Key Ecosystem **Challenges**

CRYPTO- CURRENCY ... **CBDC** ... DIGITAL **FIAT** CURRENCY

Protecting Digital Currencies

Presented by: Jacques Francoeur B.A.Sc., M.A.Sc., MBA
Chief Scientist & Founder, Security Inclusion Now USA

USA Delegate (2018,19,20) Security Expert & Contributor
International Telecommunications Union Standardization, Study Group 17: Security
Expert Network Member World Economic Forum, Blockchain Security

Today's State of Global Protection

Wealth[1]

2018 global economy estimated to be **$86 Trillion**

Internet Connected[2]

As of **June 2019**, there were **4,5B** people **connected** to the **Internet**
A **59%** penetration, based on a population of **7,7B**

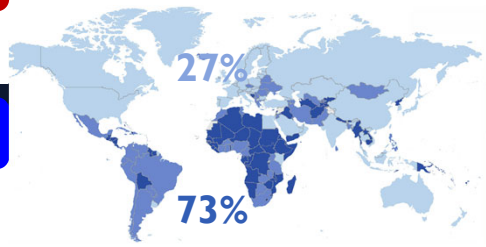
Not Sustainable

2019 Global Risks Report[3] According to the World Economic Forum

Identifies **Cyber** as the **4th** greatest risk facing the world

How well are we Protected? According to the **2018** ITU Global **Cybersecurity Index**[4]

27% or **1.2B** people **think** they are protected
73% or **3.3B** people are under protected, with **45%** with little to no **protection**



Security spending[5] estimated to be **$300B** by **2023**

27% or **1.2B** people who think they are protected will spend **~80%** of global **budget** estimated **$240B** 2023
Remaining **73%** or **3.3B** people that are under-protected will spend **~20%,** estimated **$60B** by 2023

1: https://howmuch.net/articles/the-world-economy-2018
2: June 2019 World Internet Usage & Population Statistics https://www.internetworldstats.com/stats.htm
3: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
4: Global Cybersecurity Index (GCI) 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
5: https://www.gminsights.com/pressrelease/cyber-security-market

The **Struggle** to Protect

Internet-of -**Value**

Value **Creation** *Anywhere*

Value **Consumption** Somewhere Else

Value **Creation** Force

Value **Risk** Force

Value Creation "**is Threatened by**" Value Risk

Value Creation "**is Protected by**" Value Preservation

Value **Assurance** Force

Value **Preservation** Force

Value Preservation "**is Validated by**" Value Assurance

A **Need** for a **Rethink**?

Internet-of-Value Ecosystem

Supply ***Demand***

Value **Creation** Value **Consumption**

*Anywhere - **from** the Edges*  to the Edges

Digital Currency

Value Exchange **Friction** & **Loss**?

The **Struggle** to Protect

Internet-of -**Value**

Value **Creation** *Anywhere*

Value **Consumption** Somewhere Else

Value **Creation** Force

Value **Risk** Force

Value Creation "**is Threatened by**" Value Risk

Value Creation "**is Protected by**" Value Preservation

Value **Assurance** Force

Value **Preservation** Force

Value Preservation "**is Validated by**" Value Assurance

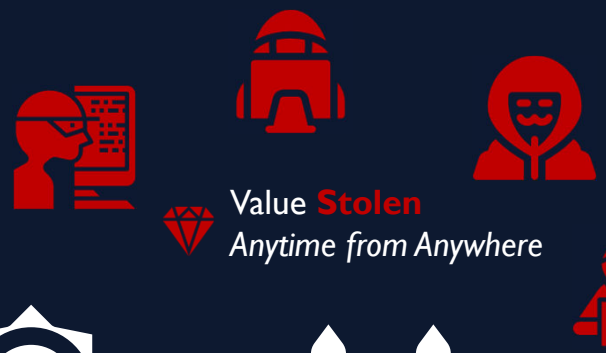
A **Need** for a **Rethink**?

