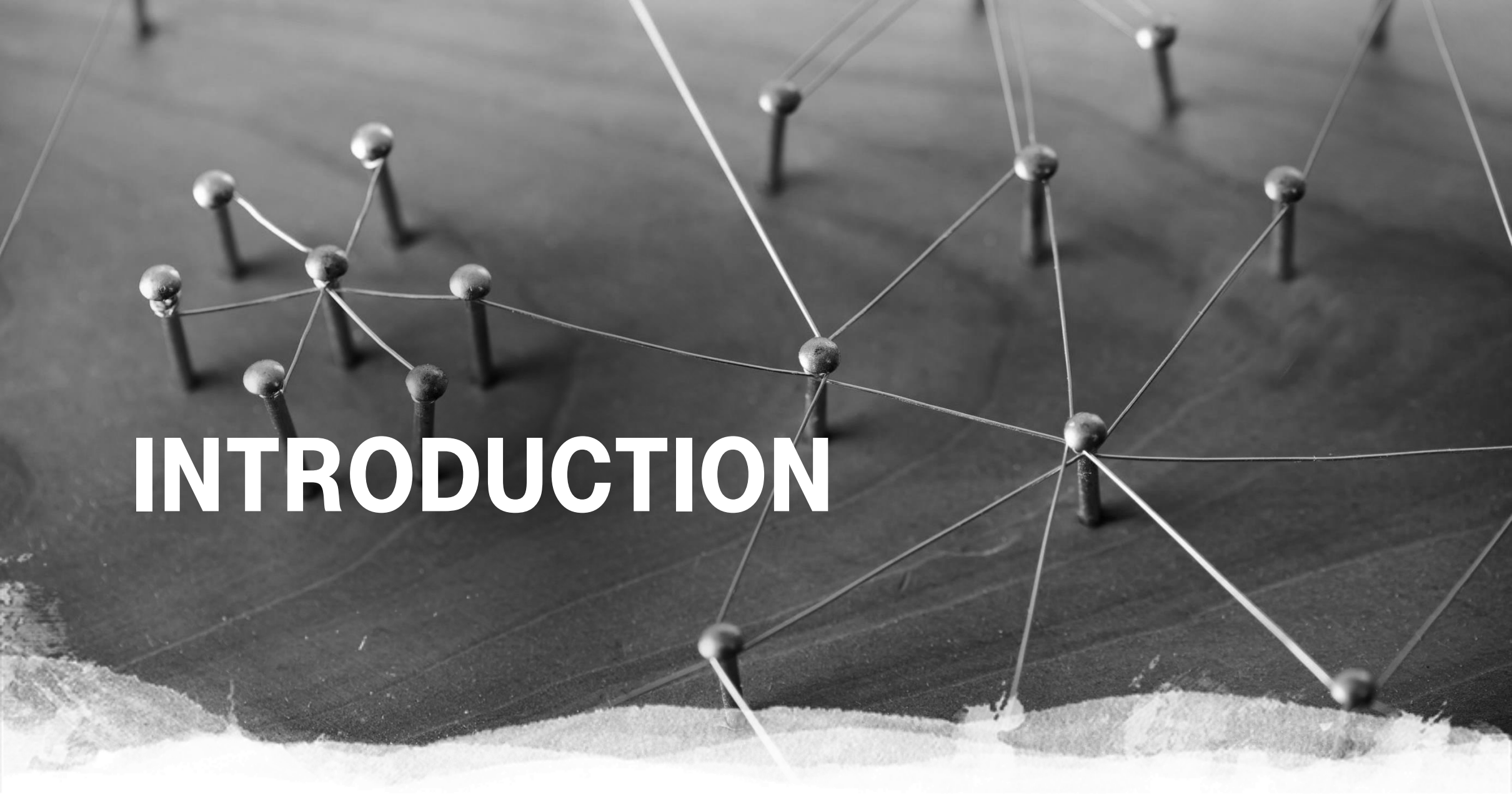
BLOCKCHAIN-BASED SMART INDUSTRY INTEGRATION

DEMYSTIPHYING BLOCKCHAIN

Ivan Gudymenko, ivan.gudymenko@t-systems.com
Marian Neubert, marian.neubert@t-systems.com

AGENDA

1. Introduction
2. The notion of a (distributed) ledger
3. Blockchain as a distributed ledger and a state machine
4. Aligning on what is valid: a variety of consesus algorithms
5. Putting it all into a real-world context: a smart industry example
6. Proof-of-concept demonstration
7. Questions and answers



