Polestar
White paper

Table of Contents

Introduction

Digital currencies are often called cryptocurrencies due to the intricate technical details related to cryptography, but it did not start here. When looking back at human history, from the cowry shells of the Asian region to the first coinage in ancient kingdoms, mankind first saw printed money in medieval times. This breakthrough was followed by modern-day electronic versions of money.

Today, there is an international banking ecosystem, which consists of banknotes, credit/debit cards, derivatives, stocks, bonds and much more. It was a combination of human ingenuity and societal commitments that drove the need to come up with innovative solutions to tackle the most intricate concept of human interaction handling the exchange of value.

Cryptocurrencies represent the next level in the evolution of money. The technology behind this new form of money called blockchain. It is entirely driven by math and is completely decentralized. Most notably, unlike all previous forms of money, cryptocurrencies are not able to be manipulated. It is essentially money 2.0. Blockchain is experiencing a period of exponential growth and adoption, not unlike the collective transition towards internet use in the 90's. Established in 2008, Bitcoin is a cryptocurrency based on blockchain. In just a matter of years, it has become a legitimate and tradable commodity on a global scale. It has massive liquidity with billions of dollars of Bitcoin traded and used daily. This exceeds the GDP of many sovereign nations. In fact, the market capitalization of Bitcoin now exceeds that of Goldman Sachs.

There are 16 million Bitcoins in circulation among thousands of holders. Bitcoin is only one of the more than 1,700 cryptocurrencies available for people to buy, use and trade. These other coins are known as altcoins. Many are based on the Bitcoin platform, others on highly liquid Ethereum and Litecoin. The features of the coin vary widely from practical to practically useless depending on the underlying technology. However, there exists a dramatic misalignment in the metamorphic shift to digital currencies. The major underlying problem is that traditional financial institutions and the related governing and operating regulations are not well aligned with cryptocurrencies.

The concept behind public banks was designed and conceived hundreds of years ago. This is the early stage of a transition towards the decentralization of the financial world. But there is resistance. The powerful and entrenched institutions are not keen to transact in cryptocurrency. And the influence of powerful special interest groups ensures that traditional banks do everything possible to reject this new form of capital. However, blockchain technology makes the adoption of cryptocurrencies possible. It is mathematically fluid and moves much faster than a central bank, a regulatory body or international fiscal treaties.

Currently, there exists an intermediate "limbo" state whereby many cryptocurrency holders are unable to benefit from the corresponding economic value. There must be a solution to this critical problem that is affecting a rapid increasing amount of people.

Polestar's platform has been designed to combine the strengths of an established banking institution with the flexibility and future-forward potential of cryptocurrency. The network enables the exchange of Bitcoin, Ethereum and other major cryptocurrencies by bridging the transition gap to fiat. It also enables unfettered user access to cryptocurrency funds at merchant point of sale locations and ATMs worldwide. Pending conclusion of bank transition, users will have the ability to store Bitcoin and other cryptocurrencies in a secure and insured wallet similarly to how customers at a typical bank account are provided for via fiat accounts.

Positioning

Information and Communication Technology companies and existing financial distributors expect simple payment services to generate new revenue business.

Even simple payment service providers expect to create a new revenue source by integrating various services within their systems such as money transfer and insurance sales, since the system users increase.

And all financial providers tie their system closely to their customers in order to collect 'big data' such as consumption patterns and temporal demand, and use this to drive future business models, or to realise further revenue streams by on-selling this data to other providers.

Polestar aims to fulfil these requirements for payment providers, delivering a completely decentralised, 'plug and play' peer-to-peer payment system that can be integrated with any financial provider, or receiver system quickly and easily, in order to facilitate crypto-payments for any products or services.

However, Polestar also aims to offer payment functionality through social platforms and, indeed, in its own standalone form (similar to PayPal for Fiat) and will easily integrate into systems via the Polestar strategic API, providing a simple payment service that anyone can apply it to his/her business.

There are many current examples of fiat-driven payment integration into social-media platforms and to mobile devices, such as:

Naver: provides one-stop payment service to establish Naver ecosystem that through Naver ID, such as shopping mall, merchant, and other Naver service in Naver website

Samsung Pay: payment Service is transforming into a service platform by linking famous shopping malls and providing rewards service.

Kakao: establishes and expands its business platform by linking its service, content, and payment system.

Major ‘simple payment’ service companies provide easy payment methods by linking their simple payment services to various services and provide circumstances where users can experience and stay in the ecosystem of their service through such an offering.

Polestar aims to deliver a platform consumable by social-media platforms, mobile devices and by any simple payment provider that wishes to easily and instantly integrate crypto-payment functionality to their existing offerings!