Digital Currency: Standards, Laws, Regulations **Ecosystem**

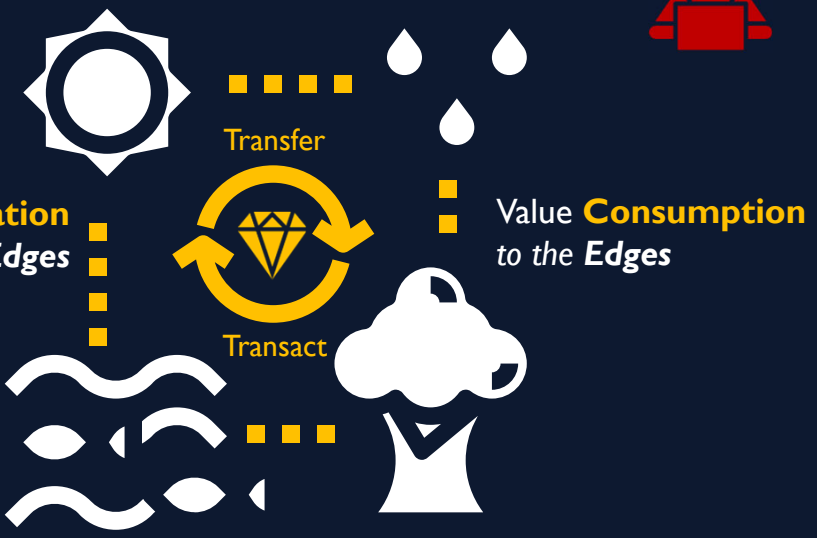
Value **Creation** *from the **Edges***

Value **Consumption** *to the **Edges***

Financial Inclusion



Value **Stolen** *Anytime from Anywhere*



Value **Creation** *from the **Edges***

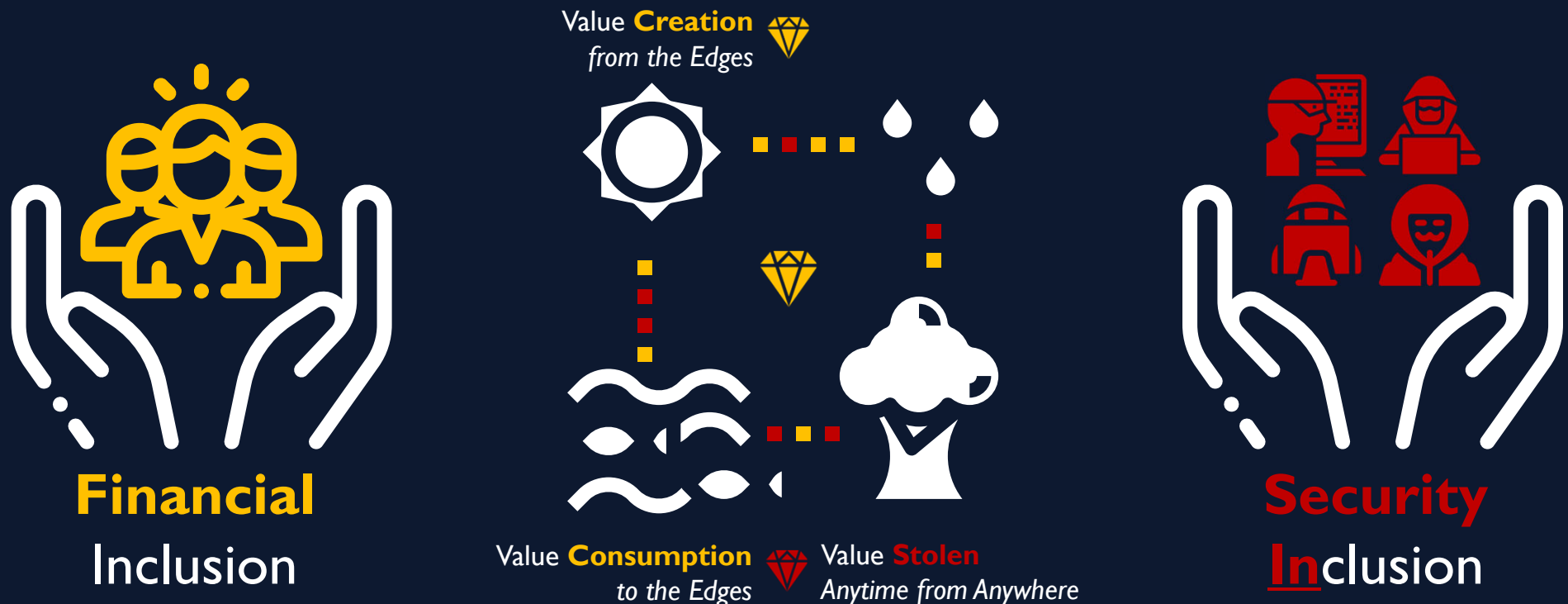
Value **Consumption** *to the **Edges***

DC
Wild, Wild West

Loss of **Confidence**

Digital Currency: Standards, Laws, Regulations

Loss of **Confidence** <<< Value **Consumption**



For Digital Currency, the Need for **Assurance**

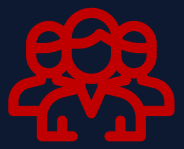
Value **Creation** *from the **Edges***

Value **Consumption** *to the **Edges***

Financial Inclusion

I created Value!

I purchased Value!



Who?

Identification for **Attribution,** Ownership
- Identifiers
- Access
- Authorization

Control = Ownership

What Value was **created?**

What Value was **purchased?**

What?

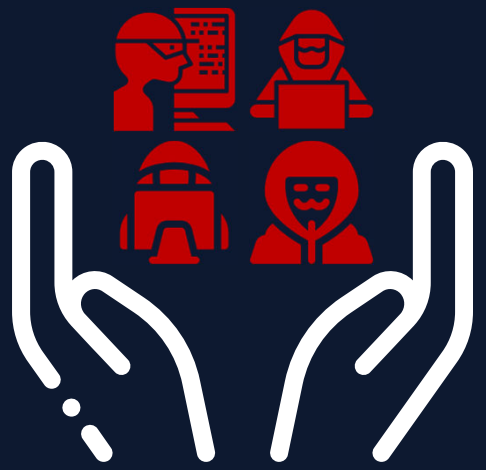
Cryptography for
- Immutability
- Confidentiality
- Authenticity
- Attribution
- Proofs
- Distributed Trust

I own Value!

Transact Away!

Assurance for:
- Trust
- Liability
- Warranties

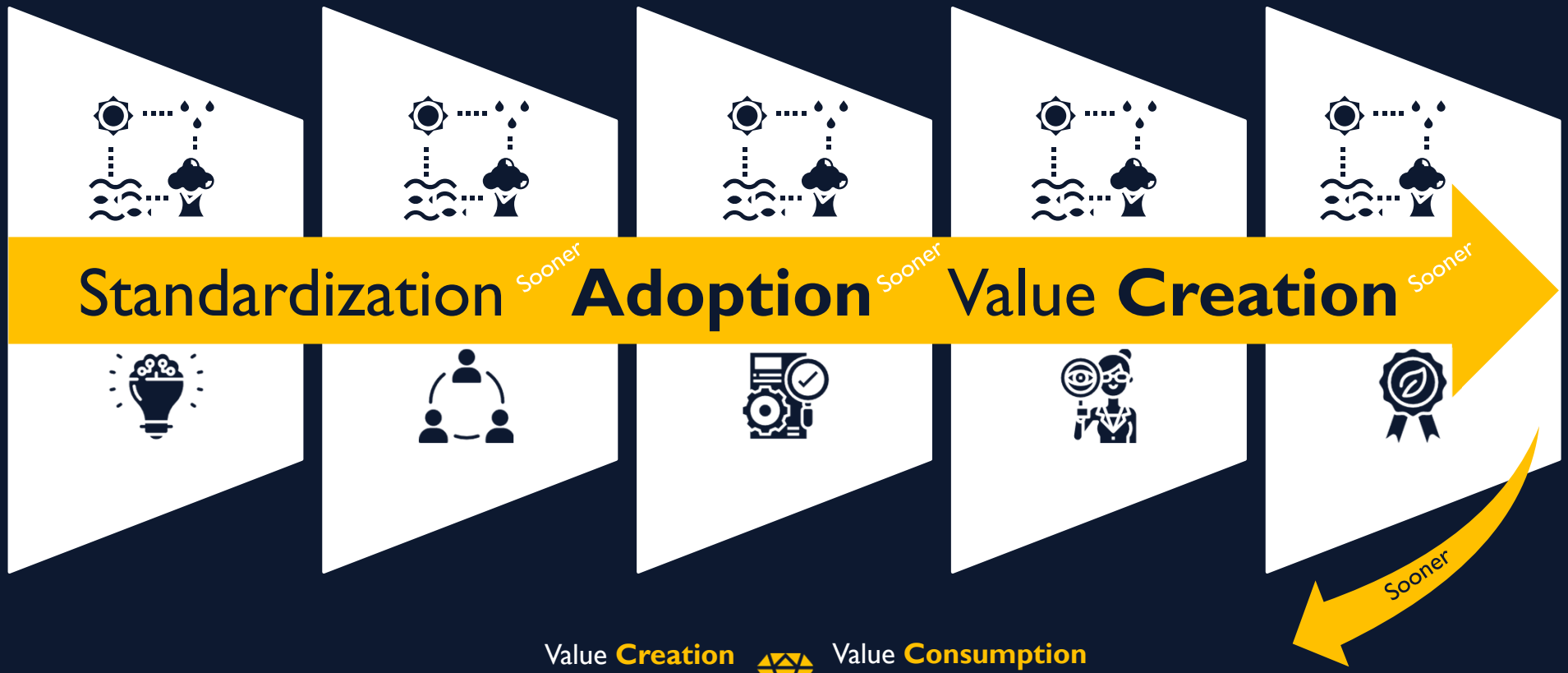
Value **Stolen** *Anytime from Anywhere*



