Tangrum:
A Next-Generation Decentralized Computation Platform

By Roy Zou

The Blockchain world is a permissionless, innovative field. We can see many awesome projects playing in this disruptive sector. After the great success of Bitcoin and Ethereum, we may think what's the next big thing after Bitcoin and so-called Next-Generation Smart Contract Platform Ethereum? Is it enough for our imagination and tailed for specific sectors in the future?

Backgrounds

Bitcoin is peer-to-peer electronic cash system. "The specific failure of Bitcoin is particularly concentrated in one place: scalability." Bitcoin is a currency focused Blockchain, Vitalik said, this world needs a Turing-complete language platform he named it as Ethereum later, "a superior foundational protocol, and allow other decentralized applications to build on top of it instead of Bitcoin, giving them more tools to work with and allowing them to gain the full benefits of Ethereum's scalability and efficiency."

Here is the question: we have Bitcoin and Ethereum now, seem that we are going to build a bright human future building on top of them, one for a general global currency, the other one is for general platform to build almost all applications using the smart contract, which Ethereum brings to this platform. The only thing rest we need to do is to create all sort of stuff on this so-called "fundamental protocol". Is that true? Obviously, Vitalik is a really brilliant guy and having a big ambitious for the future. He has some abilities, looking through something to find the fundamental flaws. We have to admit that Satoshi and Vitalik created a world where we can build a better future basing their efforts. Definitely, we need innovation in any period time. Here we introduce our project named Tangrum.

What's the problem with Bitcoin and Ethereum?

Bitcoin, as described by Vitalik, "The specific failure of Bitcoin is particularly concentrated in one place: scalability. Bitcoin itself is as scalable as a cryptocurrency can be." Bitcoin protocol itself is specifically designed for the currency token: Bitcoin, if you want to develop a more high protocol on top of it, it becomes extremely complicated or even impossible. This is also the main reason for the current block size scale dramas. Community can't make a deal with the direction of Bitcoin: a currency or a payment application. Bitcoin as a protocol is good enough for storing value, but as a scalable protocol for more advance application, is far beyond the ability of Bitcoin protocol.

Another big issue of Bitcoin is Centralization. The top 5 mining pool controls nearly 80% of Bitcoin hashrate and some own millions of Bitcoin. Having figured out the systemic problem with Bitcoin, Vitalik has come up with a new solution for it: "a cryptocurrency network that intends to be as generalized as possible, allowing anyone to create specialized applications

on top for almost any purpose application, the only limitation is your imagination." This is Ethereum. From the response of community and tons of applications are building on Ethereum platform right now, Ethereum seems be the most successful platform so far. It brings many possibilities which are difficult to achieve on Bitcoin. For the foreseeable future, Ethereum will become more and more popular and releasing its powerful potential for the blockchain technology. Another big contribution of Ethereum is forming a common design philosophy, layer structure: different layer for different level protocol like Internet. This structure proves its right due to the successful of Internet in the pass 3 decades.

Ethereum has a good philosophy for designing the protocol, but with a crappy methods.

In our perspective, Ethereum still used the old school principles to try to solve some totally new puzzles. In our eyes, they are just combining some old methods to fixing the boat, like Bitcoin itself. We all known Satoshi combine the old knowledge like cryptography and mathematics in a new way to come up with a peer-to peer electronic cash system. Ethereum has the same problem. One of most innovative is adding a Turing-complete language. Why we still need another Ethereum-like platform or even a better platform? We have Javascript, a universal, Turing-complete programming language. Why do we still need Haskell, wolfram language? Do we really need another search engine beside Google, just like Baidu (a very successful search engine in China)? Why Wechat (initial release on January 21, 2011) still be created even we already had WhatsApp (initial release on January 2009) two years later? Many other cases like Taobao vs Ebay, QQ vs ICQ. We see Ethereum as ICQ, a revolutionary product but not the last one to stand in the market. In China, QQ is the king (Wechat is from the same company Tencent), because we believe that we can make better products. NEVER STOP INNOVATION is the key spirit of our

society! Permissionless is the key characteristic in technology field. “Ethereum does not intend to be the end of all cryptocurrency innovation; it intends to be the beginning.” Vitalik said.