INTRODUCTION

IT-SECURITY@T-SYSTEMS MMS
WHO WE ARE

SECURITY

DATENSCHUTZ

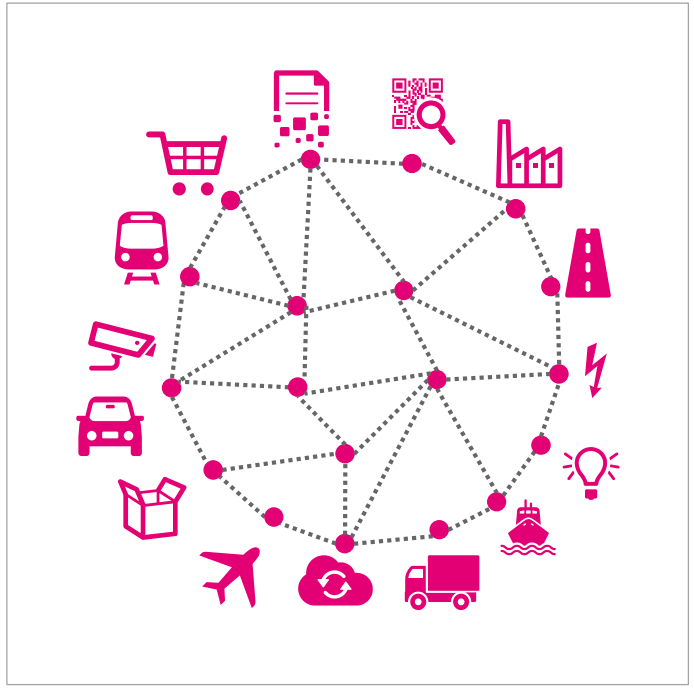
GOVERNANCE, RISK AND COMPLIANCE

MANAGED SECURITY SERVICES

TRAINING AND AWARENESS

BLOCKCHAIN

DEEPLY INTERCONNECTED WORLD
FROM PLAIN CLIENT/SERVER TO “ANY-TO-ANY”



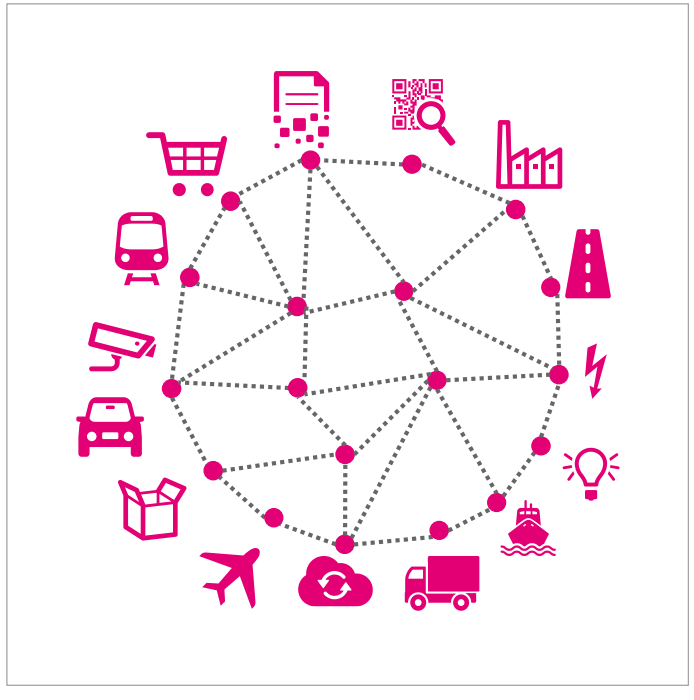
Global communication: a paradigm shift

evolution

PARADIGM SHIFT: TRUST DECENTRALIZATION
DECENTRALIZING THE “ROOT OF TRUST”

Well-defined trust models and control

“50 shades of Trust”



THE NEW CHALLENGES AND OPPORTUNITIES
HOW TO DEAL WITH “ANY-TO-ANY” AND HETEROGENEITY

- **We would like to allow as many parties to communicate as possible**
  - ... as freely as possible
  - ... as secure as possible

- **But how to avoid the anarchy, sabotage and mess?**
  - While preserving privacy, security and correctness?

- **A huge number of new-old challenges arise (yet again)**

THE NOTION OF A LEDGER
KEEPING TRACK OF THE TRANSACTIONS

- **Ledger "is the principal book or computer file for recording and totaling economic transactions" [1]**
- **Nowadays, ledgers have been largely digitalized**
- **Ledgers can been found everywhere where the (financial) transactions have to be kept track of**
- **However, every institution maintains its own ledger**
  - How to share information between different ledgers
  - And align on what is valid and what is not?
- **Correct, let's introduce a SINGLE SHARED LEDGER!**

Accounts for Demo

CASH ACCOUNT From 01/03/2003 to 29/02/2004 Select current year Select p

Date	Payee	Reference	Category	Actual (gross) Amount	Actual (gross) Balance (gross)	Recon	Ad GS
				0.00	0.00	☑	
25 MAY 0	Mr J Citizen	Lot 1 levy pa	Deposit	500.00	500.00	☑	
26 MAY 0	Local Insurance B	nsurance Ar	Insurance Bu	-269.00	231.00	☑	
31 MAY 0	Netbank	Govt Debit Te	Govt Debit Te	-2.52	228.48	☑	
31 MAY 0	Netbank	Account Ser	Account Ser	-5.00	223.48	☑	
31 MAY 0	Netbank	Interest	Bank Interest	0.52	224.00	☑	
3 JUN 03	Clarkes Grounds	Grounds Mai	Grounds Mai	-30.00	194.00	☑	

