



White Paper **2018**

**Facilitating secure
transparent payments
on a global scale**



Table of Contents

IMPORTANT INFORMATION	4
1. INTRODUCTION.....	6
2. Industry Overview.....	10
1) Global Financial Institution Payments Systems - A Blue Sky Market.....	10
2) How the Incumbent Funds Transfer Process Works	11
3) Information Within the Incumbent Funds Transfer Process	13
4) Industry Regulation.....	13
a. Anti-Money Laundering ("AML") at Financial Institutions	13
b. Ramifications of Anti-Money Laundering Laws	14
c. The Benefits of More Information	14
3. The Ivy Opportunity – A Highly Disruptive Superior Technology	15
1) Comparison to Incumbent Financial Systems.....	15
2) Comparison to Competing Cryptocurrencies	17
4. Our Tier 1 World Class Team Has Track Record of Success.....	19
5. Ivy Operational Specifications	20
1) Operational Platform Overview	20
a. Base Functionality	20
b. Peer-to-Peer Cryptocurrency to Fiat Currency Network	20
c. Software Integration	20
d. Cashier and Conversion Services	20
e. Fixed Price Transfers via Open Market Operations	21
2) Financial Institutions.....	21
3) User Functionality.....	21
a. Account Setup and Management	22
i. Sender Data Verification	22
a. Transaction Management	22
b. Ivy Purchase, Sell and Transfer	22
6. Ivy Technical Specifications.....	24
1) Overview of Technical Architecture	24
a. Public Network, ivySend, and Public Ivy Tokens (IVY)	26
b. Private Network, ivyReceive, and Private Ivy Tokens (IVYB)	26
c. Interchain Communication and the Ivy Oracle Service	27
2) Identity on the Ivy Network	28
a. Sender Identity	28
b. Financial Institution and Intermediary Identity	28
3) Blockchain Technology Application	28
4) Ivy Data Containers	30
a. Generation and Storage of Ivy Data Containers	31
b. Accessing Ivy Data Containers	31
7. Token Structure post Token Generation Event	32
8. Road Map	34
a. Tokens	34
b. Operations	34
10. Risks	36
GLOSSARY	39

Important Information

This document is a technical whitepaper setting out the current and future developments of the Ivy technology. This document is not a disclosure document. This document is specifically provided to the receiving party (**Recipient**) for the purpose of reviewing the opportunity to purchase tokens (as later described) (**Tokens**) via rights to tokens (**Rights**) granted pursuant to the Pre-Sale Commitment Letter to be issued by Ivy Koin LLC (**Ivy** or the **Company**).

Any information contained in this document, or subsequently provided to the Recipient whether orally or in writing by or on behalf of the Company or its respective employees, agents or consultants is provided to the Recipient on the terms and conditions set out in this document.

This document is confidential and is not to be copied or disseminated in any form to any other person without the prior written consent of the Company.

By retaining this document, a Recipient acknowledges and represents to the Company that it has read, understood and accepted the terms of this document. If the Recipient does not accept these terms, it must immediately return this document to the Company.

This document has been prepared solely for information purposes and to assist the Recipient in deciding whether to investigate further a possible acquisition of Rights and Tokens and may only be used for that purpose. This document is dated 16 January 2018 and has been issued and prepared by the Company based on the information available to it at that time.

This document is not intended to provide the sole or principal basis of any investment or credit decision or any other risk evaluation. Any Recipient should determine its interest in acquiring Rights and Tokens on the basis of independent investigations that it considers necessary or desirable.

Although the Company has used due care and diligence in the preparation of this document, no representation or warranty is made by the Company or any of its advisers as to the accuracy or completeness of the information in this document. No information contained in this document or any other written or oral communication transmitted or made available to the Recipient shall be relied upon as a promise or representation and no representation or warranty is made as to the accuracy or attainability of any estimates, forecasts or projections set out in this document.

No liability will attach to the Company or its advisers with respect to any such information, estimates, forecasts or projections.

This document has not been and will not be lodged with the Australian Securities and Investments Commission (**ASIC**). This document is intended to provide Recipients with information only and does not constitute a prospectus, short form prospectus or other disclosure document as defined or referred to in the Corporations Act 2001 (Cth) (**Corporations Act**) or any equivalent legislation in other jurisdictions.

Potential purchasers of Rights and Tokens should read this document in its entirety. If after reading this document you have any questions, you should contact the person who provided you with this document. The Company reserves the right to decide whether or not to make sales of Rights or Tokens to any persons in its absolute discretion.

Exclusion of Liability

The Company does not accept any liability for any loss or damage suffered or incurred by the Recipient or any other person or entity however caused (including negligence) relating in any way to this document including, without limitation, the information contained in it, any errors or omissions however caused, or its accuracy or reliability.

Disclaimer

This document is presented for informational purposes only. The information in this document may not be complete and may be changed, modified or amended at any time by the Company, and is not intended to, and does not, constitute representations and warranties of the Company. Additionally, the Company is not limited in any way from utilising the money raised from the sale of Rights and Tokens as it sees fit.

Neither the Company, nor any other advisor of the Company intends to update this document or accepts any obligation to provide the Recipient with access to information or to include any additional information or to correct any inaccuracies that may become apparent in the document or in any other information that may be made available concerning the Company, the Rights or the Tokens.

The business of the Company has only recently been formed, is a 'start-up operation' and has not had any significant operating history on which to base an evaluation of its business and prospects or the prospects of the development of the Tokens. Therefore, the information contained herein is inherently speculative.

No Recommendation

This document does not represent a recommendation to purchase the Rights or Tokens. Any decision to purchase Rights or Tokens must be based on the proposed purchaser's own circumstances, investigations, analysis and assessment of the Company's operations and prospects and of the Rights and Tokens. Potential purchasers must make their own independent assessment of the merits of purchasing Rights and Tokens and consult their own professional advisors and make such further investigations they think necessary. Potential purchasers are cautioned that any acquisition of Rights or Tokens may involve a high degree of risk.

Nothing in this document should be construed as financial product advice, whether personal or general, for the purposes of Section 766B of the Corporations Act. This document does not involve or imply a recommendation or a statement of opinion in respect of whether to buy, sell or hold a financial product.

Taxation

The acquisition of Rights or Tokens will have tax consequences, which will differ depending on the individual financial affairs of each purchaser of Rights or Tokens. All potential purchasers of Rights or Tokens are urged to obtain independent financial advice about the consequences of acquiring Rights and Tokens from a taxation viewpoint and generally. To the maximum extent permitted by law, the Company, its officers and each of their respective advisors accept no liability and responsibility with respect to the taxation consequences of purchasing Rights or Tokens.

Dollars

All currency amounts are in US Dollars unless specified otherwise.

Qualifying Statements

This document includes terms such as 'forecast', 'planned', 'targeted', 'believes', 'potential', 'estimates', 'intended', and 'aims'. These statements are based on the current understanding of the Company's business and the aspirational targets that the business holds; however, it should be noted that there is inherent risk in achieving these statements and potential purchasers should purchase Rights or Tokens on the basis that these targets may not be achieved.

Token Utility

The Company proposes that the Tokens will be used as part of a digital platform which it also proposes to develop and which would facilitate payments (**Ivy Network**). If implemented, token holders may have the ability to voluntarily de-anonymise transaction data to the satisfaction of financial institutions in order to facilitate transactions using cryptocurrency with the security and reliability of the blockchain.



Introduction

Ivy is a blockchain based technology for FIAT & Cryptocurrency business transactions which require verification in the international monetary system. The Ivy Network utilizes IVY tokens which will carry Know your Customer (KYC) and Know Your Transaction (KYT) to meet the verification requirements for transactions.

In a truly global financial market place, there is a very real need for fast & secure transactions that meet KYC & BSA / AML requirements for not just traditional FIAT currency, but also cryptocurrencies as well.

Ivy bridges the gap between the centralized traditional banking & payment systems and the decentralized blockchain network to leverage the best of both worlds – fast, decentralized processing that meets the regulatory requirements of Financial Institutions around the world.

For an individual and/or business Ivy presents the opportunity to make payments in cryptocurrencies to third parties and for the third party to receive cash.

To the banks Ivy opens new channels of deposits that will ultimately provide more revenue for financial institutions, reduce fraud losses and provide for significant automation of existing manual processes leading to substantial cost savings.

Ivy bridges the gap between the centralized traditional banking & payment systems and the decentralized blockchain network to leverage the best of both worlds...



Problem:

There is an increased scrutiny from regulators surrounding any potential transactions being linked to the proceeds of fraudulent or money laundering activities. Through embedding KYC and KYT data points into a transaction itself, Ivy's blockchain technology will provide regulatory comfort and access to large pools of global funds that would otherwise be unbankable.

Ivy solution:

Ivy provides financial institution grade technology that can be easily implemented globally.

- i. Ivy's technology will provide Know Your Transaction (KYT) information that greatly exceeds regulatory requirements as will be hashed into the blockchain and accessible as required.
- ii. Know Your Customer (KYC) to satisfy Bank Secrecy Act (BSA) and global AML requirements hashed into the blockchain and accessible as required.
- iii. Immutable records in the blockchain for audits by Financial Institutions, Compliance Departments, Bank Auditors and Potentially Regulators
- iv. Cashier services to convert Ivy tokens into fiat in traditional bank accounts via near instantaneous payment mechanisms.

The cryptocurrency market is broadening and deepening at a rapid rate, with a current cryptocurrency coin market capitalisation of US\$400bn¹.



Whilst the advantages of and potential for these currencies is well recognised, anonymity has prevented wider mainstream adoption as there are a lack of financial institutions that support transactions involving cryptocurrencies.



The primary reason for this lack of support within the global banking and financial industry is due to the applicable regulation that requires certain transaction information inconsistent with anonymity.

The Tokens will be a blockchain based cryptocurrency intended for transactions with financial institutions and embeds far more Know Your Transaction (**KYT**) and Know Your Customer (**KYC**) information into payments than incumbent payment networks, including current baseline payment systems such as the SWIFT protocol, CHIPS and Fedwire.

Token holders will have the ability to voluntarily de-anonymise transaction data to the satisfaction of financial institutions in order to facilitate transactions using cryptocurrency with the security and reliability of the blockchain.

We believe the opportunity for the Tokens is immense, with:

- A Blue Sky Market
 - Potential continued cryptocurrency market growth
 - Potential penetration of global financial institution transactions
- Our Highly Disruptive Technology
 - It is anticipated that the Ivy Network will have architectural improvements compared to Ripple, our closest peer and the global leading Altcoin. Ripple currently has a market capitalisation of ~US\$124bn²
- Our Tier 1 World Class Team, with a Track Record of Delivery

We outline in detail our proposition below and look forward to welcoming you as a Token holder.

