Xepto - A Peer-to-Peer Smart Transactions System

WHITE PAPER (v.22.07.18)

This white paper is intended to be an introduction and technical reference to Xepto (www.xepto.net), a peer-to-peer smart transactions system. This paper will be maintained and updated periodically to reflect fundamental concept (s), benchmarks, technical adjustments, improvements and up or down gradations in the project.

Abstract

Inception of peer-to peer payment systems using cryptographic currencies like Bitcoin, Ethereum and Litcoin carries within its fold a promise of individual sovereignty, anonymity, freedom and convenience. However, certain inherent discrepancies within the concept, structure, and management of these currencies leave significant room for desire. Absence of any pricing mechanism for cryptographic currencies and ambiguities associated with the valuation (or lack thereof) of these currencies, vis-a-vis other monetary units in different states, have rendered the users of cryto-currencies vulnerable to huge financial losses. A high degree of dubiousness associated with the creation of these currencies (often referred to as mining) and resultant wastage of energy, computing resources and human effort make the very concept, and associated mechanisms, highly questionable, dubious and controversial. With the result that central banks and major financial institutions across the globe are being slow and many a times hostile towards the use of these systems. The foregoing weaknesses within the structure of existing cryptocurrencies notwithstanding, it is theoretically and empirically possible to structure a cryptocurrency based peer-to-peer payment system that is easily comprehendible by common users, is resource efficient and is compliant with the native laws and regulations in different nation states. Xepto.net is a beta stage blockchain project designed as a peer-to-peer transactions system with global reach. In its fully developed form Xepto.net would be the currency of choice offering universal acceptance, freedom and requisite anonymity while being compliant with prudential, financial and legal requirements in vogue globally and across the nation states.

Introduction to Cryptography

The notion of smart contracts and digital currencies has been around for many decades now. Blinding, as a technique has been employed in cryptography to allow an agent to provide services (for example computing a function) for a client in an encoded form without knowing either the real input or the real output. Blinding technique has been, at times, applied to prevent side-channel attacks on encryption devices. The concept of blind signature, introduced by David Chaum, is a form of digital signature that requires the contents of a message being blinded before endorsement of digital signature. Blind signature can then be publicly verified in privacy related documents where the signer and the document author are unrelated and even untrusting parties. Electronic Cash (more commonly known as Ecash) was introduced by David Chaum as “anonymous cryptographic electronic money or electronic cash system”

in 1982 and was adopted by at least one commercial bank in the US. The development of Bitcoin and Ethereum Virtual Machine (EVM), however, marked the beginning of a new era in the development and use of cryptocurrency based smart contracts authored in cryptography and secured in blockchain.

Bitcoin

Bitcoin, as a properly recognized decentralized currency was, for the first time unveiled by Satoshi Nakamoto in his white paper that surfaced in 2009. The design structure of Bitcoin combined the established concept of managing ownership using public key encryption and a consensus mechanism for tracking of ownership commonly known as "proof of work". The algorithm behind proof of work mechanism was truly a remarkable achievement of its time as it solved two major problems. On one hand it provided an effective means to achieve consensus amongst nodes in a network to an agreed current state and updates applied to the Bitcoin ledger. On the other hand, it provided a system for allowing fresh entrants into the consensus process by introducing the concept of permissionless blockchain that is secure in Sybil attack environment. In the Bitcoin consensus process the weight accorded to a node is proportional to the computing power at its disposal.

Technically, Bitcoin and similar other ledgers can be viewed as “State Transition Systems” that record the state of a monetary or property ledger before and after a transaction along with the transaction that has resulted into alteration of the ledger state. In routine life it can be compared as a bank ledger showing the state of an account before and after a transaction along with the transaction that has caused the change. Refer to Diagram 1 for a graphic representation of the ledger before and after a transaction.