Security **In**clusion

The Need for **Standardization**

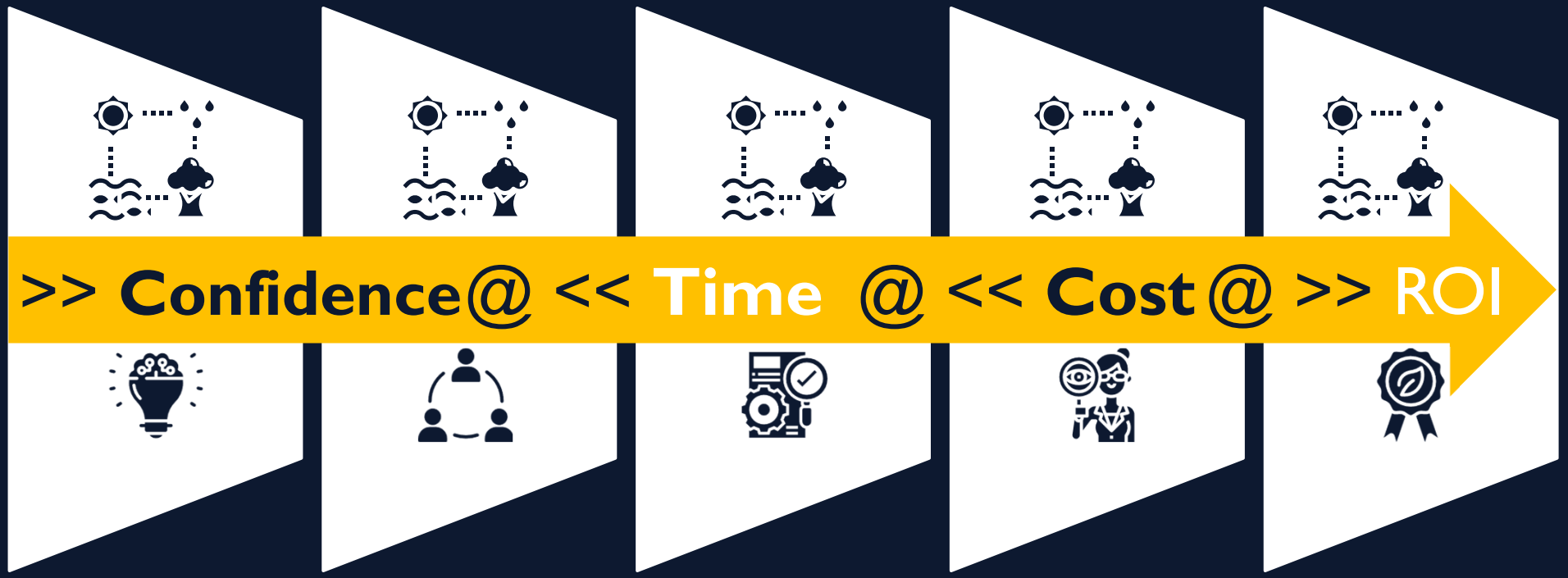
… of **performance** and **security specifications**



Value **Creation**
*Anywhere – from the **Edges***

Value **Consumption**
*Somewhere Else – to the **Edges***

Need for **Hyper** – Standardization, **Time to**



Need for Expert Collaboration

Drive **ecosystem-wide** **consensus** on Digital Currency:

- **R**equirements & **S**pecifications
  - Performance, Security & Resilience
- **M**easurement **M**etrics & **M**ethods
- **M**odels & **T**emplates for **R**euse

Need for Speed – Time to Validation

Domain Experts propose suitable specifications - input into **Validation**

Outcome - **standardized**

- **Common** specifications & requirements
- **Consistent** measurement methods & metrics
- **Comparable** models, templates & evaluations

Need for Speed – Time to Validation

Validation process:

- **Common** specifications & requirements
- **Consistent** measurement methods & metrics
- **Comparable** models, templates & evaluations

Standardized

- Models
- Measurement Metrics
- Evaluation Methods

that will ensure
Repeatability w/ **High Confidence**
for a basis of
Performance & Protection
Assessments & Benchmarking
across the **Ecosystem**

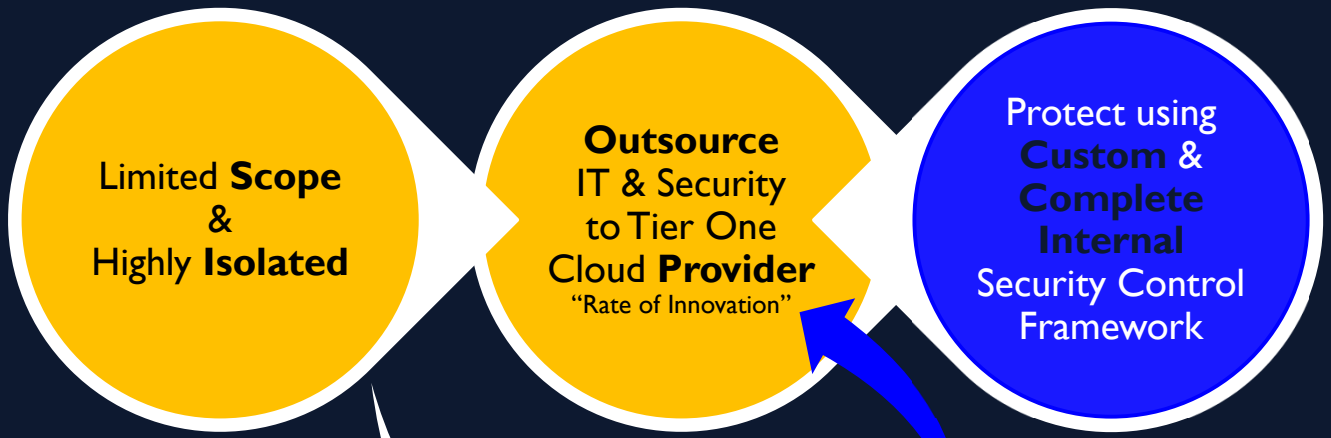
The **Need** to be: **Top Tier**

In-Scope
Small & Separate

No loss of Ownership
or Control
"The **Target**"