-
1. <https://coinmarketcap.com/> as at 16 May 2018
 2. <https://coinmarketcap.com/> as at 07 January 2018

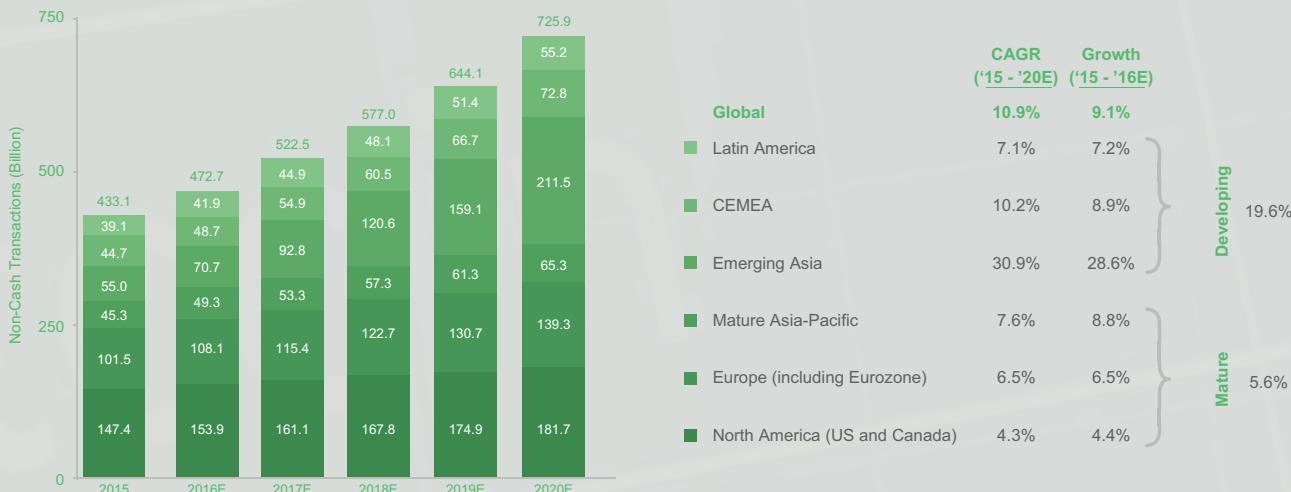
Industry Overview

1) Global Financial Institution Payments Systems - A Blue Sky Market

Global financial institution payments are significant. One platform, SWIFT, directs the transfer of nearly \$5 trillion worldwide each day, or \$1.25 quadrillion per year³.

The chart below also shows the year-over-year growth in the industry. It reveals the extent to which payments are growing faster in emerging markets, but much larger immediately addressable markets exist for a cryptocurrency based payment solution in more established regions such as North America and Europe.

Figure 2 – World Payments Report 2017⁴



3. https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf
4. Capgemini & Royal Bank of Scotland 2017

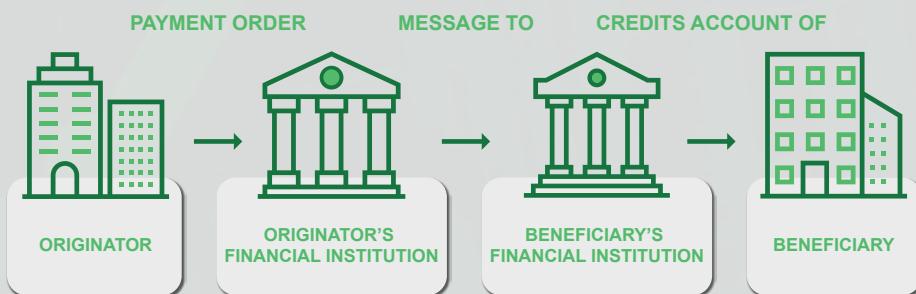
2) How the Incumbent Funds Transfer Process Works

An electronic funds transfer is a transaction in which money moves from one financial institution to another (or from one account to another) at the instruction of a financial institution's customer. Financial institutions facilitate this through the communication of electronic messages that form the basis for making the required bookkeeping entries and making funds available. Electronic funds transfers are the primary mechanism used by businesses for the transfer of money between two parties.

Financial institutions facilitate electronic funds transfers through the sending and receiving of electronic messages per understood and well-supported standards, including SWIFT and ISO 20022. The messages sent between financial institutions direct the sending bank to debit the sender's account and the receiving bank to credit the recipient's account.

The entities involved in a transfer include:

- Originator (such as a business or individual) - the initiator of the transfer;
- Beneficiary - the party who is the end recipient of the transfer;
- Originator's financial institution - the financial institution that receives the originator's transfer instructions and transmits the fund's to the beneficiary's financial institution;
- Beneficiary's financial institution - the financial institution that receives the funds and holds the account to be credited; and
- Additional/Intermediary Financial Institutions - other institutions that may be required to execute the transaction.



Frequently used payment formats include:

SWIFT	<p>The Society for Worldwide Interbank Financial Telecommunications ("SWIFT") is a member-owned messaging network used for funds transfer instructions using standardized codes.</p> <p>SWIFT is a communication network that a financial institution in one country can use to communicate with its branches or other financial institutions in a different country. SWIFT is a messaging system for funds transfer instructions, rather than a financial settlement system.</p> <p>Most international interbank messages use the SWIFT network. SWIFT divides its messages into a series of formats, known as message types. Each message type represents a type of transaction or message. The message types are separated into ten categories: (MT0xx – System Messages; MT1xx – Customer Payments and Checks; MT2xx – Financial Institution Transfers; MT3xx – Treasury Markets; MT4xx – Collection and Cash Letters; MT5xx – Securities Markets; MT6xx – Treasury Markets – Metals and Syndications; MT7xx – Documentary Credits and Guarantees; MT8xx – Travelers Checks; and MT9xx – Cash Management and Customer Status).</p> <p>On average, SWIFT records 28.4 million FIN messages per day⁵. SWIFT directs the transfer of nearly \$5 trillion worldwide each day or \$1.25 quadrillion per year⁶.</p>
CHIPS	<p>The Clearing House Interbank Payments System ("CHIPS") is a funds-transfer system that transmits and settles payment orders in US dollars for some of the largest and most active banks in the world.</p> <p>On an average day, CHIPS transmits and settles more than 446,000 "payment messages" worth \$1.5 trillion. It operates 20 hours a day and matches transactions between banks in real time⁷.</p>
Fedwire	<p>The Fedwire Funds Service ("Fedwire") is a real-time, gross settlement system jointly owned by the 12 US Federal Reserve Banks⁸. Both senders and recipients must hold accounts with Fedwire-participating financial institutions, and the transfers are same-day, non-revocable payments. Though participating institutions are all US-based institutions, Fedwire can be used as the US-based portion of international transfers.</p> <p>In 2016, Fedwire transfers averaged a daily volume of 590,209 transactions, representing \$3.05 trillion⁹. The Fedwire service operates beginning 9:00 PM the night before a business day until 6:00 PM Eastern Time (GMT – 5).</p>
ACH	<p>The Automated Clearing House ("ACH") is an electronic payment network run by the National Automated Clearing House Association ("NACHA"), a non-profit membership association supported by 10,000+ financial institutions. ACH transfers include direct deposits, payroll payments, and consumer payments (e.g. to insurance and mortgage companies).</p> <p>ACH direct debit transfers include consumer payments on insurance premiums, mortgage loans, and other kinds of bills. ACH covers the United States. The European equivalent is SEPA (Single Euro Payments Area) and the UK has three equivalent systems: BACS, CHAPS, and Faster Payments.</p> <p>The ACH Network moves \$43 trillion and 25 billion electronic financial transactions each year¹⁰.</p>

Financial institutions use various payment formats depending on the nature of transactions. In some instances, multiple payment methods may be used for a single transaction.

5. <https://www.swift.com/about-us/swift-fin-traffic-figures> (Date: 19 December 2017)
6. https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf
7. <https://www.the-clearinghouse.org/-/media/tch/pay%20co/chips/reports%20and%20guides/chips%20volume%20through%20november%202017.pdf?la=en> (Date: 19 December 2017)
8. https://frbservices.org/serviceofferings/fedwire/fedwire_funds_service.html
9. https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm
10. <https://www.nacha.org/ach-network/timeline> (Date: 19 December 2017)

3) Information Within the Incumbent Funds Transfer Process

Transactions between two parties are typically referred to in the financial industry as third-party payments. That is, transactions processed by financial institutions on behalf of parties – individuals or entities – that are not themselves financial institutions. With some notable exceptions, these transactions generally can be divided into two main types:

- Transactions processed pursuant to documents to which the financial institutions are privy, such as in the case of trade finance, where one or more financial institutions will have access to a letter of credit, a guarantee, and/or some other information such as bills of lading and other shipping information.
- Transactions processed without financial institutions having such documents. These transactions are often referred to as “clean payments”. The significant majority of third party payments processed are of this type, where the financial institutions processing the payments have relatively little visibility into the nature of the underlying transaction. In the trade finance space, such transactions are referred to as “open account trade”.

Information that might be included with financial transactions fall into two categories:

- Know Your Customer (KYC): KYC information typically includes identifying information such as the customer’s name, address, account number, and so on.
- Know Your Transaction (KYT): KYT information includes details such as the type of transaction (for example, whether the transaction involves cash, foreign wire payments, or cheques), the recipient of the funds (including its address as reported by the sender at the time of instruction), and details included in the transaction memo.

4) Industry Regulation and the Relevance of Ivy

Over the past 50 years, funds transfers have become increasingly electronic. With this advancement, and the accompanying growth in transaction volumes, financial institutions, law enforcement, and regulatory agencies are confronted with increasingly numerous and complex challenges for combatting financial crime. Jurisdictions throughout the world continue to strengthen anti money-laundering (**AML**) laws. Because nearly all countries have adopted – and commit increasing resources to the enforcement of – these types of laws, consumers and businesses are accustomed to financial institutions requesting KYC information to verify the identity of a customer when a new financial account is opened, or when a large funds transfer is made.

a. Anti-Money Laundering at Financial Institutions

Taking the United States as an example, the Bank Secrecy Act¹¹ and other requirements call for financial institutions to implement and adhere to policies, procedures and controls sufficient to provide for the detection, investigation, and reporting of suspicious activity. This includes transactions that could signify money laundering, tax evasion or other criminal activities. Similar requirements are commonplace in developed economies around the world.

Methods used to detect suspicious activity typically involve rules-based automated suspicious activity monitoring platforms that review, on a batch-processed basis, recent customer activity. These rules or scenarios flag specific transactions, or groups of transactions, for further analysis. This analysis typically involves a manual review by financial institution personnel to either eliminate the flagged activity as “not suspicious,” or to escalate the activity for further review and, potentially, onward for reporting to law enforcement.

Additionally, certain higher-risk customers are often subject to periodic ongoing due diligence reviews that involve an in-depth analysis of the transactions conducted by the customer over a period of, for example, the most recent six or 12 months. These due diligence reviews have a similar purpose to the automated transaction monitoring detection methods, which is to understand the nature of the underlying activity so that the financial institution can make decisions regarding the risks and acceptability of retaining the customer relationship, apply appropriate controls to the account(s) of identified parties, and report suspicious activity as required.