What is Tangrum?

Tangrum is a project to be the one having many advanced features blockchain platform, a general decentralized Computation Platform. The main features include a mathematical proved Proof-of-Stake consensus algorithm, a Secure Multi-Party Computation (MPC) protocol named Gastromancy Protocol, a general multi-paradigm knowledge-based programming language named Tangram, tailored for Internet of Thing, on-chain governance voting system, etc. One of targets of Tangrum is to offer a decentralized blockchain platform with a feature built on it for over 77 million companies (still growing at a rate of 11.8% per year) in China.

We will build a digital virtual society on the top of Tangrum, driven by a decentralized community.

Technology

Wuji PoS

We are developing a totally new Proof-of-Stake algorithm named Wuji, a sophisticated and mathematical proved safe Proof-of-Stake inspired by a research paper named iChing: A Scalable Proof-of-Stake Blockchain in the Open Setting (or, How to Mimic Nakamoto's Design via Proof-of-Stake). Wuji would be used to create a scalable and secure Blockchain. Bitcoin, backed up by a large-scale network of miners via proof-of-work mechanism, has proven to be a very successful blockchain project as a peer-to-peer electronic cash system. Unfortunately, these miners consume huge amount of resources (electricity and computing hardware). To address this issue, alternative blockchain constructions via proof-of-stake mechanism have been proposed. Unfortunately, those proposals either lack of security analysis or cannot scale to a large network of nodes in the open network setting where new players can safely join the blockchain protocol. Comparing with Proof of Work (PoW), no computing power will be consumed and no expensive silicon equipment will be invested for mining blocks in Wuji. There is no traditional heavy cryptographic protocol is engaged in Wuji, such as Practical Byzantine Fault Tolerance (PBFT), so it can be used to build a genuine scalable public blockchain system. Wuji adopts a very simple best chain strategy, the same as in Bitcoin, which is longer is better. Wuji is a provable secure protocol under the honest majority of stakes assumption. We believe the real recourse such as computing power can be replaced by virtual resource such as stakes efficiently.

Gastromancy Protocol

We firstly introduce an advance computation protocol named Gastromancy Protocol to develop some systems such as on-chain governance voting system, on-chain auction, especially privacy-preserving data mining system for future enterprise applications. This protocol is built by secure multiparty computation cryptography. Secure multi-party computation, or MPC, also known as privacy-preserving computation, offer high performance of efficiency, security and privacy. It is one thousand times faster than homomorphic encryption. It was developed from a secure two-party computation (2PC) which is intended to resolve the so-called Millionaires' Problem. Andrew C. Yao described a problem like this: two millionaires wish to know who is the richer and two of them don't want to let others know how rich they are. Mr. Yao developed a protocol for resolving this task. He introduced a two-party computation (2PC) later. Secure multiparty computation, we named it as MPC below, is developed on this 2PC theory. MPC is intending to resolve some tasks like this: more than two parties put some money into the pools to jointly predict some events like president election to see who will win. In general, we can describe this scheme as they jointly compute a function over their inputs. And they all don't want to let others know how much they put on this auction. For solving this question without third parties, secure multiparty computation (MPC) is introduced. MPC can be described as a simplified mathematical model below.

Given a set of participants, define as P1, P2, P3, ...,Pn

And each participant has their own input data, define as D1, D2, D3, ..., Dn

The mathematical model would be described as:

F(D1, D2, D3, ..., Dn) = def(D1, D2, D3, ..., Dn)

You can define def from as simple as who is the biggest number to some complicated questions wrote by smart contract. This computation protocol itself won't release information more than the output (or outputs). This computation protocol should be mathematical-proof secure. We are going to develop a secure multi-party computation protocol. We must know that most of cases would not be ideal situations. It means some parties would play bad when they are going to jointly participate some events. We must find out a well-resolved protocol for our on-chain systems. Combining with the Wuji Proof-of-Stake system, Tangrum would be developed into an effective and practical computation platform. It would benefit a lot for the enterprises in the future. Company can run part or all of their businesses on Tangrum.