Leverage External
Security Standard's &
Best Practices

Security
Situational
Awareness



Persistent
state of
Protection

Dynamic
Expand-on-Demand,
Contract Immediately

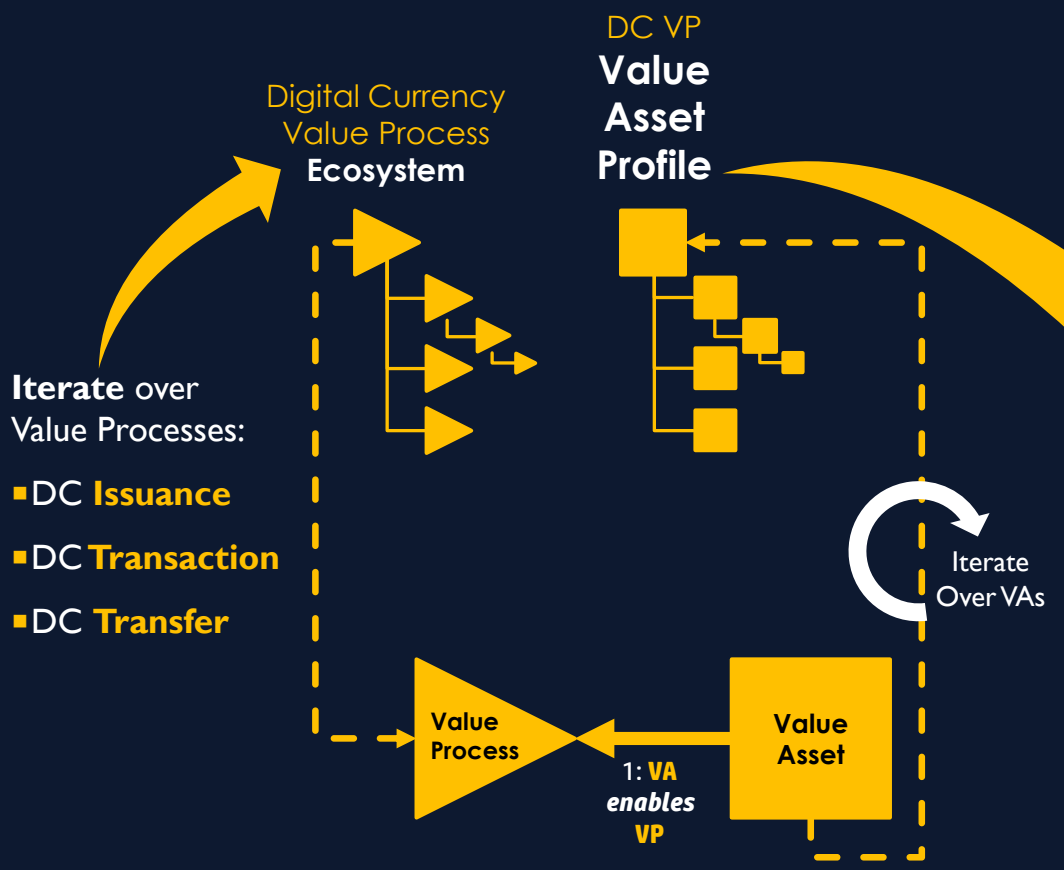
Access to **Advanced**
IT & **Secure-by-Design**
Capabilities

Secure
systematically
anchored to a defined
"**Target**"

Protection ~
Security + Assurance

Strategy
for FinTech

The **Need** for a **Common** Reference

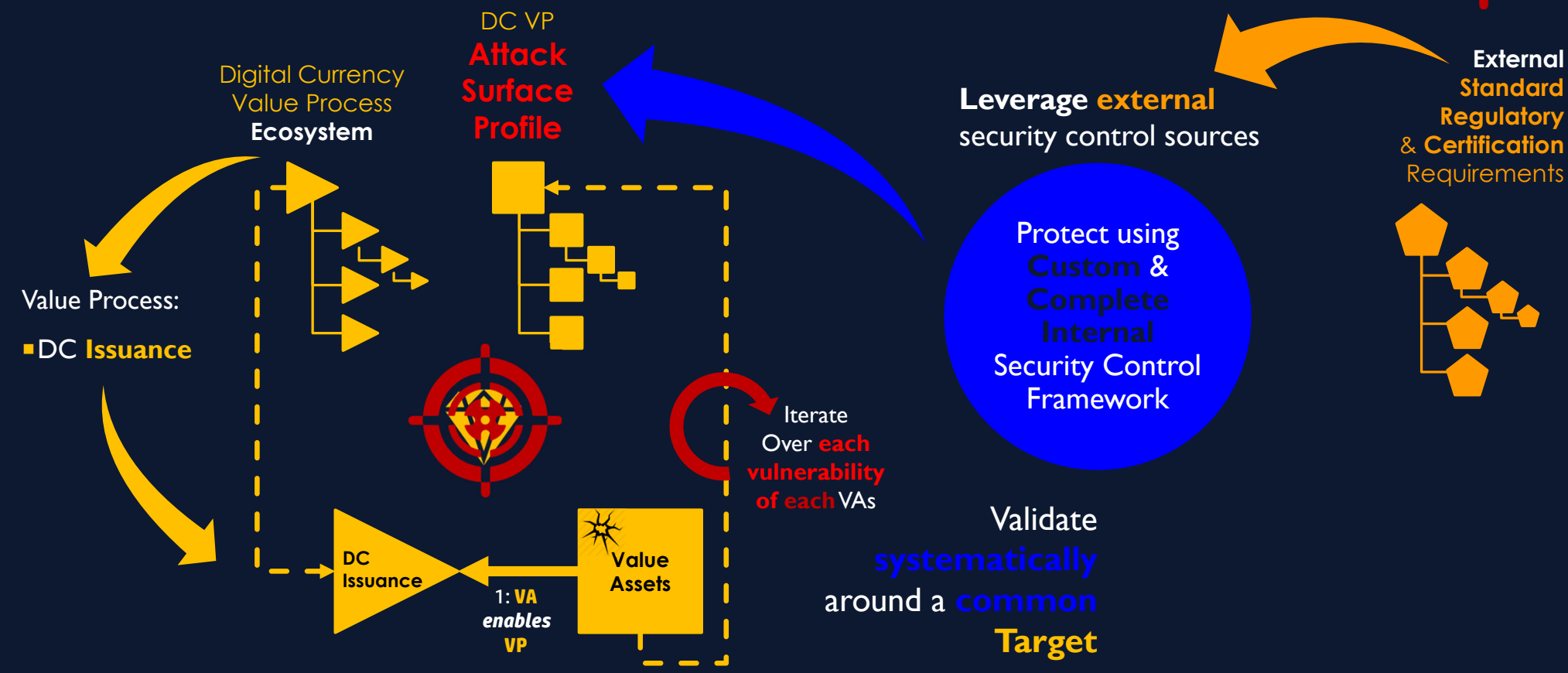


Use Case defines
Purpose & **Context**
of **a** Value Process - **scope** of applicable
Standards, Regulations & Laws

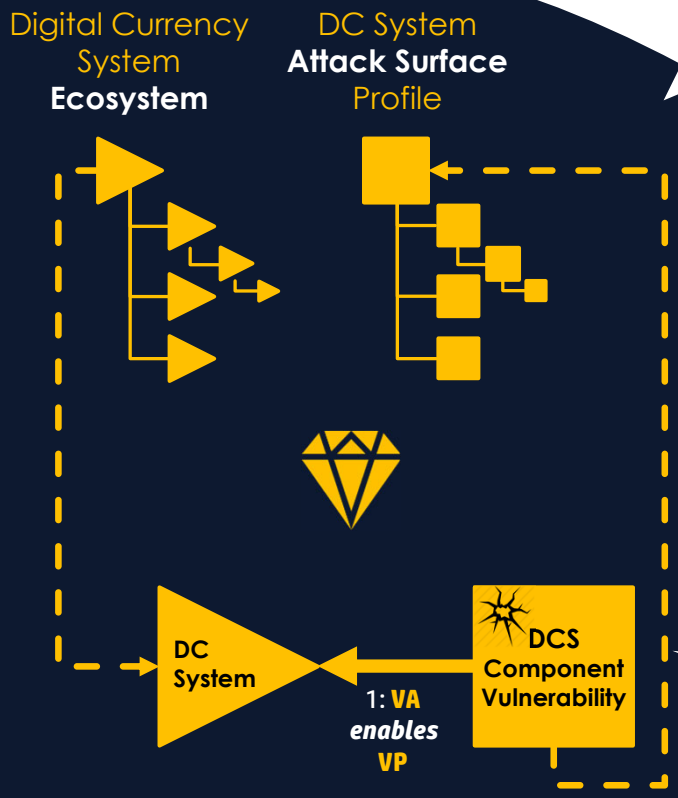
Value Asset Profile
Value Assets *enable* **Value Process**