At this point it is worth considering the size of this market, to realise the value that Polestar will bring:

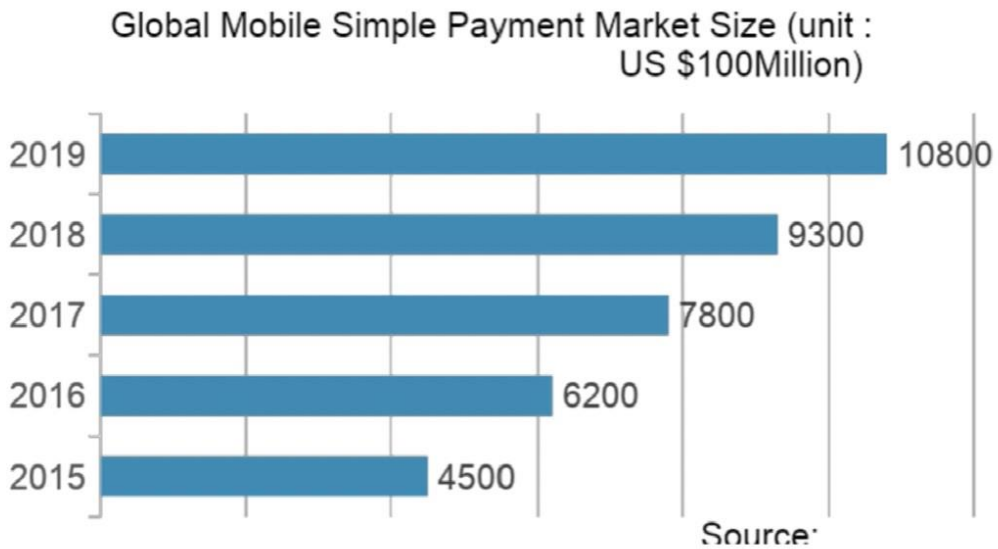


Figure 1

As you can see, in just one of our target sectors, the potential market is enormous. If we can capture even a small percentage of this market, Polestar will be massively successful.

At this point, it is now worth taking a look at the detailed list of the features we are aiming to deliver from the Polestar ecosystem, since compared to any of our potential competition, we emerge very favourably:

Polestar Features Comparison

Name parameter	CRYPTERIUM	BANKERA	Bank 4YOU	change	CRYPTOPAY	TokenPay	Polestar
Token sale status	Finished	Finished	Finished	Finished	Finished	Finished	Ongoing
Funds raized	$51,1 mil	$151 mil	$8,1 mil	$17,5 mil	$18 mil	$24,2 mil	Just started
Time went since token sale was finished	11 months	10 months	9 months	14 months	14 months	12 months	0 months
24/7 support	✗	✗	✓	✗	✓	✗	✓
Mobile bank	✓	✗	✓	✓	✓	✗	✓
Crypto-exchange	✗	✓	✗	✗	✗	✗	✓
Credits	✗	✗	✗	✗	✗	✗	✓
Crypto-acquiring	✗	✗	✗	✗	✗	✗	✓
Bank transfers	✓	✗	✓	✗	✓	✗	✓
Bank deposits	✗	✗	✗	✗	✗	✗	✓
License	✓	✗	✗	✗	✗	✗	✓
Forex Trade	✗	✗	✗	✗	✗	✗	✓
Legal and consulting services	✗	✗	✗	✗	✗	✗	✓
Loans	✗	✗	✗	✗	✗	✗	✓
Cryptocurrency mortgage	✗	✗	✗	✗	✗	✗	✓
Crypto software for ATM	✗	✗	✗	✗	✗	✗	✓
Tokenized share trading	✗	✗	✗	✗	✗	✗	✓
Cryptocurrency Note Security	✗	✗	✗	✗	✗	✗	✓
Interface	✗	✗	✗	✗	✗	✗	✓
Card	✗	✗	✗	✗	✗	✗	✓
Ease of use	✗	✗	✗	✗	✗	✗	✓

Market Analysis

Cryptocurrencies

The market cap of all cryptocurrencies is $511 billion (as of 2/19/18) Trading volumes for 24 hours have reached $22 billion (as of 2/19/18)
Exact user figures are difficult to determine due to the anonymous nature of cryptocurrencies, but there are over 71 million addresses for the top five cryptocurrencies

There are 25 million BTC addresses, 27 million ETH addresses, 1.1 million Ripple accounts, 16.4 million Bitcoin Cash addresses, and 2.4 million Litecoin addresses.

