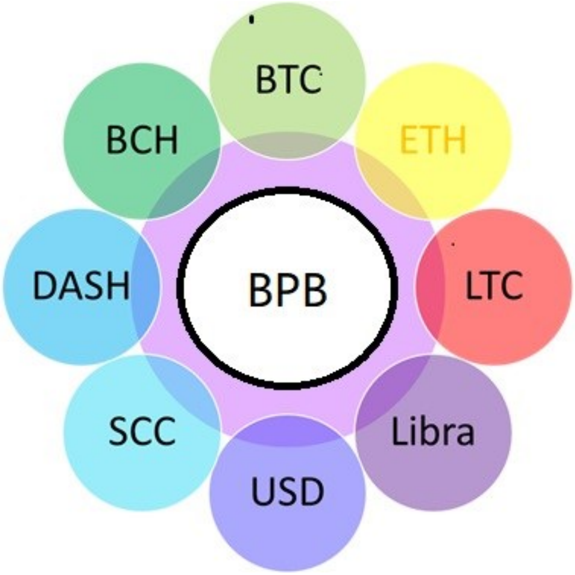
Byzantine Proof Bitcoin



The fastest The Most Cost-effective The Safest

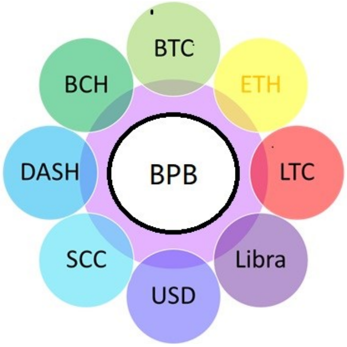
Transaction Storage Payment system are a hundred times faster than blinking

Contents：

Byzantine Proof Bitcoin

The Byzantine generals' problem is a long-standing problem of distributed data consistency. Research papers on the subject began in 1982. In 2009, Bitcoin became the first digital currency in the world that successfully solve the problem of distributed data consistency by utilizing ECDSA cryptography and the asymmetric SHA256. The approach of Bitcoin is more rigorous than that of other digital currencies. In particular, it has avoided the huge security weakness brought by the flexible smart contract of Ethereum virtual machine.

However, Bitcoin still faces a few major problems: slow transaction speed, two wallets can potentially produce same address, and 51% computing power attack. Other flexible smart contracts, such as the huge security problem in the Ethereum virtual machines, meaning that none of the current digital currencies are 100% reliable and they cannot be widely used within the commercial world. The Byzantine Proof Bitcoin (BPB) is designed to address all of the problems listed above. Moreover, these technologies can be applied to most other blockchains with or without some modification, it can connect to various blockchains and commercial bank interfaces, conduct bank-level security transactions and commercial retail payment. BPB is designed to be the world's fastest, bank-level secure crypto token and can handle millions of retail payment. BPB can achieve 3 million transaction per second, its performance is 2000x faster than Libra and 20x faster than credit card system, and will support Libra, DCEP and automatic fiat currency conversion. The goal is to make payments globally easily.



BPB is the utility token of BPBtc platform. BPB has the following characteristics:

1. **Speed**: The three-tier blockchain can achieve 3 million transaction per second, while existing credit can handle 0.15 million transaction per second.

2. **Anonymity** : BPB is built on top of Bitcoin, it is anonymity and decentralization if you only use first layer.

3. **Security**: It solves the 51% computing power attack, address overlapping, Ethereum's VM …. all addresses are multi-signature addresses, resistant to hacker attacks. It is 100% bullet proof.

4. **Fee**: The transaction fee of BPB platform coin is 1/10th of existing.

5. **Publicly Verifiable:** Because BPB transaction is publicly verifiable via blockchain browser https://bpbtc.net and 1/10th fee, while Alipay and Wechat transaction are not publicly verifiable.

6. **Legal**: U.S. federal regulators and SEC back digital dollar stablecoins. Using its 3 millions/sec transaction speed, BPB will be the hub of global digital payment revolution (Libra, USDC, USDT, DCEP, BTC, BCH, DASH……etc.).