Tangram Language

The most popular smart contract language Solidity to comply the EVM (Ethereum Virtual Machine) bytecode. It claims to code every program. It is actually a Javascript type language. Actually, Solidity is very difficult to write secure code. See what happen to Parity Multisig attack. Parity is claimed to be a very talented team to write the best client for Ethereum, but the disaster still happened again and again. Solidity has many disadvantages for coding a general smart contract. It is inefficient, low security, hard to check right.

Tangram is a symbolic discourse language which is developing by Gödel labs to fundamentally resolve the problems that Ethereum faces attacking again and again. From the DAO attack to Parity multisig attack. At the same time, Tangram is a knowledge-based programming language which can easily write a logical law and complicated computational contract.

Blockchain of Things

Tangrum will be designed into a practical platform to unlock the potential of Internet of Things, which we call the Blockchain of Things. The current Internet of Things (IoT) has a poor interoperability across platforms. Data silos, high costs and limited market potential make IoT technology hard to enter the mainstream markets. A blockchain based web of internet can reduce the cost efficiently and bring many advanced features like machine-to-machine payment, a unique crypto-ID for every item and unfakable data.

AI-on-Chain

You can't deny that AI and blockchain are two of our future technologies when we are looking at the pace of innovation. Tangrum will be revolutionized into a decentralized intelligence platform combing the artificial intelligence and Blockchain technologies. AI will be Tangrum's fundamental technology when we are developing a smart coding language Tangram and Blockchain of Internet. Except that, an AI-powered Blockchain will bring a new level computational ability to Tangrum.

Blockchain has some born weaknesses like security, scalability, efficiency, privacy, Energy consumption, accessibility, etc. AI also has some problems with trustworthiness, effectiveness, high market barriers, catastrophic risks etc. These two technologies can improve each other to be the powerful technologies in the coming future. Blockchain brings the trustlessness into AI and AI can help build a machine learning system on Blockchain.

In a nutshell, Tangrum brings a decentralized intelligence for our society. We are redesigning the entire sky of technology from scratch through releasing the full potential of AI and Blockchain technology.

Here are the main features of Tangrum will be developed in the future:

Features	Functions
Full decentralization	A censorship-resistant network without any third party interruption to deploy the any sort of applications.
Mathematical proved Proof-of-Stake algorithm	A total new Proof-of-stake consensus algorithm named Wuji.
Blockchain of Things	Offer a new autonomous machine economy, enable IoT to be the basic infrastructure of our society.
Tangram Language	A general multi-paradigm knowledge-Based Programming language named Tangram. It will make Tangrum to be the most powerful blockchain platform ever.
Multi-layer	Separate account, value transaction, contract process, Dapp interface into different layers.
Crypto-ID built-in	A general smart contract type identification system called CID for all application to use;
On-chain Governance	Community initiated fair, powered by an advanced voting system for on-chain governance.
Regulation Compliance	The best platform for enterprises to fit the regulations.
Stealth Transactions	Zero-knowledge transaction alternative.
Compatible with other platforms	You can run the same smart contract in different platform like Ethereum, EOS
Tailed for business & organization	Tangrum will be the first choice to build the enterprise decentralized blockchain applications;
A future digital Society	Tangrum will be the network to build a new digital society on it, where you can own your digital ID (Crypto-ID), storage your personal data, sharing documents, and even an organization (company) on it.

Driven by Community

Tangrum is a truly decentralized project promoted by community. Foundation, Gödel Labs will be two of these participants in this ecosystem.

Tangrum Foundation

Tangrum Foundation will working with the whole community to promote it as a most decentralized community. Tangrum foundation will be the watchdog of technology roadmap. Complied with the different jurisdiction regulations, enable the cooperation and the adoption with off-chain industries like traditional financial sector, agriculture and the most industries.

Gödel Labs

Gödel Labs will be the main development team to build Tangrum as a decentralized computational Blockchain platform. The main technologies are **Wuji**, a mathematical proved Proof-of-Stake; **Tangram** Language, a general multi-paradigm knowledge-based programming language; AI-integrated, TVM (Tangrum Virtual Machine), wallets, and other designed for future blockchain components.

