Greenshilling presents a genuine chance to have a positive effect on the environment, an opportunity to help others, coupled to an opportunity to generate.

Led by a group of environmentally conscious entrepreneurs with a wealth of business experience and proven track records of success in the internet, environmental and marketing industries. This powerful combination results in a first class opportunity with a business poised for huge growth.

We have a simple mission; to make a positive difference to people's lives and to have a positive impact on the planet.

This will be achieved by empowering people to make a difference in our world.

Enviromental Trust

The Trust sponsors humanitarian and environmentally friendly projects. People contribute by simply using Greenshilling and we add a matching contribution to selected projects. All aspects of our business contribute positively to the Environment and also to less fortunate people. Currently we support many projects such as trees for schools, Reforestation, afforestation and forestry protection in Zambia, we have also supplied biochar stoves to impoverished families in India and sponsored medical aid for orphans in China

Greenshilling and the Environment

Greenshiling rewards individuals for environmental stewardship. Associate can use carbon offset units to acquire Greenshilling mining slots. The slots produce Greenshilling coins and the carbon offsets are retired to offset greenhouse gas emissions, supporting environmentally friendly projects.

Greenshiling is a principle foundation of a powerful new marketing system that will enable business owners and direct sales professionals to maximise the true potential of digital crypto-currency.

Bringing together Greenshilling with the Ausante, Xoppon and PlaysNation programmes into one simple, integrated solution appeals to business owners and private individuals alike and situate them in prime position to lead this astonishing new industry.

Greenshilling benefits from a self building pool of global users. Our long-term goal is to establish a community of one billion Greenshilling users within the next 10 years. To achieve this aim we have adopted a simple yet financially potent marketing programme that offers private and business customers genuine benefits and a significant wealth opportunity featuring no fewer than 10 different, exciting revenue streams.

All Owners, Players, Customers and Associates are entitled to be users and promoters of Greenshilling. The ecosystem has four types of participant:

Owners – Xoppon - An Owner can participate in the Xoppon e-commerce solution, the PlaysNation Gaming Platform or both. Both of these are simple cost effective turnkey solutions for established and start up businesses alike

The E-Commerce market exceeds $2 trillion per annum. Xoppon provides a custom e-commerce shop, easy to join and simple to set up, enabling Owners to set up their own store opening up the benefits of generating income from highly lucrative online shopping. Xoppon provides Owners with the ability to sell their existing product lines, they simply market their site, sell their products, ship them and take their profits.

The unique benefits of the ground breaking Xoppon repository helps Owners source products and fulfilment through offering access to a wide choice of multiple categories of products that can be fulfilled and shipped to customers on the Owners behalf. Additionally, Xoppon offers Owners the opportunity to list their own products in the repository, providing them with a global opportunity to sell their products through the Xoppon global sales network. This additionally provides vendors with a more extensive range of products to offer to customers. Every Owner can choose to accept Greenshilling paymrnt on thoer site. Through building their own e-commerce store, an Owner can earn money 24/seven, creating an income stream that has the potential of funding them passively.

Owners – PlaysNation - The online Gaming market exceeds $100 billion per annum and online advertising exceeds $200 billion per annum. A PlaysNation Owner can earn from players making in game purchases and subscriptions and receive a percentage of gross gaming revenue. Owners can promote their site and additionally earn from advertising revenue from other businesses who advertise on the website. This enables Owners to promote their own brand or sell advertising space and promotional tools to others. They can charge for space on their Home Page, charge for space on their Special Offers Page, charge for Local, National and International Banner ads across the entire Portal, Offer Tournament Sponsorship, Offer Video features, Offer surveys and Market Research. Plus there are many more revenue generating opportunities as a PlaysNation Owner.

So in summary, an Owner can Earn from Players, Earn from Advertising Revenue, Earn Greenshilling from Activity, Retain customers and Interact with them, Promote their own Products and Opportunites or Sell Advertising Space and Marketing Solutions to Others.