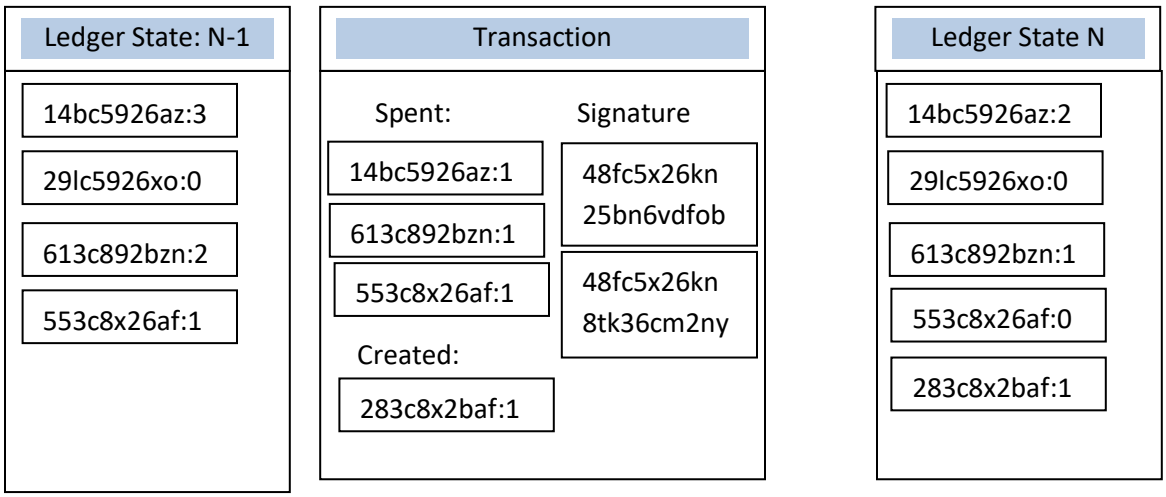

Diagram 1: The ledger state before and after the transaction that caused the transition from Ledger State N-1 to Ledger State N

Mining

Mining is a unique and interesting component of Bitcoin system. Also referred to as "Proof of Work", mining is a process by which new Bitcoins are added to its existing inventory. The process involves huge computational resources to guess work a complex algorithm and is somewhat similar to solving a puzzle. While mining may have worked well as an entry point into the Bitcoin system, it has certain inherent drawbacks. O'Dwyer & Malone (2014) estimated that Bitcoin mining used energy equivalent to total electricity consumption of Ireland in 2014. Besides, huge computing resources, infrastructure, and human intellect are spent in Bitcoin mining which makes the process non-sustainable and untenable in the long run. Also there is no intrinsic value in the Bitcoin itself and there exists no tangible mechanism to maintain value of Bitcoin in the short term or long run thus making system users highly vulnerable to price volatility and resultant losses.

Besides, some of the major issues with scripting of Bitcoin algorithm like lack of turning-completeness, value-blindness, lack of a state (opportunity for multi-stage contracts or scripts) and blockchain-blindness (as UTXO are blind to blockchain data) make it difficult to use blockchain for day to day applications.

Ethereum

Ethereum to a great extent understands and attempts to resolve the issues of energy consumption and mining difficulties of Bitcoin by provisioning an alternative framework for development of applications. Ethereum as an application platform carries powerful light client properties that facilitate sharing of common economic environment across spectrum of applications that may or may not be inter-related. In doing so the "intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of tradeoffs" that Ethereum believes will be "helpful for a large class of decentralized applications". Some of the underlying advantages for the users of Ethereum platform are: (1) Rapid development time (2) Security for small and rarely used applications (3) The ability of different applications to efficiently interact (Ethereum Whitepaper, 2018).

The Ethereum ecosystem is characterized by a state that is made up of "accounts". Each account is identified by a 20 byte address. Transactions defining the state transitions stem from direct transfer of value (and information) between accounts. Each Ethereum account contains four fields namely Nonce, Ether Balance, Contract Code and Storage (null by default). Ether is the crypt-fuel of Ethereum which is used to pay for all type of transactions. One of the major underlying philosophies of Ethereum is "non-discrimination and non-censorship" whereby the Ethereum protocol does not attempt to restrict or prevent specific categories of usage. Instead regulatory mechanisms in the protocol are aimed at regulating the harm rather than trying to prevent undesirable applications. "A programmer can even run an infinite loop script on top of Ethereum for as long as they are willing to keep paying the per-computational-step transaction fees" (Ethereum Whitepaper, 2018).

