BLOCKCHAIN TECHNOLOGY

Alternative Coins

Introduction

- Bitcoin was released in 2009
- the first alternative coin project (named Namecoin) was introduced in 2011
- In 2013 and 2014, the alternative coins (altcoin) market grew exponentially
  - A few of those became a success
  - many failed
  - A few were pump and dump scams
    - surfaced for some time but soon disappeared
- Alternative approaches can be divided into two categories
  - alternative chains
    - the primary goal is to build a decentralized blockchain platform
    - discussed in detail in Chapter 16
  - altcoin
    - the sole purpose is to introduce a new virtual currency
    - The focus of this chapter

Introduction

- Altcoins must be able to attract new users, trades, and miners
  - otherwise, the currency will have no value
- Methods to gain initial number of users
  - Create a new blockchain and allocate coins to initial miners
    - Now unpopular due to many scam schemes or pump and dump schemes
  - Proof of Burn (PoB)
  - Proof of ownership
  - Pegged sidechain

Introduction

- Altcoins must be able to attract new users, trades, and miners
  - otherwise, the currency will have no value
- Methods to gain initial number of users
  - Create a new blockchain and allocate coins to initial miners
  - Proof of Burn (PoB)
    - also called a one-way peg or price ceiling.
    - users permanently destroy a certain quantity of bitcoins in proportion to the quantity of altcoins to be claimed
      - This means that bitcoins are being converted into altcoins
    - E.g., if ten bitcoins were destroyed
      - Altcoins can have a value no greater than some bitcoins destroyed.
  - Proof of ownership
  - Pegged sidechain

Introduction

- Altcoins must be able to attract new users, trades, and miners
  - otherwise, the currency will have no value
- Methods to gain initial number of users
  - Create a new blockchain and allocate coins to initial miners
  - Proof of Burn (PoB)
  - Proof of ownership
    - proving that users own a certain number of bitcoins
      - This proof can be used to claim altcoins
    - E.g., this can be achieved by merged mining
      - bitcoin miners can mine altcoin blocks while mining for bitcoin without any extra work
  - Pegged sidechain

Introduction

- Altcoins must be able to attract new users, trades, and miners
  - otherwise, the currency will have no value
- Methods to gain initial number of users
  - Create a new blockchain and allocate coins to initial miners
  - Proof of Burn (PoB)
  - Proof of ownership
  - Pegged sidechain
    - blockchains separate from the bitcoin network
      - but bitcoins can be transferred to them
      - Altcoins can also be transferred back to the bitcoin network
    - This concept is called a two-way peg.

Alternatives to Proof of Work

- PoW was first used in Bitcoin
  - provides decentralization, security, and stability for the blockchain.
  - required properties
    - progress freeness
      - means that the reward for consuming computational resources should be
        - random
        - proportional to the contribution made by the miners
      - some chance of winning the block reward is given to even weak miners
    - Adjustable difficulty
      - Mining difficulty is regulated matching with hashing power
    - Quick verification
      - computational puzzles should be easy and quick to verify
  - Causes power shifting towards miners with large-scale ASIC farms

Alternatives to Proof of Work

- ASIC-resistant puzzles
  - building ASICs for solving theses puzzles
    - is infeasible
    - does not result in a major performance gain over commodity hardware.

Alternatives to Proof of Work

- ASIC-resistant puzzles
  - memory hard computational puzzles
    - puzzle solving requires a large amount of memory
    - initially used in Litecoin and Tenebrix
      - the Scrypt hash function was used
        - a memory intensive hash function
      - was initially advertised as ASIC resistant
        - Scrypt ASICs have now become available
          - Disproving the original claim by Litecoin.
    - it was thought that building ASICs with large memories is difficult
      - This is no longer the case
        - memory is increasingly becoming cheaper
        - It is possible to produce nanometer scale circuits

Alternatives to Proof of Work

- ASIC-resistant puzzles
  - Using multiple hash functions
    - also called a chained hashing scheme
    - The rationale is that designing multiple hash functions on an ASIC is not very feasible.
    - example is the X11 memory hard function implemented in Dash
      - comprises 11 chained hash function
    - did provide some resistance to ASIC development
      - but now ASIC miners are available commercially

Alternatives to Proof of Work

- ASIC-resistant puzzles
  - self-mutating puzzles
    - intelligently or randomly change the PoW scheme or its requirements as a function of time.
    - It may be designed in future
      - will make almost impossible to be implemented in ASICs
    - Now
      - it is unclear how this can be achieved practically.