There has been an explosion in the number of users on major exchanges:

Binance reached 5 million users on 1/10/18 Bitfinex reached 1.6 million users on 12/13/2017
Coinbase claims over 10 million users
Upbit announced 1.2 million users on 12/20/17

Digital Payments

Global non-cash transaction volumes grew 11.2% over 2014-2015 to $433.1 billion

This growth was driven to a large degree by developing markets, which recorded a 21.6% increase in 2015, while mature markets grew by 6.8%

Debit cards accounted for the highest share (46.7%) of global non-cash transactions, followed by credit cards, with 19.5% in 2015

Contactless payments (NFC) are expected to grow to $9.9 billion in 2018, an 18% increase over 2017.

The mobile wallets market is growing steadily, with mobile proximity payments expected to top $53 billion by 2019

In-store mobile payments are predicted to reach $503 billion by 2020, reflecting a compound annual growth rate (CAGR) of 80% over 2015-2020

Remittances

$53.7 billion was sent as remittances in 2016, mostly through firms like Western Union, MoneyGram, and RIA

Cross-border e-commerce market analysis

Recently, the e-commerce sector is expanding not only in Korea but also abroad, and the growth of the cross-border e-commerce market (CBeC) between countries has been remarkable.

The CBeC market is expected to grow rapidly from $233 billion in 2014 to $94.4 billion in 2020 (CAGR 27.4%).

The demand and timing for Polestar is perfect.

Competitor Analysis

There is a clear market need for the services Polestar offers, which has already bought some competitors to the space. Some offer quite good services, and we hope to see more reliable counterparties out there to work with. However, currently, there is a clear lack of legal and security focus among our competitors, which presents huge risk.

Of our competitors, only TokenPay has been awarded any kind of license, and put due focus on security. For this reason, we see them as our most serious competition.

However, TokenPay does have some shortcomings:

While security is a focus, and multi-signature cold-storage wallets do offer some protection, they don't entirely protect customers from potential hacks.

TokenPay is unable to offer wallet-to-wallet services for crypto transactions – and this is something Polestar aims to deliver from the very start. Most importantly, this feature introduces immediate peer-to-peer mobile transaction capability which we see as critical for mass adoption.

What will Polestar Offer?

The key deliverables for Polestar are as follows:

- MasterWallet with wallet-to-wallet services
- Polestar Service – integration between multiple payment providers
- Discount incentive system
- Complex Payment Services

Let's cover each of these in more detail:

The MasterWallet

As we have already covered, our closest competitor is TokenPay and they simply do not offer wallet-to-wallet crypto-transaction services within their ecosystem. We see this as a critical feature.

The MasterWallet will offer the following key functionalities:

- Security: Enhanced security with dual protection by utilisting the Samsung Knox security solution.

- Safety: Secure stability by applying the Samsung biometric identity authentication solution.

- Convenience: Asset recovery through mnemonic key even if mobile is lost.

- Scalability: Convenient asset transfer, not limited to specific regions and countries, due to the expansion of terminal and service nations of the Samsung blockchain keystore.

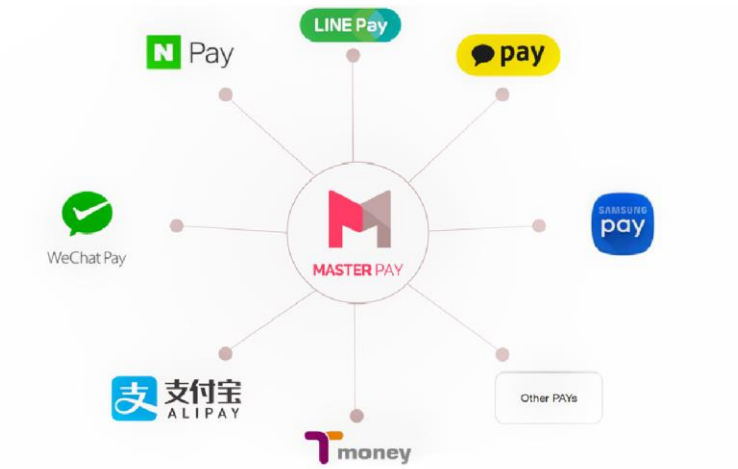
- Listed major coins such as Bitcoin, Ethereum, Ripple, BNB, USDT, which account for 90% of total transactions.

- Support for further MainNet-complete alt-coins will be added over time, and we should be able to realise further revenue streams from adding further coins, as the popularity and adoption of Polestar grows.

Polestar Service

This is the core of the Polestar platform - the capability to tie together many different payment platforms and facilitate the flow of payment between them.

