KDC COIN

WHITEPAPER

Contents

1. Introduction

“Imagine a technology that could preserve our freedom to choose for ourselves and our families, to express these choices in the world, and to control our own destiny, no matter where we lived or were born. What new tools and new jobs could we create with those capabilities? What new business and services? How should we think about the opportunities? The answers were right in front of us, compliments of Satoshi Nakamoto.”

From Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World by Don Tapscott and Alex Tapscott2.

Since the introduction of Bitcoin, blockchain technology has grown by leaps and bounds. Blockchain has allowed not only cryptocurrencies to flourish but has allowed traditional sectors such as financial institutions to utilize this technology. A sharp rise in price and usage of Bitcoin as well as other cryptocurrencies like Ethereum, Ripple, Litecoin, Dash, Monero — has shown the world that the global financial system is ready for a change. The change that will take the industry to a whole new level where transparency, data integrity, and decentralization will become the main pillars of its growth.

Bitcoin is the most known and valued cryptocurrency by the market capitalization. Altcoins is a collective name for all other cryptocurrencies, and they have been diluting Bitcoin‘s market share in recent times. Blockchain has been the dominant design of peer-to-peer crypto currencies. However, blockchain technology is still relatively young, and have the potential for exponential growth, leading to new offerings in the market.

The KDC Coin is one of such new offerings. Its state of the art solution is built around most advanced technological capabilities of SegWit & Customized Network to deliver blazing fast, secure and near-zero cost payments to anyone in the

world. It is designed to overcome well-known inefficiencies within government central banks and other

crypto currencies. It induces transactions that are fully secure, private and anonymous.

However, such a rapid upward trend in the popularity of crypto-currencies came with its drawbacks that may threaten the further integration of the digital, decentralized currencies:

1. Increasing number of attacks and forks
2. Double spending
3. Poor network security
4. A limited number of available coins
5. Increasing complexity of coin mining
6. Slow transaction processing
7. Increasing transaction fees
8. Price fluctuations
9. Lack of malleability within the network

The solution to the problems mentioned above is KDC Coin. KDC Coin is an innovative decentralized cryptocurrency incorporating the advanced technologies that tailor the needs of primary market players - users, investors, and business owners.

2. Key Technologies

Blockchain technology is the foundation of crypto currency and is the next “industrial revolution.” It is a decentralized ledger system with enhanced security, is simple in design and inexpensive to operate. This system allows for transactions to be done with complete accuracy because it is a fusion of computer peer-to-peer (p2p) technology, cryptography and database systems.

The fusion of these technologies leads to a data-storage system that is immutable and irreversible, meaning that transactions cannot be modified after signed and added to a block chain. Deals become final, and there is no double spending. Cryptography not only utilized for encrypting messages on the ledger but is also used to sign the transactions of users and to prove these transactions are valid. With cryptography, blockchain does not require extra security solutions to protect the authenticity of operations.

Blockchain’s decentralized and p2p nature means that the ledger eliminates the need for a data-center and a disaster recovery center (DRC). The result is that the ledger will always be up and running.

KDC Coin incorporates the best features of POS-based crypto currencies. KDC Coin's users can achieve better decentralization, transparency, privacy, and cost-efficiency in their financials. Low energy consumption, ease of use, and better network participation incentives work in line with doubled network capacity, smart contracts, lightweight wallet, and cloud mining to provide people from all over the world a worthwhile, stable, and more reliable way of handling their financial needs.

2.1 Proof-of-stake

The first crypto currencies based on the Proof-of-stake algorithm, or POS, appeared in 2012 with Peercoin, followed by Emercoin in 2013, and NXT and BlackCoin in 2014. The primary objective of the cryptocurrency blockchain algorithm is to achieve the distributed consensus within the network that is secured by a significant number of nodes.

POS algorithm designed as a more eco-friendly, resource efficient, and reliable alternative to crypto currencies based on the Proof-of-work algorithm, or POW, that require massive amounts of energy to maintain the proper functioning and growth of the network.

Coins of POS-based crypto currencies are created through staking. In other words, all nodes in the network that possess any amount of coins in their wallet and keep the node online are automatically included in the coin forging pool and are therefore are eligible to create and sign blocks, securing the distributed consensus.

In May 2017 the world's second largest cryptocurrency, Ethereum, announced that it would make a transition to a Proof-of-stake algorithm by the end of 2017.