Alternatives to Proof of Work

- PoW has huge energy consumption
  - A solution is proof of useful work
    - puzzles can be designed to serve two purposes
      - primary purpose is in consensus mechanisms
      - Secondary purpose is to perform some useful scientific computation
    - An example is Primecoin
      - the requirement is to find special prime number chains
        - known as Cunningham chains and bi-twin chains.
      - prime number distribution has significance in scientific disciplines
        - such as physics
      - By mining Primecoin, miners
        - not only achieve the block reward
        - but also help in finding the special prime numbers

Alternatives to Proof of Work

- PoW has huge energy consumption
  - A solution is proof of useful work
    - Another example is Proof of Storage
      - Introduced by Microsoft Research
      - provides a useful benefit of distributed storage of archival data.
      - Miners are required to store a pseudo, randomly-selected subset of large data to perform mining

Alternatives to Proof of Work

- Proof of Stake (PoS)
  - also called virtual mining
  - It was first proposed in Peercoin
  - users are required to prove possession of a certain number of coins (coins)
  - simplest form is where mining is made comparatively easier for those users who demonstrably own larger number of coins
    - benefits are twofold
      - acquiring large number of coins is difficult as compared to buying high-end ASIC devices
      - it results in saving computational resources.

Alternatives to Proof of Work

- Proof of Stake (PoS)
  - Stake types
    - Proof of coinage
      - coin age: the time since the coins were last used or held.
      - The miner is rewarded for holding and not spending coins for a period.
      - The difficulty of mining puzzles is inversely proportional to the coinage
      - has been implemented in Peercoin combined with PoW

Alternatives to Proof of Work

- Proof of Stake (PoS)
  - Stake types
    - Proof of Deposit (PoD)
      - newly minted coins by miners are get locked for a certain period.
      - miners can perform mining at the cost of freezing a certain number of coins for some time.
    - Proof of Burn
      - destroys a certain number of bitcoins to get equivalent altcoins.
      - is commonly used when starting up a new coin projects to provide a fair initial distribution.

Alternatives to Proof of Work

- Proof of Stake (PoS)
  - Stake types
    - Proof of Activity (PoA)
      - a hybrid of PoW and PoS.
      - blocks are initially produced using PoW
      - then each block randomly assigns three stakeholders that are required to digitally sign it.

Difficulty adjustment and retargeting algorithms

- In bitcoin

$$T = Time\ previous * time\ actual / 2016 * 10\ min$$

- if a new coin use the same PoW based on SHA-256 as bitcoin uses
  - it is easy for a malicious user to control the entire network.
    - using ASIC miners
- Pool hopping is a more significant threat
  - Pool can automatically switch to the new profitable currency
  - impacts the network adversely because
    - pool hoppers join the network only when the difficulty is low
      - can gain quick rewards
    - the moment difficulty goes up
      - they hop off
    - then come back again
      - when the difficulty is adjusted back.

Difficulty adjustment and retargeting algorithms

- If a multipool hops into mining a new coin
  - The difficulty will increase very quickly
  - when the multipool leaves the network
    - It becomes almost unusable because
      - it is no longer profitable for solo miners
      - can no longer be maintained.
    - The only fix is to initiate a hard fork

Difficulty adjustment and retargeting algorithms

- Kimoto Gravity Well
  - was first introduced in Megacoin
  - adjusts the difficulty for every block adaptively

*KGW = 1 + (0.7084 * pow((double(PastBlocksMass)/double(144)), -1.228))*

  - The algorithm runs in a loop that
    - goes through a set of predetermined blocks (PastBlockMass)
    - calculates a new readjustment value

Difficulty adjustment and retargeting algorithms

- Dark Gravity Wave (DGW)
  - was first introduced in Dash
  - makes use of multiple exponential moving averages and simple move averages
  - allows improved difficulty retargeting compared to KGW

Difficulty adjustment and retargeting algorithms

- DigiShield
  - has been used in Zcash
  - works by going through a fixed number of previous blocks
    - calculates the time they took to be generated
    - readjusts the difficulty to the difficulty of the previous block by
      - dividing the actual time span by averaging the target time
  - the retargeting is calculated much more rapidly
    - the recovery from a sudden hash rate change is quick
  - protects against multipools