2.1 Technical and architectural advantages:

MacroSQL is the leading real-time cluster database company in Silicon Valley, USA. Blockchain is also a simple distributed cluster database, thus MacroSQL's technology is perfectly suit for improving blockchain, which has big performance problem because it has linear general ledger structure, and needs a large amount of computation for encryption and decryption. These two aspects make it difficult for the blockchain to be fast in operations such as classification, statistics and search. It is slow because it has to linearly traverse billions of historical transactions while decrypting and parsing, and the length of each block and transaction are both not identical and cannot jump transactions or blocks. Blockchain and cluster databases need to solve similar problems: data consistency, latency, security, reliability and speed in distributed computer system. Therefore, solving data synchronization and consistency of the blockchain is one of the most perfect applications of MacroSQL's real-time cluster database and related technologies. BPB is based on MacroSQL's invention, unique cluster database and related technologies to accelerate distributed blockchain. BPB is also the world's first 3-tier blockchain, the first to fully address the Byzantine loophole, and the first commercial-grade blockchain.

The research and development of BPB began in September 2017. The early members of this team are all engineers from Silicon Valley, California. It focuses on using its own clustering database technology to achieve better transaction, fault tolerance, high-speed, data consistency and security so as to win the market. It is the only blockchain in the world that all customer addresses are re-encrypted with multi-signature BPB and all private keys are also kept offline and re-encrypted via PKI/RSA. Neither internal employees nor hackers can possibly hack. The transaction price is completely transparent via blockchain explorer. Customers can also apply for their own multi-signature private keys or multi-encrypted private keys, deep-frozen account and other security measures.

Our system is designed in such a way that it guarantees the integrity, certainty, permanence and 100% accuracy of the transaction even in the event of a power outage and computer hardware/software failure. At present, the core database technologies are concentrated in Oracle and IBM in the United States (the top 2 dominate bank transactions). With Intel's chip monitoring background, our team has significant competitive advantage in reliable financial transaction. The crypto currency itself mainly relies on the combination of ECDSA and SHA256 hash to ensure that: using private key to deduce public key, address or signature is easy; but use hash or public key to deduce private key are extremely difficult. The BPB technical team members used to be the core technical personnel of the Oracle (database No.1) and Intel (chip No.1) database joint project, mastering Intel's most cutting-edge zero-interference CPU internal monitoring technology. At the same time, we have done PKI encryption technology. Having the above three core technologies are necessary conditions for innovation in the field of high-performance blockchain. BPB team has all 3 core technologies. At the same time, MacroSQL uses its own world-first real-time cluster database and related technologies.

If the bank tells you that losing the key is equivalent to losing all your money, you do not want that bank. But the current blockchain has this same danger: losing your wallet or private key is equal to lose all your asset. BPB pioneered the POWSC algorithm to ensure bank-level security while solving the Byzantine generals' problem.

2.2 Three-tier three-dimensional architecture:

All cryptocurrencies currently have problems of slow transaction speed (a few minutes), high transaction fees ($5), and 51% computing power attacks. In addition, Ethereum smart contracts share 99% of same ERC20 standard interface and same code for receiving and sending coins. They also share same mining logic, with only the name and quantity are different from different tokens. The smart contract code is dynamically interpreted by the virtual machine. The problem is that this dynamic interpretation is highly flexible and introducing security issues. First of all, the code of this kind of virtual machine is gigantic, which is “non-deterministic” and hard to guarantee security of every line of code; At the same time, smart contracts are usually copied and modified by a programmer in a day, so it is difficult to be flawless. Since the birth of Ethereum, more than 50 major hackings have happened. A huge virtual machine can be liken to a 100,000-kilometer-long wall, and there is no guarantee that every section and every soldier will be free from negligence and vulnerabilities 7x24h; And smart contract transaction fees are higher than ETH (smart contract transaction fees are the cash cow of Ethereum). Though Bitcoin has never been compromised and is very safe, but it is slow and transaction fees are high. Therefore, it is ideal if one can solve the weaknesses of Bitcoin while utilizing its advantages.

