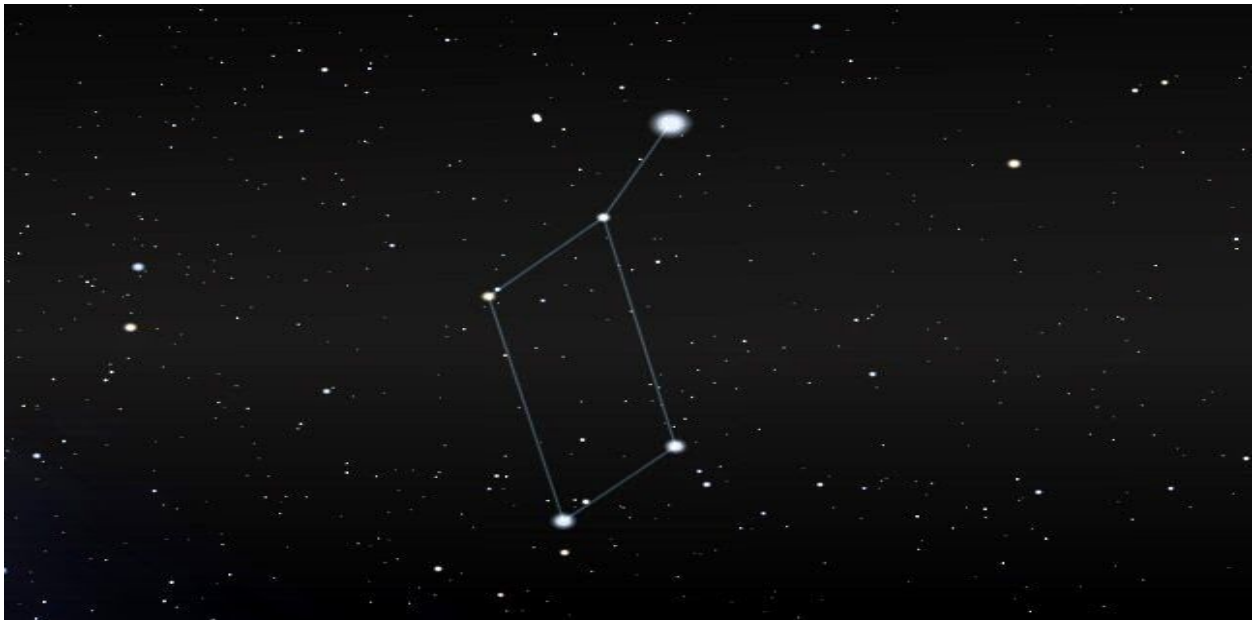

LYRA – Pure Proof-of-Stake Platform

GRAFT'S NEXT STAGE THINKING

Summary White Paper

Slava Gomzin, Dan Itkis, GRAFT Core Developers
Version 1.0 Draft
February 14, 2019

Introduction

Technology makes progress all the time. When the technology is young, the rate of progress is the fastest, with different approaches for applying the technology being tested, learning from what works and what doesn't, and evolving along various use cases.
Proof of Work based blockchains were a great first implementation of the permission-less paradigm, and are still and will likely remain a good vehicle for "storing value" given their emission properties; similar to gold.
What they are not good at however is handling high-volume, time-critical transactions (transactions on these PoW blockchains are very slow, expensive, and not user friendly).

There are two main ways that exist right now that can enable these high-volume, time-critical transactions that can stand the test of real point-of-sale environments:

1) Develop a second layer Proof-of-stake side chains - that's what the original GRAFT was all about. While much better at handling real-time transactions and high TPS, they are still subject to some of the underlying limitations of PoW.
2) By developing a separate Proof-of-stake blockchain that is disconnected from the PoW layer.

We know that second approach will win out in the end, so while we're starting with the first one, we have to make sure we don't get left behind by missing the opportunity to "skate where the puck is going". With that we'd like to lift up the curtain a little bit around our thinking regarding the next generation of GRAFT.