Regulatory expectation in this area is that financial institutions undertake enough due diligence and analysis to gain comfort that customer activity is not suspicious, otherwise the activity should be further analyzed and reported to law enforcement. Financial institutions are expected to perform these assessments on the basis of all available information; where additional information would assist, financial institutions are expected to collect it, but to do so in a manner that does not “tip off” anyone – including the customer or related party – that an investigation has been, or may be, in progress.

11. <https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html>

b. Ramifications of Anti-Money Laundering Laws

Compliance with AML laws requires that banks have sufficient information to implement, execute, and support their anomaly detection programs. Cryptocurrency and its inherent anonymity put banks in a bind, since such transactions do not naturally come with the information banks need to carry out the practices they need to identify fraudulent or illegal activity. To protect themselves, banks commonly suspend accounts that contain fiat deposits originating from cryptocurrency-related transactions, and refuse to accept gains or settlement in cryptocurrency as a legitimate medium of exchange. One implication of this decision is that legitimate businesses are unable to perform transactions involving cryptocurrencies because they are unable to bank the proceeds.

c. The Benefits of More Information

There are clear benefits from having additional information readily available, either while investigating an automated transaction monitoring system's alert, or during an activity review as part of ongoing due diligence. The additional information can help the investigator or reviewer more effectively and efficiently determine whether the nature of the activity, including the parties involved, gives rise to any doubt as to its appropriateness or legality.

This additional information can help the financial institution determine whether a customer needs to be categorized as high risk or if the institution is breaching its obligations under AML laws. In the case of routine benign activity, this information can allow a bank to more effectively focus investigative resources on other customers and their heightened risk activity.

Although traditional payment methods typically embed limited information, this additional data is generally readily available, either within the financial institution's KYC records about the instructing customer, or provided directly by the customer in transaction instructions.

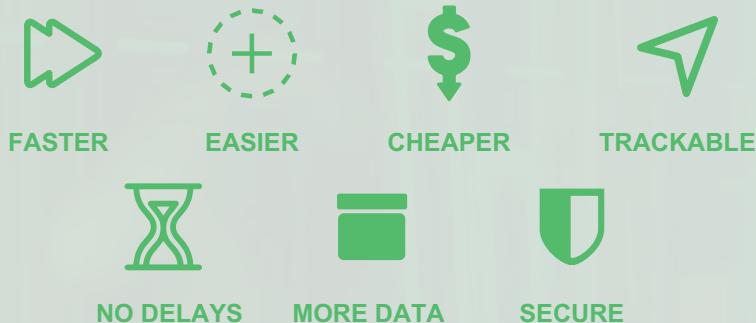
Information of the former type could include, for example, a description of the nature of the customer's business, their geographic focus, expected activity that the account(s) are likely to experience, and information regarding related parties to the account, such as beneficial owners and signatories. The transaction itself (KYT) could include information related to supporting documentation such as invoices, credit notes, shipping documentation, and information identifying the parties to a transaction (these may include more parties than the originator and beneficiary parties, such as shipping companies). It can also include documentation, or evidence of such documentation, that would show the legal permissibility of transactions, such as licences issued by U.S. Treasury's Office of Foreign Assets Control or the Commerce Department's Bureau of Industry and Security.

Embedding such information into the payment instruction mechanism, as an aspect of the supporting protocol, could prove crucial to help a financial institution's reviewer form a more comprehensive and clear picture regarding the nature of the underlying activity. By making KYC and KYT information more readily available and eliminating knowledge gaps, the financial institution can focus its attention on investigating other instances that deserve heightened scrutiny. Unfortunately, a number of protocol developments in financial technology focus heavily on interoperability and speed, considering regulatory compliance as an overlay of inconvenience that can be addressed at later points following deployment, meaning that the promise of a comprehensive solution is seldom realized.

3

The Ivy Opportunity A Highly Disruptive Superior Technology

The benefits of cryptocurrency vs incumbent financial systems are well understood:



However, the inherent anonymity of most current cryptocurrencies creates incompatibility with the current financial system.

The Ivy Network will enable KYC, KYT, and AML data supporting transactions to be captured using a blockchain-based cryptocurrency. It will be optimally designed for transactions with financial institutions, embedding far more compliance and transaction audit information than incumbent payment networks. Transaction data will be made available to satisfy the stringent requirements of financial institutions and intermediaries. When implemented, the Ivy Network will have

distinct advantages over incumbent financial systems and competing cryptocurrencies.

Ivy seeks to bridge the gap between current global financial systems and the emergence of cryptocurrencies, positioning itself as the future for global payments.

1) Comparison to Incumbent Financial Systems

When fully developed, the primary differences between the Ivy Network and traditional payment networks will be that the Ivy Network:

- will securely facilitate the transfer of cryptocurrency payments while associating KYC and KYT data via the trusted, distributed Ivy network;
- will securely store an immutable reference to supporting transaction data in a public blockchain;
- will embed more KYT information into the transfer than traditional payment methods;
- will embed more KYC information into the transfer than traditional payment methods;
- will be able to be integrated into existing banking software;
- will offer easy integration into accounting software for bookkeeping efficiency; and
- will provide revocable access to KYC/KYT data to financial institutions, accountants, company managers and others, depending on the information they require.

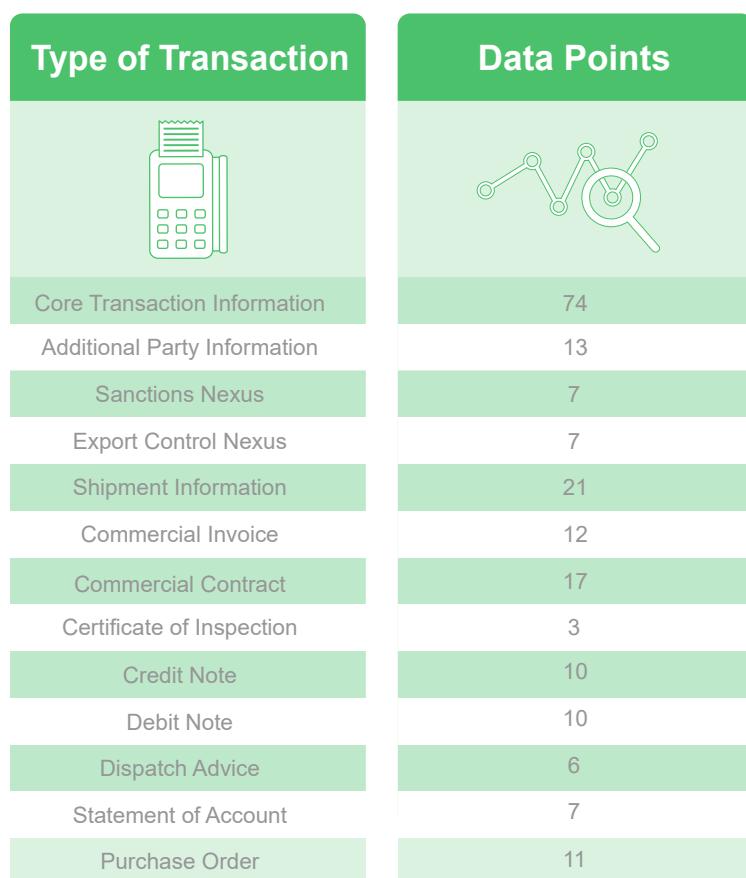


In regards to KYC and KYT, frequently used incumbent payment formats typically support collecting relatively few data points. The table below indicates the approximate volume of KYC/KYT data points included in a typical transaction:

	SWIFT	Fedwire	CHIPS	ACH
KYC and AML data points	10	17	9	10

Note: The Company is not affiliated with SWIFT, CHIPS, ACH or Fedwire. All information is provided on a general basis and is based on the available information at the time of the Company's research.

When implemented, the Ivy Network will be far more descriptive than the existing systems and processes. Depending on the type of financial transaction being performed, it is anticipated that the Ivy Network will allow for the inclusion of more than 120 different KYT data points and more than 70 different KYC data points in transaction messages. A convenient way to categorize these data points is according to the documentation source from which they might originate.



2) Comparison to Competing Cryptocurrencies

The Tokens, when fully developed, are intended to be a cryptocurrency with several distinguishing features and benefits:

Feature	Description	Benefit
 RECOGNIZABLE	The Ivy Network and related transactions allow for the clear integration of KYC/KYT/AML data in the flow of cryptocurrency transactions.	Legitimacy of parties and purpose of transaction is easily understood and used for adjudication of decisions regarding payments and deposits.
 TRANSFERABLE	Tokens will exist as a cryptocurrency that can be freely traded on a public blockchain, without encumbering associated KYC/KYT/AML information associated with its purpose for financial institutions and intermediaries.	Parties may easily use and exchange the token for its utility, allowing for an honest reflection of its value and removing ivykoin.com and cryptocurrency exchanges as sole determinants of the cryptocurrency's value.
 NON-FORGEABLE	The Ivy Network transactions and supporting data will facilitate using blockchain architecture, which enforces the immutability of assignment and transaction data.	Users of the Ivy Network will be assured of the certainty of transactional integrity and the security of data for ensuring the durability of transactions and data that support decisions related to cash movement.
 LIMITED SUPPLY	Tokens will be issued in known quantity, with known initial distribution and allocations.	Public transactions benefit from economies related to coin scarcity where private network movement provides accurate reflection of liquidity and velocity of money within the network.
 DE-ANONYMIZED ON REQUEST	All data collected is persistently secured, transported, and tracked on a private clearing network that consists of financial institutions and intermediaries.	Eligible parties have the information they need for KYC/KYT/AML functions. Parties may be added or removed without compromising the underlying security of data.



The Ivy Network, when fully developed, is anticipated to have distinct advantages over Ripple, our leading competing cryptocurrency.

Ivy	VS	Ripple
<ul style="list-style-type: none"> Designed to break KYC/KYT/AML barriers between cryptocurrency and existing financial system Up to 74+ KYC, 120+ KYT data points and customer files per transaction Decentralized system of transaction validation Public coin economics driven by utility transaction volume on public ledger 	VS	<ul style="list-style-type: none"> KYC/KYT/AML not included in core design KYC and KYT data not associated with cryptocurrency Centralized system of transaction validation Public coin economics not transparent; large, privately held reserves

Specifically, with reference to Ripple, the Ivy Network is intended to be a decentralized network of validators, consisting of financial institutions and intermediaries, who use the Tokens for the purpose of communicating KYC/KYT/AML data and for settling balances on the network. Compliance and audit are first-principle concerns in the Ivy Network. Transactions with Tokens will be initiated against a contract listed on the public Ethereum network using Tokens that are easily traded for their utility of facilitating payments to recipients of payment remittance in fiat currency at their financial institutions. This differs greatly from the use of XRP, the core Ripple currency, which has little public use aside from as a medium of exchange.