[1] https://en.wikipedia.org/wiki/Ledger

A SHARED LEDGER
MAKING IT USABLE AND SECURE

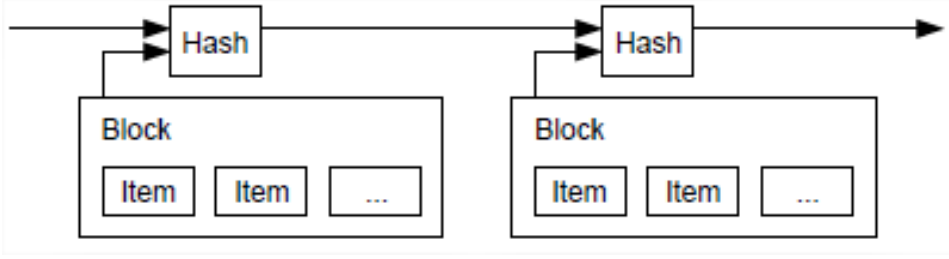
- **A distributed ledger shared between several instances/companies/institutions should be**
  - Trusted by all parties
  - Immutable
  - Usable and maintainable by all parties
  - ... and so on, and so forth

- **It has to be clear how the parties ALIGN on the valid state of the shared distributed ledger**
  - Consensus should be reached
  - The procedure must be clear, transparent and applicable for all participants

- **And many more ....**

IMPLEMENTING IT WITH A BLOCKCHAIN
BLOCKCHAIN AS A DISTRIBUTED LEDGER

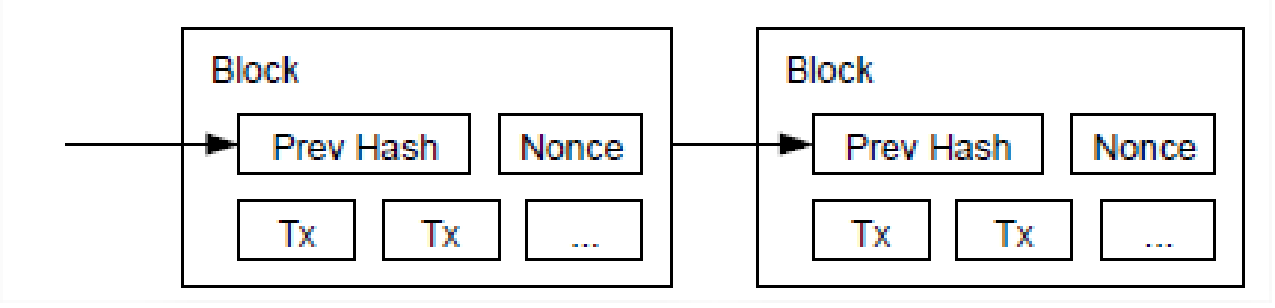
- **The data structure essentially represents a linked hash chain**
  - Therefore immutable (cannot be changed afterwards) by design
- **With a set of rules and permissions to write the data into the chain and agreeing on transactions validity**
- **With a consensus algorithm regulating which transactions are valid**
- **Consensus algorithm defines which nodes are allowed to write/validate and how**



Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System

BLOCKCHAIN AS A STATE MACHINE
MAINTAINING THE DISTRIBUTED STATE

- **The state of blockchain transactions can be seen as an append-only log**
- **The state gets updated by appending a block of transactions to the log**
  - $State_{[new]} = UPDATE(State_{[old]})$
- **WHO is allowed to update the state and under which conditions is defined by a CONSENSUS ALGORITHM**



Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System

CONSENSUS ALGORITHMS
A HEART OF EVERY BLOCKCHAIN SYSTEM

- **The security and trust model of a blockchain system is largely defined by the underlying consensus algorithm**
- **The topic of consensus algorithms is in fact fairly well researched in the area of in distributed computing**
  - Yes, some people are essentially re-inventing the wheel here, but it is out of scope of this talk ☺
- **Consensus algorithms can be very roughly divided into permissionless and permissioned**
- **Permissionless can be also referred to as decentralized**
  - e.g. as in Bitcoin, Ethereum
- **Permissioned are also known as consortium**
  - e.g. Byzantine Fault Tolerance (BFT) consensus

A blockchain system is as secure and robust, as its consensus algorithm!