Primary Objectives of the LYRA

- Create a payment system that would keep and extend the main GRAFT project principals, proposals, and achievements such as privacy, real time authorizations, buyer-friendly fee structure, multi-currency support, special merchant transaction flows, custom merchant tokens, participating economy, and more (see original GRAFT white paper for more details) [1]
- Eliminate Proof of Work altogether
- Provide virtually unlimited scalability to enable TPS (transactions per second) rates competitive with traditional payment processing networks
- Eliminate a prolonged locking of funds in user wallets (both payer and payee) caused by waiting for multiple "block confirmations"
- Reduce to the network latency that affects transaction authorization times
- Eliminate dependence on one large and continuously growing blockchain database
- Add open banking features that would provide financial benefits to all stakeholders
- Decouple the payment platform from any specific cryptocurrency

LYRA Use Cases - Bitcoin Example

Once a user created LYRA account and deposited Bitcoin, they can perform the following actions:

Receive Dividends on Your Bitcoin Deposit

A user can delegate a vote for authorizer node of their choice and start receiving dividends paid from the transaction fees processed by the authorizer..

Make a Zero-Fee Payment to Online or In-Store Merchant

No fee is charged to the buyer when paying merchant using LYRA account balance. Also, there is no Bitcoin network fee since Bitcoin is already deposited to the LYRA account.

Instantly Send Bitcoin to any person without Bitcoin or LYRA wallet using Email address

Special one-time access code will be emailed to that person. Once the recipient's LYRA account is created, the transfer is finished. The recipient can use new BTC balance to make a payment to a merchant, or send Bitcoin within LYRA network, or withdraw BTC to any Bitcoin wallet.

Instantly Send Bitcoin to another person with very small symbolic fee

The LYRA transfer fee is significantly lower than Bitcoin network fee. Since BTC is already deposited to the LYRA account, there is no Bitcoin network fee. Unlike typical Bitcoin transaction, there is no need to wait minutes to hours for several confirmations because Bitcoin is already deposited to the LYRA account, and the transfer is performed inside LYRA network.

Become an Authorizer and Earn Transaction Processing Fees

Anyone can become an authorizer by setting up an authorization node. The authorizer starts receiving dividends after it receives enough votes from LYRA account holders to move to the top of the authorizers list.

Instantly Exchange Bitcoin to Other Digital Assets

A user can exchange Bitcoin balance to other digital assets (coins, tokens, stablecoins, fiat) supported by LYRA. For example, a merchant can set up automatic exchange of payments received in Bitcoin or other crypto into fiat currency (stablecoins representing fiat currencies deposited to LYRA account) to always get payouts in fiat and eliminate any effect of crypto volatility on its business.

Withdraw Bitcoin Balance to Any Bitcoin Wallet

Bitcoin balance on LYRA account can be withdrawn and sent to any Bitcoin wallet, anytime. Thus, the user can use their Bitcoin deposit to collect dividends, but the same deposit can be used to pay anyone, anytime.

Receive Instant Payments from Your Customers

A merchant can use LYRA point of sale to receive instant payments online or in brick-and-mortar store in various fiat and crypto currencies. The payouts can be converted to another crypto of fiat currency and stored on LYRA merchant account or withdrawn anytime.

LYRA Principles

The main goal of LYRA is creating a system capable of quickly transferring money from entity A to entity B without a central authority in the middle, i.e. making an unconditional, permissionless payments. To eliminate any false expectations from the beginning: such a transfer is only possible with digitized money like crypto. Whenever “traditional” form of money is involved (cash, plastic card, bank account), it must be digitized (for A) and de-digitized (for B) using semi-centralized entity such as exchange or broker. At first glance, this is serious limitation. But looking from historic perspective, assuming crypto will supersede traditional forms of money handling, such a system eventually will become fully decentralized.

Currencies vs Payment Platforms

People often confuse between currency and payment system. Currency is Money. Payment System is a mechanism that allows currency to transact (change the owner).

US dollar is currency. Euro is currency. US dollar bills and coins (cash, banknotes) are a payment system that enables face to face transactions. Visa and Mastercard are payment systems that enable non-cash, electronic transactions. PayPal is a payment system that allows to safely transact online.

Bitcoin is native online currency (cryptocurrency, or simply crypto), with basic “built-in” payment system that allows to process Bitcoin transactions online. There are many other crypto in existence.

The world doesn’t need another currency, but it needs a permissionless, secure, private, fast, and convenient payment system that would be able to process payments and transfers both online and in brick-and-mortar stores, in various currencies and cryptocurrencies. Only decentralized payment system can provide absolute privacy, highest security, and undiscriminating access to buyers and merchants. Not to mention the fact that only decentralized payment system can operate decentralized cryptocurrencies without reducing the value of their fundamental properties.

