



INFINITY ECONOMICS PLATFORM (IEP) WHITEPAPER

Created by the IEP Community

FINAL DRAFT - **UNDER PEER REVIEW**

v.0.2 - October 3rd, 2017

www.infinity-economics.org

Table of Contents

1. Abstract	3
1.1 What is a blockchain?.....	3
1.2 Summary.....	3
1.3 TD;LR.....	3
1.4 Keywords.....	3
2. Introduction	4
2.1 Mission and Goals.....	4
2.2 Current Challenges in the Market.....	4
2.3 Addressed Issues.....	4
3. Technology	4
3.1 Technical Background.....	5
3.2 Proof of Stake (POS).....	5
3.3 Token.....	5
3.4 Nodes.....	6
3.5 Blocks.....	6
3.6 Block Creation.....	7
3.7 Accounts.....	8
3.8 Transactions.....	9
3.9 Cryptographic.....	10
3.10 Architecture.....	11
3.11 Toolchains.....	12
3.12 Integration.....	12
4. Features	12
4.1 Payments.....	12
4.2 Aliases.....	12
4.3 Messages.....	13
4.4 Assets.....	13
4.5 Currencies.....	13
4.6 Crowdfunding.....	14
4.7 Escrow.....	14
4.8 Subscriptions.....	14
4.9 Shuffling.....	14
4.10 Voting.....	15
4.11 Automated Transactions.....	15
4.12 Gateways.....	15
4.13 Proxies.....	16
4.14 Extensions.....	16
4.15 Account Control.....	16
4.16 Light Client.....	17
5. e-Governance	17
5.1 DAO Overview.....	17
5.2 Smart Contracts Solutions.....	17
5.3 IEP Solution.....	18
6. Conclusion	18
7. Sources, Additional Papers, References	19
7.1 Additional Resources.....	19
7.2 Credits and Acknowledgement.....	19
7.3 Additions.....	19
7.4 References.....	20

1. Abstract

January 3rd 2009 marked the beginning of a new era of globalization and world interconnection when the first Bitcoin transaction was conducted. Satoshi Nakamoto^[1] made possible what was once thought to be impossible – a currency and payment system not controlled by any person or organization. We know this currency as Bitcoin and the underlying technology that powers it as Blockchain. It has been 8 years since people started using Bitcoin, but only now are we beginning to understand the real potential of the blockchain technology on which Bitcoin is founded. Blockchain does to economic processes what the Internet has done to information: today, anyone can have access to the global economy on equal terms with others. In this document we talk about IEP, a multipurpose blockchain platform made for users.

1.1 What is a blockchain?

A blockchain is a distributed database which enables the creation of a digital ledger of transactions and the sharing of the ledger among a distributed network of computers. It uses advanced cryptography to allow each participant on the network to interact with the ledger in a secure way without the need for a central authority. It maintains a continuously growing list of records (blocks), each containing a timestamp and a link to the previous block.

1.2 Summary

Crypto-currencies, tokens, digital coins and other digital assets based upon blockchain technology are a mega trend that directly connect the finances of billions of people around the globe via a financial superhighway. The financial superhighway brings together billions of individuals across borders to directly trade products and services with one another anywhere over the Internet. Using blockchain technologies, the value of such financial products and services – and the transactions themselves – are stored in a system that cannot be diluted by politics, over-supply or altered in any way by third parties. The use of blockchain will significantly impact the future of financial interactions, rendering the traditional model of a centralized financial system – where individuals respond to posted numbers on a centralized computer – inadequate for the extremely large number of complex transactions that will be executed daily on the financial superhighway. IEP is a user- and service-centric multipurpose blockchain platform and a cryptocurrency based on proven crypto open source projects. IEP acts as an crypto-tech integrator, combining and enhancing existing and new crypto-tech features and services into a single powerful platform for the digital economy.

1.3 TF;LR

IEP is the next-gen financial ecosystem. Its main goal is to integrate cryptocurrencies into the traditional financial world and to create a single gateway to the market for normal users, traders, investors and financial institutions by building a new full service and limitless decentralized financial ecosystem and digital economy. In the initial phase, IEP primarily targets community-based and humanitarian development and projects. To that end, decentralized voting and messaging are implemented to allow for a DAO-like experience (Hybrid Governance) in managing community projects, whilst remaining straightforward from a technical aspect.

1.4 Keywords

cryptocurrency, blockchain, XIN, IEP, smart contracts, decentralized services,

asset exchange, currencies, escrow, blocks, nodes, extensions, proxies.

2. Introduction

Since its inception, blockchain technology has been fraught with controversy over its most natural application – value transfer using a network token. Decentralized money is a ground-breaking development, but blockchain technology cannot be reduced to this alone. Being essentially a distributed database, the blockchain allows for various types of distributed ledger entries, the nature of which depends on their interpretation by the blockchain's users. IEP is an innovative, secure, decentralized and low transaction cost payment system built by using cutting-edge cryptocurrency technologies, designed to create entire digital economies akin to traditional financial services.

2.1 Mission and Goals

IEP's Mission is to make the daunting cryptocurrency market accessible to everybody, accelerating adoption of blockchain technology and democratizing ownership of cryptocurrencies. IEP makes cryptocurrencies easier to purchase and transfer allowing the average individual to participate in the New Economy. The IEP foundation believes in the philosophical mission established by Satoshi Nakamoto. By creating a secure layer that is accessible to the average person, they put the power in the hands of the people – where it belongs.

2.2 Current Challenges in the Market

The future success of cryptocurrencies relies on their widespread use. While crypto certainly has the potential to rise as a global payment method, it remains the victim of speculation. Currently, most users are treating cryptocurrencies as speculative assets rather than using them in daily life. Given the sector's exponential growth and the way Blockchain technology is becoming increasingly mainstream, many are optimistic that digital currencies will be used more as a currency and less as a speculative asset. Though several new blockchain technologies and cryptocurrencies have emerged over the past few years, none have yet achieved the breakthrough success required for mainstream adoption –primarily due to negative publicity, bubble speculations, scams, and complicated user-interfaces. Hacking and other cyberattacks on crypto exchanges, and directly on users devices and wallets, have also contributed to the overall uncertainty which accompanies this new technology.