THE NOTION OF A “SMART CONTRACT”
BUILDING IN BUSINESS LOGIC

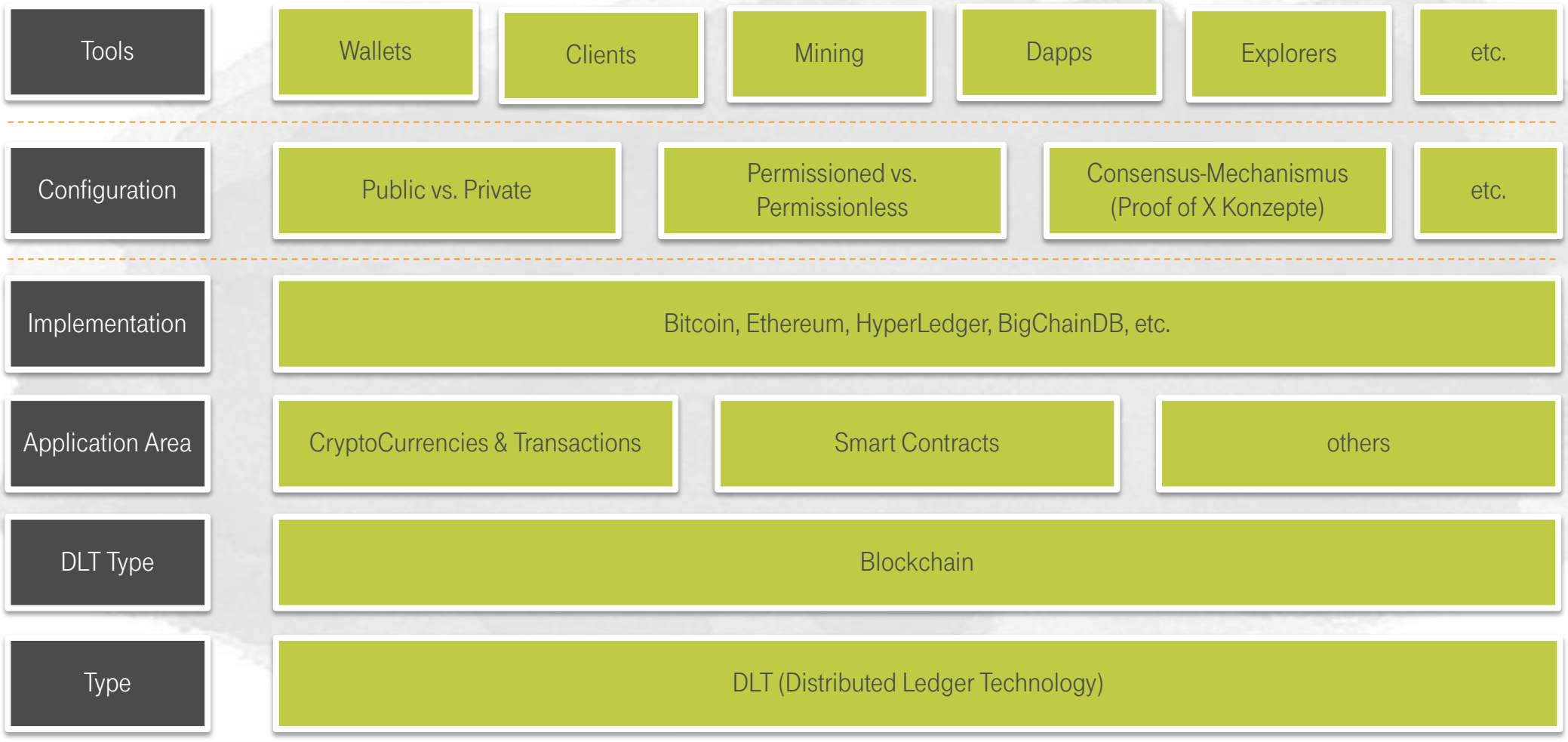
- **“Smart Contracts are self-executing contractual states, stored on the blockchain, which nobody controls and therefore everyone can trust” [1]**

- **Essentially, smart contract is a distributed application that represents business logic**

- **Smart contract properties :**
  - Self-Imposable
  - Trustless
  - Fast
  - Cheap [2]

[1] https://www.smartcontract.com
[2] https://www.cerias.purdue.edu/intel/docs/Kate_IntelTalk.pdf