Token vs Currency

Tokens have some properties of currencies: they have value and they can be exchanged to currencies or other tokens. But unlike currency, tokens typically have a specific niche, with limited applicability tailored for particular goals. For example, slot machine tokens are used to simplify and secure the operations of arcade games and casino slot machines. You cannot pay with slot machine tokens in a grocery store.

Traditional Payment Systems vs Cryptocurrencies

Traditional payment systems operate with existing, established currencies, which allows them to focus solely on payment processing domain. Crypto payment systems, in addition to payment systems, have a burden of taking care of their own underlying currency - something that is usually being taken care by national governments and financial corporations. As a result - inconvenient, insecure payment system, or illiquid, volatile currency, or both.

LYRA vs Traditional and Crypto Payment Systems

Unlike other crypto, LYRA is a pure payment system which does not have any “built-in” underlying currency or token.* Like traditional payment systems, it operates with existing currencies, so it is completely free of monetary policies, volatility, and other concerns not related to payment processing domain. As a result, LYRA has characteristics that are difficult or impossible to achieve using mono-cryptocurrency systems: high speed, virtually unlimited scalability, and versatility of payment methods. What differentiates it from traditional payment systems, however, is decentralization, which opens a pandora box of priceless features: undiscriminated permissionless access, security, privacy, low fees, open participating economy, and more.

LYRA Design Concepts

Nano was the first cryptocurrency that implemented “block lattice”, where transactions are recorded in individual accounts (blockchains) instead of single central blockchain.[2] LYRA introduces a similar concept of **chain collection** where transactions are also recorded on individual chains but *send* and *receive* blocks are not linked directly to preserve privacy.

Sharding

Each LYRA user maintains its own blockchain called **account**. Each block contains a single transaction. The network does not maintain a single chain of blocks, which allows to process transactions faster. Instead, there is a collection of individual accounts (chain collection) which effectively creates a **sharding** mechanism.

LYRA transaction consists of **send** and **receive** blocks. The sender wallet generates a *send* block and sends it to the authorizers for authorization. Once *send* block is authorized by the

quorum of authorizers, it is broadcasted to the entire network and retained by all full nodes in *chain collection*. The *send* block is added to the sender account's blockchain.

When a recipient receives the broadcasted authorized *send* block, it generates *receive* block and sends it to the authorizers for authorization. Once authorized, the *receive* block is added to the recipient account's blockchain (which is also a part of chain collection)

Comparing to traditional payment processing flow, *send* block processing is similar to authorization phase, while *receive* block corresponds to the settlement phase of the payment transaction processing. Once *send* block is accepted by the network, transaction is considered irreversible, even before the *receive* block is created by the recipient. Once the receive block is authorized, the transaction is considered fully settled.

Pruning

Both send and receive blocks contain the updated **account balance** (for sender and recipient account respectively), which enables **pruning**, i.e. all nodes don't have to store the entire chains but can only store the last blocks. Thus, wallets and other applications don't need to scan the entire blockchain in order to retrieve the current account balance, which enables real time financial transactions and dramatically reduces system requirements for CPU, memory, and disk space. This feature also solves the problem experienced by most crypto with single blockchain - continuously growing transaction database, which continuously increases the cost of operation of every network node.

Scalability

High scalability is achieved by using a chain collection of individual accounts, where transactions belonging to different accounts can be added simultaneously, without the need to accumulate them in blocks and maintain a single continuous chain of blocks. Thus, LYRA has virtually unlimited scalability, which is only limited by authorization nodes performance, and can achieve TPS (transactions per second) numbers competitive with traditional payment processing networks.

Privacy

Both send and receive blocks are protected by using the methods defined in CryptoNote white paper and its subsequent enhancements, such as unlinkable payments (aka stealth addresses) and ring confidential transactions.[3, 4] The amounts and the wallet addresses are obfuscated, i.e. an observer cannot establish a link between the sender and the recipient, or determine any transaction and account balances.

Transfer and Pay Transactions

Although Transfer and Pay are both spending transactions which use the same mechanism described above (send/receive blocks), they are processed in a slightly different way. Since Pay

transaction is intended for merchants to collect payments from their customers in real time, it is prioritized over regular transfers when processed by the network.