2.3 Addressed Issues

Cryptocurrency is a decentralized blockchainbased financial system with immutability and autonomy being its most celebrated features. Cryptocurrencies enable one to bypass intermediaries and remain independent from traditional financial institutions. However, no cryptocurrency, including Bitcoin, has managed to become a commonly used monetary asset. Merchants and service providers are reluctant to accept cryptocurrency payments as it involves additional risks of exchange losses and regulatory issues as well as high volatility. An instrument capable of becoming a perfect global payments system is commonly used as a speculative asset. This project is devised as a solution for the fundamental problem in question, and takes into account the problems and challenges faced by the current global financial system.

3. Technology

IEP is a 100% proof-of-stake cryptocurrency^[11], constructed from proven open source projects^[3] written in Java. IEP's unique proof-of-stake algorithm does not depend on any implementation of the "coin age" concept used by other proof-

of-stake cryptocurrencies, and is resistant to so-called "nothing at stake" attacks. A total quantity of 9 billion available tokens were distributed in the genesis block. Curve25519^[8] cryptography is used to provide a balance of security and required processing power, along with more commonly-used SHA256 hashing algorithms^[13].

3.1 Technical Background

Blocks are generated every 60 seconds, on average, by accounts that are unlocked

on network nodes. Since the full token supply already exists, IEP is redistributed through the inclusion of transaction fees which are awarded to an account when it successfully creates a block. This process is known as forging, and is akin to the "mining" concept employed by other cryptocurrencies. Transactions are deemed safe after 10 block confirmations, and IEP's current architecture and block size cap allows for the processing of up to 367,200 transactions per day, with unlimited scalability potential. IEP transactions are based on a series of core transaction types that do not require any script processing or transaction input/output processing on the part of network nodes.

3.2 Proof of Stake (POS)

IEP uses a system where each "token" in an account can be thought of as a tiny mining rig^[11]. The more tokens that are held in the account, the greater the chance that account will earn the right to generate a block. The total "reward" received as a result of block generation is the sum of the transaction fees located within the block. IEP does not generate any new tokens as a result of block creation. Redistribution of IEP takes place as a result of block generators receiving transaction fees, so the term "forging" (meaning in this context "to create a relationship or new conditions") is used instead of "mining". Subsequent blocks are generated based on verifiable, unique, and almost-unpredictable information from the preceding block. Blocks are linked by virtue of these connections, creating a chain of blocks (and transactions) that can be traced all the way back to the genesis block. Block generation time is targeted at 60 seconds, but variations in probabilities have resulted in an average block generation time of 80 seconds, with occasionally longer block intervals. The security of the blockchain is always of concern in Proof of Stake systems. The following basic principles apply to IEP Proof of Stake algorithm:

- A cumulative difficulty value is stored as a parameter in each block, and each subsequent block derives its new "difficulty" from the previous block's value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty.
- To prevent account holders from moving their stake from one account to another as a means of manipulating their probability of block generation, tokens must be stationary within an account for 1,440 blocks before they can contribute to the block generation process. Tokens that meet this criterion contribute to an account's effective balance, and this balance is used to determine forging probability.
- To keep an attacker from generating a new chain all the way from the genesis block, the network only allows chain re-organization 720 blocks behind the current block height. Any block submitted at a height lower than this threshold is rejected. This moving threshold may be viewed as IEP only fixed checkpoint.
- Due to the extremely low probability of any account taking control of the

blockchain by generating its own chain of blocks, transactions are deemed safe once they are encoded into a block that is 10 blocks behind the current block height.

3.3 Token

The total supply is 9 billion tokens, divisible to eight decimal places. All tokens were issued with the creation of the genesis block (the first block in the IEP blockchain), leaving the genesis account^[C] with an initial negative balance of 9 billion token. The existence of anti-tokens in the genesis account has a couple of interesting side effects:

- the genesis account cannot issue transactions of any kind, since its balance is negative and it cannot pay transaction fees.
- any tokens sent to the genesis account are effectively destroyed, since that account's negative balance will cancel them out .

The choice of the word tokens is intentional due to IEP's intention to be used as a base protocol that provides numerous other functions. IEP's most basic function is one of a traditional payment system, but it was designed to do far more.

3.4 Nodes

A node on the IEP network is any device that is contributing transaction or block data to the network. Any device running the IEP software is seen as a node. Nodes can be subdivided into two types: hallmarked and normal. A hallmarked node is simply a node that is tagged with an encrypted token derived from an account's private key; this token can be decoded to reveal a specific token account address and balance that are associated with a node. The act of placing a hallmark on a node adds a level of accountability and trust, so hallmarked nodes are more trusted than non-hallmarked nodes on the network. The larger the balance of an account tied to a hallmarked node, the more trust is given to that node. While an attacker might wish to hallmark a node in order to gain trustworthiness within the network and then use that trust for malicious purposes; the barrier to entry (cost of token required to build adequate trust) discourages such abuse. Each node on the IEP network has the ability to process and broadcast both transactions and block information. Blocks are validated as they are received from other nodes^[1], and in cases where block validation fails, nodes may be "blacklisted" temporarily to prevent the propagation of invalid block data. Each node features built-in DDOS (Distributed Denial of Services) defence mechanisms which restrict the number of network requests from any peer to 30 per second.

3.5 Blocks

As in other cryptocurrencies, the ledger of token transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred. A copy of the blockchain is kept on

every node in the IEP network, and every account that is unlocked on a node (by supplying that account's private key) has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed 1440 times. Any account that meets these criteria is referred to as an active account. In IEP, each block contains up to 255 transactions, all prefaced by a 192-byte header that contains identifying parameters. Each transaction in a

block is represented by a maximum of 160 bytes, and the maximum block size is 32KB. All blocks contain the following parameters:

- A block version, block height value, and block identifier
- A block timestamp, expressed in seconds since the genesis block
- The ID of the account that generated the block, as well as that account's public key
- The ID and hash of the previous block. The number of transactions stored in the block
- The total amount of token represented by transactions and fees in the block
- Transaction data for all transactions included in the block, including their transaction IDs
- The payload length of the block, and the hash value of the block payload

3.6 Block Creation

Three values are key to determining which account is eligible to generate a block, which account earns the right to generate a block, and which block is taken to be the authoritative one in times of conflict: base target value, target value and cumulative difficulty.