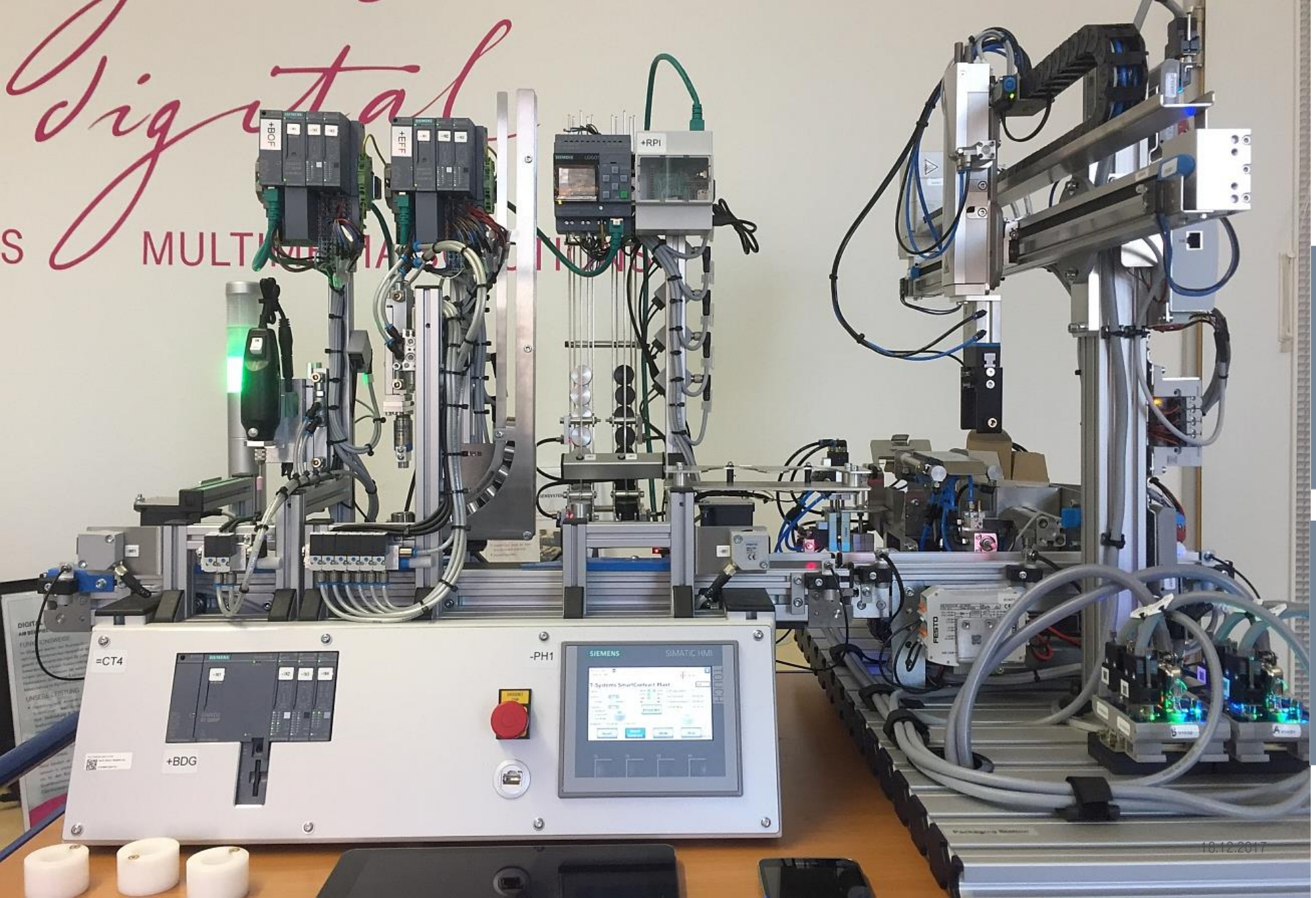
BLOCKCHAIN-BASED SYSTEMS LAYERING

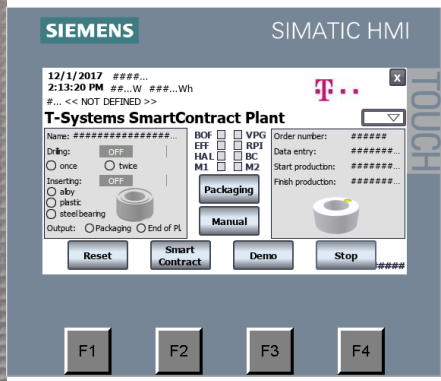


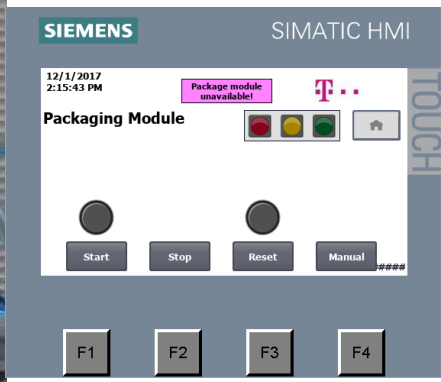
SMART FACTORY

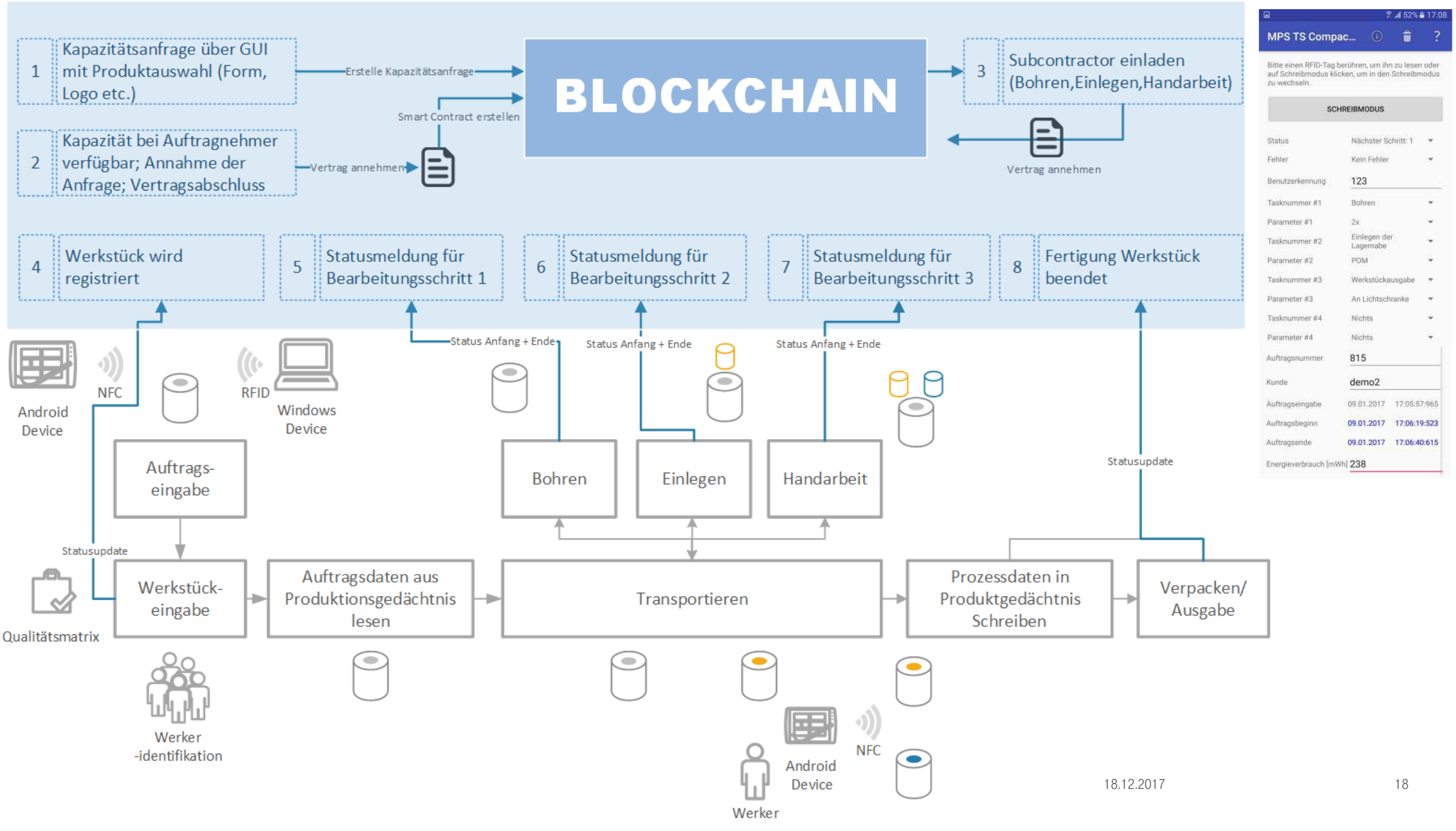
DIGITALE VERTRÄGE FÜR INTELLIGENTE FABRIKEN

SMART FACTORY
KURZVORSTELLUNG


+BOF
+EFF
+RPI
=CT4
-PH1
+BDG
SIEMENS
SIMATIC HMI
TOUCH


SIEMENS
SIMATIC HMI
12/1/2017
2:13:20 PM
T-Systems SmartContract Plant
Packaging
Manual
Reset
Smart Contract
Demo
Stop
F1
F2
F3
F4
TOUCH


SIEMENS
SIMATIC HMI
12/1/2017
2:15:43 PM
Package module unavailable!
Packaging Module
Start
Stop
Reset
Manual
F1
F2
F3
F4
TOUCH


1
Kapazitätsanfrage über GUI mit Produktauswahl (Form, Logo etc.)
Erstelle Kapazitätsanfrage
Smart Contract erstellen
BLOCKCHAIN
3
Subcontractor einladen (Bohren,Einlegen,Handarbeit)
2
Kapazität bei Auftragnehmer verfügbar; Annahme der Anfrage; Vertragsabschluss
Vertrag annehmen
Vertrag annehmen
4
Werkstück wird registriert
5
Statusmeldung für Bearbeitungsschritt 1
6
Statusmeldung für Bearbeitungsschritt 2