2.1.1. POW and DPOS Comparison

As mentioned above, the only thing that nodes within a POS cryptocurrency need to do to is to maintain the security of the network itself. Therefore one needs to have a certain amount of coins in the wallet and keep the wallet online to be eligible to earn. This mechanism eliminates the human factor in the mining/forging process and helps to avoid spending massive amounts of electricity on creating coins. It is the backbone and the most laconic property of the Proof-of-stake algorithm.

Apart from the Proof-of-Stake, two other algorithms exist in the cryptocurrency world. The Proof-of-Work (POS) and Delegated Proof-of-Stake (DPOS) algorithms, which are both meant to help blockchain reach a distributed consensus and maintain the integrity of the network.

Distributed consensus, is a term widely used in computer science and crypto currencies. It should be interpreted as a mutual consensus among the majority of its users, on whether the data about the transaction in the last block is valid. If this is the case, the distributed consensus is achieved, and the block will be successfully signed, ensuring proper functioning of the network.

If the data in the last block is false, then distributed consensus among active members of the network will not be reached, and therefore this block will not be signed, avoiding the possibility of various kinds of attacks that jeopardize the system integrity or allows for double spending.

In crypto-currencies that use POW the distributed consensus in the network is reached with the help of its active members, or miners, who need to use real computing produced by hardware to hash blocks and mine coins. Though this may seem like the most robust and true-to-life method of reaching the distributed consensus, actually it leads to several serious problems:

1. It requires massive amounts of energy due to the increasing difficulty to mine coins.

2. Miners are required to purchase expensive equipment to survive in the ever-growing mining market. The hardware gets outdated fast and eventually ends up at a landfill site, harming the environment even more.

3. Such system leads to the appearance of miner monopolies that tend to negatively influence the commission fees and transaction processing times and also leaves the possibility of carrying out a 51% attack.

Delegated Proof-of-stake, or DPOS, is the latest blockchain algorithm which is currently used by cryptocurrencies like BitShares. In its essence, it's very similar to POS, but it still has quite a few changes that make it different from the Proof-of-stake algorithm.

Network nodes in DPOS cryptocurrencies create coins in the same way as it is in the POS-based ones - by storing the currency in the wallet. However, all necessary decisions within the network in DPOS cryptocurrencies are performed via the results of elections organized by the members of the network.

At first sight, this mechanism may look more democratic and transparent, but it also makes the system complicated, potentially less secure due to the human factor involved, and decreases the user participation rate, in this way causing centralization concerns.

2.1.2. Encryption

KDC Coin uses several cryptographic algorithms for purposes of ensuring the blockchain integrity and safety of its users' coins.

The first one is ECDSA, a public key cryptography algorithm, which is associated with every coin in the system utilizing a public key, private key, and signature so that every node of the blockchain can verify the coin ownership.

The second one is a robust one-way SHA-256 encryption algorithm, which is included in SHA-2 family of cryptographic hash functions and is considered to be a classic in the majority of the world's cryptocurrencies.

The SHA-256 hash function is used to turn input data of any size in the blockchain into a string of 32 bytes that is impossible to reverse or predict. In the case of an attack upon which some or all of such input data is changed, the hash associated with this data will be changed aswell, making it impossible to create a different block of data with the same hash.

These two cryptographic algorithms ensure stable functioning of the KDC Coin blockchain network where the ownership of coins can be easily verified, and distributed consensus is achieved without the risk of double spending.

2.1.3 Blocks and block creation

Since KDC Coin is a cryptocurrency based on POS algorithm, the creation of blocks is carried out through a provision of proof that the active network node possesses a certain amount of coins and therefore can participate in the generation of blocks.

If the active network node—meaning that it is a user who keeps their wallet open—possesses a certain amount of coins, it will be eligible to enter the block creation process by sending the coins to itself and proving their ownership.

Selection of the creator of the next valid block is made by using deterministic randomization formulas that take both the stake size and the lowest hash value into account, therefore avoiding centralization of the cryptocurrency by not letting the wealthiest members of the network infinitely accumulate their capital.

2.1.4. Coins and forging process

Based on the POS algorithm, an active node of the blockchain network in KDC Coin is randomly selected. The choice is based on their stake size. The appropriate wallet will receive a daily reward or ROI for the contribution to achieving the distributed consensus.