Base Target Value

In order to win the right to forge (generate) a block, all active IEP accounts 'compete' by attempting to generate a hash value that is lower than a given base target value. This base target value varies from block to block, and is derived from the previous block's base target value.

Target Value

Each account calculates its own target value, based on its current effective stake. This value is: $T = T_b \times S \times B_e$

where:

T	is the new target value
T _b	is the base target value
S	is the time since the last block, in seconds
B _e	is the effective balance of the account

As can be seen from the formula, the target value grows with each second that passes since the timestamp of the previous block. The maximum target value is $0.17080318 \times 10e17$ and the minimum target value is one half of the previous block's base target value. This target value and the base target value are the same for all accounts attempting to forge on top of a specific block. The only account-specific parameter is the effective balance parameter.

Cumulative Difficulty

The cumulative difficulty value is derived from the base target value, using the formula: $D_{cb} = D_{pb} + 264 / T_b$

where:

D _{cb}	is the difficulty of the current block
D _{pb}	is the difficulty of the previous block
T _b	is the base target value for the current block ^[j]

The Forging Algorithm

Each block on the chain has a generation signature parameter. To participate in the block forging process, an active account cryptographically signs the generation signature of the previous block with its own public key. This creates a 64-byte signature, which is then hashed using SHA256. The first 8 bytes of the resulting hash gives a number, referred to as the account's hit.

The hit is compared to the current target value. If the computed hit is lower than the target, then the next block can be generated. As noted in the target value formula, the target value increases with each passing second. Even if there are only a few active accounts on the network, one of them will eventually generate a block because the target value will become very large. The corollary of this

is that you can estimate the time that will be required for any account to forge a block by comparing that account's hit value to the target value. When an active account wins the right to generate a block, it bundles up to 255 available, unconfirmed transactions into a new block, and populates the block with all of its required parameters. This block is then broadcast to the network as a candidate for the blockchain. The payload value, generating account, and all of the signatures on each block can be verified by all network nodes who receive it. In a situation where multiple blocks are generated, nodes will select the block with the highest cumulative difficulty value as the authoritative block. As block data is shared between peers, forks (non-authoritative chain fragments) are detected and dismantled by examining the chains' cumulative difficulty values stored in each fork.

3.7 Accounts

IEP implements a brain wallet as part of its design: all accounts are stored on the network with private keys for each possible account address directly derived from each account's passphrase using a combination of SHA256 and Curve25519 operations. Each account is represented by a 64-bit number, and this number is expressed as an account address using a Reed-Solomon^[k] error-correcting notation that allows for detection of up to four errors in an account address, or correction of up to two errors. This format was implemented in response to concerns that a mistyped account address could result in tokens, aliases, or assets being irreversibly transferred to erroneous destination accounts. Account addresses are always prefaced by "XIN-", making token account addresses easily recognizable and distinguishable from address formats used by other cryptocurrencies. The Reed-Solomon-encoded account address associated with a secret passphrase is generated as follows:

1. The secret passphrase is hashed with SHA256 to derive the account's private key.
2. The private key is encrypted with Curve25519 to derive the account's public key.
3. The public key is hashed with SHA256 to derive the account ID.
4. The first 64 bits of the account ID are the visible account number.
5. Reed-Solomon encoding of the visible account number, prefixed with "XIN-", generates the account address.

When an account is accessed by a secret passphrase for the very first time, it is not secured by a public key. When the first outgoing transaction from an account is made, the 256-bit public key derived from the passphrase is stored on the blockchain, and this secures the account. The address space for public keys (2256) is larger than the address space for account numbers (264), so there is no one-to-one mapping of passphrases to account numbers and collisions are possible. These collisions are detected and prevented in the following way: once a specific passphrase is used to access an account, and that account is secured by a 256-bit public key, no other public-private key pair is permitted

to access that account number.

Account Balance Properties

For each IEP account, several different types of balances are available. Each type serves a different purpose, and many of these values are checked as part of transaction validation and processing.

- The effective balance of an account is used as the basis for an account's forging calculations^[1]. An account's effective balance consists of all tokens that have been stationary in that account for 1440 blocks. In addition, the Account Leasing feature allows an account's effective balance to be assigned to another account for a temporary period.
- The guaranteed balance of an account consists of all tokens that have been stationary in an account for 1440 blocks. Unlike the effective balance, this balance cannot be assigned to any other account.
- The basic balance of an account represents all transactions that have had at least one confirmation.
- The forged balance of an account shows the total quantity of token that have been earned as a result of successfully forging blocks.
- The unconfirmed balance of an account is the one that is displayed in IEP clients. It represents the current balance of an account, minus the tokens involved in unconfirmed, sent transactions.
- Guaranteed asset balances lists the guaranteed balances of all the assets associated with a specific account.
- Unconfirmed asset balances lists the unconfirmed balances of all the assets associated with a specific account.

3.8 Transactions

Transactions are the only means IEP accounts have of altering their state or balance. Each transaction performs only one function, the record of which is permanently stored on the network once that transaction has been included in a block.

Transaction Fees

Transaction fees are the primary mechanism through which token are recirculated back into the network. Every transaction requires a minimum fee of 1 token while several services like aliases, assets or voting require higher fees. When a IEP account forges a block, all of the transaction fees included in that block are awarded to the forging account as a reward. Until the size of all the transactions in a block exceeds the current 32 kilobyte block size limit, the minimum fee will be sufficient for all transactions to be included in blocks. In situations where the number of unconfirmed transactions exceeds the number that can be placed in a block, forging accounts will likely select transactions with the highest fees. This suggests that transaction processing may be prioritized by including a fee that is higher than the minimum.