Customers – Xoppon - When a customer arrives at a Xoppon website, they can choose to participate as a guest or they can register as a Customer. The benefits of registering are, first it is free to join and second, customers are now eligible to participate in the Greenshilling Loyalty Reward Program. This means that they can earn customer referral rewards and spend Greenshilling with participating sites, helping the environment and good causes.   Additionally, customers can gain recognition for their philanthropic support.

Players – PlaysNation - The online games market is a very popular and growing market with more and more people spending their leisure time participating in this activity at home and on the move.

Players can enjoy a fully featured gaming platform that integrates with their desktop or laptop computer, smartphone or tablet. They Enter the PlaysNation site, choose a featured game to play and share the page with friends. They can play as a Guest or enjoy the benefits of becoming a Registered User. There are a host of additional deployments including, Facebook, Android, Virtual Reality and WeChat.

The benefits of registering are, first that it is free to join and second, they are now eligible to participate in the Greenshilling Loyalty Reward Program. This means that they can earn customer referral rewards and spend Greenshilling with participating sites, helping the environment and good causes. Additionally, they can earn Game Credits as they play.

Associates - An Associate is an independent distributor of products and services who works together with the marketing the company. Being an Associate offers an exciting income opportunity working hours that suit the individual. Associates generate income by finding new Owners for the PlaysNation Gaming Platform, new Owners for the Xoppon E-commerce Solution and also by building a team of Associates.

Associates and Owners benefit from continued high quality marketing assistance, training and support.

This unique relationship marketing incentive programme will motivate Associates to actively promote E- Commerce products and services directly to Owners, truly merging opportunities in the virtual and real worlds, resulting in win win win for Owners, Associates, Enviroway and Greenshilling.

Greenshilling Cashback
We feature a loyalty reward program which enables anyone to earn Greenshilling Cashback. A few examples of how to do this are when a Player or Customer makes a purchase, when an Owner subscribes, when a new Player or Customer is found. Greenshilling Cashback is paid to eligible participants when any positive business activity within the Enviroway universe happens, this benefits the Enviroway and good causes too!

Greenshilling Technology

Greenshilling based on PeerCoin technology: Peer-to-Peer Crypto-Currency with Proof-of-Stake

A peer-to-peer crypto-currency design derived from the technology behind Bitcoin.

Proof-of-stake replaces proof-of-work to provide the majority of the network security.

Under this hybrid design proof-of-work mainly provides initial minting but becomes largely non-essential over time. This means that the Security level of the network becomes more environmentally friendly as it is not dependent on energy consumption in the long term, providing an energy efficient, and more cost-competitive peer-to-peer crypto-currency.

Proof-of-stake is based on coin age and generated by each node via a hashing scheme bearing similarity to Bitcoin's, but over limited search space.

Block chain history and transaction settlement are further protected by a centrally broadcast checkpoint mechanism.

Introduction

Since the creation of Bitcoin (Nakamoto 2008), proof-of-work has been the predominant design of peer-to-peer crypto currency. The concept of proof-of-work has been the backbone of minting and security model of Nakamoto's design.

In October 2011, it was realized that, the concept of coin age can facilitate an alternative design known as proof-of-stake, to Bitcoin's proof-of-work system. This resulted in a formalized design where proof-of-stake is used to build the security model of a peer-to-peer crypto currency and part of its minting process, whereas proof-of-work mainly facilitates the initial part of the minting process and gradually reduces its significance. This design demonstrates the viability of future peer-to-peer crypto-currencies with no dependency on energy consumption, an important factor for Greenshilling.

Coin Age

The concept of coin age was known to Nakamoto at least as early as 2010 and used in Bitcoin to help prioritize transactions, for example, although it didn't play a particularly critical role in Bitcoin's security model.   Coin age is simply defined as currency amount times holding period. In a simple to understand example, if Mike received 10 coins from Jane and held it for 90 days, we say that Mike has accumulated 900 coin-days of coin age.

Additionally, when Mike spent the 10 coins he received from Jane, we say the coin age Mike accumulated with these 10 coins had been consumed (or destroyed).

In order to facilitate the computation of coin age, a timestamp field was introduced into each transaction. Block timestamp and transaction timestamp related protocols are strengthened to secure the computation of coin age.