Custom Notes

LYRA Custom Note (token) can be easily created by anyone by adding a new currency type and generating a genesis block. There will be reserved codes for notes created by developers for major crypto and fiat currencies. Other codes can be used for creating custom notes (tokens) such as merchant gift certificates or loyalty reward points. All notes are processed by authorizers in the same way, but only reserved notes can participate in voting process.

Transactions with LYRA Brokers

Unlike basic LYRA transactions such as transfer and pay, LYRA Broker transactions involve third-party entities in addition to the LYRA nodes. LYRA Broker is a LYRA between a fully decentralized LYRA network and the rest of the (centralized) world. LYRA Broker is an element of decentralized system. Every network user with a positive account balance can vote for a broker. The voting allows to participate in broker dividends. Similar to authorizers, brokers belong to specific owners, but removal of one or several brokers from the network does not interrupt the function of the entire network as other brokers move up in the list.

Brokers provide liquidity to the network by accepting deposits of cryptocurrency or fiat currency and returning an equivalent of their deposit in LYRA notes. The network (authorizers) and all account holders can monitor deposits in real time.

The Broker's deposit guarantees that LYRA notes are backed by actual redeemable funds. Thus, LYRA does not generate any currency, and all LYRA accounts are 100% liquid and always redeemable for the original cryptocurrency or fiat currency.

Deposit

Deposit transaction accepts the real crypto assets into the LYRA network and returns in exchange the LYRA equivalent by adding a corresponding amount of the given asset to the user account. For example, a user can deposit 1 BTC to her account by sending 1 BTC to the broker. The LYRA broker will "absorb" 1 BTC on its multisig wallet and deposit 1 BTC Note to the user account.

Instant Deposit (Instant Pay)

Instant deposit is similar to regular deposit but it happens in real time through the third party broker in order to support instant payment transactions. The LYRA user can securely paya merchant by using their preferred cryptocurrency instead of paying directly to a merchant. The broker accommodates the risk of chargebacks associated with instant cryptocurrency authorizations.

Depositing Fiat Currency to LYRA Account

The LYRA account can be funded with non-crypto methods such as bank transfer or credit card transaction using third-party providers - brokers. The broker receives funds from the user via traditional payment methods, and in exchange it deposits an equivalent amount of LYRA notes into the user account. For example, a user sends 100 US dollars to the broker using credit card. Once transaction is confirmed, the broker deposits 100 USD Notes to the user account.

Instant Deposit of Fiat Currency

Instant deposit of fiat is similar to regular deposit but it happens in real time in order to support instant payment transactions. A LYRA user can securely pay a merchant by using their preferred non-crypto payment method with the broker of their choice, instead of paying directly to a merchant.

Withdraw

Withdrawal is opposite to deposit. An account holder can withdraw funds from her LYRA balance to corresponding wallet (crypto) or bank account (fiat) through a broker.

Special Applications

Void, Pre-Auth, and Complete Transactions

The fact that every LYRA transaction consists of two blocks (send and receive) enables very important functionality which is not available on regular blockchain while widely used by payment card industry for years. Pay transaction can be either accepted by the recipient (by generating a complementary Receive block) or rejected (by generating special Void transaction).

LYRA can also easily implement pre-authorization and completion mechanism which is absolutely required for hospitality, gas stations, and other segments of payment processing industry.

Pre-auth/Complete is essentially a hard-coded smart contract. Pre-auth transaction is a send block of Pay transaction with special flag. Pre-auth must be followed by Complete, which is another transaction issued by the merchant with the change amount that cannot exceed the original pre-auth amount. Complete can be issued with zero amount which means that the entire amount of pre-auth is charged by the merchant. If Complete is not issued by the merchant within predefined time interval (7-30 days), the sender's wallet can issue a reverse transaction cancelling the pre-auth.

LYRA Plastic Payment and Cold Wallet Cards

The fact that LYRA updates the recent account balance for each block/transaction allows very lightweight implementation of spending card. The smart card has to store only one recent

transaction in order to be able to create a new spending transaction and trace the account balance correctly. The card does not need to use any external “help” in order to be able to construct the spending transaction since there is always only one input (the recent balance) used in transaction. Also, the most recent incoming transaction (receive block), if the card is “bi-directional”, can be easily requested through the payment terminal without any violation of privacy as all the account’s blocks/transactions are encrypted.