As a POS cryptocurrency, KDC Coin will start with an open ICO. During the ICO anyone will be able to purchase KDC Coin tokens and also can receive a certain number of KDC Coins as a bonus. The total number of coins that are offered to the public during the ICO equals a number of coins in the genesis block, which is 150 million KDC.

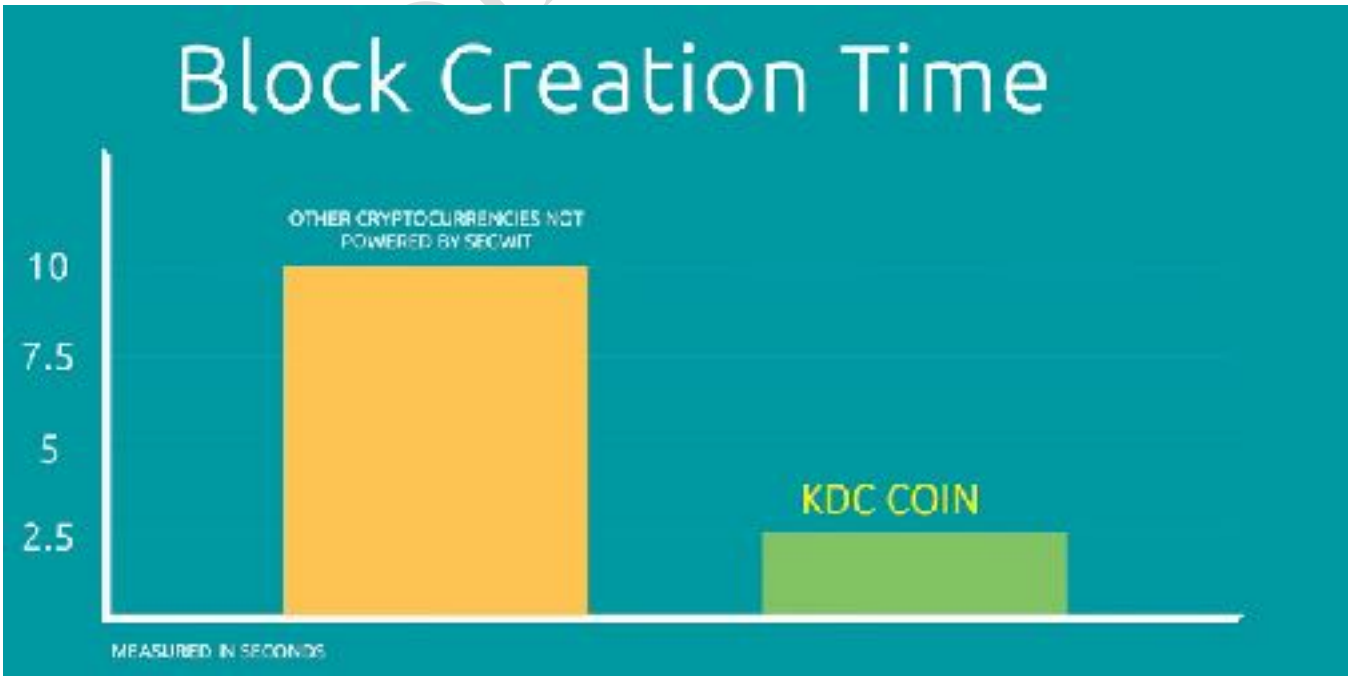
2.1.5 Nodes

The POS algorithm doesn't require massive amounts of electricity wasted on hashing blocks that are used to store a large amount of data. The nodes in KDC Coin are lightweight and use SPV, standing for the Simplified Payment Verification mode, which allows users to download only a part of the blockchain relevant to their node instead of downloading the whole copy of blockchain.

2.1.6. Transactions: fees and processing time

If we take an average transaction processing time in a POW-based cryptocurrency and compare it with the same metrics in a POS-based one, we shall see that the POS algorithm processes the transactions at least two times faster.

Thanks to the usage of SegWit, on average each block is four-times more efficient than the regular one. On top of that, the KDC Coin network creates a new block within 2.5 minutes against 10 minutes in POW-based crypto currencies.