The market potential is well recognised. Ripple is one of the largest¹² cryptocurrencies behind bitcoin.



Ripple Tokens have increased in value over 28,000% during 2017.

<http://fortune.com/2017/12/29/ripple-cryptocurrency-surge/>

* Reference date 14 Jan 2018 **Subject to raising US \$15 Million

12. <https://coinmarketcap.com/> as at 14 January 2018

Our Tier 1 World Class Team Has Track Record of Success

The Company is led by a world class team with a track record of success. The Company's highly experienced executive team is supported by a global advisory board with unparalleled industry knowledge and networks across all necessary verticals for project success.



GARY FAN
President



MIKE BECK
CTO



BOB MURRAY
Product Delivery Manager



JAMES CASKEY
VP, Marketing &
Communications



**BARTOSZ
ROBASZEWSKI**
Engineering
Manager



**DARIUSZ
CIESIELSKI**
Sr. Engineer



**JANUSZ
ZOLTANSKI**
Business Analyst



**MATEUSZ
SPYCHAJ**
Frontend Developer



**GRZEGORZ
ŁYSKAWA**
Web Developer



**ANDRZEJ
BUDZANOWSKI**
Web Developer

Advisors



ASH SHILKIN
Strategic Advisor,
CEO Change
Financial
(ASX: CCA)



ANDREW PIPOLO
Strategic Advisor,
Former Managing
Director Paypal
Japan & Australia



KIRILL GOUROV
Strategic Advisor,
Founder of
Blocktech & Full
Node Capital



FEROZ SANAUULLA
Strategic Advisor,
Former CEO Intel
Capital



**ADAM SANTA
MARIA**
Strategic Advisor,
Co-Founder and
Managing Director
at Discovery Capital
Partners



**TOM
MARCHESELLO**
Strategic Advisor,
Former Blockchain
Strategist at CME

For information on the team please visit www.ivykoin.com

Ivy Operational Specifications

1) Operational Platform Overview

a. Base Functionality

The Ivy Network is envisioned to provide the following functionality to end users. This functionality may be delivered to its constituents by desktop/web and mobile experiences:

Senders & Recipients

- Purchase or sale of Tokens;
- View cryptocurrency exchange availability and exchange rates for common cryptocurrencies;
- Estimate network charges and receive quotes for using Tokens;
- View financial institution and financial intermediary mean times for transaction settlement; and
- View KYC data access logs with respect to personally identifiable information (for senders).

Financial Institutions & Financial Intermediaries

- Maintain enterprise account and identity information;
- Manage account access settings for organization members; and
- View Token data container contents and access history.

In addition to the base features described above, the Company plans, in due course, to incorporate the following features, functionalities, and solutions into the Ivy Network:

b. Peer-to-Peer Cryptocurrency to Fiat Currency Network

Whereas the initial uses for the Ivy Network is to provide for predominantly business-to-business transactions, strong demand also exists for a simplified payment network that allows individuals to easily send, receive and manage their cryptocurrencies and easily convert them to fiat currency.

c. Software Integration

The Company will seek to integrate with existing bank software so that KYT and KYC can be distributed automatically to the correct locations within the respective bank system.

The Company also intends to integrate with major accounting software systems. The easy integration of payments and receipts from customers, including invoice details, will enable transactional data to be loaded directly into the accounting software, reducing the customer's administrative load.

d. Cashier and Conversion Services

The Company intends to develop cashier services and conversion services. Cashier services facilitate:

- The withdrawal of fiat money from bank accounts and its conversion into cryptocurrency; and
- The conversion of cryptocurrencies back into fiat money and their deposit into bank accounts.

Exchange services will allow customers to convert Tokens to and from a range of other cryptocurrencies.

By providing both cashier and exchange services, the Company intends for the Ivy Network to be an end-to-end solution, particularly for businesses making large transfers. The Company will seek to:

- Facilitate the conversion of fiat money into cryptocurrency;
- Facilitate the transfer of cryptocurrency across the globe; and
- Enable the recipient to exchange the cryptocurrency back into fiat money in their bank account.

Most importantly, it is intended that the Ivy Network will be able to do this without causing a problem with either the sending or receiving financial institution.

e. Fixed Price Transfers via Open Market Operations

Potential currency loss during the process of cryptocurrency transfers is one of the biggest inhibitors to mainstream adoption of cryptocurrencies by merchants. The Company aims to develop a fixed price solution to remove currency loss due to cryptocurrency price volatility.

The fixed price solution involves using a pool of treasury coins to be used specifically for USD fiat to USD fiat transactions involving two bank accounts. Fiat will be pulled from the senders bank account using an ODFI ("Originating Deposit Taking Financial Institution). The Ivy Network will then facilitate the conversion of the fiat into Tokens using a treasury of off-market tokens designed specifically for this purpose (see section 7).

2) Financial Institutions

With increased financial institution support, the Ivy Network has the potential to be used for the following transactions, plus many more:

- Domestic or international purchases of goods;
- Business to business services;
- General transfer of value which is destined to be fiat in a financial institution;
- Software licence purchases;
- Real estate purchases;
- Global investing;
- Large personal transfers; and
- Small personal transfers.

3) User Functionality

It is proposed that, the Ivy Network will provide a value exchange between counterparties where (1) a sending party seeks to send large sums of cryptocurrency to a receiving party and (2) the receiving party receives that cryptocurrency balance to a bank account in fiat currency.

Both senders and receivers will be able to use Tokens to move cryptocurrency into financial institutions via the Ivy Network, which will be available for purchase at ivykoin.com and publicly on major exchanges. Account holders wishing to move other cryptocurrencies through the Ivy Network must trade third party cryptocurrencies into Tokens first.

ivykoin.com will be accessible by users via phone or mobile device and from a sender's perspective will provide the following core functionality:

- Account setup and management;
- Transaction management; and
- Token purchase, sale and transfer.



a. Account Setup and Management

It is anticipated that senders and recipients will be able to create Ivy Network accounts at ivykoin.com and, after the registration process, receive unique sender identification information. The Ivy Network will save all of the sender's account information so that they do not have to provide the same information for subsequent transfers. This KYC information consists of a variety of data fields and files that represent the identity of the user, such as name, email, phone, address, and government identification.

When fully developed, accounts will be able to be managed through an online dashboard at ivykoin.com, including updating KYC and recurring transactional data. Account holders may request to connect to other Ivy Network account holders and populate a roster of known and verified cryptocurrency payment peers, which is helpful when sending frequently to the same recipients, or to quickly and efficiently send to new recipients. Account holders may make themselves visible on the Ivy Network globally and requests may be made by one account holder to add another to their own roster. They may also use Ivy Network services to convert and send Tokens to their own fiat accounts at financial institutions.

i. Sender Data Verification

The Ivy Network intends to verify basic sender data and legitimacy of bank accounts as part of the account opening process. The Ivy Network will provide initial identity document verification using various third-party services. Identity documents such as passports and drivers licenses are intended to be validated within minutes. If documents are not recognised, then the account will be placed into pending status for further investigation. Similarly, business licenses and other registered corporate documents will be able to be quickly verified.

Toward the same end, account holders' bank account information is intended to be verified using a process whereby small deposits are placed into account holders' bank accounts, and those deposit amounts are used to independently verify the successful connection between the Ivy Network and the bank account.

Despite these efforts, the Company does not guarantee responsibility for the legitimacy or illegitimacy of payments, though this practice is very similar to that taken by incumbent networks.

a. Transaction Management

Once an Ivy Network accounts is established, it is anticipated that a sender will be able to initiate a transfer of Tokens to a recipient. The sender will enter the specific transaction information into the account in advance of the transaction. The Ivy Network will request base level information for all transfers, however the required additional detail varies based on the laws and regulations that are applicable. The Ivy Network will prompt a sender to provide additional specifics related to their transaction. For example, if a sender is making a payment in exchange for goods, the information the Ivy Network embeds into the transfer might include country of origin, final destination, proof of import duties paid or other identifying information. A sender may also choose to provide additional details about the transfer – for example, a copy of the invoice with the payment. Furthermore, if a sender knows that they aren't a trusted source by the recipient, they can include information such quality assurance certificates, batch information, articles of incorporation, and other voluntary KYT information which is extensive.