Consider this diagram – it explains very clearly the goal here!

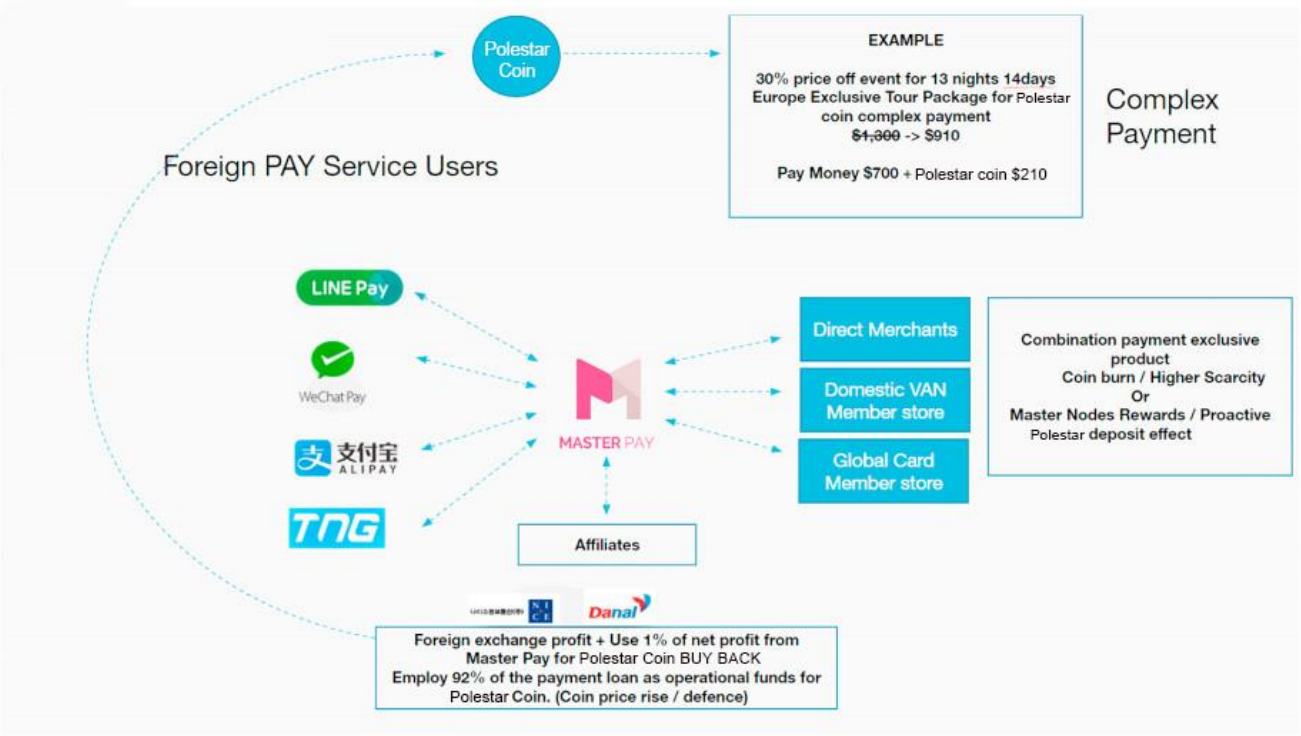


Discount Incentive System

We will offer built-in capability for providers to offer discounts for their services to encourage utilisation, and furthermore will incorporate a reward-based system to allow users to accumulate non-withdrawable Polestar tokens awarded for loyalty to the system, and providing the user with reduced cost of using the platform over time.

As our range of retail partners grows, the discount sub-system will increase and offer users a wider range of reward-based initiatives, which in turn helps promote our providers' products and services.

Complex Payment Services



Some examples of complex payment services that will be within scope of the Polestar system are:

- Foreign exchange profit using its exclusive license of Polestar(WONPAY) / Payment fee DOWN – “From 3.5% to 2.3%”