Transaction Confirmations

All IEP transactions are considered unconfirmed until they are included in a valid network block. Newly created blocks are distributed to the network by the node (and associated account) that creates them, and a transaction that is included in a block is considered as having received one confirmation. As

subsequent blocks are added to the existing blockchain, each additional block adds one more confirmation to the number of confirmations for a transaction. If a transaction is not included in a block before its deadline, it expires and is removed from the transaction pool.

Transaction Deadlines

Every transaction contains a deadline parameter, set to a number of minutes from the time the transaction is submitted to the network. The default deadline is 1440 minutes (24 hours). A transaction that has been broadcast to the network but has not been included in a block is referred to as an unconfirmed transaction. If a transaction has not been included in a block before the transaction deadline expires, the transaction is removed from the network. Transactions may be left unconfirmed because they are invalid or malformed, or because blocks are being filled with transactions that have offered to pay higher transaction fees. In the future, features such as multi-signature transactions may be able to take advantage of deadlines as a means of enforcing an expiry date.

Transaction Types

Categorizing IEP transactions into types and subtypes allows for modular growth and development of the IEP protocol without creating dependencies on other "base" functions. As features are added to the IEP core, new transaction types and subtypes can be added to support them. During integration additional transaction types like subscriptions, escrow and automated transactions are added, named as advanced transactions.

Transaction Creation and Processing

The details of creating and processing a IEP transaction are as follows:

1. The sender specifies parameters for the transaction. Types of transactions vary, and the desired type is specified at transaction creation, but several parameters must be specified for all transactions:
 - the private key for the sending account
 - a specified fee for the transaction
 - a deadline for the transaction
 - an optional referenced transaction
2. All values for the transaction inputs are checked. For example, mandatory parameters must be specified; fees cannot be less than or equal to zero; a transaction deadline cannot be less than one minute into the future; if a referenced transaction is specified, then the current transaction cannot be processed until the referenced transaction has been processed.
3. If no exceptions are thrown as a result of parameter checking:
 - (a) The public key for the generating account is computed using the supplied secret passphrase
 - (b) Account information for the generating account is retrieved, and transaction parameters are further validated:
 - The sending account's balance cannot be zero
 - The sending account's unconfirmed balance must not be lower than the transaction amount plus the transaction fee
4. If the sending account has sufficient funds for the transaction:
 - (a) A new transaction is created, with a type and subtype value set to match the kind of transaction being made. All specified parameters are included. A unique transaction ID is generated with the creation of the object
 - (b) The transaction is signed using the sending account's private key

- (c) The encrypted transaction data is placed within a message instructing network peers to process the transaction
- (d) The transaction is broadcast to all peers on the network
- (e) The server responds with a result code:
 - the transaction ID, if the transaction creation was successful
 - an error code and error message if any of the parameter checks fail.

3.9 Cryptographic

Introduction

Elliptic curve cryptography (ECC)^[8] is a public-key cryptography method that uses elliptic curves algebraic structures over finite fields. ECC provides security using smaller keys than other cryptographic methods. ECC can be used for key agreement, digital signatures, pseudo-random generators, etc. ECC can be used for indirect encryption by using a symmetric encryption scheme with the key agreement.

Key exchange in IEP is based on the Curve25519 algorithm, which generates a shared secret key using a fast, efficient, high-security elliptic-curve Diffie-Hellman function^[7]. The algorithm was first demonstrated by Daniel J. Bernstein in 2006^[8]. IEP's Message signing in IEP is implemented using the Elliptic-Curve Korean Certificate based Digital Signature Algorithm (EC-KCDSA), specified as part of IEEE P1363a by the KCDSA Task Force team in 1998^[9]. Both algorithms were chosen for their balance of speed and security for a key size of only 32 bytes.

Encryption Algorithm

When Alice sends an encrypted plain text to Bob, she:

1. Calculates a shared secret:
 - $\text{shared_secret} = \text{Curve25519}(\text{Alice_private_key}, \text{Bob_public_key})$
2. Calculates N seeds:
 - $\text{seed}_n = \text{SHA256}(\text{seed}_{n-1})$, where $\text{seed}_0 = \text{SHA256}(\text{shared_secret})$
3. Calculates N keys:
 - $\text{key}_n = \text{SHA256}(\text{Inv}(\text{seed}_n))$, where $\text{Inv}(X)$ is the inversion of all bits of X
4. Encrypts the plaintext:
 - $\text{ciphertext}[n] = \text{plaintext}[n] \text{ XOR } \text{key}_n$

Upon receipt Bob decrypts the ciphertext:

1. Calculates a shared secret:
 - $\text{shared_secret} = \text{Curve25519}(\text{Bob_private_key}, \text{Alice_public_key})$
2. Calculates N seeds (this is identical to Alice's step):
 - $\text{seed}_n = \text{SHA256}(\text{seed}_{n-1})$, where $\text{seed}_0 = \text{SHA256}(\text{shared_secret})$
3. Calculates N keys (this is identical to Alice's step):
 - $\text{key}_n = \text{SHA256}(\text{Inv}(\text{seed}_n))$, where $\text{Inv}(X)$ is the inversion of all bits of X
4. Decrypts the ciphertext:
 - $\text{plaintext}[n] = \text{ciphertext}[n] \text{ XOR } \text{key}_n$

Note: If someone guesses part of the plaintext, he can decode some part of subsequent messages between Alice and Bob if they use the same key pairs. As a result, it's advised to generate a new pair of private/public keys for each communication.