Domain **Interoperability** -
Governance & Policy drives
Architecture & Use Cases drives
Privacy, Security & Assurance

The **Need** to be **Target** Specific



The **Need** to adopt **Nomenclature**



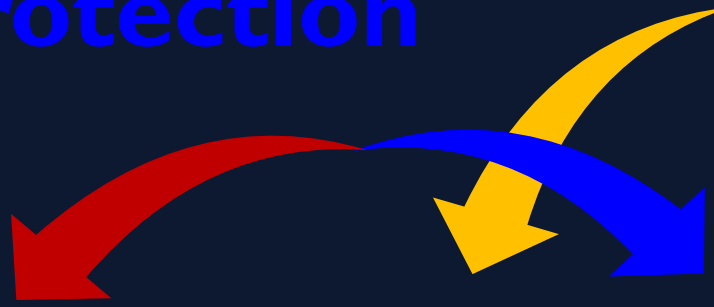
Level	DIGITAL CURRENCY **TARGET NOMENCLATURE**	Acroynm
0	Digital Currency System **Ecosystem**	DCS**E**
-1	Digital Currency **System**	DC**S**
-2	DCS Component **Domain**	DCS-C**D**
-3	DCS Component **Class**	DCS-C**C**
-4	DCS **Component**	DCS-C**O**
-5	DCS Component **Vulnerability**	DCS-C**V**

DC_#

Target Level Nomenclature

"Classification System"

+ Threat & Protection Nomenclature



Level	DIGITAL CURRENCY **TARGET NOMENCLATURE**	Acroynm
0	Digital Currency System **Ecosystem**	DCS**E**
-1	Digital Currency **System**	DC**S**
-2	DCS Component **Domain**	DCS-C**D**
-3	DCS Component **Class**	DCS-C**C**
-4	DCS **Component**	DCS-C**O**
-5	DCS Component **Vulnerability**	DCS-C**V**

LEVEL	DCS **RISK** Nomenclature	DCS **TARGET** Nomenclature	DCS **PROTECTION** Nomenclature
0	DCS **ECOSYSTEM** RISK (DCSE-R)	DCS **Ecosystem** (DCSE)	DCS **ECOSYSTEM** PROTECTION (DCSE-P)
-1	DC **SYSTEM** RISK (DCS-R)	DC **System** (DCS)	DC **SYSTEM** PROTECTION (DCS-P)
-2	DCS THREAT **DOMAIN** (DCS-R-TD)	DCS Component **Domain** (DCS-CD)	DCS SECURITY **DOMAIN** (DCS-P-SD)
-3	DCS THREAT **CLASS** (DCS-R-TC)	DCS Component **Class** (DCS-CC)	DCS SECURITY **CLASS** (DCS-P-SC)
-4	DCS COMPONENT **THREATS** (DCS-R-CT)	DCS **Component** (DCS-CO)	DCS **COMPONENT** SECURITY (DCS-P-CS)
-5	DCS COMPONENT **VULNERABILITY** ATTACK (DCS-R-CVA):	DCS Component **Vulnerability** (DCS-CV)	DCS COMPONENT **VULNERABILITY** ATTACK COUNTERMEASURE (DCS-P-CVAC):

+ Stack Nomenclature

-#.1	Application
-#.2	Service
-#.3	Protocol
-#.4	Network
-#.5	Data
-#.6	Physical

LEVEL	DCS **RISK** Nomenclature	DCS **TARGET** Nomenclature	DCS **PROTECTION** Nomenclature
0	DCS **ECOSYSTEM** RISK (DCSE-R)	DCS **Ecosystem** (DCSE)	DCS **ECOSYSTEM** PROTECTION (DCSE-P)
-1	DC **SYSTEM** RISK (DCS-R)	DC **System** (DCS)	DC **SYSTEM** PROTECTION (DCS-P)
-2	DCS THREAT **DOMAIN** (DCS-R-TD)	DCS Component **Domain** (DCS-CD)	DCS SECURITY **DOMAIN** (DCS-P-SD)
-3	DCS THREAT **CLASS** (DCS-R-TC)	DCS Component **Class** (DCS-CC)	DCS SECURITY **CLASS** (DCS-P-SC)
-4	DCS COMPONENT **THREATS** (DCS-R-CT)	DCS **Component** (DCS-CO)	DCS **COMPONENT** SECURITY (DCS-P-CS)
-5	DCS COMPONENT **VULNERABILITY** ATTACK (DCS-R-CVA):	DCS Component **Vulnerability** (DCS-CV)	DCS COMPONENT **VULNERABILITY** ATTACK COUNTERMEASURE (DCS-P-CVAC):

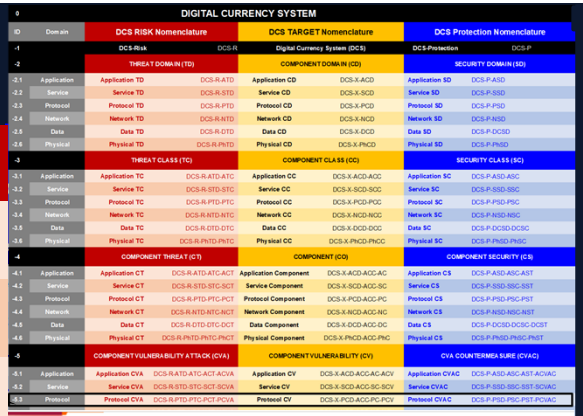
THREAT | TARGET | PROTECTION
Nomenclature