Proof-of-Stake

Proof-of-work helped to give birth to Nakamoto's major breakthrough, however the nature of proof-of-work means that the crypto-currency is dependent on energy consumption, thus introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees.

As the mint rate slows in the Bitcoin network, eventually it could put pressure on raising transaction fees to sustain a preferred level of security. This poses the question whether energy consumption must be maintained in order to have a decentralized crypto-currency? Thus it is an important milestone both theoretically and technologically, to demonstrate that the security of peer-to-peer crypto-currencies does not have to depend on energy consumption.

A concept termed proof-of-stake was discussed among Bitcoin circles as early as 2011. Generally, proof-of-stake means a form of proof of ownership of the currency. Coin age consumed by a transaction can be considered a form of proof-of-stake. The concept of proof-of-stake and the concept of coin age was independently discovered by Sunny King and Scott Nadal, developers of Peercoin, inOctober 2011. They realized that proof-of-stake can indeed replace most proof-of work's functions through a careful redesign of Bitcoin's minting and security model. This is mainly because, similar to proof-of-work, proof-of-stake cannot be easily forged. Of course, this is one of the critical requirements of monetary systems - difficult to counterfeit. Philosophically speaking, money is a form of 'proof-of-work' in the past thus should be able to substitute proof-of-work all by itself.

Block Generation under Proof-of-Stake

In our hybrid design, blocks are separated into two different types, proof-of-work blocks and proof-of-stake blocks.
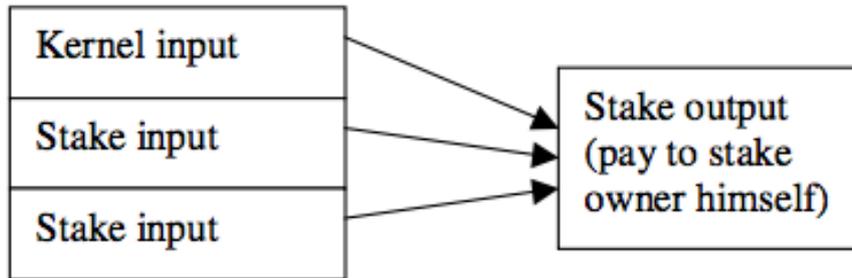

Figure: Structure of Proof-of-Stake (Coinstake) Transaction

The proof-of-stake in the new type of blocks is a special transaction called coinstake (named after Bitcoin's special transaction coinbase). In the coinstake transaction block, the owner pays himself thereby consuming his coin age, while gaining the privilege of generating a block for the network and minting for proof-of-stake. The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-of work blocks. However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved.

The hash target that stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (in contrast to Bitcoin's proof-of-work target which is a fixed target value applying to every node). Thus the more coin age consumed in the kernel, the easier meeting the hash target protocol. For example, if Mike has a wallet-output which accumulated 100 coin-years and expects it to generate a kernel in 2 days, then Jane can roughly expect her 200 coin-year wallet-output to generate a kernel in 1 day.

In this design both proof-of-work hash target and proof-of-stake hash target are adjusted continuously rather than Bitcoin's two-week adjustment interval, to avoid sudden jump in network generation rate.

Minting based on Proof-of-Stake
A new minting process is introduced for proof-of stake blocks in addition to Bitcoin's proof-of-work minting. Proof-of-stake block mints coins based on the consumed coin age in the coinstake transaction. With GreenShilling, a mint rate of 3 cent per coin-year consumed is chosen to give rise to a low future inflation rate.

Proof-of-work is kept as part of the minting process to facilitate initial minting, it is conceivable that in a pure proof-of-stake system initial minting can be seeded completely in genesis block via a process similar to stock market initial public offer (IPO).

Main Chain Protocol

The protocol for determining which competing block chain wins as main chain has been switched over to use consumed coin age. Here every transaction in a block contributes its consumed coin age to the score of the block. The block chain with highest total consumed coin age is chosen as main chain.

This is in contrast to the use of proof-of-work in Bitcoin's main chain protocol, whereas the total work of the block chain is used to determine main chain.