The BPB team members are mostly former Intel, Oracle's engineers specializing in reliable and secure database transaction. BPB uses the Silicon Valley team's 3-layer network acceleration technology (the bottom layer is an improved Bitcoin network. If you want, you can choose to only use this layer of anonymity). Layers 2 and 3 are acceleration layers. The third layer of BPB includes payment, banking and interfaces; These three layers are fully interoperable. The second and third layers also have machine learning, credit learning and confirmation mechanisms, as well as security features such as deep freezing, PKI/RSA public and private key security and other functions. PKI is a bullet-proof asymmetric encryption technology and is mainly used for VPN and SSL symmetrical key encryption. High-digit PKI is more effective against quantum computers than ECDSA/hash. A better PKI system with a length of 4096 bits or more cannot be decrypted even by large super computer for several years. The system contains various SIMD accelerators and various types of Intel pipeline real-time acceleration technology. It can guarantee that the network transaction speed is ~1000 times faster than that of Bitcoin. High speed is equivalent to using fewer computer resources and thus lower cost. High performance can simultaneously solve the two pain points of slow speed of Bitcoin and high transaction fees. The on-chain transaction fees of BPB is about 1/10~1/30 of existing coins and BPB's own payment can be even lower than that. Low transaction fees strengthen BPB's competitiveness in retail, retail coupons and games . Because of the large transaction volume in these areas, most of the transaction amount is small.

Bitcoin transaction fees are almost equivalent to $5 coffee, which is obviously not competitive. Therefore, BPB has three advantages that Bitcoin does not have. For example, BPB users can buy things anywhere in the world without store's associated with BPB. Because our wallet can automatically convert BPB into local or USD based currencies. In the long run, BPB will have a unique advantage in the retail industry because it is the first to solve the Byzantine security loopholes, and it has high-speed and low-cost. The first and third layers have been completed. You can go to https://bpbtc.org to test and watch the lightning-fast transaction speed and learn more.

2.3 Bullet-Proof Byzantine:

At the beginning of this article, we said that the current blockchains do not completely solve the security of Byzantine generals' problem. Bitcoin still faces the problem of 51% computing power tampering with blocks. Not only that, because the blockchain transaction data is irreversible and there is no identity similar to the customer in the bank, it is almost impossible to recover it after the digital currency is stolen. Crypto currency has become the heaven for hackers. And even employees of a company can pretend to send bitcoin to wrong address by mistake. Hackers can apply to become employees, and employees may become hackers because of greed; Mobile phone chips and memory are hardware without ECC fault tolerance. Mobile phones can be stolen, broken, flooded; computers and mobile phones can be attacked by Trojan horses, viruses and hackers. There are Trojan horses and viruses on 90% of computers and phones, and tens of thousands of people lost their digital wealth. Also, hash algorithms are vulnerable to quantum computers attacks......all these problems need to be solved within the blockchain ecosystem. In fact, many existing blockchains and trading platforms are very crude, very unreliable and are hacked frequently. In business, supervisors are absolutely afraid of taking any of risks listed above. How to solve these problems is the key for the wide adoption of blockchain in the commercial and financial fields.

From the fact that Ethereum and smart contracts have been breached more than 50 times; the fact that most trading platforms and wallets are often hacked, it is clear that the current blockchain and trading platforms have serious shortcomings. Because the irreversibleness and non-identity of receiver, the security requirements of customer accounts need to be hundreds of times more advanced than existing banking system and exchange, and more resistant to malicious behaviors.

In order to truly solving the problem of the Byzantine generals for the blockchain; crypto exchange hacking, non-ECC, the Trojan horses, viruses, Ethereum VM issue……etc. There is a need for some big innovations to transform existing blockchain technology. (The names of the project leaders Saoshi and Satoshi differ by one letter, maybe he has a big innovation :-). At present, smart contracts and the Lightning Network all increase transaction volume at the cost of sacrificing its security, but they cannot actually solve the problem of commercial applications. Without highly secure blockchain, storage and transmission, there can be no widespread commercial applications.

The entire BPB system adopts multi-layer, multi-level intelligence learning, address reputation, RSA key authentication, and multiple PKI security lines of defense. Large and business customers can choose the high security level settings, and can customize the design and choose which kinds of defense lines to use. BPB puts the verification, vulnerability and attack defense algorithms on the second layer. At the same time, the second layer uses MacroSQL real-time cluster database to achieve real-time data consistency, which simplifies the processing of synchronization and data correctness, and engineers can focus more on the verification of data logic. Data consistency is handed over to the MacroSQL cluster database to deal with. The security of layer 2 and 3 are designed by Juniper network security experts. There is also IDS, an online IP packet monitoring system developed by MacroSQL which monitoring real-time hacking and risky operations. Alert operator with email and phone message when hacker get in. In this way, a multi-layer real-time monitoring system is responsible for the security of the second and third layers.