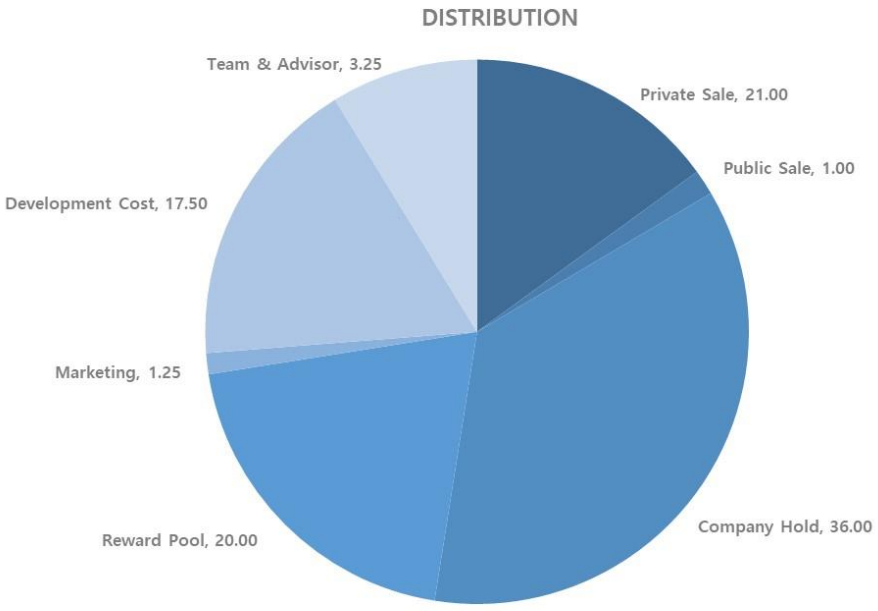
- Operate 1% out of 2.3% of the net Income for BUY BACK of Polestar and provide BTC, ETH etc., for rewarding Master Nodes of Polestar Coin

- Opening of Exclusive product only for Polestar Coin complex payment for Master Pay + Member

Token Economics

There will be 10,000,000,000 tokens generated on the Ethereum platform, yielding the ERC20format token.

The distribution of the tokens will be as follows:



	Volume	Percentage
Private Sale	2,100,000,000	21.00%
Public Sale	100,000,000	1.00%
Company hold	3,600,000,000	36.00%
Reward Pool	2,000,000,000	20.00%
Marketing	125,000,000	1.25%
Development Cost	1,750,000,000	17.50%
Team & Advisor	325,000,000	3.25%
Total	10,000,000,000	100.00%

The Polestar Token will be purchasable for ETH or BTC during the Token Sale. It is also possible that we will consider accepting other crypto-currencies.

The Polestar utility token will be used for internal transactions between all parties inside the Polestar (Polestar coin) platform.

Token Utilisation and financial model

Mechanics

- MasterPay is be a stable-coin crypto used within the platform and pegged to FIAT currency.

- Points for each Pay services can be exchanged for other pay points through MasterPay (SamsungPay, Alipay, Wechatpay, LinePay, Japan, China, Australia, Canada, Southeast Asia Pay etc.)

- Foreign currency received through MasterPay is Forex-processed, which can generate further profits from the foreign exchange process.

- Developing a different pay platform based on MasterPay and expect commission revenue reduces costs due to high bank fees and unfavorable exchange rates through MasterPay.

- The Polestar coin value will increase further by using 1% of the total currency generated in MasterPay as a resource of compensation for staking through the MasterNodePool

- MasterPay and Polestar Coin will be separated, and Polestar Coin value will fluctuate depending on supply and demand.

- Polestar coin will benefit from growing node volume and from the duration of participation in the MasterNodePool.

The final step:

Completing intelligent platform through AI deep learning based on 'big data' used by MasterPay platform, by consumers to generate detailed consumer-purchasing analysis and patterns. this accumulated data and related generated financial/purchasing profiles will offer a further revenue stream.

We also expect that the availability of these profiles will attract providers to the platform; we can offer the analysis to providers as part of the deal for their participation in the Polestar ecosystem, as an incentive.

Polestar Architectural principles

Security Considerations

Blockchains are inherently decentralized systems which consist of different actors who act depending on their incentives and on the information that is available to them. Whenever a new transaction gets broadcasted to the network, nodes have the option to include that

transaction to their copy of their ledger or to ignore it. When the majority of the actors which comprise the network decide on a single state, consensus is achieved.
A fundamental problem in distributed computing and multi-agent systems is to achieve overall system reliability in the presence of a number of faulty processes. This often requires processes to agree on some data value that is needed during computation. These processes are described as consensus.

What happens when an actor decides to not follow the rules and to tamper with the state of his ledger?

What happens when these actors are a large part of the network, but not the majority? In order to create a secure consensus protocol, it must be fault tolerant.

Byzantine Fault Tolerance

Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem. Byzantine Failure is the most difficult class of failure modes. It implies no restrictions, and makes no assumptions about the kind of behaviour a node can have (e.g. a node can generate any kind of arbitrary data while posing as an honest actor).

Byzantine Faults are the most severe and difficult to deal with. Byzantine Fault Tolerance has been needed in airplane engine systems, nuclear power plants and pretty much any system whose actions depend on the results of a large number of sensors. Even SpaceX was considering it as a potential requirement for their systems.