Proprietary LYRA Implementations

Since LYRA does not have underlying cryptocurrency, it can be easily adopted by proprietary player. Proprietary implementation of LYRA software may help centralized payment processors rapidly enter the crypto business, and/or prepare themselves for participating in the public LYRA. Since authorization nodes also become proprietary, there will be no need in voting process. However, the system will still retain the performance, fault tolerance, privacy of transactions, and security of deposits - if authorization nodes are maintained properly, in isolated environments, with appropriate key management.

Consensus Mechanism

PoW vs PoS

The continuous emission and rapidly growing supply of “mineable” coins contribute to high volatility of those coins. Continuous emission is required for proof-of-work blockchains in order to keep them going. The miners receive significant incentives in a form of block rewards, even if transaction volume is insignificant. Therefore, a mineable blockchain becomes “self-sufficient” even if it does not carry a significant payment function. In absence of voracious miners, the proof-of-stake systems can be sustainable without inflation.

LYRA deposits can perform “work”, so any balance in any currency can bring dividends to their owners - via either active participation (authorizer node operation) or passive participation (voting for authorizers). The authorizers rewards are taken from the transaction fees. Even at the beginning, when transaction volumes are low, the authorization quorum will be fully functional and secure even with small number of authorization and backup nodes. With greater adoption and transaction volumes, especially from merchant payment transactions with higher fees, more authorizers will be joining the competition, which will enable even better decentralization and higher security.

Chargebacks

In payment card transaction processing networks such as Visa or Mastercard, transaction is first authorized and then settled. While payment card transaction is “complete in full” only after it is settled, authorized transaction is typically “good enough” for a merchant to process a payment and finish a point-of-sale transaction with a buyer. Typical authorization takes a few seconds or

even hundreds of milliseconds, while the actual settlement may take several hours or even days. Moreover, the settlement is never guaranteed by the payment processor, i.e. transaction can be declined even if it was previously successfully authorized. This paradox is called “chargeback” in payment industry. Chargebacks are one of the biggest problems for merchants.

While you may have heard that chargebacks per se do not exist in crypto payments, in reality, when crypto payment transaction is successfully validated by one or more nodes (“accepted by the network”) and appears in the transaction pool, but not yet added to the block (or did not receive multiple “confirmations”), this situation is somewhat equivalent to authorized unsettled payment card transaction. The scenario is very similar: while transaction is valid, it still can be rejected later because of blockchain reorganization due to double-spending attempt, or it can be “stuck” forever in the pool and never make it to the blockchain (for example, miners can be reluctant to process it due to very low transaction fee). This is the situation with most blockchains including the big ones such as Bitcoin and Ethereum.

Two-Layer Cryptocurrency Networks

Two-layer cryptocurrencies such as GRAFT and Dash maintain two networks which allows them to process faster and more secure authorizations, at least comparing to the two scheme described above. The first-level network is blockchain itself, which consists of “regular” network nodes and performs settlement functions similar to regular blockchains such as Bitcoin. The second-level network consists of supernodes (aka masternodes) which performs real-time authorization. In addition to double-spending prevention, the second layer guarantees that the settlement will eventually take place, i.e. transaction will make it into the blockchain. Although in theory the process looks perfect, in practice there are various possible problems associated with this concept, and so there are possible ways to attack the two-layer network. Therefore, although the risk of chargeback is significantly lower (in most cases near-zero) than the one in single-layer blockchain or payment card network, it is still there.

Locked Funds Problem

Both single and two-layer networks have the same “locked funds” problem which prevents spending of unsettled funds. Typical crypto transaction consists of two records that split a single payer’s wallet balance into two outputs: 1. the payment that goes to the payee and 2. the change that goes back to the payer’s wallet. As a result, the entire wallet balance remains locked until the transaction is settled (received N confirmations). It’s important to note that payment card networks do not have this problem in most cases (with exception for pre-authorization which will be discussed separately) because they have centralized servers with up-to-date information about all transactions, both settled and unsettled.