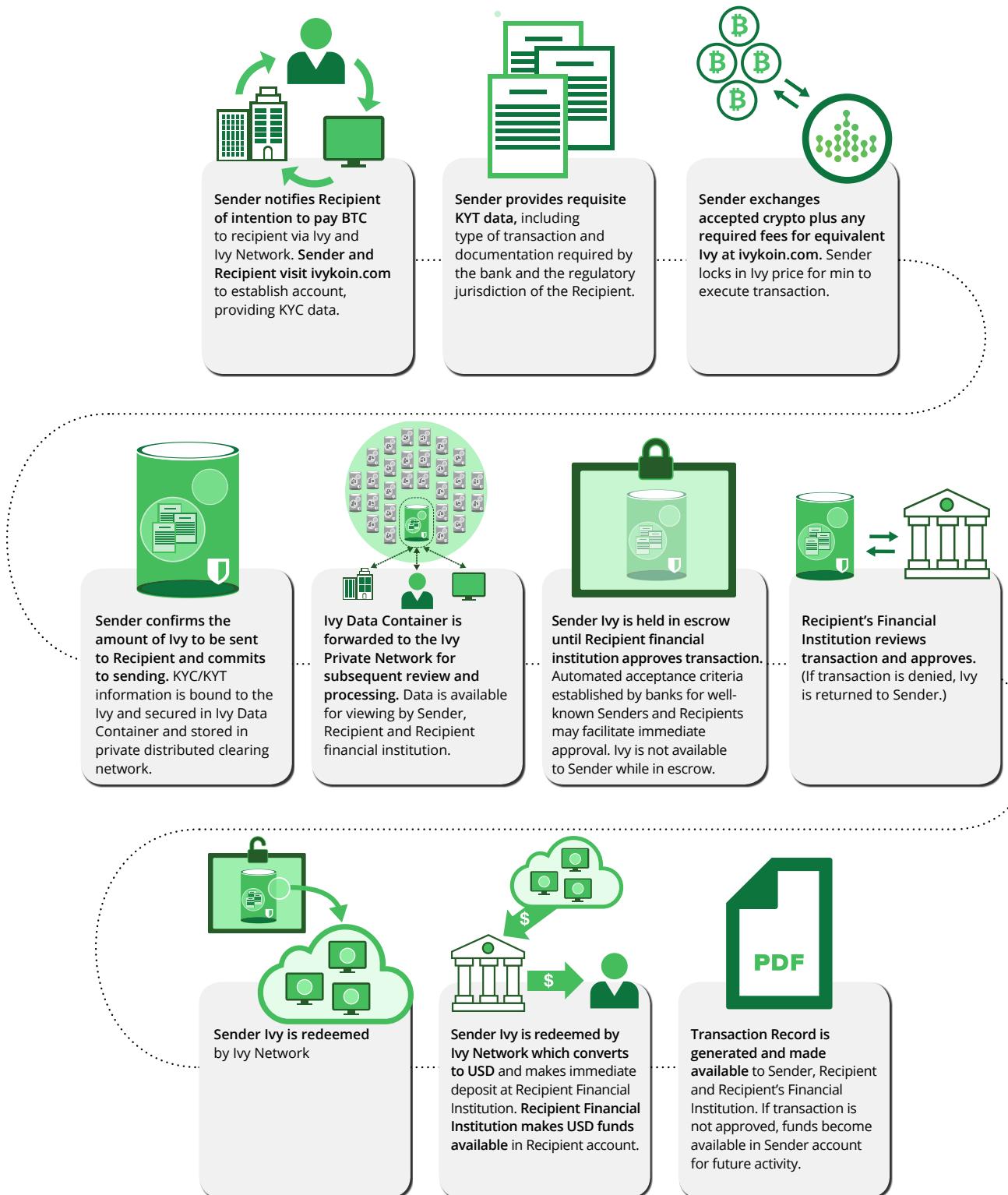
b. Ivy Purchase, Sell and Transfer

It is anticipated that the Ivy Network will facilitate the secure transmission of funds and data for the benefit of both a sender and a financial institution. When a bank is reviewing transactions for suspicious activity, it will have significantly more data points to assist in the review, as compared to legacy payment networks and more modern alternatives for payment transfers.

Payment values will be viewable by the public in the blockchain and cannot be deleted. KYT and KYC data will be encrypted and bound to Tokens sent by a sender to the Ivy Network, and are subsequently accessible to the receiving institution and receiver. This KYC/KYT/AML data can only be viewed by parties associated with the transaction.

The diagrams below depict the anticipated flow of Tokens from the perspectives of a sender, receiver and financial institution. The user interface is simple and intuitive.

Functional Process Overview of Ivy Conversion to USD



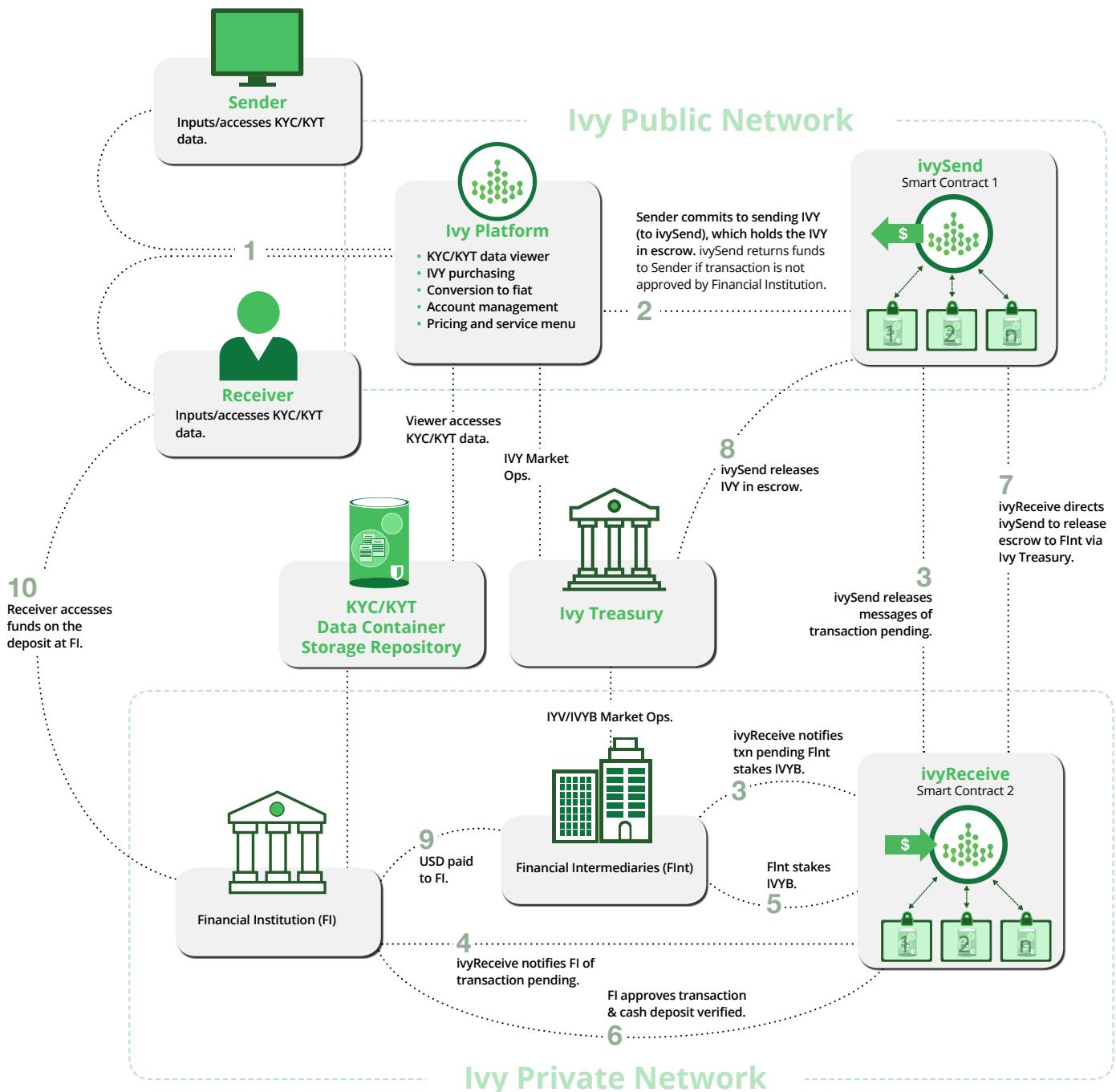
6

Ivy Technical Specifications

1) Overview of Technical Architecture

It is intended that the Ivy Network will function through the use of a dual network architecture, where senders of Tokens operate on a public network (**Ivy Public Network**), and parties that provide the financial settlement to fiat currency participate on a private network (**Ivy Private Network**). KYC/KYU/AML data supporting transactions will be captured in cryptographic containers that are generated from the Ivy Public Network interaction with the Ivy Network smart contracts and support the activities of the Ivy Private Network participants in facilitating transaction settlement. This data will be stored and accessible by the financial institution and governing regulators of the fiat balance recipients. The following technical specifications are each anticipated to be part of the Ivy Network when fully developed.





a. Public Network, ivySend, and Public Ivy Tokens (IVY)

Once the Ivy Network is operational, it is anticipated that public parties seeking to send third party cryptocurrency to the account of an intended recipient must exchange their cryptocurrency for Tokens at a public exchange or purchase Tokens directly from the Ivy Network. Ivy Public Network Tokens (**IVY**) will be authored to the ERC20 specification, available on the Ethereum network. Tokens will be submitted to an Ivy Network contract (**ivySend Contract**) on the Ethereum network, where they are subsequently held in escrow. The escrow state completes on the basis of two conditions: a) the transfer is successfully completed, in which case the Tokens are transferred to the Ivy Network, where they are sold on secondary markets or on the Company's website for either cash or third party cryptocurrency, or, alternatively burned; or, b) the transfer fails, in which case the full amount of the Tokens submitted to the Ivy Network is refunded.

An ivySend Contract is anticipated to be a smart contract that can be addressed by any number of parties interested in calling it from the public Ethereum network. While in initial implementation, it is likely to be available through the interface of ivykoin.com, through the website's direct integration with the Ethereum network. It is additionally envisioned that other parties will similarly incorporate this contract as a payment interface. An ivySend Contract is intended to operate using Ethereum network gas incentives, whereby the sender must cover the calling cost of the contract, allowing the contract's processing on the Ethereum network to occur. Should gas submitted not prove sufficient for mining public incentives, the escrow contract will never take effect to secure the sender's Ivy Network account balance, such that it might continue with the rest of the transaction. Ivy Network fees are also incorporated into the cost of the ivySend Contract process (much like wire transfers performed at traditional financial institutions).

It is anticipated that a party seeking to use the Ivy Network can use the Company's website to easily view a) common cryptocurrency to Token exchange rates at a variety of common cryptocurrency exchanges; b) expected Ethereum gas charges for successful execution of the ivySend Contract; and c) total gross Token fees (flat balance desired + gas charges + commission) for a given balance of fiat currency sought to be sent to an intended recipients account. As a number of these components are volatile in overall pricing, by using the Company's website, it is intended that a user of an ivySend Contract can receive a price quote for execution over a 10 minute period, which locks in the execution quote for a given ivySend Contract transaction of the quoted parameters, within an upper and lower limit of volatility expressed by the Ivy Network, at the time the price quote is given.

In this way, when fully developed, IVY is anticipated to offer full utility functionality for its holders and protects them from volatility in operating against the contract.

b. Private Network, ivyReceive, and Private Ivy Tokens (IVYB)

The Ivy Private Network is intended to distribute funds to the bank accounts of intended recipients by the use of private ivyNetwork contracts (**ivyReceive Contracts**). The Ivy Private Network is proposed to operate using a private, permissioned version of the Ethereum blockchain specialised coordination of financial institutions and intermediaries.

It is anticipated that ivyReceive Contract will be hosted on the Ivy Private Network. It will be the mechanism by which the settlement ledgers of participating financial institutions and intermediaries stake their participation using a private Token (**IVYB**), which will be an Ethereum-compatible, ERC20 token that operates on the Ivy Private Network. ivyReceive Contract is intended to be how the Ivy Network uses IVYB for its direct settlement of balances of recipient accounts.

When fully developed, IVYB are anticipated to be asset-backed tokens that reflect Ivy Private Network account holders that have fiat reserves capable of clearing transactions to the Ivy Network. IVYB will be pre-mined by the Company, convertible to IVY by the Company only, and given to Ivy Network account holders in proportion to their reserves in the Ivy Network. In the case of the Company's use of IVYB, the Company is intended to offer a public accounting of IVYB assets and liabilities to show that its dollar deposits on the network are always equivalent to its token holdings, whether in escrow or reserve.