Difficulty adjustment and retargeting algorithms

- Multi-Interval Difficulty Adjustment System (MIDAS)
  - Is comparatively more complex than previously discussed algorithms
  - Has more parameters.
  - responds much more rapidly to abrupt changes in hash rates

Bitcoin limitations

- Privacy and anonymity
  - Analyzing blockchain is trivial, because
    - it is a public ledger of all transactions
    - It is openly available
  - A big concern
    - By combining blockchain analysis and traffic analysis
      - transactions can be linked back to their source IP addresses
      - transaction's originator can be revealed

Bitcoin limitations

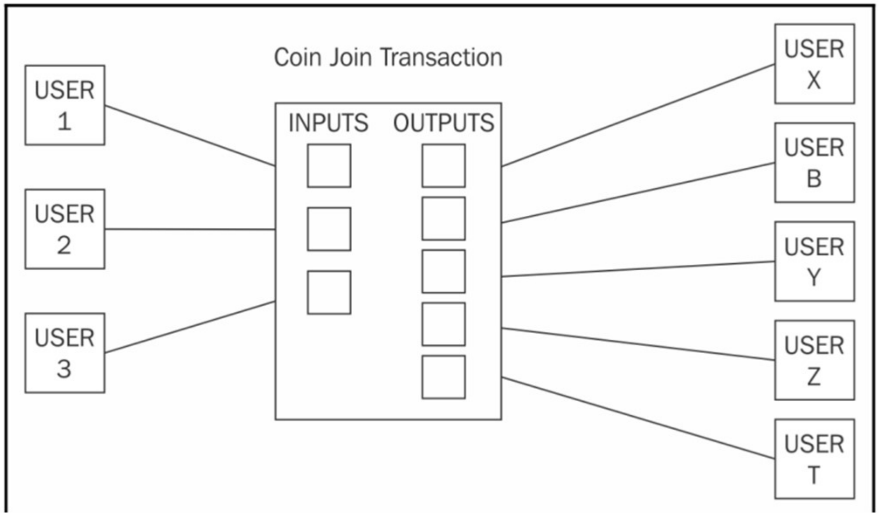
- Privacy and anonymity
  - Three types of proposals to address the privacy issue in Bitcoin
    - mixing protocols
    - third-party mixing networks
    - Inherent anonymity

Bitcoin limitations

- Privacy and anonymity
  - Mixing protocols
    - A mixing service provider is used
      - an intermediary or a shared wallet
    - Users send coins to this shared wallet as a deposit
    - Then, the shared wallet sends some other coins to the destination.
      - the same value deposited by some other users
    - Users can also receive coins via this intermediary.
    - This way
      - the link between outputs and inputs is no longer there
      - transaction graph analysis becomes useless

Bitcoin limitations

- Privacy and anonymity
  - Mixing protocols
    - Coinjoin is an example
      - two transactions are joined together to form a single transaction
        - keeping the inputs and outputs unchanged
      - core idea is to build a shared transaction
        - signed by all participants
      - improves privacy for all participants involved in the transactions



Bitcoin limitations

- Privacy and anonymity
  - Third-party mixing protocols
    - Various third-party mixing services are available
    - if the service is centralized
      - It knows about all inputs and outputs
        - poses the threat of tracing the mapping between users
      - pose the risk of the administrators of the service stealing the coins.
    - E.g., CoinShuffle, Coinmux, and Darksend in Dash
      - are based on the idea of CoinJoin transactions.
      - CoinShuffle is decentralized alternative
        - does not require a trusted third party

Bitcoin limitations

- Privacy and anonymity
  - CoinJoin-based schemes have some weaknesses
    - most prominently the possibility of launching a denial-of-service attack
      - users initially commit to signing the transactions
      - but are not providing their signature

Bitcoin limitations

- Privacy and anonymity
  - Inherent anonymity
    - includes coins that support privacy inherently
      - built into the design of the currency.
    - The most popular is Zcash
      - uses Zero-Knowledge Proofs (ZKP) to achieve anonymity
      - It is discussed in detail later in the chapter
    - Other examples include Monero
      - makes use of ring signatures to provide anonymous services.
        - a type of digital signature that can be performed by any member of a set of users that each have keys