Worthwhile to mention is that the capacity to perform multiple transactions inside the KDC Coin network is just sensational in the case of using the Customized Network protocol - a side-chain payment solution on top of the original blockchain. The Customized Network is an ideal platform for the micropayments industry.

When it comes to the transaction fees, they are estimated to be at least ten times lower than those in cryptocurrencies powered by the POW algorithm. Such a significant decrease in the transaction costs is possible thanks to a lack of physical mining of coins in POS algorithm and well-balanced distributions of coins among all active members of the network.

2.2. SegWit

Since more and more people are currently using crypto currencies for their everyday financial needs, the overall number of transactions grows very rapidly. SegWit is created to improve blockchain scalability by increasing the block size limit thus decreasing the transaction processing time and fees. The SegWit technology also enables execution of Smart Contracts as well as of side chain solutions like Customized Network mentioned above.

Due to the blockchain properties, a txid (transaction id) of a block also includes information on the previous inputs and outputs of coins and wallets associated with this transaction occupying up to 60% of the block size. The increasing numbers and size of block slow down and overload the network itself, leading to slower processing times and higher fees.

2.2.1 Overview

SegWit allows for writing up to 4MB into a single block. The scriptSig data is moved out of the transactions and blockchain, both enhancing the network performance and preventing any possibility of malleability attacks.

Apart from this, SegWit provides a broad range of other important features like increased P2SH security (P2SH encryption key length is 256 bits now), linear scaling of sighash operations, reducing UTXO growth, overall efficiency gains, and so on.

Segregated Witness, which is most often called SegWit, is a proposed update to the Bitcoin protocol that was officially released October 6, 2016, in version 0.13.1 of the Bitcoin Core and this technology is fully implemented in KDC Coin.

2.2.2 Security

All blockchain networks let their users perform a kind of escrow transactions called multisig. Multi-signature transactions require up to five signatures from different parties to sign a transaction.

Currently, the majority of crypto currencies use pay-to-script-hash (P2SH) protected by 160-bit HASH160 algorithm that is known to have loopholes, letting a corrupt multisig transaction member to steal money. In SegWit this vulnerability is fixed by using HASH160 only to sign single key transactions. All the multisig transactions are hashed using the 256-bit SHA256 algorithm.

2.2.3 Block size and network capacity

Initially, the block limit size of 1MB was set by Satoshi Nakamoto in 2010 in Bitcoin for purposes of protecting the network from DoS and spam attacks, but since then it became the default value used by the majority of world's cryptocurrencies.

Also, an increased block limit size that is introduced in SegWit improves the overall security of the network and therefore allows for a seamless and safe implementation of Smart Contracts and a broad range of second layer solutions.

Since this limit leads to slower transaction approval time and higher transaction fees within a busy blockchain network, leading to lower overall performance, SegWit increases this limit to up to 4MB per block by excluding witness data, scriptSig and scriptPubKey fields with the signature data that occupies 60% of the transaction size, out of the transaction.

With the new block weight algorithm that SegWit proposes, all non-witness data in a block amounts 4 weight units per block and the witness data takes 1 weight unit per block in the same block. This constitutes a 4x increase in the network capacity and performance.

2.2.4. Malleability and Smart Contracts

When a transaction is sent over the blockchain network, any node that processes it can make minor changes to the signature data in the txid of this transaction. These small changes cannot influence the input and output transaction information meaning that it still will be sent and received by the right people but it can make the txid information unreliable, making it more difficult to trace it within the blockchain.

Smart Contracts is a technology that adds specific logic to the transaction and serves as an evidence of possession of claim over something by someone (e.g. tangible/intangible funds and resources as well as intellectual or any other property). Smart Contracts turn a regular transaction into a powerful tool for accounting purposes.

2.2.5. Customized Network

The Customized Network is a solution that allows for sending instant and near-zero cost transactions to one or more users of the network.

The idea behind the Customized Network is to create payment channels off the blockchain so that users can send an unlimited amount of transactions between each other either by securing them with only one ledger entry in the blockchain and using the blockchain as the arbiter through Smart Contracts or by applying to a trusted third party for escrow purposes.

3. Key features

Apart from the features peculiar to the Proof-of-Stake algorithm, KDC Coin is beefed up with SegWit, and Customized Network protocols. On top of that, KDC Coin boasts a wide array of features such as user-friendly and lightweight wallets, cloud mining availability, forging incentives, and so much more. We've implemented this all to make our product convenient for everyone regardless of their financial needs.