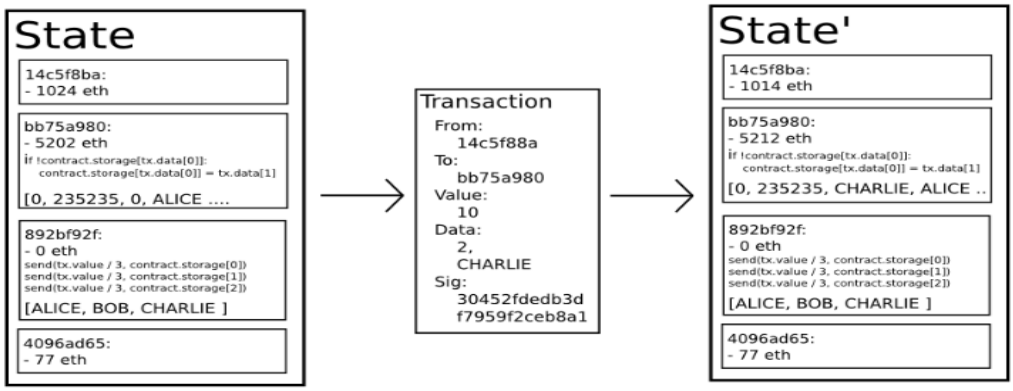

Diagram 2: Illustration of Ethereum State Transition Function
Credits: Ethereum Whitepaper (2018)

There is no denying the fact that Ethereum offers major advantages over other cryptocurrency based systems in terms of broader range and scope of permissible transactions and flexibility. However, the major users of Ethereum blockchain continue to be people with higher level of computing skills and resources. This in turn also means that a large proportion of global population is unable to take advantage of the freedom, anonymity and flexibility offered by the blockchain revolution.

Xepto - Introduction

Xepto,, is a beta stage blockchain project built around the idea of being a truly peer-to-peer smart transaction system. Xepto is structured as a permissioned blockchain built on top of open source hyperledger fabric with an open to all frontend. In its fully developed form Xepto would be the cryptocurrency of choice offering universal acceptance, freedom and requisite anonymity while being compliant with prudential, financial and legal requirements in vogue globally and across the nation states.

Xepto leverages the open source hyperledger fabric to build a system of defining an arbitrary asset or token called Xepto. The token is independent of other cryptographic and FIAT currencies in vogue except for the purpose of current valuations and comparisons. Each token has a unique serial number and a cryptographic identification string that are bound together and stored in an immutable ledger called the central repository. For the purpose of ensuring underlying data integrity and cryptographic security the central repository is replicated at participating nodes using Byzantine Fault Tolerance (BFT) as consensus mechanism to ensure that state of central repository ledger is identical at all nodes at all times.

Transactions in Xepto ledger are used to alter the ownership of Xepto token(s) in the token repositories and resultantly update the wallet balances. Each transaction records the cryptographic digest of the transaction ledger prior to the transaction, the identity of the peer or node making the transaction, the cryptographic identity of the wallet making the transaction and that of the beneficiary wallet besides other useful data, and time to keep a track of transactions overtime. The transactions may be carried out by individual wallets, exchange peers or nodes in accordance with the needs for anonymity,

legitimacy, and compliance within and outside Xepto network. A very special feature of Xepto network is persistent emphasis on meeting the prudential, monitoring and reporting regulations and regimes in and within nation states.

Xepto – Structure and Hierarchy

Xepto Wallet is like a bank account number that can be owned by the participating individuals, public or private entities, and organizations. A wallet address is a unique cryptographic combination that can be shared by the wallet owner(s) with trusted peers on required basis without much security concerns. In technical terms a wallet address is like a user's public key and adequately masks the identity of the peer to provide requisite degree of anonymity, freedom and convenience.