Delegated Proof-of-Stake

Several successful attempts have been made to eliminate proof-of-work and fully replace it with proof-of-stake. Several “high-ranking” crypto projects (EOS, Tezos, Lisk, BitShares, Nano, Ark) have implemented a **delegated proof-of-stake (DPOS)**, or based their consensus mechanism on DPOS principles (Cardano). [5] In DPOS all participants can vote for a few nodes by delegating their coin balances to the nodes they trust. The more votes (the greater stake balance) the node receives, the higher its position and the possibility of being elected as an authorizing node.

LYRA uses DPOS as its consensus mechanism applied to chain collection with separate send and receive blocks. Transactions are authorized within milliseconds because of the limited number of authorizers pre-selected by account holders, and compact blockchains consisting only of the blocks that belong to particular account.

DPOS Voting

There are authorizers, authorizer candidates, and all other full nodes. In order to become an authorizer, the candidate needs to broadcast the status update claim stating its number of votes, which is supposed to be greater than the current entry level (the number of votes of at least one of the members of the authorization sample). Each node must validate the claim by scanning all savings accounts linked to the candidate. If the claim is correct, the node updates its authorizer list and retransmits the claim to other nodes.

Incentives to Participate in DPOS

Even brilliant technological ideas won’t work if they are economically inexpedient, i.e. it is not attractive financially to the mainstream users and supporters. Most existing cryptocurrencies attract investors as they believe in continuous rise of value, which is not guaranteed, however, especially for proof-of-work blockchains with continuous growth of supply. LYRA has no “official” underlying cryptocurrency which could provide such a speculative growth. Instead, it will provide a natural growth by paying off dividends earned by participation in transaction processing. Unlike most existing hybrid cryptocurrency/payment systems that pay out block rewards to their maintainers by creating “new money” out of thin air with every new block, LYRA will generate dividends from transaction and exchange fees paid by the network users.

Voting for Authorizers through Savings Accounts

Voting Currency

A voting currency is chosen (at first by the GRAFT developers and later by the Authorizers via DAO consensus) to represent the voting rights in the network. GRFT Notes will be used as the

initial voting currency. It is preferable that the voting currency has a finite supply and be fairly distributed among the platform participants.

Voting Process

Account holder can vote for an authorizer by creating a voting currency savings account. Each savings account is linked to particular authorizer. The dividends come from transaction fees which the authorizer earns by participation in the authorization process. Thus, the very process of voting for authorizers is “masked” for the end user by the process of moving funds to the voting currency savings account. This way, the users are also motivated to vote as they participate in LYRA reward sharing, i. e. account holders become stakeholders of the LYRA system. In traditional centralized payment systems such as Visa or PayPal, the earnings are received by the corporation, and some part is distributed to stockholders. In LYRA, all the earnings are shared directly between the authorizers and savings account holders, with no corporate bureaucracy in the middle.

Timing

We’re still flushing out the details around the new Proof of Stake design and it will be some time before we commence any work on it, tentatively Q2 2019.

Conclusion

As you can see from this white paper, LYRA is attempting to combine the best ideas and technologies currently available in crypto space, such as delegated proof of stake, sharding, and CryptoNote, and apply them to the financial payment network space. We operate with concepts like “accounts” (both regular and saving) to maximally resemble the existing financial system paradigms, while “authorizers” resemble payment network methods and workflows, which enables faster adoption by mainstream users

Given the limitations of PoW, delegated proof of stake with chain collection is ultimately a better approach - faster, requiring less storage, consuming less resources, and providing more level playing field. While we recognize that DPOS is not without questions of its own, which we will address later, we believe that moving to DPOS and chain collection is crucial for the project’s long term success.

References

1. GRAFT: A Decentralized Payment Processing Blockchain Network. Slava Gomzin, Dan Itkis. https://www.graft.network/wp-content/uploads/2018/10/Graft_White_Paper_3.0_October_2018.pdf

2. Nano: A Feeless Distributed Cryptocurrency Network. Colin LeMahieu. https://nano.org/en/whitepaper

3. CryptoNote V2.0. Nicolas van Saberhagen. https://cryptonote.org/whitepaper.pdf

4. Ring Confidential Transactions. Shen Noether, Adam Mackenzie and Monero Core Team. https://lab.getmonero.org/pubs/MRL-0005.pdf

5. Delegated Proof of Stake: Features & Tradeoffs. Myles Snider, Kyle Samani, and Tushar Jain. https://multicoin.capital/wp-content/uploads/2018/03/DPoS_-Features-and-Tradeoffs.pdf