Extended protocols on top of Bitcoin

- Colored coins
  - a set of methods to represent digital assets on the Bitcoin blockchain
  - Coloring a bitcoin means updating it with some metadata
    - representing a digital asset (smart property).
  - The coin still works and operates as a bitcoin
    - but additionally carries some metadata representing some assets
  - The metadata can be
    - some information related to the asset
    - some calculations related to transactions
    - or any arbitrary data.
  - allows issuing and tracking specific bitcoins
  - Metadata can be recorded using
    - the bitcoins OP_RETURN opcode
    - or optionally in multisignature addresses
  - This metadata can also be encrypted
    - to address any privacy concerns.
  - Some implementations support storage of metadata on torrent network
    - virtually unlimited amounts of metadata can be stored.
    - Moreover, smart contracts are also supported

Extended protocols on top of Bitcoin

- Colored coins
  - can be used to represent
    - Commodities
    - Certificates
    - Shares
    - Bonds
    - Voting
    - and so on
  - a wallet that interprets colored coins is necessary
    - normal Bitcoin wallets will not work.
      - they cannot differentiate between colored coins and not colored coins

Extended protocols on top of Bitcoin

- Colored coins
  - The idea of colored coins is very appealing
    - it does not require any modification to the Bitcoin protocol
    - can make use of the already existing secure Bitcoin network. In
  - A significant use case
    - issuance of financial instruments on the blockchain with
      - low transaction fees
      - valid and mathematically secure proof of ownership
      - Fast transferability without requiring some intermediary
      - instant dividend payouts to the investors
    - possibility of creating smart contracts

Extended protocols on top of Bitcoin

- Counterparty
  - another service that can be used
    - to create custom tokens that act as a cryptocurrency
    - for various purposes such as issuing digital assets on top of bitcoin blockchain.
  - The architecture has a counterparty server
    - works based on the same idea as colored coins by
      - embedding data into regular bitcoin transactions
    - provides a much more productive library and tools
      - to support the handling of digital assets.
    - embedding the data is by using OP_RETURN
    - also called embedded consensus
      - because the counterparty transactions are embedded within bitcoin transactions
    - Uses a currency
      - known as XCP
      - as the fee for running the contract
  - Technically is an Ethereum contract
    - can store and verify bitcoin block headers

Development of altcoins

- Altcoin projects can be started very quickly
  - by simply forking the bitcoin or another coin's source code
- but several things need to be considered
  - Usually, the code base is written in C++
    - as was the case with bitcoin
    - but almost any language can be used
      - for example, Golang or Rust.
  - the challenging issue is how to start a new currency
    - so that investors and users can be attracted to it

Development of altcoins

- from a technical point of view
  - various parameters are required to be tweaked or introduced
    - Consensus algorithms
      - PoW or PoS
    - Difficulty adjustment algorithms
      - KGW, DGW, Nite's Gravity Wave, and DigiShield
        - can be tweaked to produce different results
    - Inter-block time
      - too fast might destabilize the blockchain
      - too slow may not attract many users

Development of altcoins

- from a technical point of view
  - various parameters are required to be tweaked or introduced
    - Block rewards
    - Inflation control
    - Block size and transaction size
    - Interest rate
      - applies only to PoS systems
      - Impacts the inflation

Development of altcoins

- from a technical point of view
  - various parameters are required to be tweaked or introduced
    - Coinage
      - defines how long the coin must remain unspent
        - to become eligible to be considered stake worthy
    - Total supply of coins
      - Fixed or unlimitted