Xepto Exchange Peers (Validators) are individuals, entities, or organizations that have opted to provide additional identification details for the purpose of KYC with a view to ensuring safe and secure communication between the Xepto Network, its users and regulators, if required.

A node is the highest level in the hierarchy of the system. Nodes also act as validators for larger transactions for the purpose of ensuring that transfers made through such transactions are valid, legit and conform to the financial, prudential and legal requirements in the states to which the sending and receiving wallets belong to. Depending upon prudential regulations in a country or state, a node may be a registered or unregistered enterprise capable of communicating with the local authorities for the purpose of ensuring that Xepto network is in conformity with the local financial laws and prudential regulations.

Distinctive Features

Certain fundamental features that make Xepto different from other cryptocurrencies, tokens and coins are:

a. A well established concept and definition of a digital asset that is traceable, track-able and has a unique non-reproducible and non-immutable cartographical identity.

b. A unique proof of ownership mechanism used for validating transactions to ensure that each Xepto token carries, retains and maintains its intrinsic value and is not subjected to price volatility often witnessed across the cryptocurrencies horizon.

c. A stubborn emphasis on respecting the legal, financial, judicial and regulatory regimes within and between the nation states at the same time ensuring requisite anonymity, individual freedom and choices.

Stacking for Profit

Although the core team members and founding peers have been heavily stacked right from the beginning, "Stacking for Profit" is comparatively a new feature of Xepto platform. All participating peers are allowed to stack their Xepto units at a price to be determined at the time of stacking, in the currency

of choice and fixed rate of profit. Profit is applied pro-rated on monthly basis (usually the first working day of the month).

Stacking has multiple benefits for the participating peers. On one hand it provides a means of fixed profit (steady income) at rates that are far higher than normal savings accounts at conventional financial institutions. On the other hand it protects the participating peers from unexpected shocks from drop in the price of Xepto token. Un-stacking and re-stacking at improved prices is yet another advantage of Xepto Stacking.

Profit rates currently applied to different stack tiers are as under:

# of Units Stacked	Profit Percentage	Stacking Fee	Un-stacking Fee
Less than 200	9.5 percent	Zero	US$ 0.10 per unit in the stack being un-stacked
200 to 499	10.5 percent		
500 to 999	11.5 percent		
1000 and above	12.5 percent		

Minimum stacking duration is 180 days. Early redemption fee of 5 cents per unit per month (calculated pro-rate per day) applies to pre-mature un-stacking.

Xepto Mining

Important changes have been made to the previous mining policy that will affect existing and future miners. Please read carefully to ensure that your mining status is not impacted because of these changes.

Xepto mining was introduced as a pathway for entry of new peers and miners into the Xepto network and has been gaining tremendous popularity. Xepto mining is designed to be a profitable business model for enterprising peers at the same time ensuring that the number of Xepto units is kept limited so as to retain and gain value overtime.

Levels of Xepto Mining

Public Mining Rig (PMR) is the entry level machine and is available for mining to all peers with a wallet, and at least 1 Xepto unit in the wallet. The PMR has serious limitations in terms of availability, efficiency, efficacy, latency, and redundancy of resources made available for mining.

Special Incentive for Public Miners

A special incentive program has been devised to acknowledge and honor dedication and commitment of public miners towards promoting security and acceptance of Xepto networks. Mining algorithm for public miners has been adjusted to provide greater incentive for public

miners by way of increased mining speed for every 5 additional Xepto units held in their wallet. Meaning thereby, that for every five Xepto units (above the bare minimum of 1) public miners will have their mining resources increased equivalent to 1 additional public rig. This implies that their mining speed will double at 6 units and become 3 times at 11 units and so on.