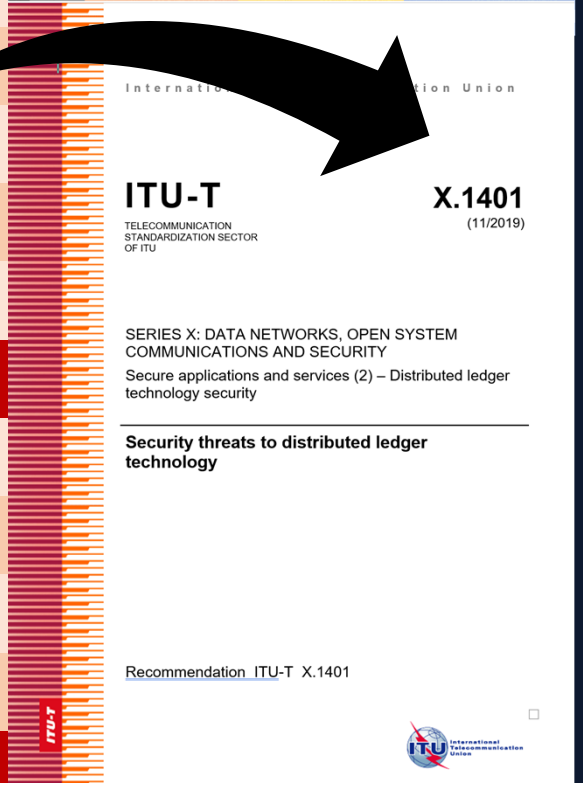
Isolate one row
- **Protocols**

0		DIGITAL CURRENCY SYSTEM					
ID	Domain	DCS RISK Nomenclature		DCS TARGET Nomenclature		DCS Protection Nomenclature	
-1		DCS-Risk	DCS-R	Digital Currency System (DCS)		DCS-Protection	DCS-P
-2		THREAT DOMAIN (TD)		COMPONENT DOMAIN (CD)		SECURITY DOMAIN (SD)	
-2.1	Application	Application TD	DCS-R-ATD	Application CD	DCS-X-ACD	Application SD	DCS-P-ASD
-2.2	Service	Service TD	DCS-R-STD	Service CD	DCS-X-SCD	Service SD	DCS-P-SSD
-2.3	Protocol	Protocol TD	DCS-R-PTD	Protocol CD	DCS-X-PCD	Protocol SD	DCS-P-PSD
-2.4	Network	Network TD	DCS-R-NTD	Network CD	DCS-X-NCD	Network SD	DCS-P-NSD
-2.5	Data	Data TD	DCS-R-DTD	Data CD	DCS-X-DCD	Data SD	DCS-P-DCSD
-2.6	Physical	Physical TD	DCS-R-PhTD	Physical CD	DCS-X-PhCD	Physical SD	DCS-P-PhSD
-3		THREAT CLASS (TC)		COMPONENT CLASS (CC)		SECURITY CLASS (SC)	
-3.1	Application	Application TC	DCS-R-ATD-ATC	Application CC	DCS-X-ACD-ACC	Application SC	DCS-P-ASD-ASC
-3.2	Service	Service TC	DCS-R-STD-STC	Service CC	DCS-X-SCD-SCC	Service SC	DCS-P-SSD-SSC
-3.3	Protocol	Protocol TC	DCS-R-PTD-PTC	Protocol CC	DCS-X-PCD-PCC	Protocol SC	DCS-P-PSD-PSC
-3.4	Network	Network TC	DCS-R-NTD-NTC	Network CC	DCS-X-NCD-NCC	Network SC	DCS-P-NSD-NSC
-3.5	Data	Data TC	DCS-R-DTD-DTC	Data CC	DCS-X-DCD-DCC	Data SC	DCS-P-DCSD-DCSC
-3.6	Physical	Physical TC	DCS-R-PhTD-PhTC	Physical CC	DCS-X-PhCD-PhCC	Physical SC	DCS-P-PhSD-PhSC
-4		COMPONENT THREAT (CT)		COMPONENT (CO)		COMPONENT SECURITY (CS)	
-4.1	Application	Application CT	DCS-R-ATD-ATC-ACT	Application Component	DCS-X-ACD-ACC-AC	Application CS	DCS-P-ASD-ASC-AST
-4.2	Service	Service CT	DCS-R-STD-STC-SCT	Service Component	DCS-X-SCD-ACC-SC	Service CS	DCS-P-SSD-SSC-SST
-4.3	Protocol	Protocol CT	DCS-R-PTD-PTC-PCT	Protocol Component	DCS-X-PCD-ACC-PC	Protocol CS	DCS-P-PSD-PSC-PST
-4.4	Network	Network CT	DCS-R-NTD-NTC-NCT	Network Component	DCS-X-NCD-ACC-NC	Network CS	DCS-P-NSD-NSC-NST
-4.5	Data	Data CT	DCS-R-DTD-DTC-DCT	Data Component	DCS-X-DCD-ACC-DC	Data CS	DCS-P-DCSD-DCSC-DCST
-4.6	Physical	Physical CT	DCS-R-PhTD-PhTC-PhCT	Physical Component	DCS-X-PhCD-ACC-PhC	Physical CS	DCS-P-PhSD-PhSC-PhST
-5		COMPONENT VULNERABILITY ATTACK (CVA)		COMPONENT VULNERABILITY (CV)		CVA COUNTERMEASURE (CVAC)	
-5.1	Application	Application CVA	DCS-R-ATD-ATC-ACT-ACVA	Application CV	DCS-X-ACD-ACC-AC-ACV	Application CVAC	DCS-P-ASD-ASC-AST-ACVAC
-5.2	Service	Service CVA	DCS-R-STD-STC-SCT-SCVA	Service CV	DCS-X-SCD-ACC-SC-SCV	Service CVAC	DCS-P-SSD-SSC-SST-SCVAC
-5.3	Protocol	Protocol CVA	DCS-R-PTD-PTC-PCT-PCVA	Protocol CV	DCS-X-PCD-ACC-PC-PCV	Protocol CVAC	DCS-P-PSD-PSC-PST-PCVAC
-5.4	Network	Network CVA	DCS-R-NTD-NTC-NCT-NCVA	Network CV	DCS-X-NCD-ACC-NC-NCV	Network CVAC	DCS-P-NSD-NSC-NST-NCVAC
-5.5	Data	Data CVA	DCS-R-DTD-DTC-DCT-DCVA	Data CV	DCS-X-DCD-ACC-DC-DCV	Data CVAC	DCS-P-DCSD-DCSC-DCST-DCVAC
-5.6	Physical	Physical CVA	DCS-R-DTD-DTC-DCT-DCVA	Physical CV	DCS-X-PhCD-ACC-PhC-PhCV	Physical CVAC	DCS-P-PhSD-PhSC-PhST-PhCVAC