7
Statusmeldung für Bearbeitungsschritt 3
8
Fertigung Werkstück beendet
Android Device
NFC
RFID
Windows Device
Status Anfang + Ende
Status Anfang + Ende
Status Anfang + Ende
Auftrags-eingabe
Bohren
Einlegen
Handarbeit
Statusupdate
Statusupdate
Qualitätsmatrix
Werkstück-eingabe
Auftragsdaten aus Produktionsgedächtnis lesen
Transportieren
Prozessdaten in Produktgedächtnis Schreiben
Verpacken/ Ausgabe
Werker -identifikation
Android Device
NFC
Werker
MPS TS Compac...
Bitte einen RFID-Tag berühren, um ihn zu lesen oder auf Schreibmodus klicken, um in den Schreibmodus zu wechseln.
SCHREIBMODUS
Status
Nächster Schritt: 1
Fehler
Kein Fehler
Benutzerkennung
123
Tasknummer #1
Bohren
Parameter #1
2x
Tasknummer #2
Einlegen der Lagernabe
Parameter #2
POM
Tasknummer #3
Werkstückausgabe
Parameter #3
An Lichtschranke
Tasknummer #4
Nichts
Parameter #4
Nichts
Auftragsnummer
815
Kunde
demo2
Auftragseingabe
09.01.2017
17:05:57:965
Auftragsbeginn
09.01.2017
17:06:19:523
Auftragsende
09.01.2017
17:06:40:615
Energieverbrauch [mWh]
238