Blockchains are decentralized ledgers which, by definition, are not controlled by a central authority. Due to the value stored in these ledgers, bad actors have huge economic incentives to try and cause faults. As a consequence, Byzantine Fault Tolerance is much needed.

There are a number of ways to implement Byzantine Fault Tolerance. The one we believe is best, and therefore have chosen for Polestar, is:

Delegated Proof of Stake

Traditional Proof-of-Stake (PoS) was largely developed to overcome the many inherent pitfalls of the Proof-of-Work mechanism. First used by Peercoin, Proof-of-Stake places a restriction on the number of blocks that a node can validate. A node can only authenticate as many transactions as its stake in the cryptocurrency or in other words the number of coins that it holds. This solves the energy problem by limiting the computational power that one node can spend on validating a transaction.

However, PoS is prone to the "tragedy of commons," when the rewards for an individual node continue reducing, and keep dropping out of the system as a result. This makes the entire

system susceptible to a 51% attack wherein a single node or a pool of nodes could end up holding more than 51% of the total computational power of the network.

In an attempt to speed up the processing time it takes for a transaction to complete while maintaining the incentive structure for nodes, the Delegated-Proof-of-Stake (DPoS) is used by such coins as EOS, Lisk, and Steem. As a variation of the Proof-of-Stake mechanism, DPoS requires nodes to vote for other users who they trust to participate in the validation process. The nodes with the highest votes then authenticate the transactions.

This means of delegation and voting renders fairness, and avoids a 51% attack on the whole process. Furthermore, the votes are weighed in accordance with the stake that a voter node holds. This means that to avoid a loss of income and reputation, a node with a high stake will not choose someone who might be capable of malicious attacks.

Polestar Service Architecture

Fundamentally this is the core of the Polestar system. To implement a multi-system payment system there needs to be a handshaking mechanism that works across all parties, and requires Polestar to establish a 'common language' between the systems to enable cross-provider communication.

To do this, we need to utilise a similar concept to AWS GLUE:

"AWS Glue is a fully managed ETL (extract, transform, and load) service that makes it simple and cost-effective to categorize your data, clean it, enrich it, and move it reliably between various data stores. AWS Glue consists of a central metadata repository known as the AWS Glue Data Catalog, an ETL engine that automatically generates Python code, and a flexible scheduler that handles dependency resolution, job monitoring, and retries. AWS Glue is serverless, so there's no infrastructure to set up or manage."

Clearly this concept is designed for a centralised solution. Polestar will extend the concept to the decentralised blockchain, utilising a Merkle-chain to facilitate the metadata repository across the platform independent of any single node or point.

But at a fundamental level, the solution we need to allow providers to communicate with one another is simply a microcosm of the larger problem that the 'Internet of Things' poses. Given this, we need to look at how this is being approached and take our solution from there.

(The Internet of Things (IoT) refers to uniquely identifiable objects (things) which can interact with other objects through the global infrastructure of wireless/wired Internet.)

Consider this model:

Overlay Network

The overlay network is akin to the peer-to-peer network in Bitcoin. The constituent nodes could be smart home miners, other high resource devices in the home, or the user's smartphone or personal computer. Each node uses Tor to connect to overlay network for additional anonymity at IP-layer.

A particular user may have more than one node in the overlay network. To decrease network overhead and delay, nodes in the overlay network are grouped in clusters and each cluster elects a Cluster Head (CH). Each node is free to change its cluster if it experiences excessive delays. Moreover, nodes in the cluster can elect a new CH at any time. Each CH maintains the following three lists:

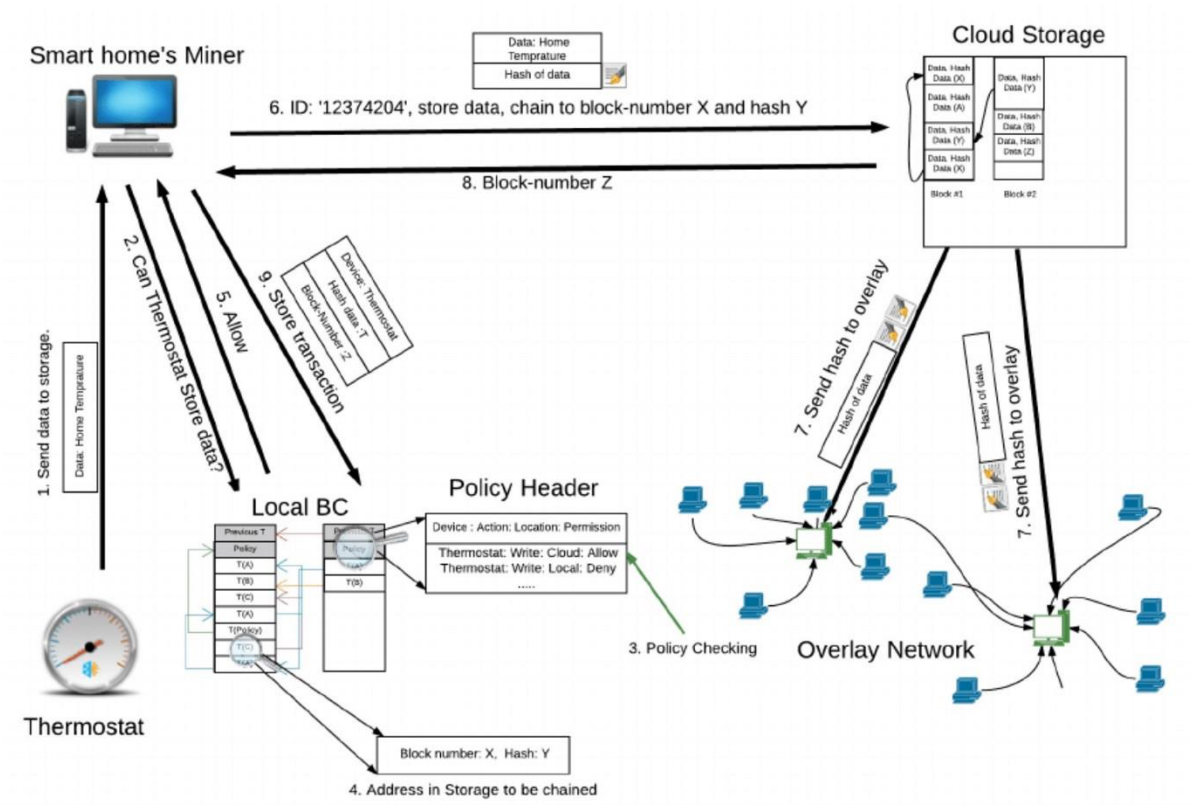
- PK of requesters: the list of PKs that are allowed to access data for the providers connected to this cluster.
- PK of requestees: the list of PKs of providers connected to this cluster that are allowed to be accessed.
- Forward list: a list of transactions sent for other CHs in the network.

An overlay BC is kept by all CHs in the overlay network, which contains multisig transactions sent by the cloud storage and access transactions.

Unlike Bitcoin mining, each CH independently decides whether to keep a new block or discard it, based on its communication with the received transaction's participants. This can lead to different versions of BC in each CH. However, in some cases discovering a particular block or transaction comes at the cost of higher delay. In case a user has more than one home and wishes to manage them together, a shared overlay consisting of the high resource devices in the multiple homes can be formed. A common miner and shared storage are selected for this shared overlay. In the overlay BC each device has a starting transaction chained to its home's starting transaction. This leads to forking in shared BC, a deviation from the Bitcoin BC where forking is not permitted due to its double spending affect. When a shared overlay exists, the high resource devices of the constituent homes maintain a table containing the block-number and hash of data for the last transaction.

Clearly an extension of this approach allows us to apply full integrity across providers within the Polestar microcosm.

Provider		Blockchainretained MetaData
	Request	



This diagram illustrates how the IOT concept can be applied across Polestar to provide a crossprovider communication method.

Financial Transaction Security Mechanism

We will use dual-key stealth addressing: this is when a sender takes a public address from a recipient and transforms it to a one-time address. This is publicly unlinkable to the original public address and to any other one-time address. Only the recipient can link all of the payments together. Furthermore, only the recipient can derive the secret key associated with the one-time address. By using the stealth addressing protocol, a recipient can publish one address and receive unlimited publicly unlinkable payments. Dual-key stealth addresses add another layer of security.

The Polestar platform incorporates dual-key stealth addresses. This refers to the pairs of spend/view keys. It allows "decoding" (or removing the unlinkability) stealth addresses without simultaneously allowing them to be spent. This is the ultimate in settlement security and anonymity and it is standard when transacting in Polestar.

The TPAY dual-key stealth address can be shared publicly by the recipient but any transaction made out to this address can not be linked back to it. It is completely anonymous. When the stealth address has been ultimately revealed to the payer, it will enable the payee to receive

infinite unlinkable payments by TPAY. That means that each payment to a stealth address computes a new unused normal address on which the funds are to be received.