Namecoin

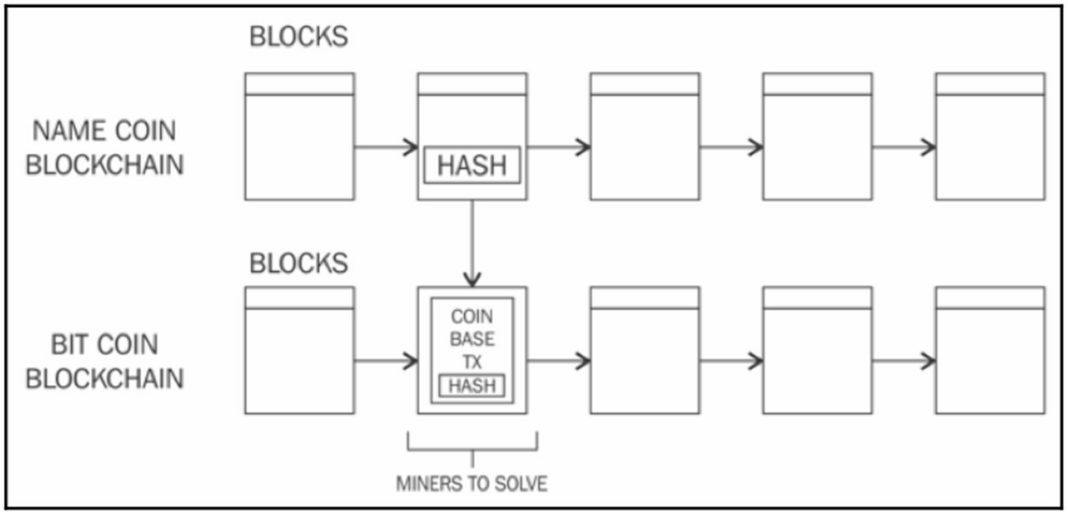
- the first fork of the Bitcoin source code
- The key idea
  - It is not to produce an altcoin
  - It is to provide improved naming
    - decentralization
    - censorship resistance
    - privacy
    - Security
    - faster
  - responds to inherent limitations in DNS protocols
    - such as slowness and centralized control

Namecoin

- is used to provide a service to register a key/value pair
- One major use case
  - it can provide a decentralized TLS certificate validation mechanism
    - driven by blockchain-based decentralized consensus
- provides the following three services
  - Secure storage and transfer of names (keys)
  - Attachment of some value to the names
    - up to 520 bytes of data
  - Production of a digital currency (Namecoin)

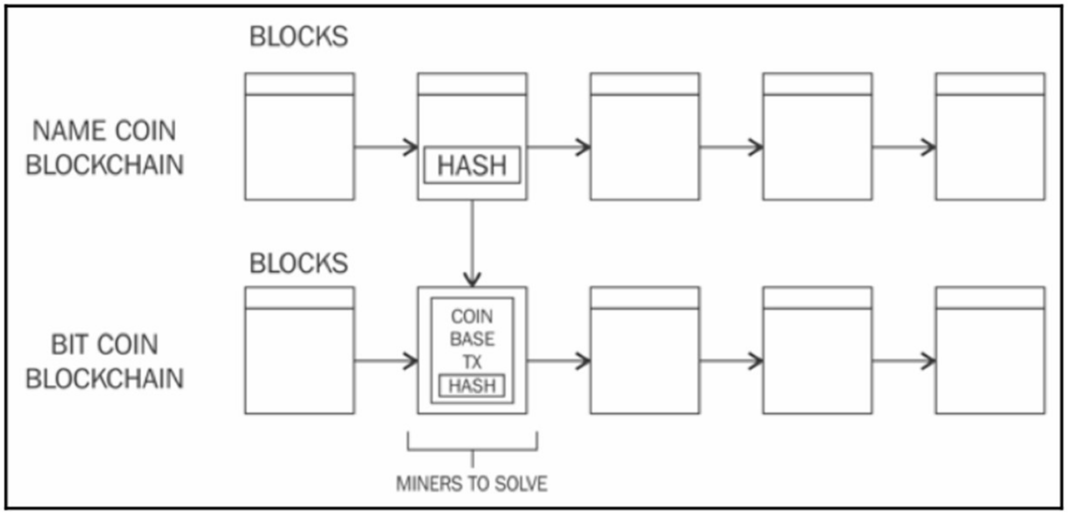
Namecoin

- introduced merged mining for the first time
  - miners create a Namecoin block
    - produce a hash of that block
  - Then the hash is added to a Bitcoin block
    - coinbase transaction scriptSig is used to include the hash
  - miners solve the block
    - at equal to or greater than the Namecoin block difficulty



Namecoin

- introduced merged mining for the first time
  - If a miner solve a hash at the bitcoin blockchain difficulty level
    - the bitcoin block is built
      - becomes part of the Bitcoin network
    - the Namecoin hash is ignored by the bitcoin blockchain
  - if a miner solves a block at Namecoin blockchain difficulty level
    - a new block is created in the Namecoin blockchain.
  - The core benefit of is
    - all the computational power spent by the miners contributes towards securing both Namecoin and Bitcoin.