Not only can the second and third layers of the blockchain monitor the correctness of the system, the second and third layers also complement the deficiencies of the Bitcoin's code check; jointly complete data correctness monitoring and credit monitoring. The first-level PKI user private key signature can confirm a single transaction very reliably, but it is not absolutely unbreakable; SHA256 can keep the block difficult to reverse, but it is also difficult to deal with quantum computers. Adding 2, 3 layers of software to collaboratively enhance the data consistency of the entire system, can make full use of all the advantages of the Bitcoin network. At the same time, it enhance automatic audit and supervision logic code to strengthen the maliciousness resistance and correctness of the network. Considering the second and third layers as the expansion and enhancement of the underlying blockchain data verification system. The third layer also has a banking and payment function. At the same time, the first layer retains some people's requirements for complete anonymity in certain circumstances. Together, the three layers form an enhanced version of the blockchain, thereby solving the defects of the blockchain system.

Moreover, the security mechanism of the banking system is introduced to address the absolute security requirements of commercial applications and individual users. This three-tier structure can fully integrate the existing advantages of the Bitcoin blockchain itself, while taking advantages of the cluster database and advantages of the banking system. These together enable BPB to fix the Byzantine defects.

This system has the following advantages:

1. All are multi-signature addresses, anti-hacking.

2. When registering, download the RSA private key/PKI (the world's strongest encryption algorithm) as the ultimate master lock, which can lock the entire account, lock and unlock various functions. The RSA file is downloaded during registration.

3. The third layer adopts PKI/RSA dual private key (twice) encryption management to increase the disaster relief options for customers, while also give customer options to manage their private key.

4. Adopt most of American banking security features and further increase these security settings, using the most secure computer language as the front end, and the most efficient technology as the back end. All of them are built from scratch by engineers who have been in the United States for more than ten years with doctors/masters degree, and bank & credit card experience.

5. The 3-layer firewall is designed by Juniper experts, and the online intrusion detection is developed in-house. The front-end DMZ, the back-end and the database all have a hardware firewall layered and network zone-partitioned.

6. Because hackers can apply to become employees, and employees can also become hackers. So online IPS monitoring is necessary. BPB also uses its own high-speed intrusion detection technology to analyze IP content and automatically alert suspicious IP packets. At the same time, it incorporates commercial firewalls for real-time online monitoring services. Intrusion detection can more accurately see the content of internal and external intrusion IP, and can record the intrusion details. It automatically sends emails to alert the staff on duty to prompt suspicious operations, and attach the details of specific suspicious operation commands. In addition, with one-way encrypted information, multi-signature multisig authorization, so even if a hacker breaks in or steals address or password, they cannot get multiple authorizations.

7. At the same time, 99% of assets are stored in offline wallet with all incoming connection prohibited, and multiple backups are encrypted for separated storage. The number of incidents of traditional bank theft is one hundred times less than that of blockchain. Of course, the bank is a closed system and the danger is much smaller. An open blockchain system actually requires extremely high-end code security design. We believe that the security, reliability, and fault tolerance of a blockchain system are far more important than any other things. If asset security is not guaranteed, the Byzantine loophole is not resolved, and the wallet is not resistant to disasters, there will be no possibility of widespread commercial application. BPB uses multi-signature addresses, fingerprints, face recognition, RSA keys, other multiple verification and AI automation can also reduce human error, theft, and reduce labor costs. Moreover, it gives customers the option of full anonymity and full decentralization of the blockchain. The algorithm details of POWSC will be announced after project completion.

8. Introduce the weight factor of high-confidence nodes such as ECC in mining. Without ECC, what you type in may not be the same as what is actually sent. For block calculation and partitioning, BPB slightly increases the weight of ECC chips and hardware, and credibility. A gradual accumulation trust algorithm is adopted for new nodes. This can deter potential sabotage attempts and encourage good behaviors.

The above forms a multi-layer approach to jointly solve the Byzantine loopholes, the security of the wallet, and ensure that the system is as robust as bank while keeping openness and transparency. These collaborate to achieve 100% reliability that is required by a wide range of commercial payment applications.

