site and checks-out, his balance gets consolidated form the off-chain ledger to the Blockchain, and registered to create an immutably record.

This solution sets a trustless offline environment to hold simultaneous, almost unlimited, off-chain operations between registered devices, secured by **ePenny Active Wallet** and **Scalability Pulse Internal Node** hashes and, at the same time, the whole system further preserves privacy because of the **CN** algorithm involved to create the Blockchain, so that no backlog can be done to trace the funds.



"Down with the Debt; down with the Taxes; down with the Rents; away with the Tithes; in a word, down with every demand upon our purses, say we, that has been made in Paper Money, and which is now to be paid in Gold Money."

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
4. Blamire W, Reform, Retrenchment, a Cash Currency, no Corn Laws, and Cheap Bread