+ Protocol Threat Vectors

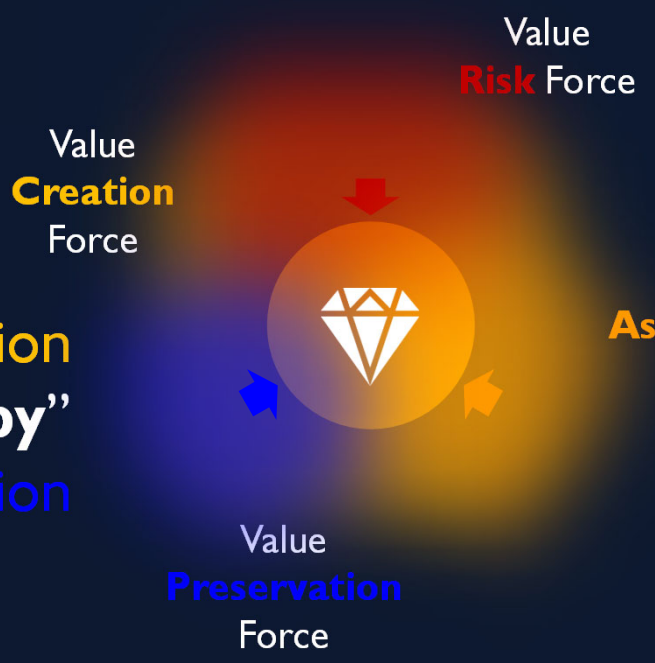
-5.3.1	**Consensus Mechansim Threats**	DCS-R-PTD-PTC-PCT-PCVA:	**CMT-**
-5.3.1.1	**51% Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**51A**
-5.3.1.2	**Timestamp Manipulation Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**TMA**
-5.3.1.3	**Bribing Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**BA**
-5.3.1.4	**Selfish Mining Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**SMA**
-5.3.1.5	**Chain Hopping Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**CHA**
-5.3.1.6	**Block Withholding Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**BWA**
-5.3.1.7	**Double-Spending Attack**	DCS-R-PTD-PTC-PCT-PCVA:CMT-	**DSA**
-5.3.2	**Smart Contract Threats**	DCS-R-PTD-PTC-PCT-PCVA:	**SCT**
-5.3.2.1	**Timestamp Dependence Attack**	DCS-R-PTD-PTC-PCT-PCVA:SCT-	**TDA**
-5.3.2.2	**Mishandled Exceptions Attack**	DCS-R-PTD-PTC-PCT-PCVA:SCT-	**MEA**
-5.3.2.3	**Integer Overflow Attack**	DCS-R-PTD-PTC-PCT-PCVA:SCT-	**OIA**
-5.3.2.4	**Predictable Random Number Attack**	DCS-R-PTD-PTC-PCT-PCVA:SCT-	**PRNA**
-5.3.3	**Virtual Machine Threats**	DCS-R-PTD-PTC-PCT-PCVA:	**VMT**





The **Struggle** to Protect

Internet-of -**Value**



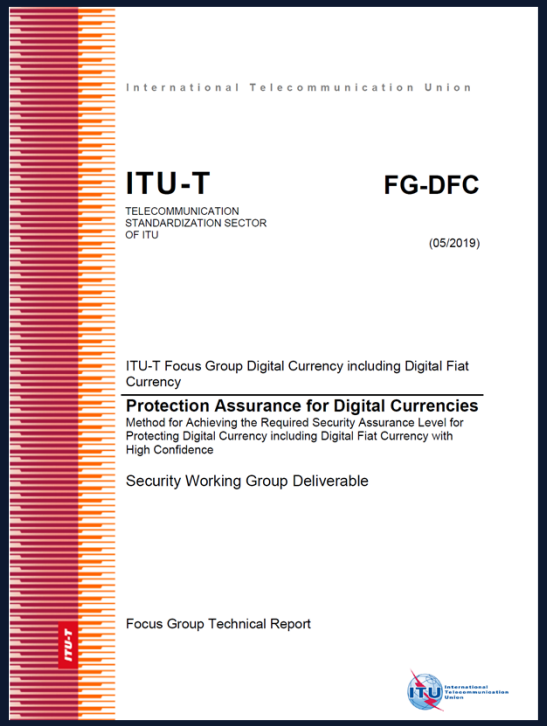
Value Creation
"is Threatened by"
Value Risk

Value Creation
"is Protected by"
Value Preservation

Value Preservation
"is Validated by"
Value Assurance

A **Need** for a **Rethink**?

Rethink to a **Relational** Model



International Telecommunication Union

ITU-T **FG-DFC**

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

(05/2019)

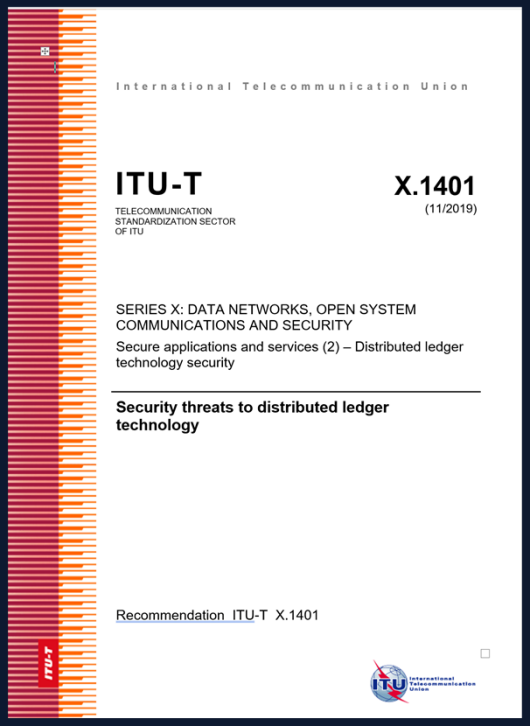
ITU-T Focus Group Digital Currency including Digital Fiat Currency

Protection Assurance for Digital Currencies

Method for Achieving the Required Security Assurance Level for Protecting Digital Currency including Digital Fiat Currency with High Confidence

Security Working Group Deliverable

Focus Group Technical Report



International Telecommunication Union

ITU-T **X.1401**

(11/2019)

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Distributed ledger technology security

Security threats to distributed ledger technology

Recommendation ITU-T X.1401

Institutionalize Relationships

Better **Standardized Input** - Better **Output**

Using

- **Common** specifications & requirements
- **Consistent** measurement methods & metrics
- **Comparable** models, templates & evaluations

Standardized

- **Models**
- Measurement **Metrics**
- Evaluation **Methods**

that will ensure

Repeatability w/ **Confidence**

a basis of

Performance & Protection

Assessments & Benchmarking

across the **Ecosystem**

Feeds **Standardized** "Creation & Issuance" Process

Please walk away with

Realize This	**Demand** This	**Accept** This	**Do** This	**Remember** This
Current approaches and methods are too costly & complex - **not sustainable**	It is time for **interoperable** -by-Design! From Massively **Heterogenous** to Massively **Interoperable**	DC use cases will need **trust standards** that are **logically** **"higher"** than other human use cases – **money**	**Participate** in the discussion and development of Standards	Participating enables one to **influence** and **shape** the future, do not miss the **opportunity**

JACQUES FRANCOEUR

SILICON VALLEY SECURITY INDUSTRY THOUGHT LEADER: 34+ YOE

Please reach out to join forces with

USA Delegate (2018,19,20) Security Expert
& Contributor
International Telecommunications Union (ITU),
Standardization, Study Group 17: Security

Chief Scientist, Security Inclusion Now USA
https://www.linkedin.com/in/**innoonewetrust**/
Jacques@SecurityInclusionNow.org

Collaboration & Validation

JACQUES FRANCOEUR

SILICON VALLEY SECURITY INDUSTRY THOUGHT LEADER: 34+ YOE

Jacques Francoeur
M.A.Sc., B.A.Sc, MBA

jacques@securityinclusionnow.org

https://www.linkedin.com/in/**innoonewetrust**/

MBA:	Concordia University
M.A.Sc:	University of Toronto Institute for Aerospace Studies
B.A.Sc.:	University of Toronto, Engineering Science, Aerospace Engineering

Chief Scientist & **Founder**
Security Inclusion Now, Silicon Valley

USA Delegate (2018,19,20) **Security Expert** & **Contributor**
International Telecommunications Union (ITU), Standardization, Study Group 17: Security

Chair: **Security** & **Assurance** Working Group
Digital Currency Global Initiative, ITU