3.1 Wallet

KDC Coin comes with an array of wallets for desktop, iOS, Android, and web applications. KDC Wallets provide all necessary features for the comfortable daily use of the cryptocurrency and do not require much space on your PC or smartphone.

The outstanding advantage of the KDC Wallet is that it requires a very tiny amount of space for its installation compared to the Bitcoin Core and therefore can be used by anyone, anywhere, and anytime. KDC Coin is designed over a Proof-of-stake algorithm, which makes full node wallets a thing of the past.

Since there’s no physical mining of coins required and the distributed consensus is achieved via proof of possession of coins in one’s wallet ; you are not obliged to download the full copy of the blockchain to use KDC Coin, resulting in less disk space usage.

3.2. Cloud mining

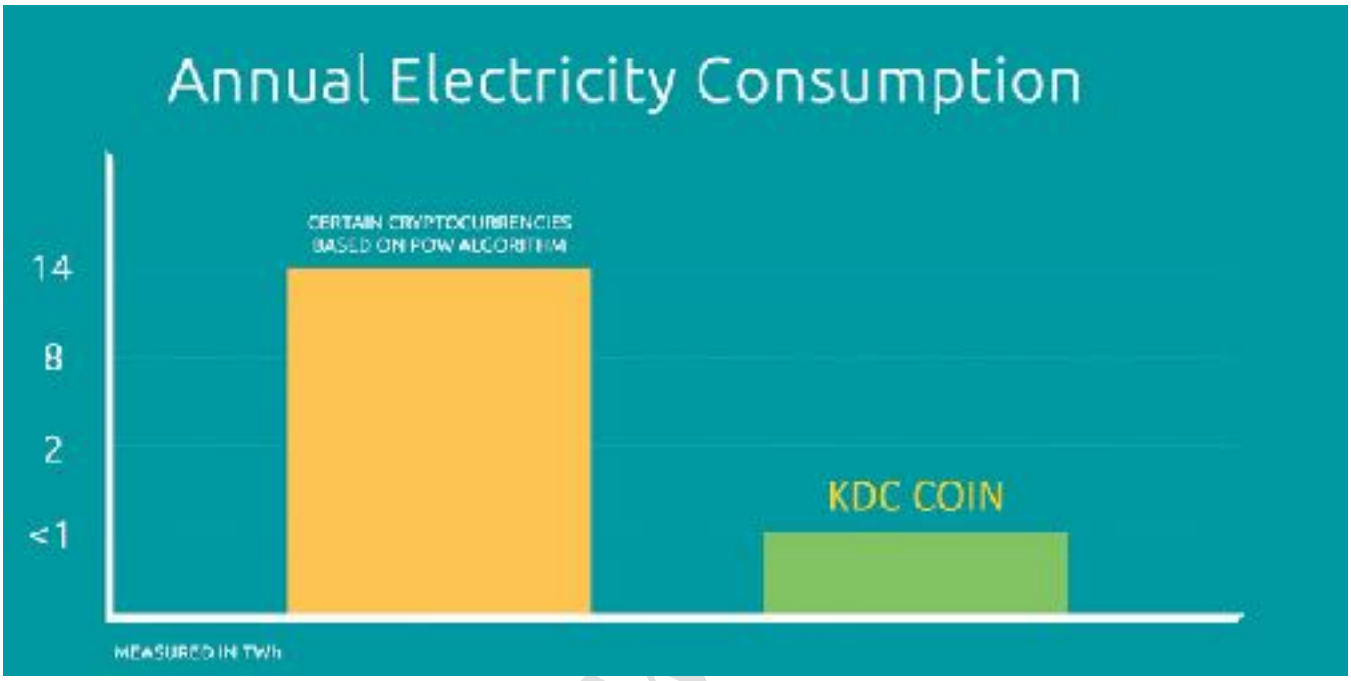
As it was mentioned above, users of KDC Coin do not need to constantly hash data using costly equipment that consumes a lot of electricity. However, to enter the coin forging pool and be able to earn with KDC Coin, one simply needs to keep the wallet online to be considered an active blockchain node.