3. Operating Model:

Currently, the global average population participation rate of the cryptocurrency market is about 0.1%. China and many other countries are starting to issue central bank digital currencies to compete with existing digital currencies such as Bitcoin. After central banks issuing CBDCs, this market will be even larger. Our founder funded most of the cluster database and blockchain research and development. The BPB utility token will enhance the R&D activity and speed up the development. We think that technological innovation is the core of our company, so our general operation is focusing on cluster database development and technology, while developing blockchain project for external identity to operate (sell product and let other identity to operate service). We do not get involved into how BPB is distributed or sold. The payment platform is profited from transaction fees.

BPB has the advantages of fast speed, low cost, no Byzantine loopholes and participating in various commercial links. For example: retail payments, games, coupons, esports. So we will continue to develop and explore this market. MacroSQL Technology and BPBtc Technology are mainly responsible for developing cluster database and 3-layer block chain network. In addition, cluster database high transaction performance advantage can also accelerate other main digital currency, fiat, central banks digital currencies. Leveraging on our high performance and low cost cluster databases, we aim to become a decentralized hub for the world's retail and commercial transactions. For details, please email: biz@macrosql.com

4. Project progress:

The payment transaction website and the background transaction system are now in operation, so you can experience the amazing high speed and security. The BPB platform currency network trial run payment transaction platform currency called BPB/BPBtc, research and development were started in September 2017, trial operation was started in January 2019. In August 2020, it was formally named as BPB (Bullet Proof Bitcoin), in order to reflecting "vulnerability-free Byzantine cross-chain Bitcoin" more intuitively. Those who are interested in the project can support the research and development by purchasing BPB. BPB issued 200 million, mining 10 million, and the total limit of 210 million is written into the blockchain. See the official website https://bpbtc.org and blockchain browser https://bpbtc.net for details. The progress of the project is as follows:

September 2017：Research and development began.

January 2018: The first layer of bitcoin network architecture was improved.

November 2018：The first layer of Bitcoin multi-signature automatic management system was improved.

January 2019：The three-layer security development was completed.

January 2019: BPBtc.com (now renamed as https://bpbtc.org) began trial operation. The platform has transaction functions and automatic management of multiple signatures.

September 2020：The security system was perfected and the blockchain browser https://bpbtc.net was opened

November 2020：The second layer of acceleration system and non-code scanning payment function.

November 2020：The second layer of acceleration system and mobile payment function will be completed.

December 2020：The cluster database and the second layer of acceleration system and mobile payment function will be completed.

February 2021：The mobile phone payment function will be completed.

March 2021：We will add the functions of docking legal tender, transaction, retail and mobile payment.

5.Team：

Tang's main research interests are data, databases, distributed databases, i ncluding Spark, Spark SQL, Spark Core, Postgres. Dr. Mingjie graduated from P urdue University in Purdue University with PhD in Computer Science. Linkedin

Dr. George Zhao's interests are mainly in the fields of big data, big data analysis, c luster database, payment and so on. George was previously responsible for big d ata analytics and risk analysis at Paypal. George is a Ph.D. in computer science gra duated from the New Mexico Institute of Mines. Linkedin

Symon Chang: Advisor. The founder of Tyan Server, former General Manager of In tel Shanghai, PhD from Stanford University, bachelor of Science from National National Taiwan University.

Tammuz Dubnov founded Zuzor, an Experience-Driven Digital company with a pro prietary system that generates interactive graphics in real-time from movement. Tammuz graduated with Honors in pure Mathematics with a minor in Computer Science and Dance, from University of California, Berkeley. LinkedIn.

Zhang Yang, Responsible for financial accounting and financial media, Master in Trinity College Dublin, bachelor in Southwest University of Finance and Economics, linked in.

Yun(Leo)Liu has over 20 years of experience in finance, e-commerce, machine learning, online travel and web services. Yun graduated from Iowa State University in 1996 with a master's degree in statistics 1996 – 1999 Linkedin

David Liu specialized in hardware and software limitation and real-time programming. He had worked on Intel's 1/billionth of a second CPU internal monitoring technology to improve performance on various databases. He has a M asters in computer science with straight As from RPI at Troy, NY. Linkedin

Mikhail specialized on intrusion detection and computer security, crypto algorithm s, he will be focusing on the security of wallet and network. He has PhD in Comput er Security & Artificial Intelligence from University of Texas at Austin with GPA 4. 0/4.0. Linkedin.