This design alleviates some of the concerns of Bitcoin's 51% assumption, where the system is only considered secure when good nodes control at least 51% of network mining power. First the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, thus raising the cost of attack for such powerful entities. Also attacker's coin age is consumed during the attack, which may render it more difficult for the attacker to continue preventing transactions from entering main chain.

Checkpoint: Protection of History

One of the disadvantages of using total consumed coin age to determine main chain is that it lowers the cost of attack on the entire block chain of history. Even though Bitcoin has relatively strong protection over the history Nakamoto still introduced checkpoints in 2010 as a mechanism to solidify the block chain history, preventing any possible changes to the part of block chain earlier than the checkpoint.

Another concern is that the cost of double-spending attack may have been lowered as well, as attacker may just need to accumulate certain amount of coin age and force reorganization of the block chain. To make commerce practical under such a system, we decided to introduce an additional form of checkpoints that are broadcasted centrally, at much shorter intervals such as a few times daily, to serve to freeze block chain and finalize transactions. This new type of checkpoint is broadcasted similar to Bitcoin's alert system.

In order to defend against a type of denial-of-service attack coinstake kernel must be verified before a proof-of-stake block can be accepted into the local database (block tree) of each node. Due to Bitcoin node's data model (transaction index specifically) a deadline of checkpointing is needed to ensure all nodes' capability of verifying connection of each coinstake kernel before accepting a block into the block tree. Because of the above practical considerations, the node's data model has not been modified but central checkpointing is used instead. The coin age computation is modified to require a minimum age, such as one month, below which the coin age is computed as zero. Then the central checkpointing is used to ensure all nodes can agree upon past transactions older than one month thus allowing the verification of coinstake kernel connection as a kernel requires non-zero coin age thus must use an output from more than one month ago.

Block Signatures and Duplicate Stake Protocol

Each block must be signed by its owner to prevent the same proof-of-stake from being copied and used by attackers. A duplicate-stake protocol is designed to defend against an attacker using a single proof of-stake to generate a multitude of blocks as a denial-of-service attack. Each node collects the (kernel, timestamp) pair of all coinstake transactions it has seen. If a received block contains a duplicate pair as another previously received block, we ignore such
duplicate-stake block until a successor block is received as an orphan block.

Energy Efficiency

When the proof-of-work mint rate approaches zero, there is less and less incentive to mint proof-of-work blocks. Under this long term scenario energy consumption in the network may drop to very low levels as disinterested miners stop mining proof-of-work blocks. The Bitcoin network faces such risk unless transaction volume/fee rises to high enough levels to sustain the energy consumption. Under our design even if energy consumption approaches zero the network is still protected by proof-of-stake. A crypto-currency is called "long-term energy-efficient" if energy consumption on proof-of-work is allowed to approach zero.

Other Considerations

The proof-of-work mint rate is not determined by block height (time) but instead determined by difficulty. When mining difficulty goes up, proof-of-work mint rate is lowered. A relatively smooth curve is chosen as opposed to Bitcoin's step functions, to avoid artificially shocking the market. More specifically, a continuous curve is chosen such that each 16x raise of mining difficulty halves the block mint amount.

Over longer term the proof-of-work mint curve would not be too dissimilar to that of Bitcoin in terms of the inflationary behavior.   The traditional observation is followed that the Market favors a low inflation currency over a high-inflation one.

Babaioff et al. (2011) studied the effect of transaction fee and argued that transaction fee is an incentive to not cooperate between miners. Under the GreensShilling system this attack is exacerbated so that transaction fees are no longer give to block owner. Transaction fees are destroyed, removing the incentive to not acknowledge other minter's blocks. It also serves as a deflationary force to counter the inflationary force from the proof-of-stake minting.   Transaction fees are enforced at protocol level to defend against block
bloating attack.

Acknowledgement

Many thanks to Sunny King and Scott Nadal for their development of Peer-to-Peer Crypto-Currency with Proof-of-Stake.

Alos thanks to Satoshi Nakamoto and Bitcoin developers whose brilliant pioneering work made project such as this possible.

References

Babaioff M. et al. (2011): On Bitcoin and red balloons.
Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)
Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)