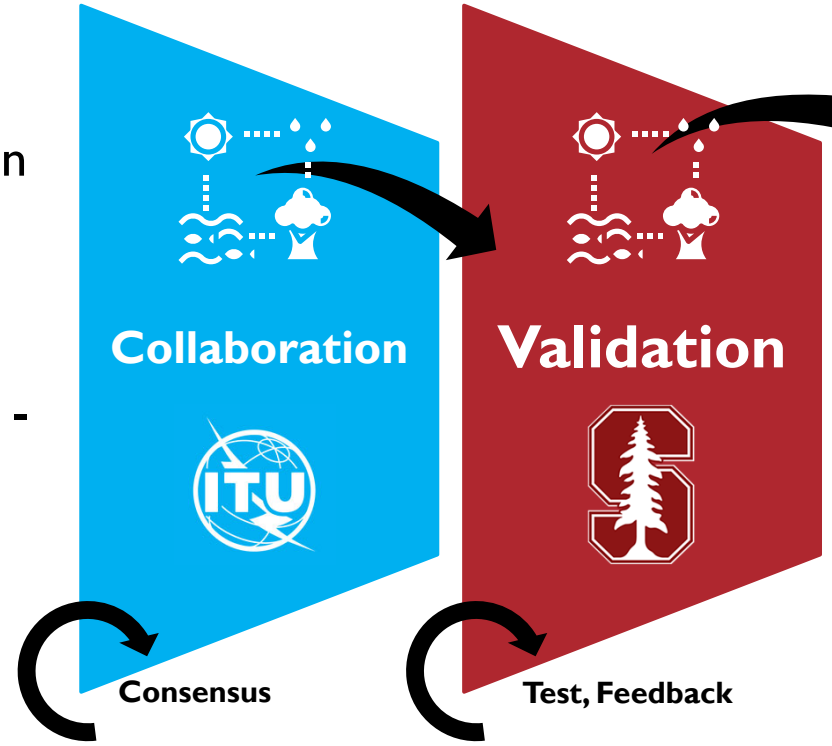
Technical Director
Future of Digital Currency Program, Stanford University
Stanford Center for Blockchain Research, School of Engineering

Expert Network Member
World Economic Forum, Blockchain Security

Digital Currency Global Initiative

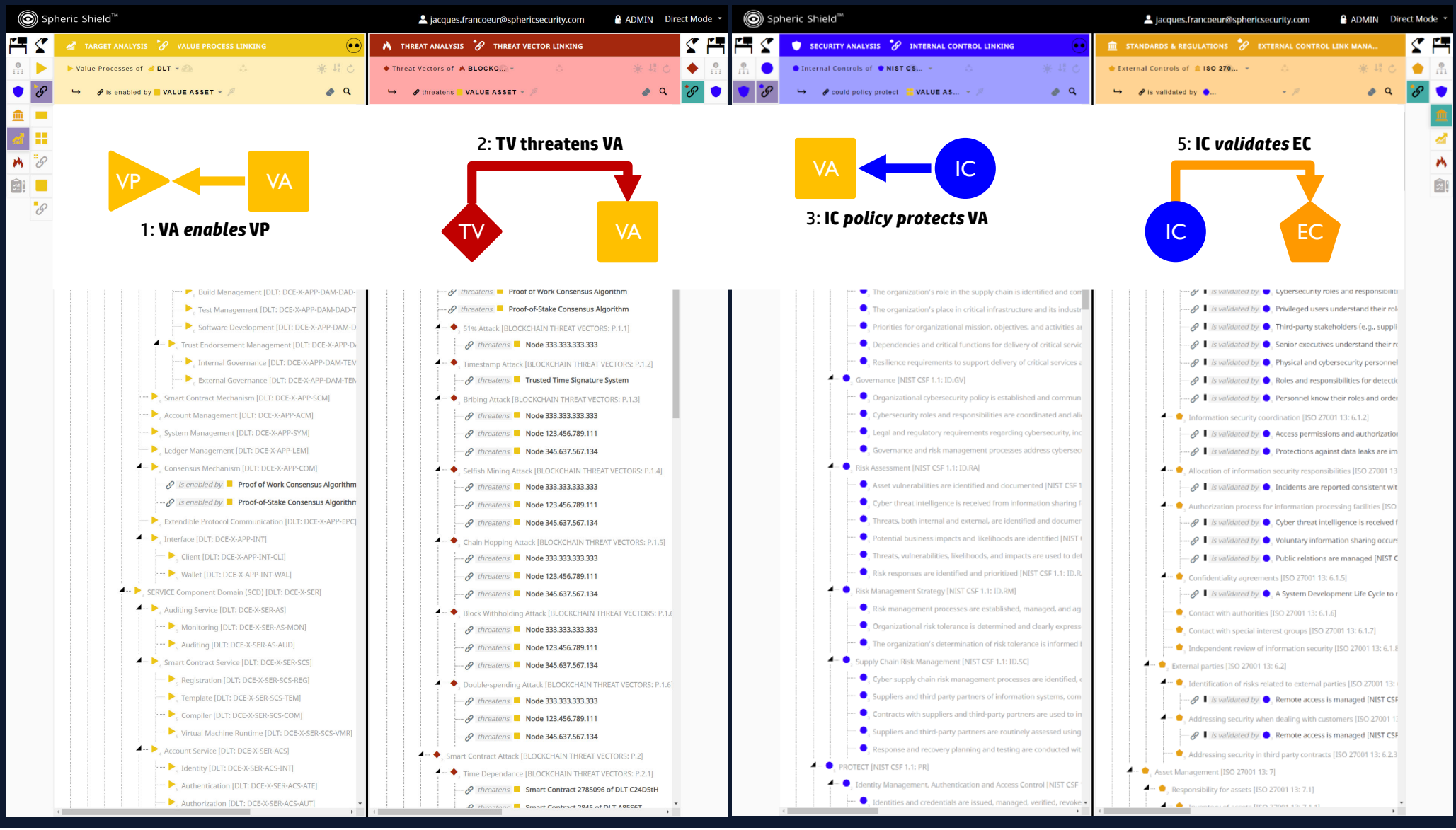
& the Stanford **Future of Digital Currency Program**

Global domain experts propose **suitable** specifications - **input** into **Validation**



Common, Consistent & Comparable specifications & requirements; measurement methods & metrics; models, templates & evaluations

Reliable & **Repeatable** processes yielding high confidence **benchmarkable** evaluations and validations across the ecosystem


Spheric Shield™
jacques.francoeur@sphericsecurity.com
ADMIN
Direct Mode
TARGET ANALYSIS
VALUE PROCESS LINKING
THREAT ANALYSIS
THREAT VECTOR LINKING
SECURITY ANALYSIS
INTERNAL CONTROL LINKING
STANDARDS & REGULATIONS
EXTERNAL CONTROL LINK MANA...
VP
VA
1: VA enables VP
2: TV threatens VA
TV
VA
VA
IC
3: IC policy protects VA
5: IC validates EC
IC
EC
Proprietary to Jacques Remi Francoeur, Copyright © 2019