Other network security experts and consultants do not elaborate here.

6. Investment Risk and Responsibility Exemption:

Policy risk is the biggest risk for crypto digital coins. At present, only Japan and Switzerland legalized crypto coins for general shopping, while most countries have limited commercial applications. On Sep 21, 2020, U.S. federal regulators and SEC back digital dollar stablecoins(even so, we still will exclude all US citizen until more clear SEC rules). The second risk is whether our platform will win the competition and serve our community well. What we can commit is that we target to make BPB the best digital coin. Currently, 90% of virtual coins are released via Ethereum platform without any research and development or innovation. It has been mentioned above that all smart contracts cannot overcome the problem of security and non-deterministic algorithms brought about by large virtual machines. The BPB is based on the bitcoin-based code that has been developed on top of Bitcoin, and has solved Byzantine vulnerabilities. It is based on our own clustered database and fault-tolerant server network, but the first layer is still fully decentralized and is 100% the same as the Bitcoin protocol, with the second and third layers greatly enhanced in terms of speed, transaction fees and security.

As with any investment, and especially in new products or ventures, there are risks. Even though our team has some of the best technical experts, and we are fully committed to do our best to make BPB our life-time achievement, the future is still mostly unknown to us, and we can’t guarantee company profitability, investment profitability, or guarantee that the BPB price will increase or stay in certain range, or that we can beat our competitors. Investors have to study carefully and compare us with other competitors to make their best decision.

BPB is an utility coin and a digital product on our platform. Coins themselves doesn’t contain shares of the company, nor enjoy any profit from the company. Product value of the coin is exchanged based on group behavior and how people value our platform service and their consensus to pay for it. It also affected by many other factors such as supply and demand, community efforts to improve the platform and R&D money raised from community. Same as Bitcoin, BPB coins are not a legal tender, and their value is not backed by any physical items, issuers or the real economy. We have no way to guarantee the value of the coin.

7. Description:

Frequently Asked Questions has many more detailed information that investors should read. Investors can write to biz@macrosql.com for private placements and pre-sale prices. The latest information can be found on the official website and blockchain browser or official Telegram group:

Official Telegraph group: t.me/bpbtc_org (Need to paste into a separate browser to open)