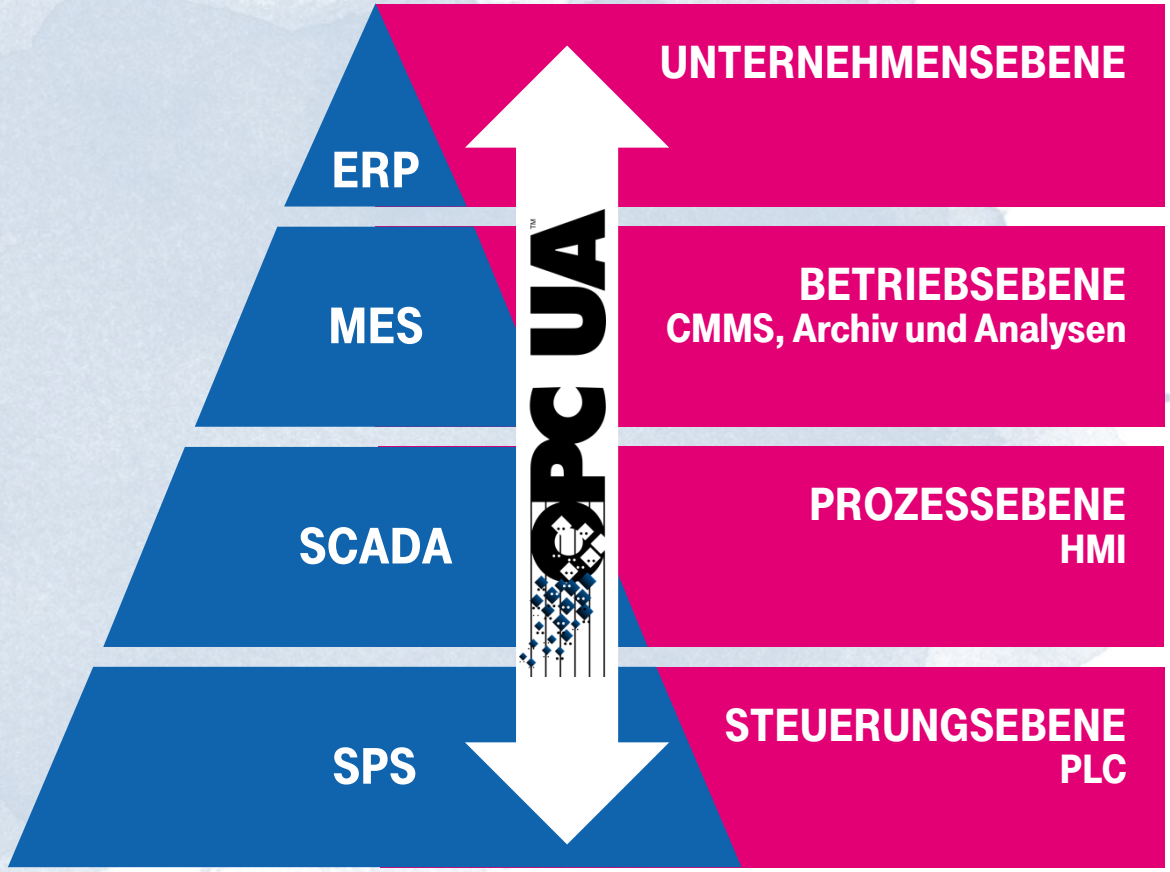
OPC UA
KURZÜBERBLICK

KOMMUNIKATION MIT OPC UA
SCHNITTSTELLEN ÜBERGREIFEND

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

LÖSUNGEN

- STANDARDISIERUNG DER TECHNOLOGIE
- OFFENE FORMATE UND SPEZIFIKATIONEN
- UNIVERSELLE KOMMUNIKATIONS-MÖGLICHKEITEN



ÜBERBLICK ÜBER OPC UA
ENTWICKLUNG

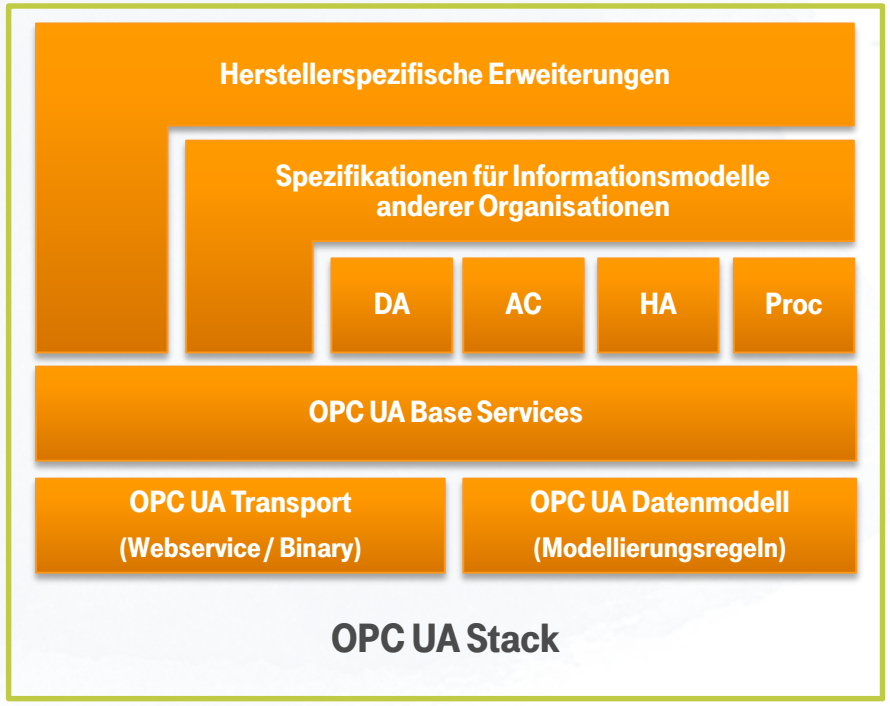
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