When message of a transaction pending arrives at the Ivy Private Network, an account holder must stake its IVYB for the opportunity to receive the represented balance; meaning that the Ivy Private Network account holder must have a balance of IVYB at least equal to the amount of the transaction. In this interaction, the process of staking the token provides the release of the supporting KYC/KYT/AML information to the institution or intermediary, from which they are prompted to accept or decline the funds (manually, or automatically, if pre-authorized). These Tokens are submitted to the ivyReceive Contract. The ivyReceive Contract has two mandatory conditions for release of staked tokens:

- a) Demonstration of Transaction Approval – Upon the review of applicable KYC/KYT/AML information, an agent of the applicable financial institution sends either an approval or a denial response back to the ivyReceive Contract. Here, there are two potential outcomes: a) the transaction goes through successfully, in which case the IVYB are returned and the IVYB

value on deposit by the Ivy Private Network account holder at the financial institution for the intended recipient's account; or, b) the transaction fails, in which case the IVYB are refunded to the financial institution; and

- b) Demonstration of Cash Deposit – A monitor of the status of Ivy Private Network account holder's bank account provides the mechanism by which demonstration of cash deposit by the financial institution into the recipient's account has occurred. This status may require either custom integration for the purpose of observing the account state, or similar using account access services from vendors such as Yodlee¹³, Xignite¹⁴, or Plaid¹⁵. Either way, the business-to-business arrangement between the Ivy Network and the financial institution will stipulate what the timing constraints for release of funds between the accounts are.

If both the 'demonstration of transaction approval' and the 'demonstration of cash deposit' are shown as true, the party staking IVYB on the Ivy Private Network is eligible to receive payment from the unlocked ivySend Contract on the Ivy Public Network. If both conditions are false, or until they are otherwise set to true, the ivySend Contract on the Ivy Public Network may be redeemed by the sender. Transaction approval may be withheld by a financial institution as it seeks to clear identified compliance requirements through the use of KYC/KYT/AML data submitted with the Ivy data container. Using metadata associated with the transaction and container, it is possible to facilitate a degree of automated clearing on the basis of country of origin, nature of goods exchanged in commerce, or other configurable rules as desired by the processing financial institution or intermediary. Just the same, manual workflow may require that escrow be maintained for an extended period of time. The default behaviour for submissions is for sender escrow to be determined by outcomes on the Ivy Private Network; however, it is envisioned that delays with the bank KYC/KYT/AML process, and communication between sender and recipient may also require some accommodation, whereby after a given period of delay, the sender may unwind the process by choosing to retrieve a Token deposit from escrow.

It is intended that the ivyReceive Contract maintains an observable balance of all pending staked transactions. Permissions on the Ivy Private Network provide isolation of the individual balances and workflow status of settlements pending at each of the Recipients' Financial Institutions and supporting Financial Intermediaries. In this way, the private token, when locked in the ivyReceive Contract is intended to, a) provide visibility to the process of consideration by which the financial institution or intermediary is considering the validity of the balance transmission; and, b) provide a throttle for the financial institution operations, such that they may not stake a disproportionate amount of transactions without clearing them to satisfaction. Of course, this also raises the question of what compels the financial institution or intermediary to make the deposit as required at all. For this purpose, the Ivy Network will be able to report the service levels of each of the financial institutions and intermediaries on its network. Clearly, if a financial institution is not serving the needs of its clients, the clients should have the ability to consider other options or opportunities from among the other participants on the Ivy Network where transfer receipt is either more timely or reliable.

c. Interchain Communication and the Ivy Oracle Service

The Ivy Network is intended to serve as a functional intermediary between the Ivy Private Network and Ivy Public Network detailed above, listening to and responding to events associated with the ivySend Contracts and ivyReceive Contracts.

It is anticipated that state changes in the ivySend Contract are observed by authorized Ivy validators participating on the public Ethereum network. Similarly, state changes in the ivyReceive Contract are observed by Ivy Network validators participating on the Ivy Private Network. Both of these validator sets will be able to inform the Ivy Oracle Service that provides attestation to the state of each escrow contract and facilitates their respective functions.

Of specific interest is how value moves from the Ivy Public Network ledger balance to the Ivy Private Network ledger balance. This is intended to involve a value transfer from IVY to IVYB, which occurs upon the approval message to the ivyReceive Contract and demonstration of posted balance to a recipient's bank account. At the point when these two events occur, the IVYB is released, and the IVY in the escrow agreement is claimed by the Ivy Network. The IVY receives the determination of the IVYB transaction on the Ivy Private Network ledger through the use of the Ivy Oracle Service and its constituent validators to the Ivy Private Network. When the IVYB was committed to the ivyReceive Contract, the public address of the sender to the IVYB will be recorded. This public address was used for sending the Ivy transaction container of KYC/AML information. Subsequently,

13. <https://www.yodlee.com/>

14. <https://www.xignite.com/>

15. <https://www.plaid.com/>

this address is used as a settlement account address for the Ivy Network to privately settle its own transactions against the network.

2) Identity on the Ivy Network

When fully developed, it is intended that the Company will manage two types of identities on the Ivy Network: sender identities, and financial institution and intermediaries identities.

a. Sender Identity

The Ivy Network is intended to require senders to register with the network prior to sending currency. It is assumed by the Ivy Network that recipients are identified by their respective financial institutions and intermediaries as part of establishing an account.

For establishing a sender account on the Ivy Network, self-sovereign identity is sufficient; however, additional transaction information may be required for authorization against the Ivy Network. This information is submitted and stored by the sender on the Ivy Network to establish an account and allow for the Company to provide attestation for specific transaction types where supporting information is required. Copies of sender sovereign identity information are packaged in the Ivy data container as part of the submission of the transaction to the intended balance recipient's financial institution and other intermediaries. While specifically restricted to their purposes, these credentials may be accessed and are relevant for extended periods of time beyond the transaction. Using the Company's website, it is possible to monitor who and when these credentials are being accessed on a continuing basis.

b. Financial Institution and Intermediary Identity

It is intended that Ivy will rely on the good hiring practice and vigilance of information security practices at the financial institutions and intermediaries where it communicates data. It would be largely impractical for the Company to keep track of all employment events, corporate and HR-related activities. Accordingly, the Ivy Network will require the identity of relevant compliance staff at financial institutions, intermediaries, and interested agencies to be registered with the Ivy Network for the purpose of enabling and disabling access to distributed containers of KYC/AML data. The Ivy Network will be updated on relevant employment actions of financial intermediaries on a timely basis.

It is anticipated that financial institution managers may log into the Ivy Network to manage the access and permissions of relevant staff to ivyReceive Contract functions and container data. All activities of identified users can be centrally tracked and managed, and individual transaction container history viewed.

3) Blockchain Technology Application

Consensus on distributed ledger is the function by which validators, sometimes called miners, determine the accurate representation of data as appropriate to reflect correct ledger balances given the transactions submitted to the network. Given the opportunity for network and system disruptions, it is easy to anticipate that there are opportunities by which some parties may be disconnected and miss important data during their unexpected absences.

Just the same, in a network where there are shared perspectives, there need to be established mechanisms to come by one settled outcome of the truth. In networks such Bitcoin and Ethereum, the current mechanism is called 'proof of work'. Proof of work encourages validators to compete on the basis of computing power and electricity to validate transactions submitted to the network. Having more computing power helps validators solve cryptographically difficult problems that are subsequently submitted to the network for the right to append captured transactions as blocks to the network (incidentally, these blocks of transactions are validated on the predication of other blocks that have been previously submitted, creating a chain—hence the term 'blockchain'). As the blockchain grows, new blocks increase in difficulty to append—and validators compete at great expense for the value of both validation incentives and block rewards they hope to capture and redistribute within their networks. While providing for a notion of byzantine fault tolerance, this process is both expensive and slow for a private network. Consequently, this is why Bitcoin and Ethereum both process fewer than 20 transactions per second¹⁶. Alternatively, a consensus mechanism called 'proof of stake', implemented by Tendermint and proposed as the 'Casper' consensus improvement to Ethereum moves the expense of gaining the right to append ledger transaction blocks from investment in computing and electrical power to investment in the cryptocurrency itself¹⁷. In proof of stake, a party with proportionally more

16. <http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>

17. CIT

cryptocurrency has proportionally more likelihood of appending the next block of transactions. Because each validator is ‘staked’ in the network, the network can potentially punish the validator by reclaiming their interests in the network for malicious behaviour that results in the production of false transaction blocks that requires subsequent correction by the rest of the network. Challenges occur from this approach for two main reasons, however: a) any single party or colluding parties with 51% of the network value has a greater likelihood of winning consensus; and b) a malicious majority cannot be overruled through the investment in computing power, as proof of work allows. Moreover, just as proof of work requires validation incentives to reward validators to capture transactions in the form of block rewards, proof of stake similarly uses incentives (e.g.: ‘gas’) to prevent the submission of transactions that create work without commensurate financial value on the network (e.g.: spam).¹⁸

In financial payments networks, specifically private and permissioned network are more readily organized and governed by shared interest than public anonymous networks, so issues of aligning incentives to prevent suspect behaviour give way to concerns regarding practical throughput and resilience of coordinating functions that facilitate accurate and compliant settlement. Networks including Stellar and Ripple use their own validators, or shared participation of validators to shield their direct inputs to network results,¹⁹ whereby external and malicious participants are unlikely. Here, their consensus is focused on resilience and availability of distributed ledgers through their networks. As a result, throughputs are higher.²⁰

The Company envisions the Ivy Private Network as consisting of validation nodes sponsored by entities other than itself. The Ivy Private Network will be validated directly by financial institutions and intermediaries, who are independent, yet aligned. In this environment, spam messages from permissioned network participants seem highly unlikely, and even deleterious to their shared goals for participating in the Ivy Network in the first place. Greatly reduced likelihood of network spam and aligned incentives removes the need for block rewards that typically incentivize public blockchain networks. For consensus, the use of a scheduled byzantine fault tolerant algorithm, such as Istanbul BFT makes most sense.²¹ In this consensus algorithm, each participant creates blocks on a scheduled, round-robin basis and submits its results to the rest of the network, which must vote with a 2/3 majority to approve the leader’s block calculation. This approach allows approximately 1/3 of validators on the network may prove to be malicious while still proving the network resilient. Specific benchmarks of Istanbul BFT indicate that it is capable of ~1000 transactions per second,²² which reflects the total estimated network of interagency transactions that happen today between FedWire, SWIFT, and ACH today.²³

For its purposes, it is anticipated that the Ivy Private Network will initially adopt the use of Quorum, JP Morgan Chase’s implementation of permissioned Ethereum using the Istanbul BFT consensus algorithm.²⁴ This implementation of Ethereum has a number of potential benefits for the Ivy Network: a) it provides the benefits of the Ethereum blockchain as validated and improved in the context of a global financial institution; b) it provides interoperability with smart contract development and investment that can be prototyped and made portable to any number of other Ethereum Virtual Machine (**EVM**) supporting environments (including Ethermint, Qtum, and even the public Ethereum blockchain);^{25,26} and, c) given its familiarity as an alternative blockchain in the financial community, its adoption and use provides a baseline of community and support most likely to be echoed in the same financial institutions and intermediaries that the Company seeks to support its network functions. Quorum additionally supports alternative consensus algorithms based on authority of the leading validator, should higher transaction throughput be required and stability of the intentions of network participants allow for reductions in block validation overhead.