Litecoin

- a fork of the bitcoin source
- uses Scrypt as PoW
  - originally introduced in the Tenebrix coin
- allows for faster transactions than bitcoin
  - Has faster block generation time of 2.5 minutes.
- Difficulty readjustment is achieved every 3.5 days
  - roughly due to faster block generation time.
- total coin supply is 84 million

Litecoin

- Scrypt is a sequentially memory hard function
  - key idea
    - if the function requires a significant amount of memory to run
      - then custom hardware such as ASICs will require more VLSI area
      - would be infeasible to build

Litecoin

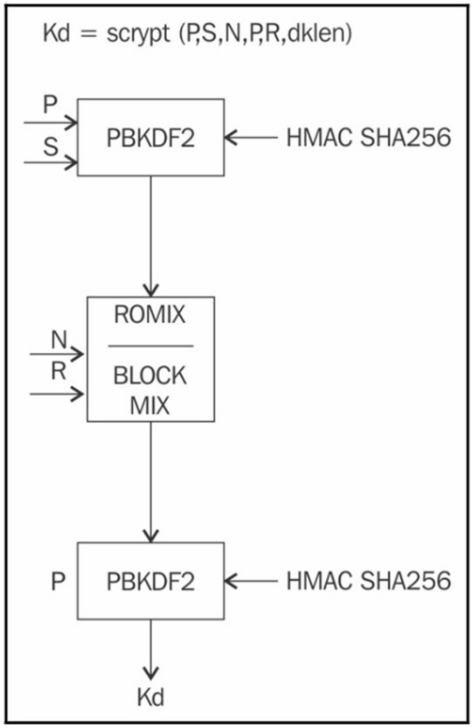
- Scrypt is a sequentially memory hard function
  - is based on a phenomenon called Time-Memory Trade-Off (TMTO)
    - If memory requirements are relaxed, then it results in increased computational cost
    - makes it unfeasible for an attacker to gain more memory
      - it is expensive
      - It is difficult to implement on custom hardware

Litecoin

- Scrypt is a sequentially memory hard function
  - uses the following parameters to generate a derived key (Kd) $Kd = scrypt\ (P, S, N, P, R, dkLen)$
    - Passphrase: a string of characters to hash
    - Salt: a random string that is provided to Scrypt functions
      - to provide a defense against brute-force dictionary attacks using rainbow tables
    - N: a memory/CPU cost parameter
      - must be a power of 2 > 1
    - P: the parallelization parameter
    - R: the block size parameter
    - dkLen: the intended length of the derived key in bytes

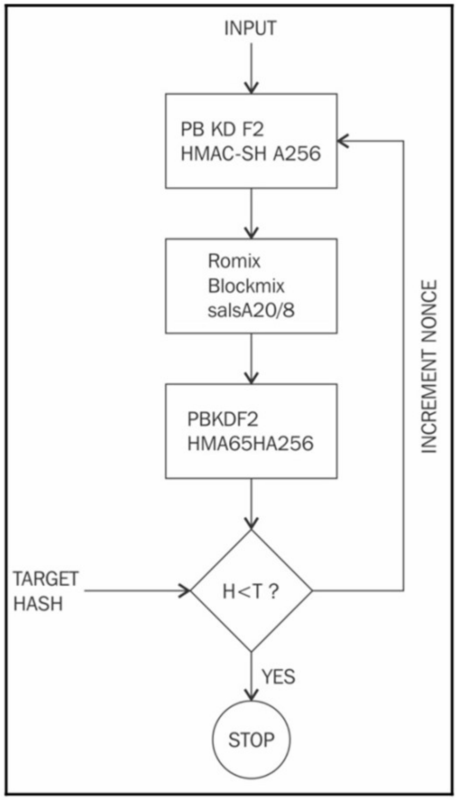
Litecoin

- Scrypt is a sequentially memory hard function
  - the algorithm takes P and S as input
  - Applies PBKDF2 and SHA-256-based HMAC.
  - Then the output is fed to an algorithm called ROMix
    - internally uses the Blockmix algorithm to fill up the memory
      - using the Salsa20/8 core stream cipher
    - requires large memory to operate
    - enforce the sequentially memory hard property
  - The output is finally fed to the PBKDF2 function again
    - to produce a derived key