HAUPTNACHTEILE VON OPC WERDEN BEHOBEN:

- Starke Authentifizierung und Validierung eingebaut
- Kommunikation über Firewall/Domänengrenzen möglich
- Skalierbar und Redundant, Plattformunabhängig, Fehlertolerant
- Nicht nur der Transport sondern auch die Semantik wird definiert

DEFINITION 2003-2006, RELEASE 2006,
SEIT 2010 IEC-NORM (IEC 62541)

- Spezifikation und Teile der OPC UA-Stacks seit 2015 Open-Source
- Implementierungen für .NET, ANSI C/C++ und Java verfügbar
- Verschiedene Hersteller bieten fertige SDK‘s



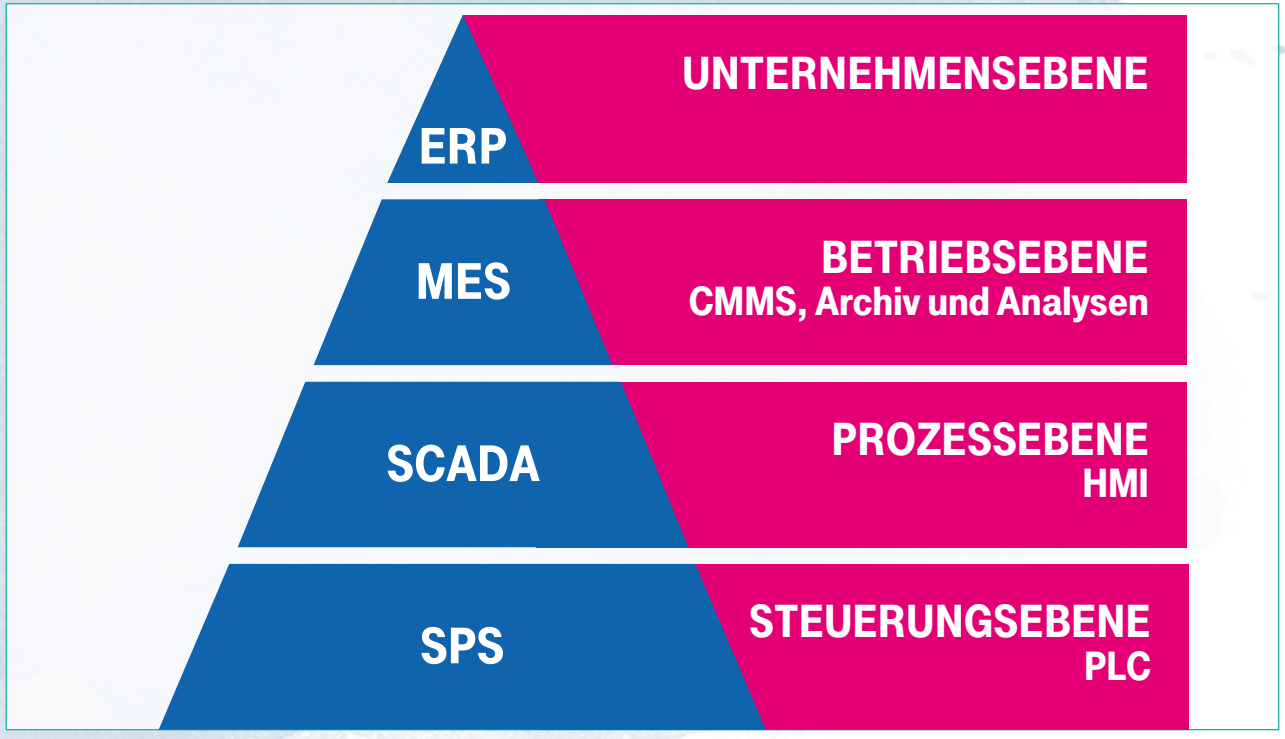
OPC UA IMPLEMENTIERUNG
ROBUST UND SKALIERBAR

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Performance
- Hohe Geschwindigkeit in der Kommunikation
- Kleiner Memory-Footprint
- Geringe Last auf dem Zielsystem

Redundanz
- Konfigurierbare Timeouts und Retransmits
- Hochverfügbarkeit auf Applikations- und Netzwerkbasis

Skalierbar
- Vom Mikrocontroller bis zum Enterprise-Server
- Gateways zum Aggregieren implementierbar




Q&A