18. In public settings, potential spam transactions can crowd legitimate transactions, creating an environment similar to that which exists in the settings of a denial of service attack; if validators are consuming effort with worthless transactions, valuable transactions have a harder time being processed.

19. CIT - Stellar sharding

20. CIT

21. Byzantine fault tolerance or (BFT) is a reference to a problem in computer science that addresses coordination issues within networks of distributed systems, commonly referred to as the byzantine generals problem, whereby any single system actor, left to their own devices, is incentivized to work in their own interest, instead of the honest interests of the network.

22. <https://www.slideshare.net/YuTeLin1/istanbul-bft>

23. CIT

24. <https://github.com/jpmorganchase/quorum>

25. CIT [Ethermint Whitepaper]

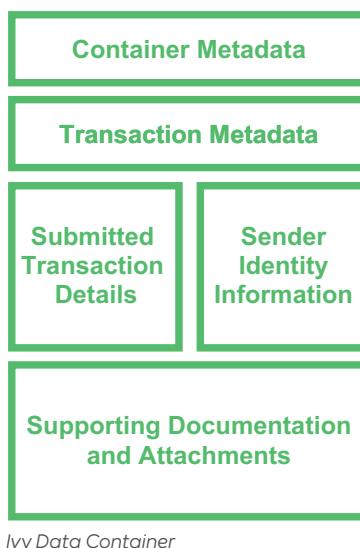
26. CIT [Qtum Whitepaper]

Private network nodes further coordinate the exchange of data using IPFS and BigchainDB to ensure availability and data integrity.^{27,28} A logical representation of a private network node is shown in the figure below:



4) Ivy Data Containers

It is anticipated that the Ivy Network will use dxChain cryptographic containers to store KYT/KYC/AML data in a date container (**Ivy Data Container**). Users submit their data through the distributed application interface on the Ivy web site at the time they request the transfer of currency. This specific container format of the Ivy Data Container is shown in figure below:



Contents of the Ivy Data Container are intended to include:

- Container metadata
- Transaction metadata
- Submitted transaction Details
- Sender identity information (as applicable)
- Supporting documentation and attachments

Using this format, each component of supporting data is independently and persistently encrypted to secure access at rest and during exchange using standard AES-256 symmetric and 4096 bit RSA asymmetric cryptographic methods, and SHA-384 message digests. Digital signature based on RSA asymmetric keys are anticipated as vulnerable to both Grover's²⁹ and

Schor's³⁰ algorithms regarding the applications of quantum computing to the determination of black-box function inputs and

27. <https://ipfs.io>

28. <https://www.bigchaindb.com>

39. https://en.wikipedia.org/wiki/Grover%27s_algorithm

the factoring of large numbers, respectively, these algorithms will be upgraded to reflect the availability of quantum resistant algorithms, as better understanding and support by industry becomes available.³¹

Cryptographic containers are intended to provide for a few key features to the Ivy Network:

- Provide persistent control and protection of all communicated information;
- Provide ability for the Ivy Network to add or remove parties to the container after initial receipt; and
- Provide the sender with surety that the specifics of their transaction with the recipient are confidential.

Through the use of Ivy Data Containers, individual behaviours against the network can be tracked and verified.

Ivy Data Containers are intended to store both structured and unstructured content collected from the ivySend Contract submission process. Where applicable, Ivy normalizes the collection of data within the Ivy Data Container to comply with data sets, codes, and formats of the ISO 20022 standard.³²

a. Generation and Storage of Ivy Data Containers

When fully developed, upon submission of content to an Ivy Network contract, a request is made to the Ivy Network to generate a container of the relevant data. The application will send submitted KYT/KYC/AML data to the Ivy Network, and return the container identifier back to the sender. The sender submits their Ivy deposit and the generated container identifier to the ivySend Network contract.

When generated, the Ivy Data Container becomes resident on an IPFS file system that is hosted within the scope of the Ivy Private Network. The Ivy Private Network file system will allow for sharing of relevant content within the network.³³ Three separate writes of the container are made to the Ivy Private Network to ensure file redundancy, as only local copies are guaranteed upon request. A mapping of these container identifiers and object identification points on the Ivy Private Network are stored in a BigchainDB network that is shared between the nodes of the Ivy Private Network.³⁴

Retrieving Ivy Data Containers involves querying the BigchainDB network by the container identifier of the generated container to receive the relevant object identifiers for retrieving related containers. Within the Ivy Network, this functionality is abstracted and maintained by a hosted service on the permissioned network. Ivy Data Containers may be copied and stored freely without violating their underlying security model.

b. Accessing Ivy Data Containers

It is intended that access to Ivy Data Containers is managed by a network-bound access management service, that is responsible for handling requests for specific portions of Ivy Data Container content and providing requisite access on the basis of the following criteria (for the purpose of simplification, users, systems, and processes of systems are treated as user requests):

- a) the requesting user's organization – the determination of whether the KYC data relates to a transaction that occurred by the requesting user's organization, or, alternatively, if the requesting user's organization is a regulator;
- b) the requesting user's submitted credentials – the determination of whether the requesting user's credentials are current per communication between Ivy Private Network account holders and the Ivy identity management environment; and
- c) specific administrative restrictions placed on the requesting user's submitted credentials and the specific types of identity information being requested. For example, specific information identified as Personally Identifiable Information may not be available to all requesting users. These restrictions are coordinated between administrators from constituent financial institutions and the Ivy Network.

Upon successful authorization to the Ivy Data Container, requested content is presented to the requesting user or process.

30. [https://en.wikipedia.org/wiki/Shor's_algorithm](https://en.wikipedia.org/wiki/Shor%27s_algorithm)

31. <http://nvlpubs.nist.gov/nistpubs/ir/2016/NISTIR.8105.pdf>

32. <https://www.iso20022.org/>

33. <https://ipfs.io/>

34. <https://www.bigchaindb.com>

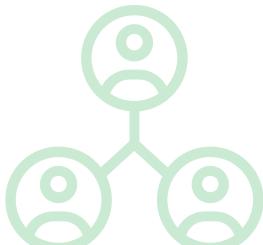
Host: Token Generation Event

7

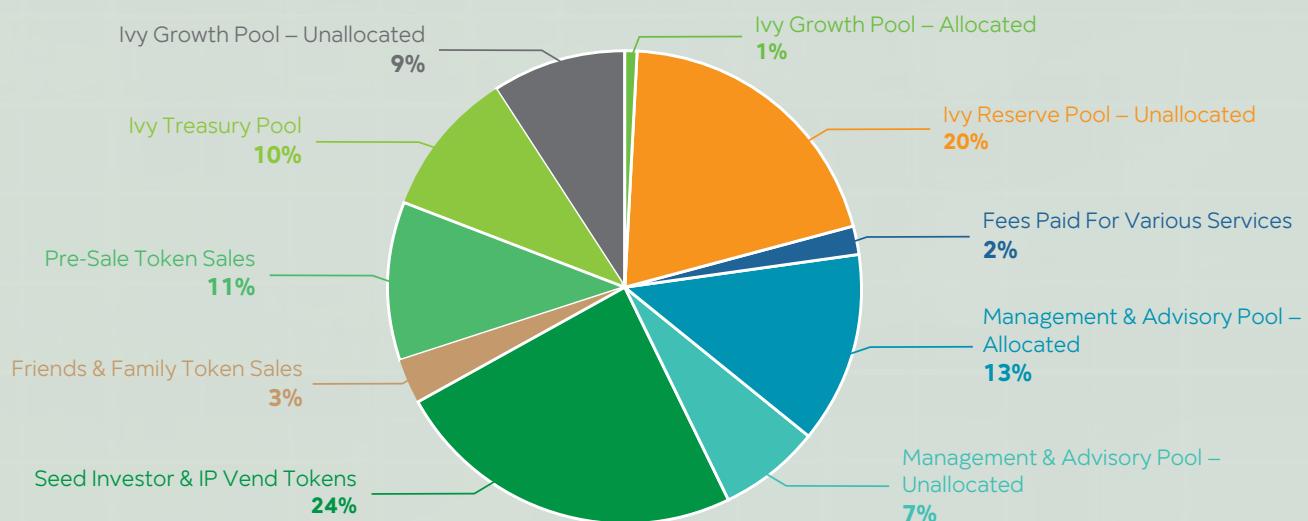
Token Structure post Token Generation Event

Token Structure (Post TGE) – clear breakdown

Pre-Sale Token Price	US\$0.10
Tokens offered in private sale	170 million
Amount raised through private token sale	US\$17 million
Token Generation Event	April 2018
Total token issuance	1.6 billion



Ivy Token Distribution



Total Token Supply: 1,610,924,200 (100%)

Pre-Sale Token Sales – Tokens purchased in the pre-sale token sale.

Friends & Family Token Sales – Tokens purchased in the friends & family token sale.

Seed Investors & IP Vend Tokens – Tokens purchased by seed investors and used to acquire IP.

Ivy Growth Pool – Used to incentivize partners including financial institutions to test and adopt Ivy.

Fees Paid For Various Services – Tokens used to pay for marketing costs, exchange fees and other services.

Management & Advisory Pool – Incentivize current advisors and future management to join the company.

Ivy Reserve Pool – Only used to fund further development and operating costs if required.

Ivy Treasury Pool – Used to facilitate ivySend transactions and other treasury functions.

8

Roadmap

The following dates and events are anticipated and aspirational respectively.

H2
2017

Establishment of Partnership with ASX:CCA

Partnership with US award winning ASX listed Fintech Solutions and Blockchain Investment Company Change Financial Limited

H1
2018

Token Security Audit

Smart Contract coding and auditing

Token Generation Event

The Token Generation Event allows to substantially accelerated platform development and incentivization of early users onto the Platform

Business Development

Recruitment for key positions. Ivy community development, marketing and introduction to mainstream media

Application Development

Establishment of a test network with smart contracts

Open Communication with Financial Institutions

Develop communication channels for Financial Institutions to begin Due Diligence process of Ivy technology

Private Sale (US\$17 million)

Completion of heavily oversubscribed private token sale of US\$17 million

Partnership with First major bank

Signing of MOU with first multi-billion dollar bank

Exploratory Meetings with Regulators

Engage with regulators regarding Ivy Project

**H2
2018**

Test Network

Live test network at www.ivyproject.com

Regulatory Whitepaper

Release of result of US Regulatory Whitepaper

Key Partnerships with Financial Institutions

Financial institutions testing Ivy beta product on live network

Begin Distribution of Growth Pool

Begin distribution of tokens for Financial Institutions to test and adopt Ivy

2019

First Financial Intermediaries

All Fiat/Crypto Conversions Live

Marketing and Partnership

Accelerated Financial Institution partnerships as the blockchain technology transitions into mainstream society

Development of Minimum Viable Product (MVP)

Public network live

IvySend live with legacy interbank systems

Direct IVY sales and market operations live

IvyReceive live with IVYB interbank funds transfer

It is intended that the development of the Ivy Network will occur in two Phases over 2018 and 2019. In Phase 1 of development of the Ivy Network, payments are received directly from the Company via legacy interbank payment methods such as ACH or wire. In Phase 2, banks receive payments from Ivy Network validators who facilitate private IVYB transfers on the network and immediate, direct payments to member Financial Institutions through accounts they maintain there. Over time, the Company will seek to:

- Build the network of participating Financial Institutions globally
- Expand conversion capabilities to include many more fiat currencies and digital assets
- Develop partnerships with organizations who can benefit from the Ivy Network
- Develop improved methods for KYT/KYC/AML data verification

9

Risks

Rights and Tokens are considered highly speculative and the purchase of Rights and Tokens carries with it a number of risks. The Directors strongly recommend that potential purchasers consider the risk factors described below, together with information contained elsewhere in this paper, and consult their professional advisers before deciding whether to acquire Rights and Tokens.