3.10 Architecture

First-generation cryptocurrencies were primarily designed as payment systems. IEP recognizes that decentralized blockchains can enable a broad range of applications and services, but is not prescriptive about what those services should be or how they should be built. By design, IEP strips away unnecessary complexity in its core, leaving only the most successful components of its predecessors intact. As a result, IEP functions like a low-level, foundational protocol: it defines the interfaces and operations required to operate a lightweight blockchain, a decentralized communication system, and a rapid transaction processing framework, allowing higher-order components to build on those features. Transactions in IEP make simple adjustments to account balances instead of tracing sets of "input" or "output" credits. In addition, the core software does not support any form of scripting language. By providing a set of basic, flexible transaction types that can quickly and easily be processed, IEP creates a foundation that does not limit the ways in which those transaction types can be used, and does not create significant overhead for using them. This flexibility is further amplified by IEP's low resource and energy requirements, and its highly readable, highly organized object-oriented source code.

3.11 Toolchains

IEP is focused on industry standards for all platform developments. The core is written in enterprise friendly Java^[D], the backends are powered by NodeJS^[E] and all frontends are build with AngularJS^[F], making it easy to allocate developer resources anytime, anywhere. Cross platform apps are build with electron^[G]. The default backend storage is MongoDB^[H]. This toolchain gives the foundation much more freedom to choose the best developers/contractors for all upcoming programming tasks, since the developer communities for those tools is matured and large with plenty of proven components and frameworks, ready to use.

3.12 Integration

The cryptospace is evolving very rapidly. New technologies and powerful protocols and components are developed daily. To address this devstream IEP monitors the whole crypto development attentively for additional features worth adding to the IEP platform either for the core or for the services. New transaction types can be added on the fly to expand the core with powerful features as needed. This way IEP acts as a crypto-feature-integrator to always provide state of the art building blocks for the digital economy. All new features are introduced to the community for voting and acceptance prior to implementation.

4. Features

IEP is designed to integrate building blocks for the digital economy and therefore relies heavily on secure and robust off-chain infrastructure to reach the average user. To achieve this objective, the IEP core and client is built for easy extensibility^[14] and connection to others, very useful protocols and networks. IEP isn't meant to act, as most cryptos, as an island but to embrace and welcome all new technologies, from very classical to the most advanced. Most

services are based on IEP's enhanced core implementations like proxies and gateways. Services can be public or private, running as UI-less bots or even as extensions within the wallet UI. Services play a very important role in IEP's future development and growth strategy, therefore the foundation will facilitate the enhancing of those services and initiate or even develop

community relevant services like the enhanced encrypted messaging/chat or news services with external contractors. The list of realized/planned services is growing constantly. Please refer to wallet extensions to get an overview about already implemented and planned services.

4.1 Payments

Tokens (XIN) are most relevant to the user. A transfer transaction type is used to transfer tokens from one account to another. A small encrypted message can be attached to each transaction for an additional fee. The fee for a simple transfer is 1 token. Token transfers are simple and fast and cost effective and mostly settled within just 60 seconds. Anonymous transfers are possible using the built-in coin shuffling function.

4.2 Aliases

The IEP Alias System feature essentially allows one piece of text to be substituted for another, so that keywords or keyphrases can be used to represent other things - names, telephone numbers, physical addresses, web sites, account numbers, email addresses, product SKU codes and more. Immediate applications are simple: you can create an easy-to-remember alias for your IEP account, for example. But since the Alias System is open-ended, it can be used to implement a decentralized DNS system, shopping cart applications, proxies into other blockchains, oracles, references to stored files in bittorrent or IPFS^[6] or even as your entry point into decentralized webhosting like ZeroNet^[2]. Aliases can be edited, transferred or sold to public or specific accounts with the built-in alias marketplace.

4.3 Messages

Encrypted Messages commonly take the form of SMS-length communications between users. Transmission of encrypted data messages up to 160 bytes in length from any account to any other account as a single message. Encrypted messages can also be attached to many transactions like token transfer, asset transfer, currency transfer. Encrypted messages are permanently stored into the blockchain and limited in size to prevent blockchain bloat. Encrypted messages requires a dynamic fee, based on it's size and should be used for important and immutable messages. The encryption algo is AES. The upcoming, community based messenger service allows up to 1.000 bytes and last 1.000 messages without a service fee. Messages can also be used to trigger transaction events for instance to chain payments or to invoke distributed services.

4.4 Assets

The Asset Exchange is IEP's built-in decentralised trading engine. Using the Asset Exchange you can create, buy and sell assets that represent data beyond simple coin transfers which opens up wide-ranging possibilities. The Asset Exchange is based on the 'coloured coins' concept whereby a coin or a set of coins can be designated ('coloured') to represent something-else. By contrast, many crypto currencies only ever operate as just that - currencies, and nothing more. However, since the blockchain provides a trustworthy and permanent ledger of all transactions, it can be used to record far more diverse information than purely currency transactions. IEP tokens can be designated ('coloured') to represent other crypto coins, stocks/bonds, property, commodities, or even ideas. As a result, the IEP network can be used to trade almost anything. The Asset Exchange is suitable for most use cases where users like to buy and sell virtual company shares, fiat-pegged assets, rewarding points or even crypto backed assets but not for HFT trading since the Asset Exchange is decentralized and running with a 60s. blocktime confirmation. The Asset

Exchange is completely decentralised and completely unregulated. The substantial benefits this offers are freedom, cost savings, lack of intervention and so on but also comes at a price. There is no hand-holding or policing, and scam assets can be and often are created. Whilst the community generally picks up on these relatively quickly, if you make a mistake then there is very little recourse as transactions are irreversible. Before buying an asset, you should at least understand what an asset represents and clarify any doubts with the issuer.

4.5 Currencies

The currency entity is the basic building block of the IEP Currencies System. A currency has a unique name and code and uniqueness is guaranteed by the protocol, currencies can be deleted and their code can be reused under certain conditions. The total currency supply is divisible into currency units. Like assets, currency units supports decimal positions implemented as a client side feature. The maximum number of currency units which can be issued per currency is similar to token $10^9 * 10^8$. The actual maximum units supply is set by the currency issuer. The currency issuer is the account which issues the currency and pays the issuance fee. The issuer is responsible for setting the currency properties and in some configurations has additional control over the currency usage. Like asset balance, currency units can be transferred between accounts.