Core Team Members

Roy Zou

Chief Blockchain Engineer

Twitter: https://twitter.com/bitkio_royzou

Github: https://github.com/zoulaihui

Owned a master degree of controlling engineering, be involved in Bitcoin and Blockchain community since 2011, Roy is one of the founding member of Dogecoin and Ethereum Classic community, Ethereum Classic ETCDEV Team advisor and General Secretary of Ethereum Classic Consortium.

Roy is an entrepreneur, advisor & investor of Blockchain startups and founder of BITKIO & Gödel Labs.

Bernhard K. Meister

Blockchain Researcher

https://www.researchgate.net/profile/Bernhard_Meister3

Bernhard held a PhD in theoretical physics from Imperial College, London, and was an associate professor at People's University of China in Beijing. He is teaching part-time quantitative finance courses at the Chinese University of Hong Kong.

Bernhard started his career as a fixed income proprietary trader at Goldman Sachs and subsequently worked at various financial institutions to acquire exposure to a wide range of financial products. Bernhard has extensive experience as a consultant, initially at McKinsey & Company, and later for companies like China Construction Bank and Yahoo! Japan.

Fanfei Chong

AI Researcher

Linkedin: https://www.linkedin.com/in/fanfeichong/

Fanfei held a PhD in Mathematics from Vanderbilt University. He is an experienced Statistical Analyst with a demonstrated history of working in the financial services industry. He is proficient in building predictive model using Machine Learning algorithms in a variety of settings, including credit risk model, scorecard model, and image-recognition.

Stewart Mackenzie

Developer

Twitter: https://twitter.com/sj_mackenzie

Github: https://github.com/sjmackenzie

Stewart Mackenzie is the founder of Fractalide. Stewart has programmed computers in multiple industries such as security, making use of cryptography, logistics, and control systems and most recently in the cryptocurrency space a member of the Ethereum Classic development team. He enjoys programming language theory in particular purely functional programming languages and distributed programming languages. Stewart studied computer science in the University of Johannesburg, South Africa, and in his spare time tries to have fun building ion traps.

Iven Li

Developer

Github: https://github.com/onlyerlee

Iven have over 13 years' experiences in java development and system architecture has been in Shenzhen Kingdee R&D center, Shenzhen Yougou online mall R&D center. Proficient in big data processing, distributed computing and high concurrent cluster architecture.

Treasury

Tangrum is learning the lessons from other communities like Dogecoin which the development team lacks off the fund to support their. 20% of block reward will be given to a treasury fund automatically to support the future development of Tangrum project. This will based on a decentralized treasury accessed through the on-chain voting mechanism by token holders. This fund can be used to community building, promotion activities, enterprise partnership and the future TIPs (Tangrum Improvement Proposals).

Governance

This is a community management base on an on-chain governance system, including a decentralized blockchain-based governance model to upgrade the protocol and funding the whole ecosystem in the future. Token holders have the right to vote on community proposed TIPs (Tangrum Improvement Proposals).

Roadmap

Hundun

Q1 2017 Project initiated;

(The former name of project is Tangreum);

Pangu

Azure Dragon

Q4 2017 Project launches;

White Tiger

Q1 2018 Tangrum Contribution Period;

Vermilion Bird

Q1 2019 Tangrum mainnet launches;

Black Tortoise

Q1 2020 Gastromancy Protocol deploys;

Tao

Leibniz

Q1 2021 Tangram Language launches;

Gödel

Q1 2022 AI-enabled Tangrum is ready for the world.

Long March

Apparently, Tangrum is a massive project like Ethereum. It would take us years and years to develop. We now have a dedicated development team consisting members including the university professors, long time cryptocurrency developers, high talented programmers and blockchain engineer. We've already done some research on consensus algorithm and TVM (Tangrum Virtual Machine). There is still a long road to develop this project for us.

Vision

We are not going to replace Ethereum, Tangrum can be seen as the next-generation of Blockchain platform. We are seeking some talented guys to join us. To build a better future for this society. We are going to shape a Brave New World.

------end------