If any of the following risks are unacceptable to potential purchasers, then the potential purchaser should not purchase Rights or Tokens.

The order of the risks set out below is not intended to have any bearing on the likelihood of such risk arising, or importance of any such risk to any particular purchaser.

Purchases of Rights and Tokens should only be undertaken by individuals or entities that have significant experience with, and understanding of, the usage and intricacies of cryptographic tokens, like Bitcoin and Ether, and other blockchain-based software systems. Purchasers should have a functional understanding of storage and transmission mechanisms associated with other cryptographic tokens. The Company is not offering advice and the Company will not be responsible for any lost funds, Rights or Tokens resulting from actions taken by, or omitted to be taken by purchasers.

Loss of access

Tokens may be stored in a wallet and be accessible with (inter alia) key signatures. Loss of the requisite private key(s) associated with a purchaser's digital wallet will result in loss of the stored Tokens. If a purchaser does not maintain an accurate record of its private key or the password used to access its private key, this may lead to the permanent loss of access to its Tokens. Purchasers must safely store their passwords in one or more backup locations that are well separated from the primary location. Any third party that gains access to a purchaser's private key may be able to gain access to the purchaser's Tokens. If a potential purchaser does not have such experience or expertise, then it should not purchase Rights or Tokens.

Risks associated cryptocurrency protocol

Tokens are based on cryptocurrency protocols. Any malfunction, unexpected functioning, forking, breakdown or abandonment of the Ivy protocol may have a material adverse effect on Tokens. For example, this might adversely impact a purchaser's ability to transfer or securely hold Tokens. In addition, advances in cryptography or the development of quantum computing, could render ineffective the cryptographic consensus mechanism that underpins the Ivy protocol. Any such impact could adversely affect the value of Tokens.



Mining attacks

Tokens are susceptible to attacks by miners in the course of validating Token transactions on the Ivy blockchain, including, but not limited to, double-spend attacks, majority mining power attacks, selfish-mining attacks and race condition attacks. Any successful attacks present a risk to the Tokens, including, but not limited to, accurate execution, recording of transactions involving Tokens and expected proper payment operations.

Hacking, cyber threats and security weaknesses

Hackers, individuals, other malicious groups or organizations may attempt to interfere with the Tokens and any platform on which they are traded in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing.

Advances in code cracking, or technical advances such as the development of quantum computers, could present risks to the Tokens, which could result in the theft or loss of Tokens.

Markets risk

The Company cannot fully control the actions of any or all purchasers of Tokens. Even if secondary trading of Tokens is facilitated by third party exchanges, such exchanges may be relatively new and subject to little or no regulatory oversight, making them more susceptible to fraud or manipulation. Furthermore, to the extent that third parties do ascribe an external exchange value to Tokens (e.g. as denominated in a fiat currency), such value may be extremely volatile and diminish to nil. If a purchaser chooses to use Tokens on exchanges it is at the purchaser's own risk. Such exchanges are independent of and are not operated or controlled by the Company.

Risk of exchanges

Cryptocurrency exchanges on which Tokens may trade may be relatively new and are likely to be largely unregulated and may therefore be more exposed to fraud and failure than well-established regulated exchanges. Where cryptocurrency exchanges representing a substantial portion of the volume in Token trading are involved in fraud or experience security failures or other operational issues, such cryptocurrency exchange failures may result in a reduction in the price and value of Tokens.

Uninsured and transaction losses

Unlike funds held in accounts at banks or some other financial institutions, Tokens are generally uninsured unless a purchaser specifically obtains private insurance. In the event of loss of Tokens or the loss of the ability to use the Tokens, there is no public insurer or private insurance arranged in respect of the Tokens.

If Tokens are stolen or incorrectly transferred, such Tokens may not be recoverable and the Company takes no responsibility for their recovery. As a result, any incorrectly executed Token transactions could adversely affect the value of Tokens.

Cryptographic token transactions are not reversible without the consent and active participation of the recipient of the transaction or, in theory, control or consent of a majority of the processing power on the host blockchain platform. Once a transaction has been verified and recorded in a datablock that is added to the blockchain, an incorrect transfer of a Token or a theft of a Token generally will not be reversible and there may be no compensation for or avenues of legal or other recourse in respect of any such transfer or theft. Such loss could adversely affect the value of Tokens generally.

Uncertain regulations, enforcement actions and geopolitical events

The regulatory status of the cryptographic tokens, blockchain and distributed ledger technology is unclear or unsettled in many jurisdictions. It is difficult to predict how or whether regulatory agencies may apply existing regulation with respect to such technology and its applications, including the Tokens. It is likewise difficult to predict how or whether legislatures or regulatory agencies may implement changes to law and regulation affecting blockchain and distributed ledger technology and its applications, including the Tokens.

Regulatory actions could negatively impact the Tokens in various ways, including, for purposes of illustration only, through a determination that Tokens are a regulated financial product or instrument in one or more jurisdictions that attracts disclosure, registration or licensing requirements or by the banning of the use of or dealings with Tokens altogether.

The Company may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approvals or meet the relevant regulatory requirements to operate in such jurisdiction.



Political or economic crises may motivate large-scale sales of Tokens, which could result in a reduction in the price and adversely affect the value of Tokens. Cryptographic tokens such as the Tokens are subject to supply and demand forces based upon the desirability of an alternative, decentralised means of transacting, and it is unclear how such supply and demand will be impacted by geopolitical events. Large-scale sales of Tokens would result in a reduction in the liquidity of such tokens.

Tax

The tax characterization of Rights and Tokens and the tax ramifications of holding Rights and Tokens is uncertain in many jurisdictions. Purchasers must seek their own tax advice in connection with purchasing Rights and Tokens, which may result in adverse tax consequences to Purchasers, including but not limited to withholding taxes, income taxes and tax reporting requirements. Purchasers bear the sole responsibility for any taxation requirements, in purchasing, using and holding Tokens.

Unfavourable currency fluctuations

The Company intends to use the proceeds from selling Rights to fund the maintenance and development of the Tokens. The proceeds of the Offer will be denominated in United States dollars. If the value of United States dollars fluctuates unfavourably during or after the Offer, the Company may not be able to fund development of the Tokens.

Extreme volatility

Tokens are not intended to represent any formal or legally binding investment and will not necessarily be tradable on any public market once developed. In addition, cryptographic tokens that possess value in public markets have demonstrated extreme fluctuations in price over short periods of time on a regular basis. Such fluctuations are due to market forces and represent changes in the balance of supply and demand. Exchanges and public markets are independent of and are not operated by the Company. Trading on any exchanges or public markets is at each purchaser's own risk and the Company cannot and does not guarantee any market liquidity or saleability of Tokens.

Additionally, different regulatory requirements in different jurisdictions and the potential inability of citizens of certain jurisdictions to open accounts at exchanges located throughout the world, the liquidity of Tokens may be materially different in different jurisdictions. This would likely be reflected in significant price discrepancies between markets. It is also possible that the value of Tokens will drop significantly in the future. Any such drop in the value of Tokens could adversely impact the Company's ability to raise funding for continuing operations including the development of the Tokens.

It is possible that a competing cryptographic currency could have features that make it more desirable than Tokens to a material portion of the cryptographic token user base, or that there could be a general reduction in the use of cryptographic tokens due to an overall reduction of confidence in the technology. Any such occurrences may result in a reduction in demand for and use of Tokens, which could have a negative impact on the price of Tokens generally.

In addition, a lack of stability in the cryptocurrency exchanges and the closure or temporary shutdown of cryptocurrency exchanges due to fraud, business failure, hackers or malware, or government-mandated regulation may result in greater volatility in the price of Tokens.

Intellectual property rights claims

Third parties may make intellectual property ownership claims relating to the Rights or Tokens and/or their source code or other underlying intellectual property. Regardless of the merit of any intellectual property claim or other legal action, any threatened action may adversely affect the value of Tokens.

Unanticipated risks

The Rights and any to be developed Tokens represent a new and relatively untested technology.

In addition to the risks noted above, there are other risks associated with any purchase of Rights or Tokens, the holding of Rights and Tokens and the use of Rights and Tokens, including risks that the Company has not anticipated.

Unanticipated risks may come in the form of variations or combinations of the risks set out above or otherwise.

Glossary

ETHEREUM

Ethereum is a leading decentralized platform for smart contracts, utilizing the Solidity programming language. It is an open source, public blockchain-based distributed computing platform.

ETHER

The value token of the Ethereum blockchain platform is called "ether".

SMART CONTRACTS

Smart Contracts are programming abstractions that explicitly represent the exact terms of the exchange relationship between parties. Smart Contract terms must be satisfied and confirmed as "truth" prior to a transaction to be recorded and executed. The Smart Contracts are written in a programming language called Solidity. All such Smart Contracts are stored publicly on every blockchain node.

IPFS

Is an open source, decentralized file system protocol that provides a permanent method for the creation, storage and sharing of documents. IPFS nodes form the basis of the distributed file sharing network. It is a high throughput, based on a block storage model. It utilizes hashes for file identification that can create a robust environment for the unalterable data storage.

SOLIDITY

Smart Contracts for blockchain are written in a programming language called Solidity.

X509

A cryptography standard for the definition of public key certificates. It is a key component of secure communications and can be used to validate "digital signatures" in electronic transactions. X.509 is defined by the International Telecommunications Union, (ITU) a United Nations agency charged with the global coordination of telecommunication and standards.

PKI

Public key infrastructure (PKI) is a set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and is a key component of public-key based encryption systems.

CHAIN OF TRUST

A chain of trust is established by validating each component of hardware and software from the bottom up. This ensures that only trusted software and hardware can be used by validating each hardware and software component in the chain.

DATA FIELDS

The amount of data sent in a transaction varies depending on the requirements as defined by the parties and as required by the Smart Contract that governs the transaction. Ivy does not verify Customer data (beyond a simple account opening process) rather, Ivy facilitates.



www.ivykoin.com