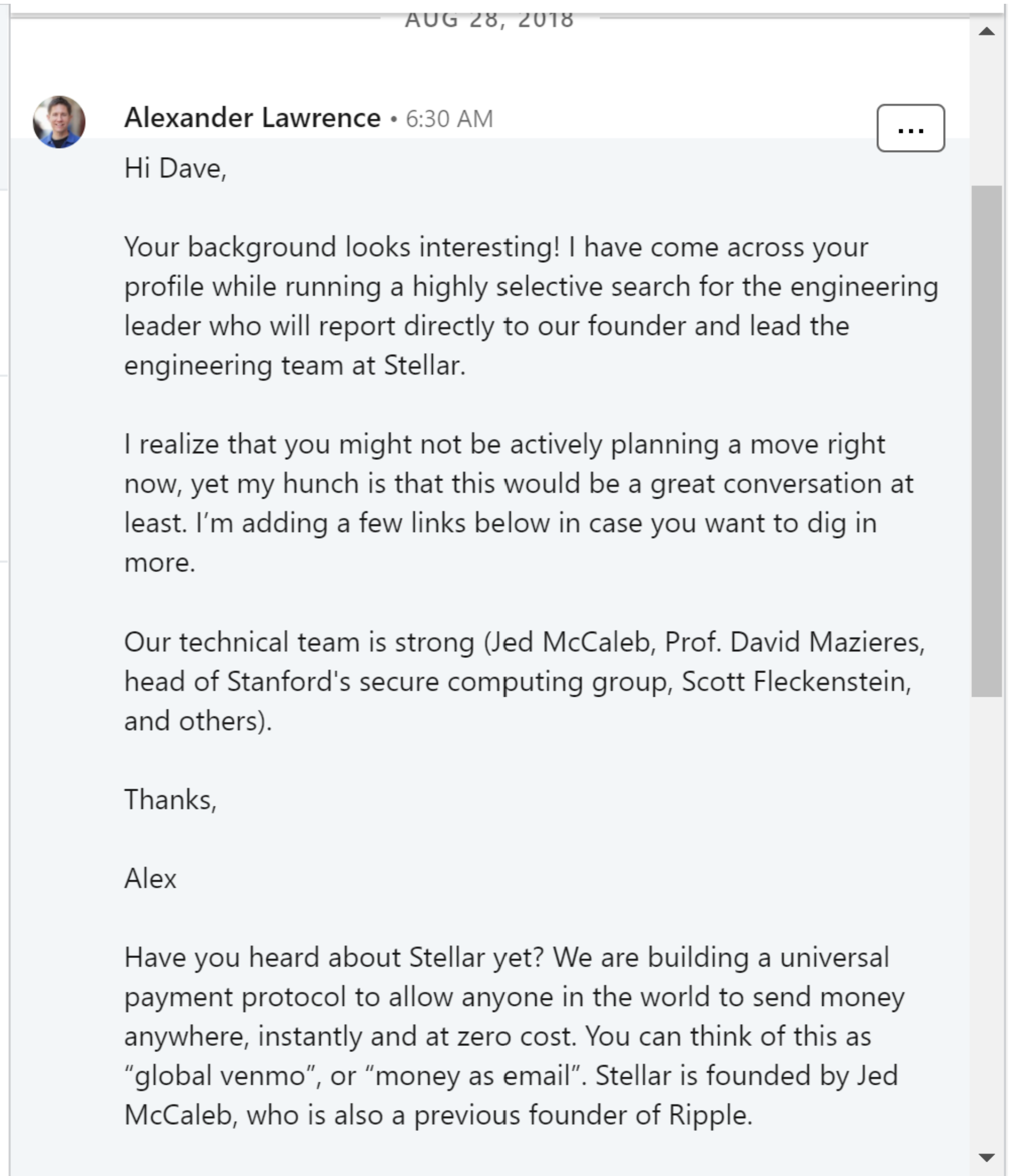
Official website: https://bpbtc.org

Blockchain browser: https://bpbtc.net

8. Team reputation within the cluster data and blockchain industry:

Dave, who is the founder of our team, has been researching database limits and chip limits for years at Intel, Oracle, and MarkLogic. He is an expert in fast, reliable database transaction. McCaleb and Stanford professor David Mazieres invited him to lead the Stellar technical team. McCaleb is the founder of the world's first blockchain exchange which is Mt. Gox, and he is also the founder of Ripple, Stellar.

Below is the invitation letter:



AUG 28, 2018

Alexander Lawrence • 6:30 AM

Hi Dave,

Your background looks interesting! I have come across your profile while running a highly selective search for the engineering leader who will report directly to our founder and lead the engineering team at Stellar.

I realize that you might not be actively planning a move right now, yet my hunch is that this would be a great conversation at least. I'm adding a few links below in case you want to dig in more.