4.6 Crowdfunding

Crowdfunding is the practice of funding a project or venture by raising monetary contributions from a large number of people. Crowdfunding is a form of crowdsourcing and of alternative finance. Crowdfunding is generally based on three types of actors: the project initiator who proposes the idea and/or project to be funded, individuals or groups who support the idea, and a moderating organization (the "platform") that brings the parties together to launch the idea. During 2013 \$5.1 billion USD was raised by millions of individuals! However the biggest disincentive to using websites such as Kickstarter is their fees. Kickstarter demands 5% of the money raised as a fee, and payment processing fees are another 5%, which in the era of blockchain technology is a little difficult to justify. Based on the built-in currency feature IEP offers this 'platform' as a fully automatic decentralized solution for simple, fast and affordable crowdfunding. Crowdfunding can be used to fund a wide range of for-profit entrepreneurial ventures such as artistic and creative projects, medical expenses, travel, or community-oriented social entrepreneurship and charity and humanitarian projects.

4.7 Escrow

An escrow service allows safer payment by securely holding a buyer's coins in escrow until the terms of the sale are met and as a result the buyer releases payment to the seller. In most cases no dispute is filed and no 3rd party action is needed. IEP provides a decentralized escrow service based on the new enhanced transaction types. If you're selling your car or house using IEP decentralized asset service you can easily put the funds up in Escrow and when the title is delivered in your name you release the money. Even the title can be delivered using a IEP Smart Contract and get this, it costs less than a few pennies to make all of this happen and unlike traditional banking and selling transactions it doesn't cost hundreds or thousands of dollars. Escrow can have as much as up to 10 co-signers and provides several decision actions like return, split, release.

4.8 Subscriptions

Managing and Scaling Subscriptions were complex. Until now. IEP offers decentralized recurring payments that users can initiate and cancel at any time. Recurring payments work well for services that require multiple payments over time or just to fund special accounts to ensure a minimum balance height. Subscriptions are built on the new enhanced transaction framework and allows users to make payments of any size and interval to other accounts. Subscriptions are an important new feature for the upcoming digital marketplace.

4.9 Shuffling

CoinShuffle^[5] improves user privacy by frustrating attempts to link transactions to a particular user. A participant can increase their anonymity set by making it impossible to determine exactly who paid who because inputs and outputs are indistinguishable (even to other participants). Each participant knows which output they own, but cannot link the inputs and outputs of the other participant. CoinShuffle also allows the identification and elimination of malicious participants caught misbehaving. Coin Shuffling is an effective privacy feature and it enables participants to mix their funds quickly and efficiently with other participants funds by creating a random mapping between existing participants accounts and new recipient accounts provided by the users. The shuffling algorithm is based on a paper by Tim Ruffing^[5] and was originally developed to be implemented in Bitcoin itself. CoinShuffle differs from other existing solutions like ZeroCash^[12] in terms of speed and complexity.

4.10 Voting

Blockchain technology lends itself well to use in voting systems. By providing a secure way for each person to register their vote on a public record whilst still maintaining the option for users to remain anonymous, and with little possibility for anybody to tamper with those votes, the blockchain is able to offer significant improvements over current systems in terms of security and transparency. The secure, encrypted, consensus-based nature of the IEP network allows the implementation of a voting system that guarantees anonymity and security, without relying on a central authority to tally votes. The IEP Voting System enables any account to create a poll with one question and up to 10 answers. Accounts are eligible to vote in the poll based on a minimum required balance of token, an asset or a currency. Voting consists of selecting an integer range value to associate with one or more answers as specified during poll creation. An answer is given weight based on one of four voting models and then its weight is multiplied by the associated range value to compute a corresponding result. The four voting models specify weight as: one per voting account, or equal to the balance per voting account of token, an asset or a currency. An aggregate weight for each answer is computed as the sum of all individual vote weights; likewise an aggregate result is computed. Individual votes are saved until at least 1441 blocks after the poll completes, typically more than a day. After this time, votes are deleted and only aggregate weights and results remain available.

4.11 Automated Transactions

One of the most promising applications of the block chain technology are smart contracts. Smart contracts are computer programs that can automatically execute the terms of a contract. Anyone familiar with computer programming would be aware of what is known as an if-then-else statement, where a program executes a certain task if certain conditions are met and does not if the conditions are not present. Smart contracts implement this on the block chain and have the potential to extend this into another growing field, and that is the internet

of things, bringing the world of sci-fi closer to reality. For instance Atomic Cross Chain Transactions allow for truly decentralized trading between cryptocurrencies. This can, for example, enable a trader to exchange token with a coin that provides a mixing service for the purposes of privacy, and then send it to a new wallet. Another smart contract example that IEP would be able to support are auctions. IEP enables you to create a smart auction contract. Participants in the auction would then send money to the contract, and anytime anyone sends more money than the previous bidder, the previous bidder's money is automatically refunded. Future smart contracts that IEP intends to support include autonomous corporations, gambling, self-mixing and smart properties. Smart contracts are being touted as the 'killer app' of the cryptocurrency industry, and the race is on to develop applications that will radically transform our work, life and play going forward into the future.

4.12 Gateways

An application-gateway is a device (node) that acts as a "gate" between two networks. Today service developers are facing many problems when building custom services, distributed to a huge number of clients. Firstly, they need to master several different technologies and go through framework specific APIs. Secondly, applications developed for one framework will not work in another framework and thirdly, the data collected and the actions provided by devices needs to be mapped to the service model. IEP's application gateways provides a convenient solution for service developers to access several services and protocols. Gateways are an important future development part for the IE platform to 'connect' services like IPFS^[6] (Interplanetary Filesystem), used for decentralized storage, ZERONET^[2], used for decentralized hosting and Tendermint^[4], used for side- and private chains solutions^[10]. Since gateways are running within core-scope services can directly interact with IEP's blockchain and transaction models. When a client program establishes a connection to a destination service, it connects to the IEP application gateway. The client then negotiates with the node in order to communicate with the destination service. In effect, the client establishes the connection with the destination and acts on behalf of the client. Due to it's transparent API access, if configured, gateways are reachable from within IEP's smart wallet. This expands the wallet feature set greatly. Gateways can be used for public or private services.