Aforementioned is definitely a better and a lot more eco-friendly way of maintaining the blockchain integrity and security yet it might likewise lead to some little unnecessary power spending. This is one of the reasons why KDC Coin offers a cloud mining service available for all of its users irrespective of whether they are just regular users or big investors.

The cloud mining services will be provided by KDC Coin and several other trusted third-party companies so that the cryptocurrency members can enjoy a wide selection of payment options and service conditions tailored especially to their needs.

3.3 Low energy consumption

According to publicly available statistics, currently, some of the POW based crypto-currencies use up to 14.18 TW/h of electricity annually, which is comparable to the total power consumption in the entire country of Slovenia



A rapid growth of any POW based crypto currency will undoubtedly lead to a sustainable increase in electricity consumption

3.4. Agility and cost-efficiency

Since KDC Coin is based on the Proof-of-Stake algorithm, which was also developed to make crypto-currencies more resource efficient and eco-friendly, our users don't need to buy expensive equipment also known as ASICs. Most likely these ASICs get obsolete within just one year after purchase and eventually end up at the rubbish dump.

It's a waste of massive amounts of electricity on performing unnecessary calculations.

4.Risks and risk management

Cryptocurrencies offer a whole range of tools and measures that are meant to contribute to the development of a more transparent, just, and open global financial market and ensure the security and growth of the investor's capital.

Like any other complex and elaborate systems, cryptocurrencies as a thing present certain flaws and risks associated with any financial instrument. In the sections below we will explain such risks and talk about the ways of balancing them and cutting their impact down to the reasonable minimum.

4.1 Security: attacks and hard forks

There are various kinds of attacks and vulnerabilities to which a crypto currency can potentially be exposed. The most significant of these threats are a majority attack (51% attack) that has to do with monopoly problems and a double spending attack.

A most devastating attack can be performed when one of the nodes of the blockchain possesses 51% or more computing power of the whole network and therefore gains complete control over it. Such attacks may theoretically take place in the POW-based cryptocurrencies only. In such a case the evil doer needs to purchase some serious mining equipment with the total cost of more than $15 billion. That sounds like a lot, but in fact, it is doable.

A 51% attack is not realistic in KDC Coin network for the two following reasons:

1. KDC Coin is a POS-based cryptocurrency, the attacker will need to possess at least 51% of all network resources. A hacker will need to purchase at least 260 million of KDC Coins, which is 51% of the block right after launch.
2. Even if such an attack happens, it won’t be beneficial for the attacker himself. This attack will affect the market rate of the

cryptocurrency negatively, meaning that the hacker will be attacking himself and will suffer from losses.

When it comes to double-spending attacks, in KDC Coin they are prevented by confirming every transaction that a specified block contains. To be confirmed and considered as valid by the blockchain, a transaction needs to receive at 6 or more confirmations.

4.2. Centralization

Another issue for all crypto currencies irrespective of whether they are based on POW, POS, or DPOS algorithm is centralization concerns.

Since it's both illogical and too costly to perform a 51% attack for a POS-based cryptocurrency, the centralization of the network in KDC Coin is very unlikely.

As an additional measure against centralization, the creator of the next valid block in the KDC Coin blockchain will be selected using deterministic randomization formulas. These formulas are based on the stake size and the lowest hash values that will limit wealth accumulation possibilities and ensure that the cryptocurrency doesn't get centralized.

5. Conclusion

This whitepaper has been prepared to provide the most detailed information about KDC Coin concerning its key characteristics and features, the most important technologies used in its development, and risks associated with it.

We have succeeded in finding out and establishing that the Proof-of-Stake consensus KDC Coin is based on fact to be a more secure, just, and eco-friendly as well as less corrupt and less difficult to use in comparision to the Proof-of-work algorithm.

At the same time, the latest technologies that KDC Coin is powered on like SegWit and Customized Network and the proprietary features like cloud mining and forging incentives make it a truly agile, cost-efficient, and user-friendly tool that can satisfy the needs for financial freedom of any person irrespective of their place of birth, technical competence, or social status.

Despite the potential of micropayment systems very few systems have been successful as their acceptance is limited to certain communities such as specific online games or social networks.

KDC coin is a new progressive crypto currency, which supports an unlimited number of transactions between different devices at high speed with its Customized Network technology, which makes it a viable option for micropayment. KDC Coin has already signed contracts with some big players around the world, and we are ready to take the financial industry to the next level.