Conclusion

Hopefully you now have an understanding of the purpose of Polestar, the space it aims to fill in the payment-industry, the competition (or lack of) and how the fundamental model of IOT can be applied to make this cross-payment system a reality!

We will be producing further, more detailed papers on the cross-platform mechanics as we grow, since as new providers emerge, and show interest in Polestar, we will need to adapt and scale – we absolutely anticipate having to update our approach and our protocols accordingly, since the complexity of the cross-provider communication solution grows exponentially as new providers are introduced. This makes Polestar a highly complex undertaking, but also an incredibly lucrative one – as you will have learned by our market analysis.

We hope this whets your appetite for the project and look forward to your further participation in this venture with us.

Polestar Team

Wee Pyeong Hwan

(Vice President, SAMSUNG Electronics, Network/IT Professional)

- Academic Degree : Bachelor, Pusan National University, Electronic Engineering (1990 Feb.)

• Samsung Electronics : 29 Years and 11 Months (1990 Jan. ~ 2019 Nov.)

Professional Service (Network Design and Optimization Consultantant)

• AMPS, CDMA, WCDMA, M-WiMAX, LTE, 5G Network Operating

• Technical Support for Global Mobile Telecommunication Network Operator (USA, Japan, India, China, UK, Malaysia, etc)

Lee Jung Jae

(Director / Network · IT Professional)

• Graduated from Seoul National University of Science and Technology in February 2000.

• U.S. Intercom Headquarter IT Division Worked

• Executive Director of Evereltriple Mobile Division

• CEO of IT Business company ‘ETRIESS’

Sim Young Dae

Executive Director in Information Technology and Business Development
Particular expertise in IoT, AI(Machine Learning), Data Science, & BlockChain (STO)

- Kwangwoon University / **PhD Candidate in Electronics**
- Hoseo Graduate school of Venture / **Doctor course completion in Venture Business**
- George Washington University, US / **Masters of Electrical Engineering(Electrophvsics)**
- Kwangwoon University, Korea / **Bachelor of Engineering in Electronicsr**

Eric Garland

(VP, Vodafone, IT/Telecommunication)
- Academic Degree : Masters, University of Groningen, Computer Sciences - Information Science : Database -- Relational Database (2001)

- Vodafone : VP M2M , 5 years, 10 months.
- Vodafone : Network Engineer, 3 years 2 months
- Bite : Network Engineer, 2 years, 4 months.
- Tele2 : Application Integration Engineer, 2 years 8 months.

Simon Collins

(BD&L, British Petroleum, Energy & Telecommunication)
- Academic Degree : MBA, University of Copenhagen, Economics - Economic Systems (2005)

- British Petroleum: Business Development & Licensing Manager, 4 years 6 months
- Oracle: Sales team lead, 3 years 5 months.
- Anglo American: External relations, 3 years 1 month
- Prudential PLC: Business Development associate, 1 year 11 months

Alexey Vrangel

(Back-end lead, Yandex, IT)
- Academic Degree : PhD, Moscow Technological University, Computer Sciences - Theory Of Computation : Computational Complexity Theory (2013)

- Yandex: Leading back-end developer, 3 years 11 months
- Walmart: Project lead, 2 year 2 months
- Mail.ru group: Senior back-end developer, 2 years 1 month
- Nginx: Back-end developer, 1 year 1 month

Daniel Liljeström

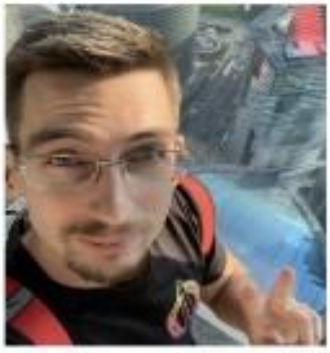
(Unilever, Innovation projects director, Logistics)
- Academic Degree : PhD, KTH Royal Institute of Technology, University, Philosophy - Logic : Mathematical Logic (2004)

• Unilever: Innovation projects director, 4 years 11 months

• IKEA: Project manager, 5 years, 3 months

• Assa Abloy : Team lead, 3 years 7 months

• Husqvarna: Business logic management, 3 years 1 month



Guus Smeets

(Heineken, Leading front-end developer, IT)
- Academic Degree : MS, Delft University of Technology,Computer Sciences - Artificial Intelligence : Expert Systems (2012)

• Heineken Holding: Leading front-end developer, 3 years

• Randstad Holding: Senior front-end developer, 2 years 2 months

• ING group: Front-end developer, 2 years 10 months

• Airbus: Intern front-end developer, 1 year