4.13 Proxies

A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. IEP provides several in-core proxies which can be extended easily and accessed with simple HTTP GET requests. Proxies are playing an important role in IEP's interconnectivity strategy, enabling the IE platform to 'reach out' for additional services and features running within the core-scope. Running within core-space enables proxy data to interact with IEP's blockchain, transactions and notification system, making it easy to build public or private services. Due to it's transparent API access, proxies are reachable from IEP's smart wallet too. Current proxies are used to fetch realtime data from exchanges and blockexplorers for the cryptocurrency market but they are not limited to those and more proxies, connecting to common data services are in development.

4.14 Extensions

Extensions enables third-party software developers to add functionality to the IEP Smart Client Interface. Extensions/Services are an important part for the IEP platform to gain traction in common markets, accessible directly by the smart wallet. In most cases those extensions are based on services built by developers to 'connect' those to the IE platform for instance due to paymentlogic or dataservices. Since plugins have unrestricted access including sensitive data and functionality, it is very important to install only trusted extensions. If there is any doubt, install an extension only on the Testnet or on Mainnet with accounts having small balances. Extensions are authored by third party developers and getting an intense peer review prior to release. The foundation will prepare a 'best practice' and signed/approved extension marketplace including a comprehensive code review and ranking.

4.15 Account Control

Account security is possibly the leading issue with the use of crypto-currency: how can a user secure digital funds so that they are completely safe from theft, given the increasing sophistication of malware and hacking techniques. Account control enhances the security of accounts and ensures that only specific people have access to funds, under specific conditions. Multisignature (multisig) for instance refers to requiring more than one key to authorize a transaction. This enables users to create accounts that can only transact with the approval of holders of specified Assets or Currencies, or to make transactions subject to Votes on spendings. Multisignature (often called multisig) is a form of technology used to add additional security for token transactions. Multisignature requires additional users to sign (approve) a transaction before it can be added onto the block chain. Phasing is another feature that allows certain phasing-safe transactions to be created with conditional deferred execution based on the result of a vote, on a list of linked transactions or on the revelation of a secret; or simply with unconditional deferred execution.

4.16 Light Client

The classic Bitcoin approach is essentially a way to synchronize a distributed system through common transaction logs. It requires that each network node store the full copy of the transaction history. Obviously this does not scale well, since eventually not every node will be able to store the full history. There are different ways to mitigate this - a simplified payment verification procedure that allows storage of only that data essential for a given node; off-chain transactions; bidirectional payment tunnels; reducing blockchain bloat; working directly with the system state. With the simplest approach, where all nodes are equal at Genesis block, centralization may emerge as low-capacity nodes have to rely on full, high-capacity nodes that can afford to store the full blockchain. Of course, emerging centralization brings trust issues, since lightweight nodes have to trust the full nodes and can become a victim of a rogue full node. However, there are ways to mitigate this, such as polling several nodes, maintaining trusted nodes lists, and so on. IEP provides a new structure for these tasks by leveraging the peerexplorer. The foundation maintains a base of trusted high capacity servers to ensure sufficient nodes available for clients. A node rating algo is used to rank the top nodes, count in the CPU load, processors available and more node metrics in realtime to 'load-balance' the client requests for optimal performance.

5. e-Governance

From its beginning IEP is designed to run as a 100% community driven project, meaning that the power to decide about all platform related matters belongs to

all community members based on their voting power. This approach can be seen as a DAO by its core definition since everything is decentralized from platform to service development, from running nodes to marketing and documentation. IEP follows these principles right from the beginning by handing over the power to decide to its users, the only way a solid and fair crypto platform should be established to prevent single points of failure. An IEP foundation was created to execute the communities will, no matter what whales, vip's or developers decide. To provide a tamperfree environment the platform built-in e-governance features are used and used consequent to improve the IEP platform. For instance all IEP features were voted on for release by the community prior to release.

5.1 DAO Overview

Decentralized autonomous organizations^[1] have been seen by some as difficult to describe. Nevertheless, the conceptual essence of a decentralized autonomous organization has been typified as the ability of blockchain technology to provide a secure digital ledger that tracks financial interactions across the internet, hardened against forgery by trusted time-stamping and by dissemination of a distributed database. This approach eliminates the need to involve a bilateral accepted and trusted third party in a financial transaction, thus simplifying the sequence. The original theory underlying the DAO was that by removing delegated power from directors and placing it directly in the hands of owners, the DAO removed the ability of directors and fund managers to misdirect and waste investor funds. The first known DAO was/is bitcoin but it lacks some important functions to fulfill the 'optimal' DAO. Simply defined, a mechanism called e-Governance is missing to function as an expression of the token holder's will.

5.2 Smart Contracts Solutions

The first code based only DAO was launched as a Smart Contract, running on the ethereum blockchain as an investor-directed capital fund having no conventional management structure or board of directors. The DAO was crowdfunded via a token sale in May 2016. It set the record for the largest crowdfunding campaign in history, but in June 2016, hackers exploited a vulnerability in the DAO code to enable them to siphon off one third of The DAO's funds to a subsidiary account. Due to this hack, a hard fork occurred where the original un-forked blockchain was maintained as Ethereum Classic, thus breaking Ethereum into two separate active cryptocurrencies. Regardless of the hack, even this code based DAO needed actors in the physical world, named 'curators', to monitor and manage the DAO decisions on behalf of the DAO token holders which leads to the conclusion that, no matter how advanced code based DAO's are, ultimately any DAO needs human interaction to specify, organize and monitor deliverables, responsibilities, and other operating parameters for external contractors.

5.3 IEP Solution

Learning from the above problems and definitions, IEP DAO can be viewed as a hybrid DAO. By using a much more flexible and advanced e-Governance platform, and the final human input, provided by the Foundation, counts too. Compared to code based only DAOs IEP has the following advantages.