Litecoin

- Litecoin mining uses specific parameters
  - N= 1024, R = 1, P=1, and S = random 80 bytes producing a 256-bit output
  - due to these parameters
    - Litecoin ASIC development turned out to be not very difficult

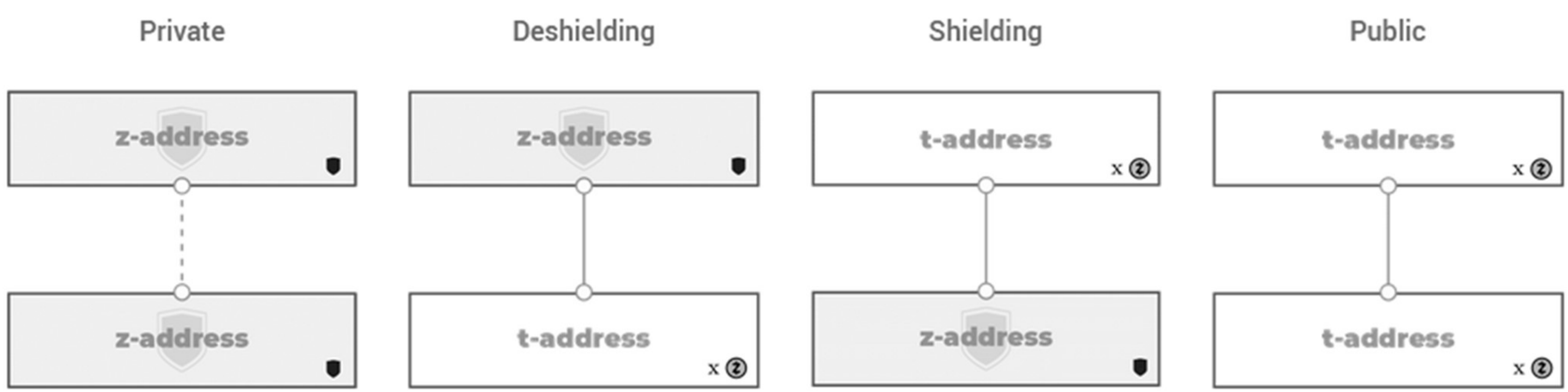


Primecoin

- uses searching prime numbers as a PoW
  - Not all types of prime number are allowed
  - Only Three types of prime numbers meet the requirements
    - Cunningham chain of the first kind ($p_{i+1} = 2p_i + 1$)
    - Cunningham chain of the second kind ($p_{i+1} = 2p_i - 1$)
    - bi-twin chains $n-1, n+1, 2n-1, 2n+1, \ldots, 2^k n - 1, 2^k n + 1$
- difficulty is dynamically adjusted
  - For every block
  - By changing the chain length
- verification is quick enough
- total number of coins is community-driven
  - no definite limit on the number of coins

Zcash

- a privacy-protecting, digital currency
- people can transact efficiently and safely with low fees.
- Shielded Zcash ensures transactions remain confidential
  - while allowing people to selectively share transaction information
- addresses are either
  - private (z-addresses)
    - start with a “z”
  - transparent (t-addresses).
    - start with a "t."
- four transaction types:



Zcash

- A Z-to-Z transaction
  - appears on the public blockchain
  - Has A memo field
    - allows the sender to include relevant information to the receiver
    - useful for passing along messages and instructions
  - it is known to have occured and fees were paid.
  - But the addresses, transaction amount and the memo field are all encrypted
    - possible using zero-knowledge proofs
  - The owner of an address can disclose z-address and transaction details using
    - view keys
      - Address owner can disclose all incoming transactions and the memo field
      - Address owner does not have access to the sender address
        - unless identifying information is included in the memo field
    - payment disclosure
      - Either the sender or receiver may disclose transaction-specific details
      - The receiver may disclose a transaction value and memo
        - but does not have access to the sender's address

Zcash

- A T-to-T transaction works just like Bitcoin
  - The sender, receiver and transaction value are publicly visible.
- shielded transactions in Zcash
  - can be fully encrypted on the blockchain
  - yet still be verified as valid by consensus rules
    - using zk-SNARK proofs

Zcash

- zk-SNARK
  - allow one party (the prover) to prove to another (the verifier) that a statement is true
    - without revealing any other information
  - E.g.
    - given the hash of a random number
    - can convince the verifier that
      - the number exists
      - he in fact know such a number