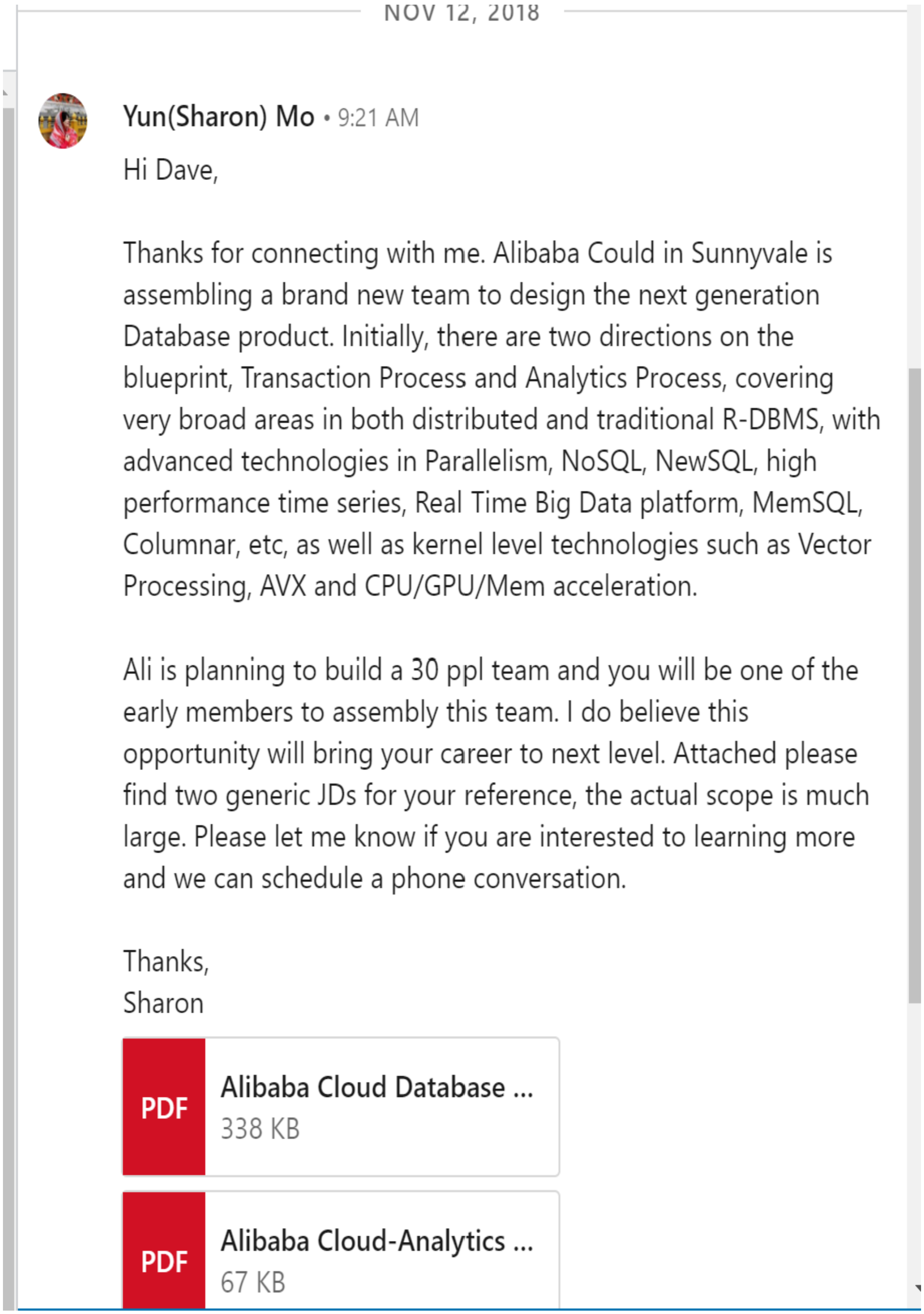
Our technical team is strong (Jed McCaleb, Prof. David Mazieres, head of Stanford's secure computing group, Scott Fleckenstein, and others).

Thanks,

Alex

Have you heard about Stellar yet? We are building a universal payment protocol to allow anyone in the world to send money anywhere, instantly and at zero cost. You can think of this as "global venmo", or "money as email". Stellar is founded by Jed McCaleb, who is also a previous founder of Ripple.

Below is the invitation that Alibaba invited Dave to set up a clustered database team next to his home in California:



NOV 12, 2018

Yun(Sharon) Mo • 9:21 AM

Hi Dave,

Thanks for connecting with me. Alibaba Could in Sunnyvale is assembling a brand new team to design the next generation Database product. Initially, there are two directions on the blueprint, Transaction Process and Analytics Process, covering very broad areas in both distributed and traditional R-DBMS, with advanced technologies in Parallelism, NoSQL, NewSQL, high performance time series, Real Time Big Data platform, MemSQL, Columnar, etc, as well as kernel level technologies such as Vector Processing, AVX and CPU/GPU/Mem acceleration.

Ali is planning to build a 30 ppl team and you will be one of the early members to assembly this team. I do believe this opportunity will bring your career to next level. Attached please find two generic JDs for your reference, the actual scope is much large. Please let me know if you are interested to learning more and we can schedule a phone conversation.

Thanks,
Sharon

PDF Alibaba Cloud Database ...
338 KB

PDF Alibaba Cloud-Analytics ...
67 KB