Shared Mining Rig (SMR) is the next level mining machine available to premium users. The SMR provides requisite speed, efficiency and efficacy for business level mining of Xepto constituent sub-units. The current annual fee for SMR is equivalent to **35 Xepto** units. Additionally the miner must have a minimum balance of at least **65 Xepto** units in the wallet. The Shared Mining Rig management is fully automated, requires minimal skills and is designed to cover the costs within the year in addition to generating requisite profit for the entrepreneur having rights over the machine. Xepto Networks guarantees to buy 60 percent production of shared mining at the going price at the time of offer to sell

Dedicated Mining Rig (DMR) is the top of the line business level mining machine made available to highly trusted peers only. The current annual charge for DMR is equivalent to **350 Xepto** units in addition to a balance of at least **650 Xepto** units in the user's wallet. The Dedicated Mining Rig management is fully automated, requires minimal skills and is designed to cover the costs within the year in addition to generating requisite profit for the entrepreneur having rights over the machine. Xepto Networks guarantees to buy 60 percent production of Dedicated Mining Rigs at the going price at the time of offer to sell.

Important Notice:

Existing Xepto premium miners have been allowed upto 31st of March 2022 to make up balances in their wallets associated with their mining ledgers. No extension will be granted beyond that date.

Estimated Mining Yield

Xepto mining results are measured in terms of "Raw Yield". Xepto Mining Machine mines 1 millionth fraction of Xepto unit in a single turning. A Public Mining Rig (PMR) completes approximately one turning per 30 seconds, thereby producing a Raw Yield of 0.000002 Xepto in a minute. A Shared Mining Rig (SMR) completes 60 turnings per 30 seconds thereby giving a Raw Yield of 0.00012 Xepto in a minute. A Dedicated Mining Rig (DMR) completes 700 turnings in 30 seconds thus producing a Raw Yield of 0.0014 Xepto in a minute. While Public Mining suffers from lack of speed, consistency and latency issues, a miner with SMR can expect to mine upto 65 Xepto Units in a year. A miner with DMR can expect to mine 725 Xepto units in a year. Besides, performance bonuses are applied to the wallets of premium miners. Xepto mining model ensures that system fees are covered within the first 6 months of mining leaving 6 months of production as profit for the miner. This is working on the assumption that the price of Xepto unit stays at the same level throughout the year. In real world a miner can expect to make better profits than these estimates as the price of Xepto improves over time.

Liquidating (Selling) Raw Balance

This is the newest feature being added to Xepto Network. With a view to providing greater liquidity and flexibility to Xepto miners, all miners are eligible to sell their raw balances for cash in the currency of their choice. Proceeds from such liquidation will be made available to respective miners immediately in real time. With a view to avoiding extremely tiny transactions, the minimum raw balance (MRB) that can be liquidated has a modest limit of 0.010000. A Raw Liquidation Commission (RLC) of 10 percent will be charged by the system for all such expedited liquidations. It is important to note that liquidated raw balance will be directly deducted from your mining ledger and will not show in the Total Mined figures after having been liquidated. The cash ledgers will, however, show all required details and price (s) applied to transactions.

How to Become a Miner

Any individual with a minimum of 1 Xepto unit can opt for FREE mining using a Public Mining Rig (PMR) by signing up using a simple form available via Miscellanea -> Commence Mining link. To be a premium miner, a user would need to make up the required number of Xepto units in his or her wallet, enough to be paid as the annual fee and the minimum required in the wallet after payment of fees. You can apply by opening a ticket from Miscellanea->Open a Ticket link from user dashboard.

Xepto Referral Program

Xepto has recently implemented a referral system whereby registration of new members will be allowed only with referral from at least one existing member. The referral program has two fold objectives:

a) To enhance the security of the Xepto Network.
b) To introduce a reward system for the peers who help induct new peers/miners into the system.

Any peer can generate a referral link from his / her profile (account settings) page and send it to their referred peers who can then register following the link. The referral code will automatically be entered into the required space if a proper link is followed to the registration page.

For each new member who starts mining at the basic level (public rig), the referring peer will get a bonus of 0.100000 points added to his/her raw mining balance. For every five members referred, the referring peers will have their mining resources increased equivalent to 1 additional public rig. This implies that their mining speed will double at 5 referrals and become 3 times at 10 referrals and so on.