1. Flexibility in e-Governance

IEP DAO offers a rich set of already built-in governance tools, accessible and easy to use out of the box for the average user. These tools are transparent, simple to set-up and also easy to monitor, without the need for complicated code constructs which are hard to test and to predict.

2. Common Sense Enabled

While a maximum of automation has its benefits, it lacks flexibility, and you can't code common sense. The Foundation is deeply convinced that common sense is an important component to prevent mis-use and act dynamically on unforeseeable problems. As mentioned above, a final human view with a healthy portion of common sense enriches the DAO and makes it much more robust. Common sense is the final bastion if something goes wrong with the DAO.

3. Fine granulation for proposal votings

Code based proposal voting is limited to transactions/counting (yes/no) only. The IEP built-in voting system has many advantages since it supports multiple choices and multiple voting models. This results in much more precise proposal votings compared to simple yes/no solutions. In many real world decisions a simple yes/no isn't sufficient.

4. Complete Transparency

Proposals and voting on those proposals are not encapsulated in difficult to read contracts/code. This allows non-developers to verify and monitor the whole proposal and voting outcome simply by looking at the chain. Blockexplorer and the tools already built into the wallet are sufficient for full transparency.

5. Automated Transaction as additional DAO solution

While the Foundation prefers the above described DAO structure, the platform supports code based DAO's too. The Automated Transactions (AT) feature (Alpha Status) can be used to create Smart Contracts running on the IEP blockchain. It's free to any user/developer to build its own private or public DAO at minimal costs. Please see AT features for more information on building a DAO running on the IEP blockchain.

6. Conclusion

In this paper, we put forth the concept of a platform for a digital economy. Cryptocurrencies are changing the world right now, solving the problems of trust and security, uniting financial institutions, big investors, everyday users, and representatives of small, medium and large businesses into a single global system. The IEP decentralized crypto ledger platform is an ambitious project bringing together several changes on integration, client side features and middleware system arrangements to form the basis to software solutions suitable for financial applications of today and into the future. Based on this new model, intermediaries will develop their own financial services and build a distributed super financial market via IEP. We believe that a flexible, decentralized, value exchange system is the future of the new global financial infrastructure, and will help to promote financial inclusion and standardize future financial transactions. IEP's design philosophy is in many ways the opposite from that taken by many other cryptocurrencies today, relying on cooperation and feature integration over island solutions.

7. Sources, Additional Papers, References and Tools

IEP would like to express sincere gratitude to everyone who has contributed to this paper with its encouragement and consistent involvement.

7.1 Additional Resources

- 7.1.1 IEP Doc section, <http://www.infinity-economics.org/docs/>
- 7.1.2 IEP API section, <http://www.infinity-economics.org/api>
- 7.1.3 IEP Download section, <http://www.infinity-economics.org/download/>
- 7.1.4 IEP Chain Tools, <http://infinity-economics.org/preview/>

7.2 Credits and Acknowledgement

7.2.1 Whitepapers: Nxt, Burst, Heat, Fimk, NEM, Ethereum, Tendermint, IPFS

7.3 Additions

[A] This is defined as the account's current balance, minus amounts related to all unconfirmed, sent transactions. In general, this is the account balance that is displayed in real-time in a client interface.

[B] Nxt, Burst, FIMK, NEM, IPFS, ZeroNet, Tendermint

[C] The genesis account address is XIN-NTLK-Z5GA-WNAV-GW378

[D] Java SE Runtime Environment
<http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html>

[E] Node.js is a JavaScript runtime built on Chrome's V8 JavaScript engine
<https://nodejs.org/en/>

[F] AngularJS, One framework. Mobile & desktop
<https://angularjs.org/>

[G] Electron, Build cross platform desktop apps with JavaScript, HTML, and CSS
<https://electron.atom.io/>

[H] MongoDB, Building on the Best of Relational with the Innovations of NoSQL
<https://www.mongodb.com/>

[I] All possible block parameters are verified, including the effective balance of the block generator's account. This proves that the generating account actually contains the effective balance (stake) that won it the right to generate the block.

[j] See 3.6 for an explanation of these parameters and how they are used.

[k] For more information:
http://en.wikipedia.org/wiki/ReedSolomon_error_correction

[l] See 3.6 for more information on how this balance is used.

7.4 References

[1] Satoshi Nakamoto. Bitcoin: a Peer-to-Peer Electronic Cash System. (n.d.). Retrieved July 06, 2014, from <https://bitcoin.org/bitcoin.pdf>

[2] ZeroNet, Open, free and uncensorable websites using Bitcoin cryptography and BitTorrent network, <https://zeronet.io/>

[3] Nxt Whitepaper, <http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt>

[4] Tendermint: Consensus without Mining, 2014
<https://tendermint.com/static/docs/tendermint.pdf>

[5] P2P Mixing and Unlinkable Bitcoin Transactions*
<http://crypsys.mmci.uni-saarland.de/projects/FastDC/draft-paper.pdf>

- [6] IPFS is the Distributed Web,
<https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf>
- [7] Wikipedia, Diffie–Hellman key exchange,
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
- [8] Yung, M., Dodis, Y., Kiayias, A., Malkin, T., & Bernstein, D. J. (2006). Curve25519: New Diffie–Hellman Speed Records. *Public Key Cryptography*, 2006, 207–228. doi: 10.1007/11745853_14
- [9] The Korean Certificate-based Digital Signature Algorithm
<http://grouper.ieee.org/groups/1363/P1363a/contributions/kcdsa1363.pdf>
- [10] Sidechains. Deposit/withdrawal sidechain,
<https://www.blockstream.com/sidechains.pdf>
- [11] What Proof of Stake Is and Why It Matters
<http://bitcoinmagazine.com/6528/>, 2013.
- [12] Matthew Green et al. Zerocash: Decentralized anonymous payments from bitcoin. <http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf>, 2014.
- [13] National Institute of Standards. FIPS 180-2, Secure hash standard, August 2000. <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.
- [14] JavaScript, Object Notation. See <http://json.org/>