Convertibility and Encashment

Xepto token (s) can be instantly converted to gold, silver, and other fiat currencies and withdrawn as cash or commodities. A user is usually allowed one withdrawal per 7 days. Dedicated miners can make upto two withdrawals in a week. A withdrawal request can be made through a system generated ticket specifying the amounts to be withdrawn from specified cash / commodity ledgers. Payments / deliveries are made through the global network of participating peers. A user can expect to receive payment / delivery within 48 hours of having made the request. This timeframe is likely to significantly

improve during the next few months as the peer network becomes bigger and banking channel transactions are incorporated into the system.

Compensation - Validating Peers

Validators (Validating Peers) can be thought of as Xepto Network's backbone. Validators play a significant role in terms of answering queries, assisting new peers and miners, resolving issues, and validating transactions to ensure consistency, accuracy and persistency of transactional data within the Xepto system. They also provide the necessary liquidity needed to ensure efficient and smooth completion and finality of transactions and asset exchanges. The role of Validators is likely to evolve over time as the system matures and becomes popular.

With a view to compensating existing and future Validators it has been decided to allow Validators to charge Cash Reimbursement Commission (CRC) at the rate of US Dollar 5.00 plus 0.5 percent of the amount being reimbursed by them per transaction. Valued Peers making Cash Withdrawal Requests and handling validators may decide the exact amount in other currencies by using currency exchange rates available at www.xepto.net and updated every minute. Since CRC is a matter between peers and validators, the details posted in cash ledgers need not show CRC calculations and amounts.

Minimum Withdrawal Limit

With a view to reducing system costs minimum Cash Withdrawal Limit (CWL) of US Dollar 20.00 (equivalent amounts in other currencies) has been imposed. This has been done with a view to reducing overload on system Validators and lower transaction costs to the system.

HFT Market Place

Highly Fungible Tokens (a.k.a. High Fungibility Tokens) is a concept unique to Xepto Exchange Platform.

While NFT (Non Fungible Tokens) market has seen an unprecedented growth triggered primarily by universal hype surrounding global crypto markets, most NFTs (especially digital art tokens) are abstract in nature where buyers are usually stuck with the digital ownership finding little liquidity to resell their ownerships. Global NFT market place is flushed with tokens that have little relevance to real life scenario thus leaving no scope for financial growth for NFT buyers. In most cases sale of high priced art NFTs is fake, alluring and misleading. We at Xepto Networks feel that while it may be perfectly fine for individuals with innumerable wealth to buy digital art as NFTs with a view to satisfying their aesthetic sense, inflate personal egos and/or project powerfulness and for artists to produce NFTs for the niche market, NFTs in general have little impact on common people's lives.

Highly Fungible Token (s) Market Place at Xepto Networks is planned to be designed for the benefit of ordinary people with small disposable incomes. It is proposed to start HFT issuance with real estate based tokens that preclude/minimize the chances of loss to token holders at the same time providing ample liquidity to enable quick disposal of some or all of their tokens when required.

The HFT Market Place at Xepto Exchange Platform scheduled to be introduced by Jun30, 2022 has been delayed till the end of Year 2022. Pre-sale may commence earlier.

Future Utilities and Use-cases

Xepto is planned as a functional use-case platform with dedicated and third party utilities and applications that would be fully integrated with the Xepto blockchain via REST APIs and peer channels. Users can already buy and sell gold and silver in real time. A marketplace is scheduled to be fully functional by mid 2022 for trading real estate, digital and physical graphic art, music pieces and other forms of arts besides open source travel insurance and tour auctions.

Continuing Development

Xepto network, as also this white paper are under constant development. Any changes will be reflected in the upcoming versions of the software and this document. Please check back more often to stay updated. Visit www.xepto.net to register a free wallet and start mining for FREE or become a premium miner within the Xepto Network.

Thanks

Team Xepto

Phoenix, AZ